Conference Paper

Users' Acceptance of Using Biometric Authentication System for Bahrain Mobile Banking

Zainab Mirza, Eman Alsalem, Fatima Mohsin, and Wael Mohamed Elmedany

Information Technology College, University of Bahrain, Bahrain

Abstract

The mobile banking authentication is considered as a major security risk for the financial sector; this risk can affect their interest, hence the purpose of this study is to evaluate the users' acceptance of using the fingerprint authentication as a biometric method for users' authentication and identification in Bahrain mobile banking. The model used in this study is an advanced version of Technology Acceptance Model (TAM), where the developed model for this study tests the factors that could affect the users' acceptance of using the fingerprint in Bahrain mobile banking services on a sample of 315 banking customers, the data has been analyzed by the Statistical Package for Social Science (SPSS). The finding indicates that all factors are significantly affecting the users' acceptance of using biometric authentication in Bahrain mobile banking and they are accepting this technology to be used.

Corresponding Author:
Wael Mohamed Elmedany
waelelmedany@gmail.com

Received: 18 September 2018
Accepted: 10 October 2018
Published: 15 October 2018

Publishing services provided by Knowledge E

© Zainab Mirza et al. This article is distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use and redistribution provided that the original author and source are credited.

Selection and Peer-review under the responsibility of the Sustainability and Resilience Conference Committee.

OPEN ACCESS

1. Introduction

Mobile banking (M-Banking) services could be defined as financial services that are remotely offered through the Internet, these services are performed using a mobile device, where the mobile device refers to a smartphone, tablets or Personal Digital Assistant (PDA) that are used to access the mobile banking applications [1]. Since the banking industries have been shifted some services to be available online such as accessing to all online banking needs, money transfer, enquiries on accounts and credit cards...etc. [2, 3]. Thus, raising the security and privacy has become a major concern for people who use the mobile banking where the security significantly affect the customers toward using it [4], the biometric authentication and identification system come to be the solution [5], where biometric authentication refers to a system that

used to precisely recognize an individual identity based on his/her physical characteristics like fingerprints, voiceprint, facial characteristics and more [6]. The Telecommunications Regulatory Authority (TRA) [7] stated that 98% of individuals are using the internet in Bahrain in which Bahrain takes the first rank globally for mobile broadband penetration, thus, made Bahrain community an attractive target that motivate the banking industries to provide mobile banking services and maintain the largest number of customers. Those customers who intend to use the mobile banking want to ensure its privacy and security and to succeed in implementing the biometric authentication system as a layer of security, the banking industries need first the customers to accept this new technology. Since the user acceptance affect the adoption of the mobile banking, this study aims to evaluate the customers' acceptance of using biometric authentication system for Bahrain mobile banking services based on a developed model from Technology Acceptance Model (TAM) [8], this model is tested to answer the core study question that is what are the factors that mainly affect the customers to use the biometric authentication system in their mobile banking services.

The rest of the study consists of the following sections: the literature review is presented in section 2, it covers the significance of mobile banking, attacks targeting it, biometrics as security solution in banking, fingerprint as authentication in mobile banking, mobile banking in retail banking and other mobile payment gateways in Bahrain, and finally user's attitude and acceptance model. The methodology is presented in Section 3. Section 4 presents the analysis. Then conclusion and the recommendation are presented in section 5.

2. Literature Review

2.1. Significance of mobile banking

For the last few years, the use of mobile devices has become a daily necessity for all people to fulfill their needs in both professional and personal life, where mobile devices are being utilized beside laptop computers, and even replacing them [9]. This rapid progression and change have forced the banks and financial institutions to follow the era and remain competitive and maintain customers' satisfaction in the highest level. Related report showed that customers tend to be more loyal to a bank and recommend it based on the banking services provided [10]. Thus, they have started to offer mobile

access and provide several services for customers through online services and mobile banking applications [11].

Mobile banking (m-banking) has been defined as a robust system for banking and financial services [12]. Thus, utilizing these services is crucially important for both investors and service providers, and a powerful tool for financial inclusion. Moreover, mobile banking is playing a significant role for Mobile-Commerce [13]. In addition, According to Community Banking Connections report, there is a tend to acquire mobile banking as it provides them with enhanced and competitive opportunities by reaching geographically remote markets, overcoming infrastructure limitations and improving efficiency, and helping in marinating market [14].

