Global Journal of Information Technology: Emerging Technologies

Volume 12, Issue 2, (2022) 136-148

www.gjit.eu

Security and privacy concerns in mobile payment services

Nadire Cavus [a*], Near East University, Nicosia, Cyprus / Near East University, Computer Information Systems Research, and Technology Centre, Nicosia, Cyprus.
Atanda Adeoluwa[b], Near East University, Department of Computer Information Systems, Nicosia, Cyprus.

Suggested Citation:
Cavus, N & Adeoluwa, A. (2022). Security and privacy concerns in mobile payment services. *Global Journal of Information Technology: Emerging Technologies*. *12*(2), 136-148. https://doi.org/10.18844/gjit.v12i2.8264

Received from; May 22, 2022, revised from; July 24, 2022, and accepted from October 19, 2022
Selection and peer review under the responsibility of Assist. Prof. Dr. Ezgi Pelin YILDIZ, Kafkas University, Turkey.

Abstract

Mobile technology is becoming more central to human life, especially with the current ongoing global pandemic which points out that there will be an increasing need for mobile payment service as it requires little or no contact in making payments. However, mobile payment is not among the most commonly used mobile utilities because of the security and privacy concerns posed by mobile payment. The prime aim of this study is to determine the security and privacy concerns with the highest existence and then address them by identifying a rational and objectively agreed approach on how to resolve the problems discovered. A sensitive Analytical Hierarchy Process (AHP) Pairwise Comparison approach will be used to solve the security and privacy challenges associated with mobile payment services. This study shows that leakage of personal data is the highest risk concern by most users of the mobile payment system (MPS) while loss of "intended purchase" has the lowest risk concern from what we could derive.

Keywords: AHP Model; Mobile Technology; Mobile Payment Services; Pairwise Comparison.

* ADDRESS FOR CORRESPONDENCE: Nadire Cavus* Near East University, Department of Computer Information Systems, Nicosia, Cyprus / Near East University, Computer Information Systems Research and Technology Centre, Nicosia, Cyprus.
E-mail: nadire.cavus@neu.edu.tr Tel: +90 (392) 223 64 64 / 3114.

1. Introduction

In 1983, electrical architect Charles Walton got the main patent for an RFID gadget. In 1997, Coca-Cola presented portable installments utilizing a set number of candy machines. In 2011, Barclay's collaborated with Orange and dispatched Europe's first contactless versatile installment. Google dispatched Google Wallet that very year and afterward Apple Pay was dispatched three years after the fact. Versatile installment is typically alluded to as the installment administrations executed through a cell phone (Ganesan et al, 2020). An individual can utilize a cell phone to pay for different sorts of administrations and products, rather than ordinary techniques, for example, charge cards and money (Elgharnah & Ozdamli, 2020; Salama, Uzunboylu & Alkaddah, 2020; Karagozlu, 2020).

In gauge, the exchange volume for versatile installment overall is required to hit up to 14 trillion by 2022 (Rolfe, 2018). Toward the finish of 2017, there were 30% portable installment clients out of 1,6 billion shoppers around the world. The huge development of portable business (m-Commerce) exceptionally affects versatile installment notoriety. Market patterns in retail buying have consistently advanced toward progressive versatile-based installment entryways throughout the last decade. A new review by Sun et al, (2020) showed that 93.2 percent of clients in China cover their eatery bills utilizing MPS. The ubiquity of versatile installment administrations has continuously ascended lately.

In terms of capabilities, our smartphone devices are somewhat close to regular desktop computers and notebook and as a result, they face the very same security and privacy issues as conventional computing devices does (Kaldiyarov et al., 2018; Al-Johali, 2019; Salama & Arab, 2022). It is much worse in their case due to memory and storage constraints. Mobile phones, especially our modern-day smartphones have gained insufficient consideration as regards security and privacy concerns as developers are more interested in the creation of new features and applications which most of the time exposes us to even great security risks.

Furthermore, mobile services are prone to network load which as it sounds refers to the amount of data(traffic) being carried by the network. Google has announced that there are currently more than 2 billion active Android smartphones monthly (Popper, 2018; Markoska, 2019). If you need to install an application on your device, you will have to grant access to the application to access your camera, internet, location, etc and this can lead to security and privacy issues.

