Risk of electronic payments of the banking sector in Sri Lanka: Case of Colombo district

HMBP Ranaweera
Department of Business Management, Faculty of Management Studies,
Rajarata University of Sri Lanka, Mihinlate, Sri Lanka
buddiranaweera@yahoo.com

Abstract
Electronic commerce is spreading and popularizing at a fast pace in the world due to novel changes of information technology. E-payment is a vital part of electronic commerce. Through this study, it is aimed to identify the risk of electronic payments of the banking sector. Probing the available literature, security risk, perceived risk, operational risk and financial risk were identified as the dimensions of risk that influence on risk of e-payments. Thus, dimensions of risk are the independent variables and the risk of e-payments was treated as dependent variable of the study. 200 e-payment users were selected conveniently from Colombo district to validate the research model and structured questionnaire was administered to gather responses. The Structural Equation Modeling was applied to analyze the collected data. The results revealed that the financial risk is highly considered by the users of e-commerce than other types of risk associated with e-payments. Accordingly, recommendations are brought to reduce the associated risks for e-payments in banking sector. This would help with all the e-payment systems to provide secure and reliable service for banking customers.

Keywords: *Electronic payments, Financial risk, Operational risk, Perceived risk, Security risk, Sri Lanka, Structural Equation Modeling*

1. Introduction

Electronic payments are financial transactions made without the use of any paper documents. It is a mode of payment based on electronic network. E-payments became one of the most critical issues in successful business and financial services (Kim, Tao, Shin & Kim,2010). Along with the increase of internet users, e-payment system has been growing rapidly today, while good electronic payments have a number of advantages over the traditional payment methods (Junadi & Fenrianto, 2015). Electronic payment provides convenience, trust and time savings, and also service providers would benefit from faster payment and better tracking of accounts (Cheng, Hamid and Cheng, 2010). Debit card, credit card, electronic cash, e-wallets are some popular e-payment instruments (Rachna & Singh, 2013).

Practically, there are two distinct types of e-payment systems, accounts - based and electronic transition based payments (Rachna & Singh, 2013). Electronic payment usage, particularly card -based payment instruments not only sidesteps are popular due to the problems in carrying a large sum of money (Dzemydiene, Naujikiene, Kalinauskas & Jasiunas, 2010). The basic online payment process includes customer action, payment authentication by the operator (e.g. credit card's number, ids, passwords) and payment to the seller's account. Therefore, e-payments provide successful transaction between the parties (Vos, Marinagi, Trivellas, Eberhagen, Skourlas& Giannakopoulos, 2014).In addition to that, bank sector participates as an issuer and acquirer. The issuer holds payer's account and acquirer holds payee's account and assets. And also good e-payment systems ensure the effectiveness of monetary policy and facilitate smooth and stable economy (Seng, 2008).

Currently, in Sri Lanka ATM services, Debit cards, Credit cards, E-cash and internet banking facilities are available as e-payment instruments. Credit cards are used to purchase goods and services (Rachna& Singh, 2013). It is a type of card that has credit card number, expiry date, and name, address and contact number (Aziz, Mohamed & Zakaria, 2015). Credit cards are most secured and frequently used method in e-payment transitions (Kim, Tao, Shin & Kim, 2010). Process in use of credit cards for online transactions over the internet is not much different from offline transitions in physical market (Junadi & Fenrianto, 2015). Credit card is the payments tool that using commonly today. And also, Debit card is a plastic card issued by the bank and it requires a bank account, no interest charges related to this card. It replaces cash and checks (Rachna & Singh, 2013). Debit card method combined with Automatic Teller Machines (ATM) and internet banking. When customer pay with debit card money will automatically deducted from their bank account (Kim, Tao, Shin & Kim, 2010).In addition to that, electronic cash is software based method, online token payment system. When the token purchased by the customers, e-cash software allows them to spend the digital money at any shop that accepting e-cash (Rachna & Singh, 2013). Bank will give the token when consumers will deposit sum of money or credit card (Junadi & Fenrianto, 2015). Both customers and merchant have to sign up with the bank or company before using the e-cash. This method was developed as a replacement of using credit card for internet purchases (Kim, Tao, Shin & Kim, 2010).