However, with this remarkable evolution and the increasing use of mobile devices, the vulnerabilities and the risk of malware attacks on mobile banking applications have exponentially increased. In [13] a Security Testing for Android Mobile Banking Apps (STAMPA) was performed to show and signify the possible threats and vulnerabilities at "mobile application code level, network level, and device level" through a detailed discussion and a detailed automated security testing for m-banking apps. Hence, this could help for applications development in terms of security and privacy.

2.2. Mobile banking attacks

Statistics predict a growth in mobile application users by 53% in 2021 [15], thus, attacks targeting users and financial applications are predicted to increase, common types of attacks could be summarized as [16]:

- Phishing: occurred when an attacker pretends to be a legitimate financial institution that asks the user to submit private bank information, the hacker could send emails, SMS, or even make phone calls telling people their account is locked and asking them to provide their account username and password.

  Due to rise of phishing and related attacks, sensitive applications such as online banking increasingly prefer more secure authentication alternatives. Their solutions usually fall into a group called two-factor authentication. By having a secondary factor, user authentication not only depends on something-you- know but also on something-you-have. As a result, setting up a fake site for collecting user passwords is no longer sufficient to conduct a successful attack [17].

- Man-In-The-Middle Attacks: achieved by eavesdropping on the communication between the mobile application and bank while verify the transactions, usually when users used unsecure data connection, i.e. free Wi-Fi network, attacker would attempt to send a fake bank server certificate to the mobile application, and if accepted, user's personal information would be compromised. Unfortunately, two-factor authentication by itself does not provide protection against MITM attacks as it occurs in real time [17].
- Key Logger Software: basically, record user's actions and send account names, numbers and passwords to the hacker. In [18] there is a detailed description and survey about keyloggers on smartphones and how motion-based tap inference attacks work. Thus, how keylogger, is functioning when no physical keyboard exists on those smart devices. Moreover, the paper lists various countermeasures approaches to mitigate risks.

2.3. Biometrics in banking industry

Banks tend to adopt biometric authentication seeking both enhanced security and better customers experience. A Chinese study's results showed that the security concerns were the most important factor that motivated user's adoption of online and mobile banking [19].

Moreover, adoption of biometrics authentication in mobile banking looks more promising as users' familiarity with biometrics authentications increased given that they became a part of smart mobile devices, from Touch ID to voice and face recognitions, as per a report by EyeVerify [20], which conducted in March 2017 and surveyed sample of 1,002 U.S. adults users who have used biometric authentication for mobile financial services in one year span. Which indicated that the implementation of biometrics reflects positively on brands and gains users' trust whom believed biometrics to be the most secure followed by two-factor authentication and one-time password tokens or codes, where 82% believe that banks offering biometric authentication are addressing mobile security, 78% believes that mobile applications with biometrics are more secure, and 82% believe biometrics are more secure than passwords for mobile banking and payment transactions. Moreover, 80% believe applications that have access to their bank accounts should also use biometric authentication to keep accounts secure. Additionally, EyeVerify stated that people acceptance for new of biometrics including eye, face and voice recognition is growing as they get comfortable

and familiar with the concept of using physical characteristics to authenticate their identities. Thus, banks can offer more biometric options for mobile logins, for both convenience and security [20].

A report by AWARE, a provider of biometrics software products, services, and solutions, that implement fingerprint, face, and iris recognition and authentication solutions, about "How Biometrics Expand the Reach of Mobile Banking" indicated the potential of both security and convenience of mobile banking to be improved by biometrics. Thus, in compression to using passwords, or combination of password and a secondary authentication such as PIN and one-time password OTP, biometrics authentication enhances security for the application and ensures user's authenticity; as these credentials are based on what people know, which could be compromised by hackers through phishing, man-in-the- middle attacks, keyloggers, or other breaches [21].Furthermore, it presented how most mobile banking applications lacking in security aspect due to the use passwords to authenticate users, given that passwords requirements tend to be complex as an attempt to make more secure, which in result make them inconvenient, and add cognitive pressure into users, whom ultimately reuse these passwords or write them in insecure mediums. Verizon's "2018 Data Breach Investigations Report" found that use of stolen credentials and passwords is the top variety of hacking in web applications breaches. Along with, malware botnets that target users' personal devices to collect login details of banking applications [22].

A joint research between MasterCard and University of Oxford "Mobile Biometrics in Financial Services: A Five Factor Framework." explored and addressed the factors affect the adoption of biometric authentication based on two separate studies, first study of users' attitudes towards the adoption of biometric authentication for online payment use cases; and second is an opinion survey of a targeted group of financial services professionals. The users' study confirmed consumers preference for biometrics as a secure, convenience and user-friendly authentication. However, the industry survey highlights gaps in experience and importance on different aspects of deploying biometric system, which ultimately prevent fully utilization of the adopted biometrics. Then, they identify five key factors and set a framework based on them that contribute to the success of a biometric system in financial services. They proposed holistic framework to achieve mobile biometrics' full potential consists of: Modality Performance, Usability, Interoperability, Security, Privacy [23].