1.1. Literature review

The reliability of mobile phones has not been entirely proven for end users (Gursel, 2018; Isik & Jallad, 2019). There has been little research into risk evaluations of mobile payment protection, and it is unclear how risk events affect security breaches that occur by smartphones. One of the most serious threats is the loss of a mobile. Since it is difficult to prove the identity of the true owner, the individual who steals or grabs the cell phone can make money transactions without permission (Dzafri et al, 2020). Numerous cases of pharming, spoofing, phishing, sniffing, and malware have been identified for mobile devices in terms of threats and challenges. Cybercriminals target the mobile payment infrastructure by launching a slew of threats and attempts on mobile devices, compromising consumer privacy and causing financial damage (Wang et al, 2012; Çelik, Özgür, & Yavuz, 2018).

Based on the expert review, we hope to define the protection and privacy risk incidents that affect mobile payment acceptance and purpose in this article. Potential risk incidents and their implications for mobile payment platforms should be carefully defined, as this would result in safer

payment services for end users. As a result, a core goal of this study is to design an effective qualitative risk evaluation method that elicits input from a variety of experts.

The following risk events and consequences have been listed for expert reviews after reviewing several previously published papers that are properly cited and relevant to this subject (Tables 1 and 2). These risk events and consequences will be included in this article, and each one is given an alphanumerical reference below, with A denoting Alternatives and C denoting Consequences (Ganesan et al, 2020):

Table 1

Risk events corresponding to alternative

Consequences	Criteria
Financial loss	C1
Confidential data loss	C2
Unavailability of Device	C3
Leakage of Personal data	C4
Loss of Intended Purchase	C5

Risk Events	**Alternatives**
Malware	A1
Phishing	A2
Network device spoofing attack	A3
Sniffing on legitimate data network	A4
Loss or theft of a device	A5
Unauthorized physical device access	A6
Vendor Backdoor	A7
Fake application	A8
User Negligence	A9
Technical Failure of the network	A10

Table 2

Consequences corresponding to criteria

1.1.1. Analytic Hierarchy Process Model

The Analytic Hierarchy Process (AHP) is the most widely used MCDM (Multi-Criteria Decision Making) technique developed by Saaty (2008). The demonstration of the progressive system is the most important aspect of this ideology. The problem might be a highly strong, multi-standards circumstance that is causing contact. A pairwise correlation of the several components can be constructed, with the characteristics in each cell reflecting the dominance of one component over another in comparison to certain specified metrics. This scaling formulation will result in the greatest eigenvalue issue for each pecking order. Another major benefit of AHP pairwise comparison is that it helps an expert to compare the consequences against alternatives and relies on expert decisions to establish priority scales (Ganesan et al, 2020).

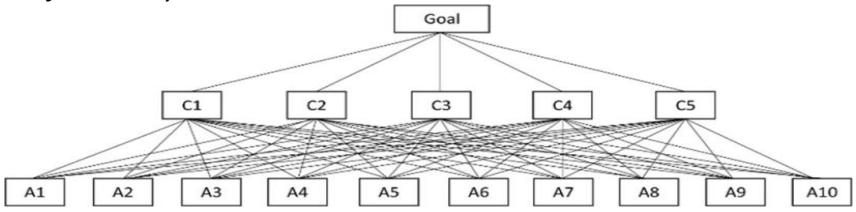
AHP has been applied in many decision-making processes such as evaluating e-payment system factors influencing mobile banking use in Iranian banks, prioritizing alternative strategies to control malaria in the state of Nigeria, identifying the reason for defects in Heritage Building in Malaysia, etc.