Very interesting thing is, the difference between cash transaction and an electronic payment is that e-payment transaction often involves multi-parties such as payment intermediaries, authorizers, and payment clearers and settlers (Seng, 2008). At this stage, there are some negative impacts on reducing the performance of e- payment systems by increasing risk involved with e-payment. Furthermore, Rachnaand Singh (2013) mentioned that, E-payment systems have received different acceptance level throughout the world; some methods of electronic payments are highly adopted while others are relatively low. Though, both customers and service providers can benefit from e-payment system which leads to increase national competitiveness. In the long run, more in depth studies are needed to examine the dimensions of consumers' satisfaction towards e-payment systems. The successful implementations of e-payment system depends on how the risk dimensions perceived by consumers as well as sellers (Cheng, Hamid and Cheng, 2010). In this scenario, this study

investigated about different types of risk are associated with electronic payments in the banking sector. So that, the study focused on identifying the antecedents of risk named as security risk, financial risk, operational risk and perceived risk which make influences to reduce the acceptance of e-payments. Upon completion of the study, outcomes provide recommendations to service providers and policy makers to improve the quality of electronic payment system in banking sector.

2. Antecedents of risk towards e-payments

Electronic payments are a payment mode which is based on online network. E-payment can be defined as the process of payment made without the use of paper instruments. The e-payment systems consists of online credit card transaction, electronic wallets (E-wallet) electronic cash (E-cash), online stored value systems, digital accumulating balance systems, wireless payment systems, digital checking payment systems, smart card etc. and excludes physical cash or checks (Junaid & Fenrianto, 2015; Cheng, Hamid & Cheng, 2010). Rachnaand Singh (2013) mentioned that, e-payments are becoming one of the most popular type of service which will be affected by the growth of ICT and the popularity of e-service on the whole.

There are significant risk and challenges regarding the use of electronic payment systems. The risks to the online payments are burglary of payments data, private data and fraudulent rejection on the part of customers. Therefore, and until the use of electronic signatures is wide spread, we must use the technology vacant for the moment to guarantee a reasonable minimum level of security on the network. With respect to the payment methods they have been analyzed, it is impossible to say that any one of them is perfect, although each one of them has advantages as opposed to others (Rachna & Singh, 2013).

Security risk

While using electronic payments, user concern on privacy and security to make the payment safe and secure. For an example when using credit card, the user have to key in the information on credit card number, expiry date, name, address and contact number (Aziz, Mohamed and Zakaria, 2015).Security of electronic payment product is important when the e- payment transactions are done through an open (online) system (Seng, 2008).According to Alexandru (2015) reviewed that, many users make payments electronically, instead of using cash or cheques. Hundreds of electronic payment systems have been developed to provide secure internet transactions. In order to secure these transactions two cryptographic methods are used in electronic payment systems which includes secret key (used to encrypt and decrypt the initial transmission to the recipient) and the public key (which use both a private and public key).According to Seng (2008) security of e-payment is one of the most important issues influencing user acceptance as well as reducing the system's vulnerabilities and security of e-payment products is important especially when the e-payment transactions are done through "open" systems."Online payment systems for the internet are an easy target for stealing money and personal information. Customers have to provide credit card and payment account details and other personal information online" (Rachna & Singh, 2013, 29p).

Moreover, according to Junadiand Fenrianto (2015) security relates to how the electronic payment system can protect consumer transactions. Furthermore, AL-ma Aitah and Shatat (2011) mentioned that, Web security means the ability of the web sustain and protect the personal sensitive information from any altering, misuse, disclosure, destruction or taken by unauthorized persons such as Internet intruders and hackers. In addition, the web security system must prevent unauthorized users to use the computer system and control access to the network from inside and outside the organization.