2.4. Fingerprint authentication for mobile banking

Fingerprint-based authentication is the new solution and the promising candidate to replace password-based authentication due to the rapid progress in electronic transactions. Fingerprint-based authentication is the most reliable, accurate, famous and user-friendly technique among all the biometrics. [24] Have proposed a security scheme to secure mobile devices, which includes fingerprint biometric for authentication. The security's analyzation results have demonstrated that the suggested scheme provides secure, strong, and reliable remote authentication for mobile users over insecure cyberspace.

For higher-level of security, [25] stated that the providers of e-banking services should consider merging this biometric method to increase the security and privacy level of E-banking services and to protect against security attacks. While, [11] described a systematic multi-factor biometric fingerprint authentication approach used to improve the security of online-banking in public cloud, where this proposed approach provides high-secure identity validation process for verifying the legitimacy of remote users.

Other research paper has introduced a hardware prototype named OffPAD (Offline Personal Authentication Device). It was developed to add up a higher level of security, strengthen authentication assurance, and to improve usability in E-banking. According to [26] OffPAD is a trusted device that supports different forms of authentication that are necessary for trusted interactions (i.e. user authentication, server authentication). Furthermore, it provides fingerprint authentication for accessing sensitive information via fingerprint pad [27].

[28] Developed a Java based Mobile application that has login and payment options using fingerprint authentication to simulate Mobile Banking. They performed sample test for application and reported as highly secure, successful and user-friendly.

[29] Suggested taking human-centered approach to maintain the security challenges resulted from using biometric authentication systems, and pointed the risks come with the promised convenience of using these systems. Thus, sensitive data are subjected to be stolen or leaked, money transfer for instance could be performed digitally, which as convenience as it could be it exposes these data to adversary worldwide. Moreover, they pointed that even with following guidelines and best practices regarding managing passwords by choosing strong once, change passwords more frequently, never share them or write them down, that would not get the

expected outcomes, as all these guidelines increase the cognitive loads and thus the user would eventually violate the guidelines nonetheless. Among the figures in their papers, users reused 50% of passwords up to 4 times. Thus, the end user is the weakest of any system as users will weaken the security in their efforts to use the system. Finally, their study proposes that designers need to consider the human factors that impact end-user behavior.

2.5. Mobile banking in retail banking of Bahrain

According to Central Bank of Bahrain CBB [30], Bahrain's banking system consists of both conventional and Islamic banks and it is the largest component of the financial system, with over than 85% of total financial assets. Whereas, the conventional segment includes 23 retail banks, 69 wholesale banks, 2 specialized banks as well as 36 representative offices of overseas banks, the Islamic segment, offering a host of Sharia compliant products and services include 6 retail banks and 18 wholesale banks [30].

The authors of [31] started with the difference between e-banking and m-banking and used an extended Technology Acceptance Model TAM to study the customers' perception of m-banking and the factors that influence the adoption in Bahrain. They had total of 15 hypothesis, which were tested using linear regression analyses. Their finding emphasis on certain factors that must be considered by banks in Bahrain to improve customers' experience, mainly: continues improvements on ease of use and usefulness along with providing access to more critical information and services as some banks were merely providing functionality of checking balance, besides, risks and security issues of using mobile applications should be taken more seriously and they should work toward gaining more customers' trust considering developing the technical infrastructure of mobile banking services to ensure reliable and timely offering of services to customers.

Most of the Banks, as shown in Figure 1 as representative sample, on Bahrain use variation of username and password authentication schemes, Touch ID is only used by three banks as latest checked on June 2018, all are overseas banks, HSBC is in process of adopting it in Bahrain as well. Whereas the remaining have the two-factor authentication security scheme, One-Time Password OTP.

Figure 1: Authentications of Banks of Bahrain Mobile Application.

2.6. Financial initiatives and mobile payment applications in Bahrain

- BenefitPay: National Electronic Wallet Payment System in Bahrain, convenience, safe and secure way to Pay and transfer money without the use of cash or cards. The App works after adding and saving means of payment data securely, which could be debit card or bank account, and then transaction made via using QR Code Scanning Technology. By December 2018 credit cards would be linked as well, and would ultimately supports payments: using Credit cards, P2P transfers through Fawri+, Bill payments through Fawateer. As of techniques of security

used by BenefitPay, the user will set a PIN and Fingerprint to use either one of them for accessing the Mobile App [32].