The current advancement of a versatile installment is presented security dangers and weaknesses (Asante et al, 2019). AHP is utilized in this paper to make a model that focuses on hazard occurrences as choices dependent on security suggestions as boundaries. The actions engaged with pairwise correlation are as per the following all in all;

1. Identify the issue to be addressed and establish a goal for resolving it.
2. Create a hierarchical model based on the goals, criteria, and alternatives.
   (a) Goal: Determine the consequences and risk incidents influencing mobile payment security and privacy.
   (b) Criteria: As security consequences, criteria are obtained from literature analysis in this AHP Model.
   (c) Alternatives: Risk events detected by literature analysis that have an impact on mobile payment security and privacy are being seen as alternatives (Figure 1).

Figure 1

Hierarchal model of this study



3. Create a matrix of pairwise comparisons for criteria and alternatives. The matrix compares elements in the upper level by pair concerning a criterion.

Figure 2

Pairwise comparison matrix for criteria

$$A = \begin{array}{c} \\ C1 \\ C2 \\ C3 \\ C4 \\ C5 \end{array} \begin{array}{c} \begin{array}{ccccc} C1 & C2 & C3 & C4 & C5 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Figure 3

Pairwise comparison matrix for alternatives

$$B = \begin{array}{c} \\ A1 \\ A2 \\ A3 \\ A4 \\ A5 \\ A6 \\ A7 \\ A8 \\ A9 \\ A10 \end{array} \begin{array}{c} \begin{array}{cccccccccc} A1 & A2 & A3 & A4 & A5 & A6 & A7 & A8 & A9 & A10 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

(a) For pairwise examinations, AHP uses the Eigen esteem approach. The pairwise scale has a size of 1 to 9. The pairwise examination scale is appeared in table 3;

Table 3

Pairwise Comparison Scale

Numerical Values	Description	Explanation
1	Equal importance of both elements	Two elements contribute equally
3	Moderate importance of one element over another	Experience and judgment favor one element over another
5	Strong importance of one element over another	An element is strongly favored
7	Very importance of one element over another	An element is very strongly dominant
9	Extreme importance of one element over another	An element is favored by at least on order of magnitude

4. By comparing each variable in the corresponding matrix, we'll be able to compute the priority vector, which is the matrix's normalized Eigenvector. The sub-steps for calculating the matrix's normalized Eigenvector are described below (Ganesan et al, 2020).

(a) Complete the pairwise matrix with reciprocal value to the opposite of dominant selection. For example (Figure 4);

Figure 4

Pairwise matrix example

$$A = \begin{array}{c} \\ C1 \\ C2 \\ C3 \\ C4 \\ C5 \end{array} \begin{array}{c} \begin{array}{ccccc} C1 & C2 & C3 & C4 & C5 \end{array} \\ \begin{bmatrix} 1 & & 7 & & \\ & 1 & & & \\ 1/7 & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix} \end{array}$$

In this pairwise matrix, the user supports C1 over C3, then the lower diagonal is filled using this formula (Figure 5): -

Figure 5

Reciprocal value formula

$$a_{ji} = \frac{1}{a_{ij}}$$

(b) Sum each column of the pairwise matrix

(c) Create another matrix divide each element of the matrix with the sum of its column, and obtain the normalized relative weight of the priority vector, with wi(i=1…n) such that:

$$Cw=\lambda max\ w$$

Where w is the priority vector of weights and λmax is denoted as the maximum Eigenvalue of the comparison matrix, and it is needed to calculate the consistency index (CI).

5. Prioritize the alternatives and consequences based on the relative weight of the matrix
6. To validate the scoring consistency of pairwise comparison by the experts, AHP computes the consistency ratio (CR) for each pairwise matrix
   (a) The consistency ratio is calculated by AHP as seen in figure 6:

Figure 6

Consistency ratio calculation

$$CR = \frac{CI}{RI} \times 100$$

$$CI = \text{Consistency Index} = \frac{\lambda max^{-n}}{n-1}$$

$$RI = \text{Random Index} = \frac{1.98(n-2)}{n}$$

n = total number of criteria

   (b) The overall consistency ratio (CR) is determined by adding the Prioritization Weight Percentage to the number of all ranks, with the weighted consistency index (CI) in the nominator and the weighted random consistency index (RI) in the denominator. The consistency ratio value is critical for determining how much the pairwise matrix structure consistency extends. CR<0.1, for example, implies an appropriate degree of accuracy, while CR≥0.1 indicates otherwise (Ganesan et al, 2020).