If the client wants to maintain privacy, then they choose those payment methods which guarantee a higher level of privacy such as E-cash or Net Bill Checks. If the priority is security, they use Smart Cards. The successful implementations of electronic payment systems depend on how the security and privacy dimensions perceived by consumers as well as sellers are popularly managed, in turn would improve the market confidence in the system (Rachna& Singh, 2013).According to Aziz, Mohamed and Zakaria (2015) obtained as an example, when using credit cards, the user has to key the information on credit card number, expiry date, name, address and contact number. If the business does not take any safety measures to maintain the confidentiality of their user's data, it can be manipulated by irresponsible third party. On other hand, Kim, Tao, Shin and Kim, (2010)contends that security issues are also of concern for small value-payment transactions. For large value transactions, security is the most critical issue, and the use of encryption and other security mechanism should be accordingly considered in order to reduce e-payment transaction risk, and e-payment service providers should allay the security concern of consumers and promote customers belief in the trustworthiness of service. Some e-payment service providers merely concentrate on technical protection and ignore the importance of security statement in the system.

Moreover, Seng (2008) pointed out that inadequate control could result in virus injection or successful attack by hackers, who could access, retrieve and use confidential customer information. Apart from that, the most common threats include viruses, worms and Trojan horse. Viruses are spread via email or by downloading infected files. Viruses are a nuisance threat that can be categorized as a denial of service (DOS) tool due to the fact that they only interrupt electronic communications. Worms can be categorized as special viruses that spread using direct Internet connections and Trojan horse programs launched against client systems pose the greatest threat to the e-Payment systems because they can avoid or disrupt most of the authentication and authorization mechanisms used in an electronic transaction. The Trojan horses aim to sensitive data (e.g. passwords, confidential data, etc.) and send it back to their owners to gain access to third-party computers and thus take control of them remotely. (Alexandru,2015).Phishing and pharming are method used to solicit personal information by posing as a trustworthy organization. In recent years both pharming and phishing have been used for online identify theft information. Usually the attacker sends an email seemingly from a reputable credit card company or financial institutions that request account information, often suggesting that there is a problem. When users respond with the request information, attackers can use it to gain access to the account (Aziz, Mohamed & Zakaria, 2015).Spamming or E-mail bombing that is caused by a hacker targeting one computer or

network, and sending thousands of email messages to it. Sending unsought commercial emails to individuals is also achieved placing software agents into a third-party system and setting it off to send requests to an intended target. Drive-by downloads are malware infections that represent a major threat to e payment. Users get diseased with such malware simply by visiting a particular website. These websites often contain authentic content, but have been contaminated by harmful programs that smuggle malicious codes into the site (Alexandru, 2015). Considering above literature evidences, following hypothesis is suggested.

H_1 *- Security risk makes influence positively on risk of e-payments of the banking sector in Colombo district.*

Perceived risk

According to Aziz, Mohamed and Zakaria (2015,588p) perceived risk is known as "Using e-commerce, users do not have a chance to see the product physically before the actual purchase take place. Thus, the seller may take advantage by giving false information on the product attributes and conceal any information that may have an impact to the buyer in the future". However, Simon and Victor (1994) stated that consumer behavior involves risk in the sense that any action of a consumer may lead to unpleasant consequences. Perceived risk affects all purchase decisions and consumers' behavior, by deterring them to buy (Vos, Marinagi, Trivellas, Eberhagen, Skourlas, & Giannakopoulos, 2014).On the other hand, perceived risk arises when a consumer performs transaction via the electronic channel like a web site (Cheng, Hamid and Cheng, 2010). While using e-commerce, user does not have a chance to see the product physically before the actual purchase take place. Therefore, perceived risk is user's subjective expectation (Aziz, Mohamed and Zakaria, 2015).There are two basic approaches used to define the concept of perceived risk, as a function of uncertainty of the purchase outcome and the consequences associated with unfavorable purchase outcomes (Simon & Victor, 1994).