- bWallet: is a FinTech services as a digital mobile wallet application provided by Batelco and Arab Financial Services, launched in January 2018 promising convenience payment solution. It supports load money from debit card, maximum of 200 at time, make Peer-to-Peer money transfer to mobile user, make cashless payments quickly to merchants, request money from other bWallet users. If money sent to a mobile user who don't have bWallet account, an SMS would be send as a notification and user would be requested to create a bWallet account, however, money would be in hold for 5 days in case the receiver didn't register, and the amount will be returned to the sender, as for payment for merchant, it could be through QR code or entering mobile number and amount. Authentication of the App is using mobile number as a User ID, and 4 digits number as password [33].

- SADAD, which means payment in Arabic, is a payment gateway channel in Bahrain started in 2010, its payment platform has been integrated directly with the top telecoms companies, Ministry of Electricity and Water, Touch & Remit service through ICICI Bank sending money to India, Charity, Tourism, Media and Gaming voucher of iTunes, Google Play, eBay, Amazon, XBOX & PlayStation and others. Their business based on more than 750 kiosks in Bahrain along with online payment gateway in their website, and mobile app. As authentication it requests 4-digit code to login to the mobile app, it doesn't save cards and payments details, however, it has the feature of loading money to the account [34].

2.7. User's attitude and acceptance

The possibility of using biometric authentication for e- banking to enhance the e-banking adoption and utilization in UK using TAM model was analyzed in [35], in their study, they considered two more parameters to the biometric security. The conclusion has shown that customer's understanding of biometrics security can positively affect their attitude and acceptance to use the biometric authentication system. Moreover, self-efficacy has positively influenced the users' perception toward the biometrics security. In addition, [36] extended the conventional technology acceptance model

(TAM) to examine whether user perceptions of biometric security influence their attitude and intention to use the biometric in their mobile banking or not.

Users acceptance of secure biometrics authentication system based on an extended unified theory of acceptance and use of technology (UTAUT) Model was studied in [37], with the aim to explore factors affecting user's acceptance of biometric authentication systems, specifically the use of fingerprint authentication systems in e-commerce websites with consideration to the sociocultural of the Saudi community. The conceptual framework they used was based on (UTAUT) model with three moderating variables: age, gender and education level and other intrinsic factors such as self-efficiency and biometric system characteristics.

The causes of the limited acceptance of mobile payments in developed countries were studied in [38], the study was based on conducting quantitative study based on applying (UTAUT) model to explore the factors affecting nonusers' intentions to adopt remote mobile payment in the United Kingdom. Their findings revealed that performance expectancy, social influence, innovativeness, and perceived risk significantly influenced nonusers' intentions to adopt the system, whereas effort expectancy did not.

Another study about resistance of adopting mobile banking in a developing country based on Pakistan [39], used a modified Technology Acceptance Model with the integration of four perceived risk dimensions (financial, privacy, time and security). The results indicate a negative association of financial and privacy risks towards the attitude of mobile banking technology, and significant positive impact of perceived ease of use and perceive usefulness on people's attitude towards mobile banking.

2.8. Protection of biometric data

Due to the characteristics of biometric identifications, there are potential risks and exposures that threaten the users and subsequently the community to be subjected to identity theft or the reuse of biometric, [40] proposed best practices for the processing of biometric data, taking privacy and data protection into consideration. The best practices discussed were based on the 7th Framework Programme Turbine which is supported and funded by the EU Commission and have creation of multiple trusted revocable protected biometric identities, which are irreversible and unlikeable, as the main recommendation. On the other hand, [41] conducted a qualitative study on implementation of trusted identity management systems, aiming to design model for trusted

identities framework. Their main findings were that trusted identities depend on institutional collaboration, user empowerment, system quality, information quality and service quality. However, high privacy concern is associated with low levels of trust, hence society must strive for trusted identities ecosystems.

3. Methodology

3.1. Paper model and methodology

The objective of this paper is to evaluate user's acceptance of using biometric authentication system for Bahrain mobile banking services, specifically the fingerprint. The paper study depends on a modified model that derived from Technology Acceptance Model (TAM) proposed by Davis, (1989). (TAM) model was developed to study the user's acceptance toward new technologies, where it has been conducted to investigate Malaysian citizens toward using the M- Government [42], also it has been conducted by [43] to study the factors that could affect the use of mobile government applications in Saudi Arabia, similarly, it has been used by [8] to study Community Perception of the Security and Acceptance of Mobile Banking Services in Bahrain. The previous studies depended on the original model (TAM) that consist of Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Attitude Toward Using (ATU), Behavioural Intention to Use (BIU) and the Actual System Use (ASU), and they modify it to suit their studies.