1.2. Purpose of study

All transactions conducted on a mobile device are subject to the threats found in all mobile users. There are many kinds of cyber-attacks in which cybercriminals search for flaws in technologies and manipulate them to defraud citizens (Jang-Jaccard and Nepal, 2014). The prime aim of this study is to determine the security and privacy concerns with the highest existence and then address them by identifying a rational and objectively agreed approach on how to resolve the problems discovered. This article then goes on to a critical literature review of security and privacy violations, followed by testing methods, and ultimately, the proposed AHP pairwise comparative system is analyzed using result analysis.

1.3. Research Questions:

- Why security and privacy issues exist in Mobile Payment Services by accessing the risk impact
- Which of the security and privacy risk has the highest impact on MPS?
- How do we go about solving them?

2. Materials and Methods

2.1. Data Collection instrument

The expert interviews aided in the creation of an AHP model of risks, consequences, and their interrelationships. Furthermore, all of the threats and effects are outlined to all eight experts at the outset. Protection and privacy risk evaluation recognizes essential security protections in software and

helps to prevent program security flaws. Doing a risk assessment helps an enterprise to evaluate an application's vulnerability from the perspective of an attacker. As a result, performing an analysis is a critical step in risk management;

The following measures are considered for the security and privacy risk assessment model, according to the research study: -

(a) First, similar material from previous research is analyzed to classify identified assets and threats associated with smartphone use.
(b) The data is then used as the foundation for interviews with domain experts for AHP pairwise comparison.
(c) The experts' feedback is gathered to expose the AHP model's prioritized risks and consequences.

Eight experts were selected to assist in this interview based on relevant parameters such as their backgrounds, subject matter skills, and work expertise. Furthermore, when choosing specialists, two primary goals are taken into account. To ensure the accuracy of the information available, the expert's expertise and knowledge in the domain must be important and excellent. First, the expert's category must consist of many specializations and minimal correspondence for systematic research. Second, the expert's experience and knowledge in the domain must be relevant and excellent. This expert was chosen using the Analytical Hierarchy Process (AHP) core principles, which explicitly specify that only experts or professionals in the subject of the study issue should be used. These specialists are people I've known for a long time, and I chose them because they regularly utilize mobile payment services in their daily lives.

Table 4

Lists of Experts

No.	Job title and responsibility of experts
1	System Administrator in a Bank
2	Research Assistant at a University
3	Programmer in an IT solution company
4	Banker
5	Cryptocurrency Trader
6	Customer Service personnel in a Bank
7	Information Technology Senior researcher in a university
8	CEO of an IT solution company