Simon and Victor (1994) identified that, the uncertainty consequences approach measures perceived risk as a function of the uncertainty of the purchase outcomes and the consequences associated with unfavorable purchases outcomes. Uncertainty may not be just in terms of product attributes but also in terms of pricing whether it is overpriced, delivery defer the delivery due to stock out and also the company itself, whether it exists or not. All of these uncertainties and associated risks are also believed to have effect of user's acceptance (Aziz, Mohamed &Zakaria, 2015). In addition, Simon and Victor (1994) mentioned that,one can conclude that the amount of purchase has a more significant effect on the perceived risk of cash payment than other payment methods. The impact on the perceived risk of credit card and other payment methods are small except in the dimension of performance risk. Uncertainty can be mitigated by talking to different providers prior to a purchase and by customer deliberation that is, shopping around and looking at alternative offerings in terms of price, promotional material, and the track record and reputation of alternative providers (Okeke, 2013). Further, he has noted that customers perceive greater risk when buying service than tangible goods. Perceived service as riskier than products because services are intangible, non-standardized, and often sold without guarantees or warrantees. Consumers

can rarely return a service to the service provider since they have already consumed it and some services are so technical or specialized that consumers possess neither the knowledge nor the experience to evaluate whether they are satisfied, even after they have consumed the service (Okeke, 2013).

During the purchasing process, the customers will confront different kind of risk, some of them can be perceived by themselves, some of them can't, some of them can be extravagated, and some can be dwindled. Thus, the perceived risk may be different from the actual risk because the risk can't influence the buying decision without knowing it (Hong & Li Yi,2012).According to the Simon and Victor (1994) simply stated that risk component approach identifies and measure the several basic dimension of the overall perceived risk in buying behavior (e.g. Performance risk, physical risk, psychological risk, social risk and time-loss risk).Consumers develop strategies to reduce risk, allowing them to act with confidence and enable decision making. Therefore, several strategies to reduce risk, such as buying known brands or patronizing known stores, collecting information about the product, looking for guarantees and evaluating products with free samples. (Nepomuceno, Laroche& Richard, 2012).

When people shop on-line, they perceive more risks than shopping in stores or supermarkets because they can't check the commodity before they get them due to the dummy of the network and the worry of the after-sale service quality. As a solution, new household shopping style, shopping on-line use internet as its exchanging media, so it is not easy to identify each other's identity with uneven information. Therefore, a lot of new risks emerged which are not covered by traditional trade circumstance. (Hong & Li Yi,2012).Perceived risk can lead to reduce the usage of consumers' intention to use e-payment system. Therefore, perceived risk should be taken into contemplation when designing e-payment system in order to increase the consumers' intention to use. It is noted that the constructs of the e-payment system should include efficiency and good design while providing security to reduce the risk that support the ease of use and effectiveness of the e-payment that can lead to consumers' intent to use e-payment system (Kim, Tao, Shin & Kim, 2010).Accordingly, following hypothesis was developed based on above literature support.

H_2-Perceived risk makes influence positively on risk of e-payments of the banking sector in Colombo district.

Operational risk

Throughout the e- payment process, operational risk arises from the loss of system break downs and incorruptions of system exposes (Macaulay, 2008). Failures such as disconnection, time-out of ICT service would result in disruption to normal business transactions. It would affect to the economic activities in a country (Arif&Hinti,2014).And also, operational risk arises due to lack of understanding about security and confidentiality (AL-ma Aitah & Shatat, 2011).In addition, operational risk arises from the potential loss due to significant insufficiencies in the system design which lead to reliability or integrity issues. It may impair the system's ability to complete settlement, create liquidity pressures for system as a whole, curtail the system's ability to monitor and manage its credit exposures and

result in errors, delays, or frauds in system operation (Seng,2008).According to Arif and Hinti (2014, 239p) argued that "The definition of operational risk is a challenge". Rachnaand Singh (2013) in his review, concluded that, Malfunctioning IT systems and telecommunication failures, categorized as operational risk, are the usual source of problem affecting local bank's ATM network. The risk may be heightened if the customers are not adequately educated about the importance of security precautions (Seng, 2008).

In addition to external attacks on electronic money and electronic banking systems, banks are exposed to operational risk with respect to employee fraud: employee could surreptitiously acquire authentication data in order to access customer accounts, or steal stored value cards. Inadvertent errors by employees may also compromise a bank's systems (Basel Committee on Banking Supervision, 1998). Operational risk can also arise from customer misuse, and from incompetently designed or instigated electronic banking and electronic money systems. Security considerations are paramount, as banks may be subject to external or internal occurrences on their systems or products. Many of the specific possible manifestations of these risks apply to both electronic banking and electronic money (Arif & Hinti, 2014).Beside from that, the risk that hardware or software problems, human error or malicious attack will cause a system to breakdown or malfunction giving rise to financial exposures and possible losses(Power, 2003).The system is exposed to the risk of a disruption or break-down of systems due to system obsolescence, incompatibility and design flaws. Over confidence on outsourcing may also expose the system to operational risk of not properly moderated (Seng, 2008).