3.2. The proposed model

This paper depends on a proposed model that extracted from [8] model and it has been modified to fit with the paper context, where this model consists of Intention to Use (IU), Perceived Usefulness (PU), Perceived Ease of Use (PEOF), Social influence (SI), Quality of the Internet connection and website (QI), Attitude toward using (ATU), Awareness of services (AS). Each factor defined based on the paper context where (IU) defined as the degree to which users are intending to use their fingerprint to access and do their mobile banking transactions, (PU) defined in terms of the degree to which users believe that using their fingerprint would enhance mobile banking usability, then (PEOU) defined in terms of the user's effort that they take to perform their transactions using the fingerprint that it assumed to be free from effort. (ATU) defined in terms of user's behavior toward using this technology whereas (SI) defined in terms to what

extend the users are affected by their society to use the fingerprint in mobile banking services. The (AS) defined in terms of user's knowledge, awareness and confident that this technology is secure, Furth more, (QI) defined based on the degree to which users are affected to use the fingerprint by the quality of internet and website. Figure 2 illustrates the adapted model that derived from previous studies with its hypotheses, where the relationships between the model factors chosen based on affirmation of numerous researchers as table 1 and Figure 2 show the positive relationship between the mentioned factors as shown below.

Table 1: The proposed hypotheses with references

Factors Relationship	References
SI → PU	[8]
AS → PU	[8]
QI → PEOF	[8]
PU → ATU	[42]
PEOF → ATU	[42]
ATU → IU	[42] , [43]
PEOF → PU	[42]

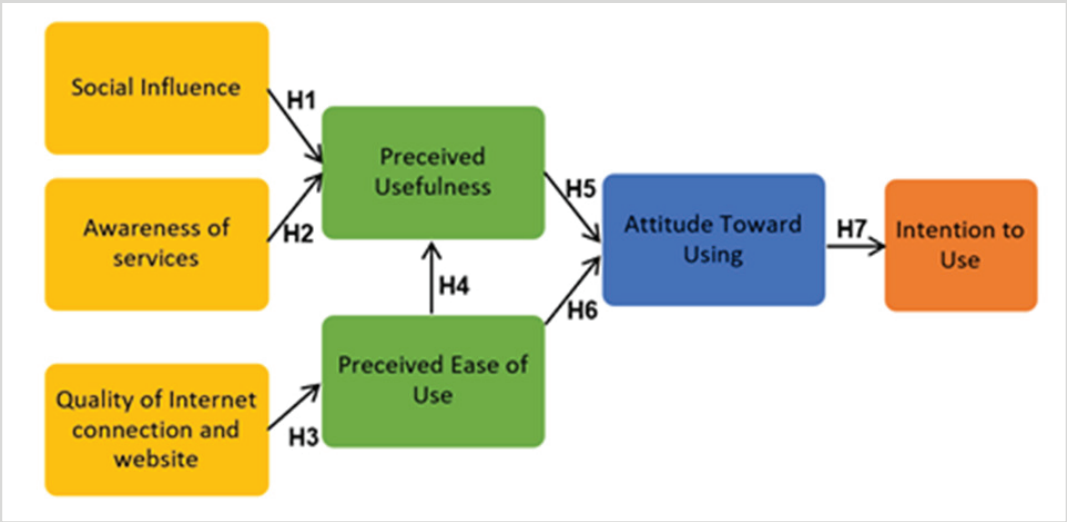

Figure 2: The proposed model and hypotheses.

4. Analysis

4.1. Result and discussion

This section represents the analyzed respondent's answers that have been collected with an online survey, this survey was distributed over a sample of Bahrain population that is 300 where 315 respondents have been obtained. To analyze the obtained answers a Statistical Package for Social Science (SPSS) was used, as table 2 shows the demographic characteristics of Bahrain mobile banking users followed where with Chi-Square to test the proposed hypotheses in table 3 and 5.

The tested model has proved its reliability with Cronbach's Alpha greater than 0.7 that is mean the measurement stays stable over the time and the validity of each factors components was tested in which they return values greater than 0.05 that is acceptable.

Table 2: Demographic Characteristics of Bahrain Mobile Banking Users.