2.2. Analysis

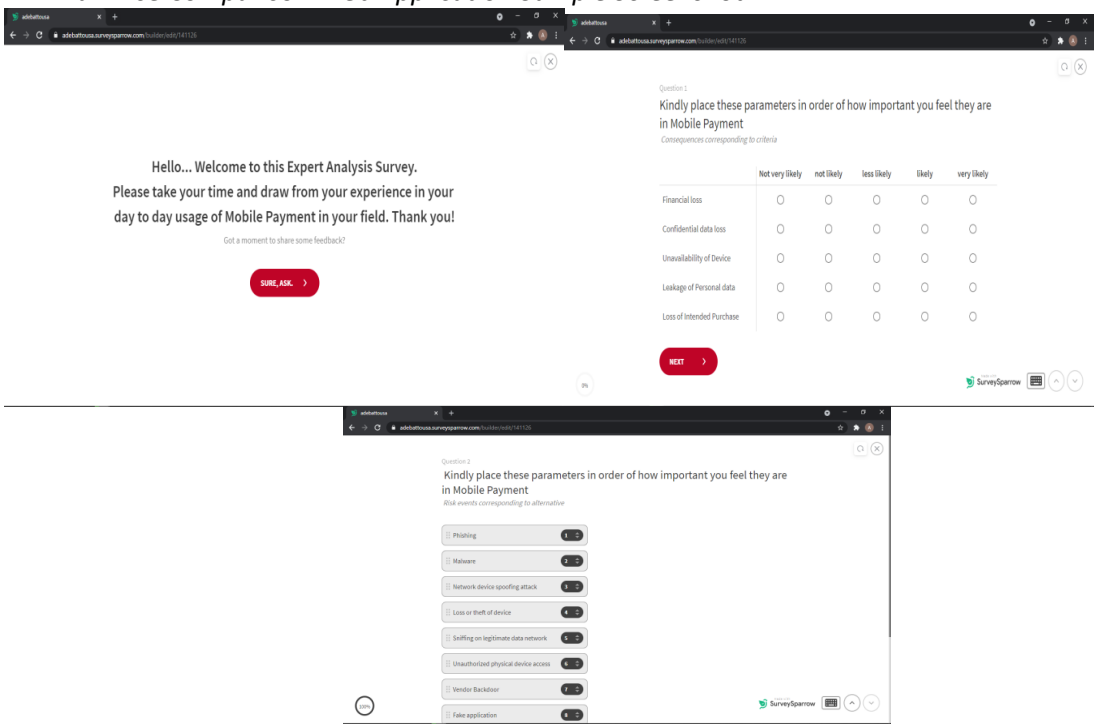
The study used an AHP Comparison Tool. During the interview, an interactive online interface was created to assist the experts in taking part in the pairwise comparison. In AHP, pairwise comparisons of all priority values are usually expressed in the form of a matrix. Considering the number of pairs in the alternatives and criteria, it is tedious for experts to use the matrices and manually compute the value.

The application helps experts to pick their preferred side of the valuation in a pairwise relation by simply rotating the slider in the application. The program is hosted in the cloud. To ensure safe, all data obtained from experts is stored in the cloud. The interview took place during this COVID-19 pandemic, and the experts participated in the interview via online conversation before filling out the survey form. The web application was created on an open source website (www.surveysparrow.com)

through https://adebattousa.surveysparrow.com/ link, accessed on May 12, 2021, which offered a 14-days free trial for creating and generating survey review. The trial period was used to conduct this research before it expired.

Figure 7

AHP Pairwise Comparison Web Application Sample Screenshot



3. Results

3.1. Elicitation by experts

Based on the literature, experts described a list of shared risks and consequences associated with mobile payment, and the information was used to evaluate the problem and consequences. The experts used the AHP pairwise comparison tool to express their preferred viewpoint on the prioritization of outcomes and risk events. In summary, each specialist was able to discern all of the dependencies between risks and consequences. The AHP Pairwise Comparison Matrix is used to compute each expert's input. The consistency ratio is determined after every other specialist gives a different weight prioritization to consequences and risk events (Tables 5 and 6).

Table 5

Experts Prioritization weight percentage for every consequence

	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6	Expert 7	Expert 8
Financial loss	17%	6%	21%	5%	33%	37%	12%	15%
Confidential data loss	37%	29%	30%	31%	28%	21%	42%	35%
Unavailability of device	6%	16%	4%	18%	7%	29%	6%	6%
Leakage of Personal data	37%	40%	39%	41%	29%	10%	36%	41%
Loss if intended purchase	3%	7%	4%	9%	3%	3%	3%	4%
Consistency Ratio	0.09	0.09	0.02	0.07	0.08	0.08	0.09	0.07

Table 6

Experts Prioritization weight percentage for every risk event

	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6	Expert 7	Expert 8
Malware	9%	7%	9%	4%	5%	9%	10%	6%
Phishing	10%	14%	8%	6%	6%	9%	6%	5%
Network device spoofing attack	8%	8%	10%	6%	4%	13%	12%	6%
Sniffing on legitimate data network	8%	8%	8%	5%	4%	4%	4%	4%
Loss or theft of mobile device	15%	17%	16%	22%	27%	15%	28%	27%
Unauthorized physical device access	14%	6%	4%	25%	20%	10%	25%	20%
Vendor Backdoor	7%	14%	10%	8%	5%	9%	6%	5%
Fake Application	15%	7%	19%	8%	9%	6%	6%	9%
User Negligence	7%	10%	7%	14%	14%	15%	12%	14%
Technical failure of network	8%	5%	8%	5%	7%	9%	7%	7%
Consistency Ratio	0.09	0.07	0.07	0.09	0.09	0.02	0.08	0.08