Further, operational risk arises with respect to the controls over access to a bank's critical accounting and risk management systems, information that it communicates with other parties and, in the case of electronic money, measures the bank uses to deter and detect counterfeiting. Controlling access to bank systems has become increasingly complex due to expanded computer capabilities, geographical dispersal of access points, and the use of various communications paths, including public networks such as the Internet. (Basel Committee on Banking Supervision, 1998). Furthermore, Arif and Hinti (2014) concern that, it is necessary to wish that the models of operational risk in the near future provide the same level of transparency and accessibility as those used in market or credit risk. This is a must if it wants to effectively integrate operational risk in a comprehensive system of risk management. Accordingly, with above evidences it seems that operational risk can be seen when a user does a transaction using e-payment methods in the banking sector. Thus, it is proven that risk of e-payment is backed by operational risk associated with e-payments. Hence following hypothesis was derived.

> ***H_3*** *- Operational risk makes influence positively on risk of e-payments of the banking sector in Colombo district.*

Financial risk

The risk involved with e-payment alternatives will lead to financial loss. Financial loss means that the consumer cannot get a refund when needed or is not able to reverse the transaction or to stop payment after discovering the mistake. However, it does not include the loss of credit float when using cash or e-payment instruments (Simon & Victor, 1994). Cheng, Hamid and Cheng (2010, 126p) have proven that "the risk that use of that mode of payment will cause financial loss. Situation in which it is not refundable or the transaction is not reversible". Bank engaged in electronic bill payments programs may face financial risk if a tried party intermediary fails to carry out its obligations with respect to payment. Banks that purchase electronic money from an issuer in order to resell it to customer are also exposed to financial risk in the event the issuer defaults on its obligations to redeem the electronic money (Nepomuceno, Laroche & Richard, 2012).

According to AbMananand Shafiai (2015) argued that one type of financial risks is credit risk which is chosen as the risk has negative repercussions on the sustainability. Further, he stated that risk is a common thing that has to be faced by all financial institutions and they cannot avoid it: however, they can take action to reduce it. Risk is the possibility that the outcome of an event could result in an adverse situation. More specifically in finance, risk refers to the probable loss of income and asset value. Seng (2008) mentioned that the financial risk is also called replacement cost risk, that is, the risk of loss of unrealized gains on unsettled contracts with the defaulting participant. The replacement cost depends on the instability of the transaction price and the amount of time that elapses between the trade date and the settlement date. According to Nepomuceno, Larocheand Richard (2012) high levels of system security when associated with mental intangibility led to higher perceptions of financial risk. In other words, when the product is mentally intangible and consumers have high concerns for system security the financial risk associated with the purchase is higher. It is interesting to note that financial risk is associated only with mental intangibility and not with generality or physical intangibility, indicating that the first is cognitively harder to bear when it comes to this type of risk. So that, those who are doing transactions in online mode by using e-payment systems face such kind of financial risk. Due to this kind of risk, users are afraid to accept or use the e-payments in the banking sector. Accordingly, it was motivated to propose the following hypothesis to be tested in this study.

H_4-Financial risk makes influence positively on risk of e-payments of the banking sector in Colombo district.

The aim of the research study is to identify the risk of electronic payment systems and make the appropriate recommendations to improve the e-payment systems. Above argument, gives the idea that four types of risk mentioned above have an impact on the performance and acceptance of the e-payments. As a result of these risk there is a reduction in the efficiency and effectiveness of the e- payment system.