Demographic	Factor	N	Percent (%)
Gender	Male	115	36.5
	Female	200	63.5
Age	17 or younger	8	2.5
	18-20	84	26.7
	21-29	102	32.4
	30-39	72	22.9
	40-49	38	12.1
	50-59	9	2.9
	60 or older	2	.6
Education	Secondary or less	77	24.4
	Diploma	80	25.4
	Bachelor	147	46.7
	Master	9	2.9
	PhD	2	0.6
Occupation	Employed (Government)	42	13.3
	Employed (Private)	73	23.2
	Self employed	24	7.6
	Not employed	26	8.3
	Retired	5	1.6
	Student	145	46.0

Table 3: Pearson Chi-Square Tests for Demographic Data.

Demographic Factor	Value	df	Asymptotic Significance (2-sided)
Gender	44.589[a]	37	0.183
Age	413.136[a]	222	0.000
Education	267.126[a]	148	0.000
Occupation	195.944[a]	185	0.277

4.2. Demographic characteristics analysis

From 315 respondents (63.5%) represent the female proportion where the smallest proportion is (36.5%) that represent the male respondents. The largest proportion (46.7%) of respondents by education group were those aged between 21 to 39 with (32.4%) and (22.9%). Based on the occupation, (46%) were students and (23.2%) were work in the private sector. table 3 represent the finding from Chi- square that test the demographic factors, by referring to the accepted criteria that is less than 0.05, the age and education have Sig. value that is close to 0.000, thus are related to the intention to use the biometric authentication system where the gender and occupation does not affect the intention toward using the biometric authentication system for mobile banking with value of 0.183 and 0.277.

Based on the Asymptotic Significance in table 4, all the hypotheses were closed to 0.000 that are less than 0.005 in which it verifies the results of the hypotheses, and by referring to table 5 (Pearson Symmetric Measures) that represent the tested hypotheses using Chi-square, all *Hypothesis Accepted/Rejected* proposed hypotheses have Approximate Significance close to 0.000, therefore it positively verifies that all hypotheses are related.

To determine the correlations between the internal variables Perceived Usefulness PU, Perceived Ease of Use PEOU, Attitude toward Using, and Intention to Use IU, Pearson correlation were used. As table 6 represent that there is no issue regarding the collinearity which confirm also that there is no linear regression problem in this study since all the findings in the table less than 0.8 where the highest value is 0.691.

Table 7 summarizes that Bahraini users are mostly welling and accepting to use the biometric authentication system for mobile banking services.

Table 4: Chi-Square Tests.

Hypothesis	Value	df	Asymp. Sig. (2-sided)
H1: SI → PU	3051.247[a]	1768	0.000
H2: AS → PU	2001.426[a]	1360	0.000
H3: QI → PEU	2579.408[a]	1376	0.000
H4: PEU → PU	2679.571[a]	1088	0.000
H5: PU → ATU	2529.458[a]	1224	0.000
H6: PEU → ATU	2574.635[a]	1152	0.000
H7: ATU → IU	2638.284[a]	1332	0.000

Table 5: Pearson Symmetric Measures.

Table 6: Correlation Analysis of Internal Variables.

Hypo.	Value	Asymp. Std. Error[a]	Approx T[b]	Approx Sign.
H1	0.669	0.041	15.908	.000
H2	0.280	0.064	5.151	.000
H3	0.509	0.057	10.470	.000
H4	0.625	0.049	14.154	.000
H5	0.618	0.048	13.924	.000
H6	0.627	0.045	14.244	.000
H7	0.623	0.045	14.107	.000
	PU	PEOU	IU	ATU
PU	1			
PEOU	0.625**	1		
IU	0.691**	0.620**	1	
ATU	0.618**	0.627**	0.623**	1

5. Conclusion and Recommendations

In conclusion, this paper aimed to study the user's acceptance of using biometric authentication system for Bahrain mobile banking. In addition, it was concerned to examine this topic because no such system exists yet, and since these technologies are still developing and evolving in Bahrain. The literature review section reviewed various related papers that emphasize the importance of mobile banking adoption. In addition, it summarized results of previous studies that utilized biometrics authentication methods for online banking (particularly fingerprint authentication). Moreover, it reviewed some papers that studied the user's attitude and acceptance towards the proposed topic. The paper used a quantitative method using online questionnaire

Table 7: Hypotheses Summary.