The weighted prioritization of consequences and risk events is a contingent value, and each risk event is compared pairwise concerning each consequence. According to table 5 and table 6, financial loss, confidential data loss, and personal data leakage rank highest among experts. The majority of experts rank the critical consequences of mobile payment and the potential risk cases, loss or theft of the device, and unauthorized physical device access as high. Furthermore, since all of the outcome and risk cases have CR<0.1, we should assert that expert opinion is consistent and acceptable. Figures 8 and 9 show the average of the consequences and risk events of the 8experts in a pie chart respectively.

Figure 8

Average relative weights vector of each criterion concerning the goal

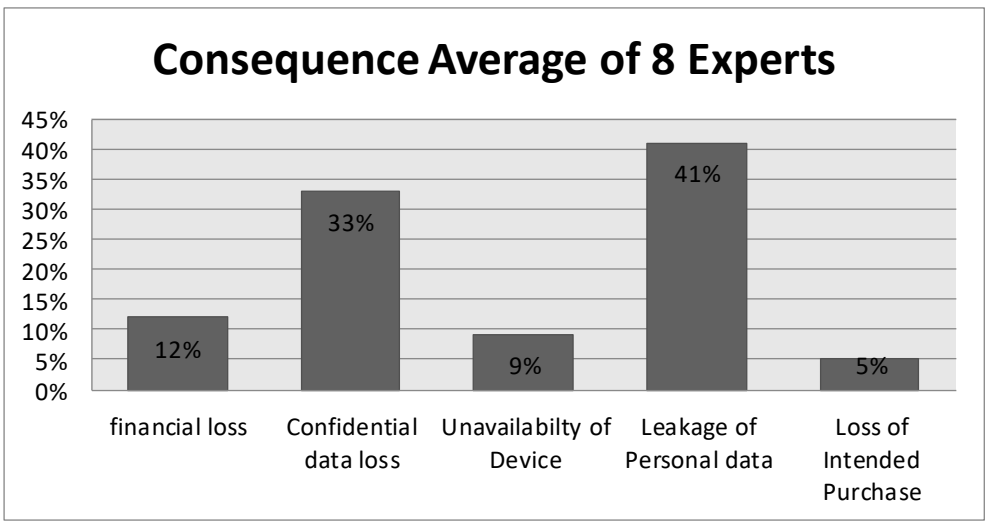


Figure 9

Average relative weights vector of each alternative concerning the criterion

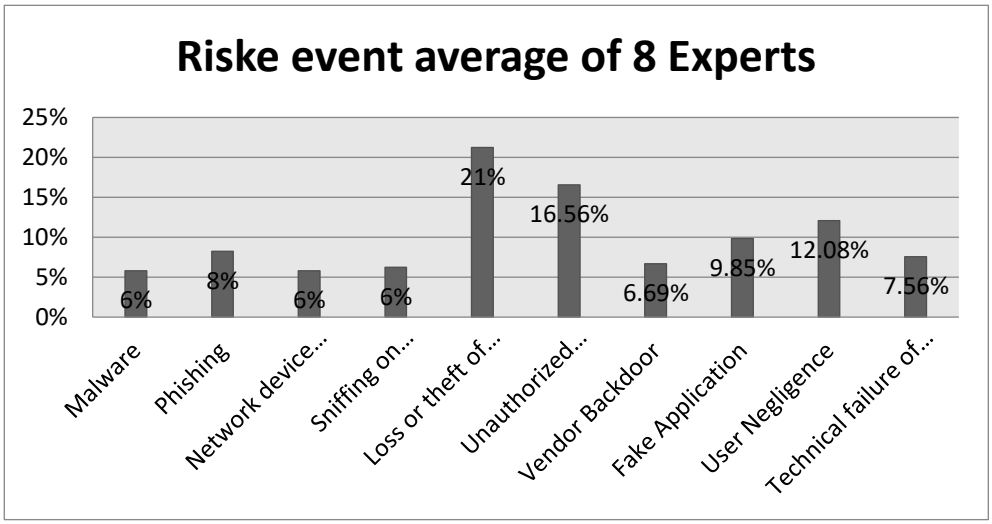


Table 7 displays the average weight for all expert judgment parameters concerning the target. It is clear that Leakage of Personal Data, with an average weight of 41%, is the most significant contributor to mobile payment security threats, whereas Loss of Intended Purchase, with a weight of 5%, is the least significant contributor.