Research Methodology and Analysis

By administering a structured questionnaire, primary data were gathered from 150 respondents who are in Colombo district and they were based for analysis of this study. The Convenience sampling technique was applied by following survey strategy under the deductive reasoning approach. For capturing quantitative data from a large sample, survey strategy is appropriate (Saunders et al., 2009). Quantitative data is more suitable to apply statistical techniques and make the inferences (Shajari & Ismail, 2013). Gathered data was entered into a data sheet created in SPSS 16.0 and scrutinized. Analysis was performed by using AMOS 20.0.

Well – known and firm method called as Structural Equation Modeling (SEM) applied in many research fields (Khine, 2013; Lei & Wu, 2007; Anderson & Gerbing, 1988) is used for the analysis purpose. Testing the structural relationships hypothesized based on literature evidences is the goal of the SEM. SEM is best to evaluate the model fit as one of the modern statistical approach as well as multiple variables can be handled simultaneously with more confidence and efficiencies (Byrne, 2010). In SEM, two models are used to perform the analysis named as measurement model and structural model. (Anderson & Gerbing, 1988). Measurement model is evaluated by the Confirmatory Factor Analysis (CFA) and model fit indices generated from CFA determine the model fit with the cut-off values recommended by (Hair et al. 2006; Anderson & Gerbing, 1988). Having confirmed the model fit with fit indices, it can go for further analysis. The fit indices found from the CFA are summarized in Table 01.

Table 01- Fit indices of the model

Chi-square	GFI	AGFI	CFI	NFI	TLI	RMSEA	RMR	p-value
1.118	0.952	0.914	0.952	0.925	0.987	0.028	0.038	0.274

Three kind of model fits (Absolute, Incremental and Parsimonious) can be used to determine the goodness of fit of a research model. Among them, absolute fit is the best model fit to evaluate a model. However, if a model is not fit with absolute fit indices then can go for other two to assess the model. According to Hair et al. (2006) Normalized Chi-square, Root Mean Square Error of Approximation (RMSEA) and Goodness of Fit Index (GFI) are considered as absolute fit indices and these indices are the most significant as well as show goodness of fit (Hair et al. 2006). Adjusted Goodness of Fit Index (AGFI), Comparative Fit Index (CFI), Normed Fit Index (NFI) and Trucker Lewis Index (TLI) are fallen under the Incremental fit indices while Normalized Chi-square is considered as parsimonious fit index. Fit indices shown in Table 01 confirms that this particular model is fit showing good fit under absolute fit criteria as chi-square value (1.118) is less than 5 which is accepted as cut-off (Hair et al. 2006). RMSEA (0.028) is below the accepted cut-off value of 0.08 and GFI (0.952) also is matching with cut off value of 0.9. The values of other fit indices (AGFI, CFI, NFI and TLI) also show a good fit of the model. Furthermore, RMR value (0.038) is below the 0.08 (Cut-off) showing good fit. Accordingly, overall, it seems that this particular proposed model has a good fit and confirmed the validity of the model.

Direct paths/Hypotheses			Estimate	P - value	Hypothesis	Support or not
Security risk	--->	Risk of e-payment	.137	0.216	H_1	Not supported
Perceived risk	--->	Risk of e-payment	.084	0.324	H_2	Not supported
Operational risk	--->	Risk of e-payment	.048	0.653	H_3	Not supported
Financial risk	--->	Risk of e-payment	.329	0.004	H_4	supported

Table 2 - Standardized Regression Weights

The P values appear in the Table 2 give hints for the hypotheses developed with the construct of risk of e-payment while determining one hypostasis is supported and other three are not supported. The detailed discussions with derived results are presented in coming section.