Hypothesis	Accepted/Rejected
A: Gender	Rejected
B: Age	Accepted
C: Education	Accepted
D: Occupation	Rejected
H1: SI → PU	Accepted
H2: AS → PU	Accepted
H3: QI → PEU	Accepted
H4: PEU → PU	Accepted
H5: PU → ATU	Accepted
H6: PEU → ATU	Accepted
H7: ATU → IU	Accepted

based on Technology Acceptance Model (TAM) to evaluate user's acceptance of using biometric authentication system (fingerprint) for Bahrain mobile banking services. Eventually, this paper can recommend in enhancing the security of mobile banking services and spread awareness among the citizens of Bahrain regarding the adoption of biometric authentication for mobile banking as they accept this technology to be used.

Acknowledgment

This work has been fully supported by Dr. Wael Elmedany Associate Professor at the University of Bahrain.

References

[1] M. Monahan, "What Are The Three Big Trends In Mobile Banking In 2014?," February 2014. [Online]. Available: https://www.javelinstrategy.Com/Blog/2014/02/18/.

[2] NBB, "Mobile Banking," 2018. [Online]. Available: https://www.nbbonline.com/en/personal/everydaybanking/services/mobile-banking.

[3] Standard Chartered Bank, "Mobile Banking App," 2017. [Online]. Available: https://www.sc.com/bh/ways-to-bank/sc-mobile-app.

[4] S. Abdullatif and V. Manual, "The Effect Of Mobile Banking, Security Systems And Information Systems Among Customers' Preference Of Banks In Bahrain,"

International Journal of Advanced Research and Publications, vol. 1, no. 4, pp. 58-64, October 2017.

[5] D. Hodgkinson, "Mobile Banking 2015: Global Trends and their Impact on Banks," July 2015. [Online]. Available: https://home.kpmg.com/content/dam/kpmg/pdf/2015/08/mobilebanking-report-2015.pdf.

[6] W. Stallings and L. Brown, Computer Security: Principles and Practice, 3rd ed., Upper Saddle River, NJ, USA: Prentice Hall Press, 2014.

[7] CommsMEA, "Percentage of individuals using internet in Bahrain grows to 98%," 15 October 2017. [Online]. Available: https://www.commsmea.com/17655-percentage-of-individualsusing-internet-in-bahrain-grows-to-98.

[8] A. Mashhour and Z. Saleh, "Community Perception of the Security and Acceptance of Mobile Banking Services in Bahrain: An Empirical Study," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 6, no. 9, pp. 46-54, 2015.

[9] J. M. CristóvãoVeríssimo, "Enablers and restrictors of mobile banking app use: A fuzzy set qualitative comparative analysis (fsQCA)," Journal of Business Research, vol. 69, no. 11, pp. 5456- 5460, 2016.

[10] Bain & Company, "Customer Loyalty in Retail Banking," Bain & Company, 2012.

[11] S. Nagaraju and L. Parthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," Journal of Cloud Computing, vol. 4, no. 1, pp. 1-46, 1 December 2015.

[12] M. Bhardwaj and R. Aggarwal, "Understanding Dynamics of Mobile Banking Adoption by Youth: Empirical Evidence from India," FIIB Business Review, 2016.

[13] S. Bojjagani and V. N. Sastry, "STAMBA: Security Testing for Android Mobile Banking Apps," in Advances in Signal Processing and Intelligent Recognition Systems, Trivandrum, India, 2015.

[14] J. F. Combs, "Mobile Banking Risk Identification and Mitigation," 2014. [Online]. Available: https://communitybankingconnections.org/articles/2014/Q1/mobilebanking-risk-identification-and-mitigation.

[15] N. Bhas, "Retail Banking: Digital Transformation & Disruptor Opportunities 2017-2021," Juniper Research, Hampshire, 2017.

[16] M. Burnette, "Hackers Target Your Mobile Bank App; You Can Fight Back," 7 August 2017. [Online]. Available: https://www.nerdwallet.com/blog/banking/banking-apps-security/.

[17] K. Bicakci, D. Unal, N. Ascioglu and O. Adalier, "Mobile Authentication Secure Against Man-In-The-Middle Attacks," Procedia Computer Science, vol. 34, pp. 323-329, 2014.

[18] M. Hussain, A. Al-Haiqi, A. Zaidan, B. Zaidan, M. M. Kiah, N. B. Anuar and MohamedAbdulnabi, "The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks," Pervasive and Mobile Computing, vol. 25, pp. 1-25, 2016.

[19] S. Laforet and X. Li, "Consumers' attitudes towards online and mobile banking in China," NTERNATIONAL JOURNAL OF BANK MARKETING, 2005.

[20] EyeVerify, "The Retail Banking Biometrics Confidence Report," EyeVerify, Kansas City, 2017.