Table 7

Average weight prioritization for every consequence

Consequences	Total	Priority Rank
Leakage of Personal data	41%	1
Confidential data loss	33%	2
Financial loss	12%	3
Unavailability of device	9%	4
Loss if intended purchase	5%	5

Table 8 computes the average weight assigned to each alternative concerning each criterion. Loss or theft of the device is classified as having a high effect on mobile payment security based on the priority rank of each alternative. According to experts, losing the device has a greater effect on consumers than malware, which is rated as the lowest priority.

Table 8

Average weight prioritization for every risk event

Risk Events	Total	Priority Rank
Malware	5.78%	10
Phishing	8.23%	5
Network device spoofing attack	5.79%	9
Sniffing on legitimate data network	6.23%	8
Loss or theft of device	21.23%	1
Unauthorized physical device access	16.56%	2
Vendor Backdoor	6.69%	7
Fake Application	9.85%	4

User Negligence	12.08%	3
Technical failure of network	7.56%	6

4. Discussion

The objective of the study is to use a qualitative approach to analyze mobile payment technology information security risk evaluation. The expert elicitation using the interview approach is the basis for an AHP model with dependencies on consequences and risk incidents. Our study indicates that the majority of mobile payment system end users have either been a victim of risk events or have heard of someone being a victim of risk events that result in various types of consequences (Jawale & Park, 2018; Kar, 2020). This has resulted in some fear/resentment towards accepting this technology solution of making payments using their mobile devices, even though it's going to make their lives easier.

These risk events were chosen as the primary causes after studying previously published publications to have a better grasp understanding the primary reasons why security and privacy concerns exist in mobile payment systems.

5. Conclusion

The priority classification of results indicates that the leakage of personal data is endorsed by most experts as the highest weighted average. The result is confidential data loss and financial loss that are also at a high priority level. The alternatives of mobile payment risk events, which indicate loss or theft of devices to have the highest average weight, as well as unauthorized Physical Device Access, are yet another significant finding of the report. The interpretation of this is that the greatest threat is the loss or theft of a device which can lead to confidential data loss and leave the user exposed.

For future study, the MACBETH approach can be used which simply means Measuring Attractiveness by a Categorical Based Evaluation Technique while AHP can be used to rank the relative significance in better decision-making.

References

Al-Johali, K. Y. (2019). Using mobile applications to teach vocabulary: Saudi EFL teachers' perceptions. *Global Journal of Foreign Language Teaching*, *9*(1), 51–68. https://doi.org/10.18844/gjflt.v9i1.3968 (Original work published February 28, 2019)

Asante, D., Opoku-Mensah, E., & Darko, P. A. (2019). Application Of Two-Stage Mcdm Techniques In Evaluating The Performance Of Electronic Payment Systems In Ghana. *International Journal of Data Mining & Knowledge Management Process*, 09(03), 01–18. https://doi.org/10.5121/ijdkp.2019.9301

Çelik, Ö. & Yavuz, F. (2018). The effect of using mobile applications on literal and contextual vocabulary instruction. *International Journal of Learning and Teaching*, *10*(2), 126–136. https://doi.org/10.18844/ijlt.v10i2.3407

Das, A., & Khan, H. U. (2016). *Security behaviors of smartphone users. Information & Computer Security*, 24(1), 116–134. https://doi.org/10.1108/ics-04-2015-0018

Dzafri D, Wong A., and Xiung J. (2020), "(update) *A TNG eWallet account allegedly 'hacked', RM3000 reloaded by card*," SoyaCincau.com, 12-Mar-2020.