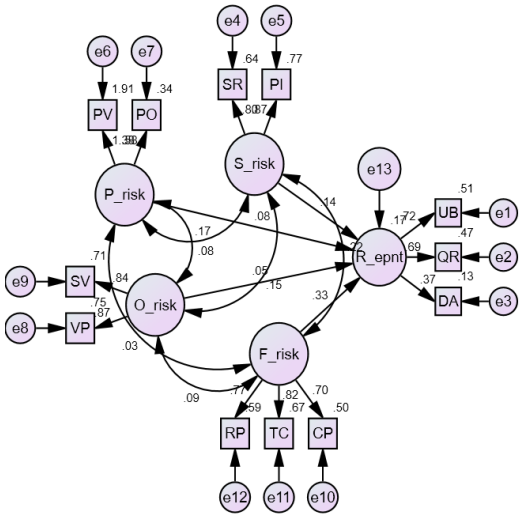

Figure 1 – Structural model

3. Result and Discussion

The study mainly focuses to investigate the positive influences of security risk, perceived risk, operational risk and financial risk towards the risk associated with e-payments among the e-payment users of the banking sector in Colombo district. The findings of the Pearson correlation analysis reveal that there is a weak &positive influence of security risk on risk of e-payments. Therefore, this finding confirmed with the result of Seng (2008),Rachna& Singh (2013) and Aziz, Mohamed & Zakaria (2015). Further it was noted that weak & positive relationship between perceived risk and risk of e-payments. However, the relationship was not significant. This finding does not confirm the findings of Simon &Victor (1994) and Vos, Marinagi, Trivellas, Eberhagen, Skourlas, & Giannakopoulos (2014). As well as, the relationship between operational risk and the risk of e-payment was not significant and reported very weak positive influence of operational risk towards the risk of e-payment. Thus, this finding does not match with the findings of Arif and Hinti (2014), Seng (2008) and Basel Committee on Banking Supervision (1998). Correlation between financial risk and risk of e-payment was proved with the result of the correlation analysis. According to the structural analysis of SEM, the key finding of the study is the positive influence of financial risk on risk of e-payments. Therefore, the finding confirm with the results of Cheng, Hamid and Cheng (2010) and Nepomuceno, Laroche & Richard (2012). Accordingly, it was reported

that only 9.5 percent of risk was explained by the developed model with the data collected from Colombo district in Sri Lanka.

4. Conclusion and recommendation

With the analysis performed in this study, it could conclude that among the different types of risk, the most important risk is the financial risk towards the risk of e-payment. Thus, e-payment users pay more attention on financial risk when they do the transaction in online business. In addition, the study shows practical contribution to the area of risk associated with e-payments. Finally, it can be concluded that the risk of e-payments in the banking sector can be reduced through focusing on the different types of identified risk in this study such as security risk, operational risk, perceived risk and financial risk.

Accordingly, some recommendations could be suggested in order to reduce the different types of risk associated with e-payments and they may help to enhance the online payment system without the fear of risk. According to the revealed results of the correlation analysis, security risk was a considerable factor for e-payments. Therefore, some e-payment users face some sort of security issues, because online transactions are an easy target for stealing money and personal information, thus the security of e-payment is a significant issue which determine user acceptance of the payment methods. So that, study recommends to provide strong security platform for e-payment users by combining various means. Furthermore, perceived risk also should be considered and should follow the actions to reduce the perceived risk when do the e-payments in online environment. Hence, well enriched awareness programs should be arranged for e-payment users before transactions are taken place. Then user's subjective anticipation will remain with the desired outcomes of the transaction. By doing so, can obtain a better online service. Results revealed that financial risk also makes strong influence on risk of e-payment methods. Thus, system developers should pay more attention to reduce the financial risk by providing stable systems for online users.

5. Limitation and Future Research Directions

Few limitations were identified for this study and they can be considered in future studies. In this study, the focus is only given to e-payment users who were in banking sector, Colombo district. Therefore, generalization of conclusion cannot be made on every e-payment users in the country. Only four types of risk were considered in this study. For future research, other types of risk can be considered to provide a wider and in-depth understanding about the risk in e-payments while expanding the geographical area under the study.

Reference

Aziz Ab, N. H., Mohamed, I. S., Zakaria, N. B. (2015). Security, Risk and Trust Issues among Muslim Users for Online Businesses. *International Accounting and Business Conference, Iabc, 31,* 587-594.

AbManan, S. K., and Shafiai, M. H. B. M. (2015). Risk Management of Islamic Microfinance (IMF) Product by Financial in Malaysia. *International Accounting and Business Conference, Iabc, 31,* 83-90.

Alexandru, B. (2015). Security issues and solutions in e-payment systems. *Fiat Iustitia*, *1*, 172-179.