[21] AWARE, "How Biometrics Expand the Reach of Mobile Banking," September 2017. [Online]. Available: https://www.aware.com/wpcontent/uploads/2017/09/aware-biometrics-mobile-banking-ebook-2.pdf. [Accessed 20 May 2018].

[22] Verizon, "2018 Data Breach Investigations Report," Verizon, New York, 2018.

[23] G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman and I. Martinovic, "Mobile Biometrics in Financial Services: A Five Factor Framework," University of Oxford, Oxford, UK, 2017.

[24] M. K. Khan, J. Zhang and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," pp. 519-524, 2008.

[25] A. Fatima, "E-Banking Security Issues – Is There A Solution in Biometrics?," Journal of Internet Banking and Commerce, vol. 16, September 2011.

[26] A. Jøsang, C. Rosenberger, L. Miralabé, H. Klevjer, K. A. Varmedal, J. Daveau, K. E. Husa and P. Taugbøl, "Local user-centric identity management," Journal of Trust Management, p. 1, 2015.

[27] D. Migdal, C. Johansen and A. Jøsang, "DEMO: OffPAD - Offline Personal Authenticating Device with Applications in Hospitals and e-Banking," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, New York, 2016.

[28] L. Sharma and M. Mathuria, "Mobile banking transaction using fingerprint authentication," in 2018 2nd International Conference on Inventive Systems and Control (ICISC) , Coimbatore, India , 2018.

[29] J. Still, A. Cain and D. Schuster, "Human-centered authentication guidelines," Information and Computer Security, vol. 25, no. 4, pp. 437-453, 2017.

[30] CBB, "Banking," Central Bank of Bahrain, [Online]. Available: http://www.cbb.gov.bh/page-p-banking.htm. [Accessed 3 June 2018].

[31] A. AlSoufi and H. Ali, "Customers' perception of m-banking adoption in kingdom of Bahrain: an empirical assessment of an extended TAM model," International Journal of Managing Information Technology (IJMIT), vol. 6, no. 1, pp. 1-13, 2014.

[32] BENEFIT, "BENEFITPAY," Bahrain's Electronic Network For Financial Transactions, [Online]. Available: https://www.benefit.bh/Services/BenefitPay/. [Accessed 4 June 2018].

[33] Batelco, "Batelco and Arab Financial Services Partner to launch bWallet: A new FinTech Service," 10 January 2018. [Online]. Available: http://batelco.com/news-media/batelco-and-arabfinancial-services-partner-to-launch-bwallet-a-new-fintech-service/.

[34] SADAD, "Pay Anywhere, Anytime," Sadad Bahrain, [Online]. Available: https://sadadbahrain.com/about-us.html. [Accessed 4 June 2018].

[35] R. Tassabehji and M. A. Kamala, "Improving E-Banking Security with Biometrics: Modelling User Attitudes and Acceptance," in 2009 3rd International Conference on New Technologies, Mobility and Security, Cairo, 2009.

[36] D. Ahmad and M. Hariri, "User Acceptance of Biometrics in Ebanking to improve Security," Business Management Dynamics, pp. 1-4, 2012.

[37] F. AL-Harby, R. Qahwaji and M. Kamala, "Users' Acceptance of Secure Biometrics Authentication System: Reliability and Validate of an Extended UTAUT Model," in Networked Digital Technologies, Berlin, Heidelberg, 2010.

[38] E. L. Slade, Y. K. Dwivedi, N. C. Piercy and M. D. Williams, "Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and Trust," Psychology & Marketing, pp. 860–873, 8 January 2015.

[39] I. Arif, S. Afshan and A. Sharif, "Resistance to Adopt Mobile Banking in a Developing Country: Evidence from Modified TAM Model," Journal of Finance and Economics Research, vol. 1, no. 1, pp. 23-38, January 2016.

[40] E. Kindt, Security and Privacy in Biometrics, London: Springer London, 2013, pp. 339-367.

[41] J. K. Adjei, "Towards a trusted national identities framework," pp. 48-60, 2013.

[42] A. Althunibat, N. A. M. zain and N. Sahar, "Modelling the factors that influence mobile government services acceptance," African Journal of Business Management, vol. 5, no. 34, pp. 13030-13043, 28 December 2011.

[43] R. Alotaibi, L. Houghton and K. Sandhu, "Factors Influencing Users" Intentions to Use Mobile Government Applications in Saudi Arabia: TAM Applicability," International Journal of Advanced Computer Science and Applications, vol. 8, no. 7, pp. 200-211, 2017