Elgharnah, K. G. E., & Ozdamli, F. (2020). Determining parents' level of awareness about safe internet use. *World Journal on Educational Technology: Current Issues*, *12*(4), 290–300. https://doi.org/10.18844/wjet.v12i4.5182

Ganesan, T., Ong, T. S., Cheah, W. P., & Connie, T. (2020, September). *Assessment of Security Risk Impact on Mobile Payment Services. 2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*. https://doi.org/10.1109/iicaiet49801.2020.9257829

Gursel, C. (2018). Symptoms associated with mobile phone usage among Turkish university students. *International Journal of Innovative Research in Education*, *5*(2), 41–50. https://doi.org/10.18844/ijire.v5i2.1251

Isik, B., & Jallad, S. T. (2019). The potential of social media and nursing education: E-professionalism, nurse educator learner role, benefits, and risks. *New Trends and Issues Proceedings on Advances in Pure and Applied Sciences*, (11), 30–38. https://doi.org/10.18844/gjpaas.v0i11.4310

Jang-Jaccard, J., & Nepal, S. (2014). *A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences*, *80(5), 973–993*. https://doi.org/10.1016/j.jcss.2014.02.005

Jawale, A. S., & Park, J. S. (2018). *Towards trusted mobile payment services: a security analysis on Apple Pay. International Journal of Internet of Things and Cyber-Assurance, 76*. https://doi.org/10.1504/ijitca.2018.10011254

Kaldiyarov, D., Nurmukhankyzy, D., Bedelbaeva, A., Kaldiyarov, S., Lemechshenko, O., & Baltabayeva, A. (2018). State modification and market mechanism for agroindustrial complex management in the region. *International Journal of New Trends in Social Sciences*, *2*(1), 01–08. https://doi.org/10.18844/ijntss.v2i1.3643

Kar, A. K. (2020). *What Affects Usage Satisfaction in Mobile Payments? Modelling User Generated Content to Develop the "Digital Service Usage Satisfaction Model." Information Systems Frontiers*. Published. https://doi.org/10.1007/s10796-020-10045-0

Karagozlu, D. (2020). Determination of cyber security ensuring behaviours of pre-service teachers. *Cypriot Journal of Educational Sciences*, *15*(6), 1698–1706. https://doi.org/10.18844/cjes.v15i6.5327

Markoska, R. (2019). Managing ICT solutions for training and evaluation of C++ programming skills in e-learning ecosystem. *New Trends and Issues Proceedings on Humanities and Social Sciences*, *6*(7), 33–41. https://doi.org/10.18844/prosoc.v6i7.4509

Popper B. (2018), "Google announces over 2 billion monthly active devices on Android," The Verge, 17-May-2018.

Rolfe, A. R., Markantonakis, K., & Sauveron, D. (2016). Recovering from a lost digital wallet: *A smart cards perspective extended abstract. Pervasive and Mobile Computing, 29, 113–129.* https://doi.org/10.1016/j.pmcj.2015.06.018

Saaty, T. (2008). "*Decision making with the Analytic Hierarchy Process". Int. J. Services Sciences Int. J. Services Sciences. 1. 83-98*. 10.1504/IJSSCI.2008.017590.

Salama, R., & Arab, D. A. (2022). Designing an Android-based mobile app to address issues with online shopping. *Global Journal of Computer Sciences: Theory and Research*, *12*(2), 93–106. https://doi.org/10.18844/gjcs.v12i2.7528

Salama, R., Uzunboylu, H., & Alkaddah, B. (2020). Distance learning system, learning programming languages by using mobile applications. *New Trends and Issues Proceedings on Humanities and Social Sciences*, *7*(2), 23-47. https://www.un-pub.eu/ojs/index.php/pntsbs/article/view/5015

Sun, S., Yu, K., Xie, Z., & Pan, X. (2020). *China empowers Internet hospital to fight against COVID-19*. Journal of Infection, 81(1), e67–e68. https://doi.org/10.1016/j.jinf.2020.03.061

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone Security Challenges. Computer, 45(12), 52–58. https://doi.org/10.1109/mc.2012.288