AL-ma Aitah, M., and Shatat, A. (2011). Empirical Study in the Security of Electronic Payment Systems. *International Journal of Computer Science Issues (IJCSI), 8* (4), 393-401.

Arif, F. Z. E., and Hinti, S. (2014). Methods of quantifying operational risk in Banks: Theoretical approaches. *American Journal of Engineering Research (AJER), 3* (3), 238-244.

Anderson, J.C. and Gerbing. D.W. (1988). „Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach". Psychological Bulletin, *103*(3), 411-423.

Basle Committee on Banking Supervision. (1998). Risk management for electronic banking and electronic money activities. *Electronic money,97* (122), 1-25.

Byrne, B.M. (2010). Structural Equation Modeling with AMOS. Basic Concepts, Applications and Programming (2nd edition). New York/London: Routledge.

Cheng, A. Y., Hamid, N. R. A., and Cheng, E. H. (2010). Risk Perception of the E-payment System: A Young Adult Perspective. *Recent Researches in Artificial Intelligence, Knowledge Engineering and Data Bases,* 121-127.

Dzemydienė, D., Naujikienė, R., Kalinauskas, M., Jasiūnas, E. (2010). Evaluation of security disturbance risks in electronic financial payment systems. *Intellectual Economics, 2*(8), 21-29.

Hair, J., Black, W., Babin, B., Anderson, R. and Tatham, R. (2006), Multivariate Data Analysis, 6 edn, Pearson Educational International -Prentice Hall, Upper Saddle River- New Jersey.

Hong, Z., and Li Yi (2012).Research on the Influence of Perceived Risk in Consumer Online Purchasing Decision. *International Conference on Applied Physics and Industrial Engineering, 24 part b,*1304 – 1310.

Junadi, and Fenrianto, S. (2015). A model of Factors Influencing Consumer's Intention to Use E –payment System in Indonesia. *International Conference on Computer Science and Computational Intelligence (ICCSCI), 59,* 214-220.

Khine, M.S. (ed.), (2013). Application of Structural Equation Modeling in Educational Research and Practice, Sense Publishers. All rights reserved.

Kim, C., Tao, W., Shin, N., and Kim, K. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9(*1*),* 84-95.

Lei, P.W. and Wu, Q. (2007).An NCME Instructional Module on Introduction to Structural Equation Modeling: Issues and Practical Considerations", Educational Measurement: Issues and Practice, 33-43.

Macaulay, T. (2008). Convergence of Operational and Credit risks: Additivity of risk - Paper I of III. 1-6.

Nepomuceno, M. V., Laroche, M., Richard, M. and Eggert, A. (2012). Relationship between intangibility and perceived risk: moderating effect of privacy, system security and general security concerns. *Journal of Consumer Marketing, 29* (3), 176-189.

Okeke, T. C. (2013). Perceived Risk/Security and Consumer Involvement with Electronic Payments in Nigeria: A Discriminant Analysis. *IOSR Journal of Business and Management, 14* (6), 57-67.

Power, M. (2005). The Invention of Operational Risk. *Review of International Political Economy 12*(4),1-20.

Rachna, and Singh, P. (2013). Issues and Challenges of Electronic Payment Systems. *International Journal for Research in Management and Pharmacy, 2*(9), 25-30.

Saunders, M., Lewis, P., and Thornhill, A. (2009). Research methods for business students (fifth edition), Pearson Education, FT Prentice Hall publishers.

Seng, L. C. (2008). The development of e-payments and challenges for central banks in the SEACEN countries, *The South East Asian Central Banks (SEACEN),*1-342.

Shajari, M. and Ismail, Z. (2013). „Testing an Adoption Model for E-Government Services Using Structural Equation Modeling", International Conference on Informatics and Creative Multimedia, 298-303.

Simon, S. M. Ho.,and Victor, T. F. (1994). Consumer's Risk Perceptions of Electronic Payment Systems. *International Journal of Bank Marketing, 12* (8), 26 – 38.

Vos, A., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G. (2014). Risk Reduction Strategies in Online Shooing: E –trust perspective, Procedia - Social and Behavioral Sciences. *ICININFO, 147,* 418-423.