End-users' Perception of Cybercrimes towards E-banking Adoption and Retention

Taha Abbas  
Senior Officer Corporate Affairs,  
Amreli Steels Limited (ASTL)  
Karachi, Pakistan  
taha.abbas@amrelisteels.com

Kashif Arif  
1Faculty of Business and Economics  
University of Malaya, Kuala Lumpur, Malaysia  
2Department of Accounting and Finance  
Salim Habib University, Karachi, Pakistan  
kashif.arif@shu.edu.pk

Abstract—The advancement of information and communication technology (ICT) has resulted in dynamic changes in the operations of various business sectors all over the world, while causing inconvenience to users and making stakeholders' lives easier. However, the advancement in the same has brought major concerns for businesses, such as cybercrime. This study focuses on identifying the impact of cybercrime on the adoption of e-banking services in Pakistan. The study aims to understand the impact of hacking, identity theft and phishing on the adoption of E-banking in Pakistan. The data was collected from 384 banking customers through structured questions containing the demographic questions as well as questions related to the constructs used in the study. The findings of the study suggest that hacking, phishing and identity theft negatively affect the adoption of E-banking in Pakistan. The results of the study are discussed in line with the existing literature. The study limitations and future research areas are also discussed.

Index Terms—Cybercrime, Information and communication technologies, Phishing, Spam, Identity Theft, Hacking

I. INTRODUCTION

Since the early 1990s, the banking sector has been globally dependent on the conventional banking system and processes to deliver banking amenities to its customers. There is a gigantic revolution and technological advancement in the banking sector that has made banking heavily dependent on technology [1]. Considering the vicious circle of advanced technology and e-commerce facilities, banks have adopted various digital platforms which are desirable for customers as well as for banks, and through this, banks can provide ease to customers.

The rapid advancement of the internet and digital technology has had a massive impact on almost every aspect of human activity, from consumers and business centers to the financial and investment industries. Modern technology has simplified business processes, from the mobilization of deposits to payment processes; these technologies have enabled customers to get a unique experience with greater ease and convenience. However, it should be noted that the negative aspect of this technological advancement has brought unintended concerns such as phishing, identity theft, hacking, and other cybercrimes. [2] point out that the more organizations adapt to this paradigm shift and move their daily operational tasks to online platforms, the more they are exposed to privacy (technological theft) and other crimes in cyberspace. Cybercrime can cause significant losses in the banking industry because it prevents customers from using e-banking services.

The banking sector worldwide must be free of cybercrime threats because banks run the economy and ensure economic growth, which can only be guaranteed by people saving money in banks. Therefore, the banking sector needs to guarantee that customers are free from any kind of cyber threats and that they have safe and secure transactions. These protocols ensure people's trust in banks to save their money. However, today's cybercrimes have been significantly augmented by the ongoing phase of digitalization and are the greatest threat to the security of banking transactions and customer bank accounts.

Moreover, due to the more substantial dependence on information and communication technology, the banking sector is more prone to the risk of cybercrime [3]. Malinka, Huňák, Hanáček and Hellebrandt [4] recognized the fact that the number of banks that are the prime targets of cyber attackers has gone up due to the fast pace of digitalization and internet banking. The primary concerns associated with relying on communication technology include electronic mail spam, which results in phishing, identity theft on credit and debit cards, and hacking. The banking sector of Pakistan is yet to be developed to give proper information security to customers.

Hence, the recent case of ATM skimming which occurred at HBL, one of the top tier banks in Pakistan,
involved the loss of 10.2 million to the customers and the bank. This incident brought significant information security challenges and concerns which have resulted in consumers losing trust towards e-banking services. Najaf, Mostafiz and Najaf [5] recognized that cybercrimes not only cause financial loss but also bring down customers' trust, and confidence and threaten banks' reputation. This research is intended to highlight the negative impact of cybercrime, which is deteriorating customer trust and the adoption of e-banking services all over Pakistan.

The objective of the study is to identify the impact of phishing on the adoption of e-banking services. In addition, it investigates the effect of hacking on the adoption of e-banking services in Pakistan. Lastly, the study intends to identify the impact of identity theft on the adoption of e-banking services. Phishing, hacking, and identity theft are three of the most common and devastating cybercrime activities, which are subjugating the intention of banking customers to adopt e-banking services in Pakistan.

II. THEORETICAL FRAMEWORK

A. Routine Activity Theory

Cohen and Felson developed the Routine Activity Theory in 1979, which tends to state that crime is a normal behavior of an individual, and it just needs an opportunity to make him commit [6]. The Routine Activity Theory discusses three elements, which need to be present for a crime to take place; they include the motivation and intention of a criminal and the ability to act on this inclination; a suitable target to pursue crime, and the absence of surveillance or guardian, which can prevent the crime from happening in the first place. All three of these elements need to converge in the space and time available for the offense to occur. The study by Mugari, Gona, Maunga and Chiyambiro [7] applied the Routine Activity theory to the most common type of cybercrime in banks, which is phishing.

It was further highlighted in the study of Loughran, Paternoster, Chalfin and Wilson [8] that the increasing number of people using the internet is associated with the presence of a suitable offender ready to grab the opportunity. This, in turn, sheds light on the increasing number of individuals knowing about phishing through technological knowledge. It was further argued that the more people were using the internet banking system and other internet devices, the more likely they would become suitable victims of cybercrime [9]. According to the report from the Pakistan Telecommunication Authority, 78 million of the population are active users of broadband services (36.86% of the total population) as of December 2019 [10], which is a 19.06% increase in the users compared to that of the year 2016 when the users were at 17.8% of the total population. This increase in internet acceptance has increased the overall risk for offenders in cybercrime and suitable victims of these crimes.

Further to this theory, it was also highlighted that the absence of capable guardianship has always been associated with a lack of awareness. In terms of banking services, the capable guardians may include Computer Emergency Response Teams (CERTs), law enforcement authorities, account holders, banks, or any other individual or agency [7], that have the possible power to discourage the offenders like State Bank of Pakistan. The absence of these guardians increases the potential risk of cyber-attacks on e-banking services.

III. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

Although cybercrime has comprehensive identification around the globe, it has no universally accepted definition [11]. The characterization of cybercrime is dependent on its association, means, and consequences. According to the research done by the national cyber security center in 2013, cybercrime is defined as any criminal activity that targets ICT or any information that has been processed through the internet or any other computer device. Finally, cybercrime encompasses all actions involving the hacking of personal data via internet devices, which are both the primary tools and the targets of cybercriminals.

A. Cybercrimes in the Banking Sector

Due to the ongoing effect of digitization, cybercrime in the financial sector, especially in the banking sector, has grown intensely. As Kanda, del Río, Hjelm and Bienkowska [12] demonstrate, not every evolution or development is free from mess and many of them are accompanied by some niche that is demoralized by offenders for disruptive objectives. Today, the financial sector around the globe is reliant on technology to provide ease of services to customers and to run daily banking operations. However, due to its dependence on digital technology, the banking sector is exposed to various threats [13]. In recent times, there have been several different instances of electronic fraud and cybercrime in which there was a monetary and physiological loss to the clientele, and the banking sector was the chief target of hackers. Because the banking sector is important to the economy and processes billions of transactions, hackers are motivated to make money. These crimes in the financial industry have different features, and the arrays of online attacks can be segregated into different regions based on the activities or operations.

Cybercrime in the global scenario tends to project upon various areas of cybercriminal activities in e-banking services. Some of the most popular, in terms of
financial loss globally, cybercrimes are phishing, identity theft, and hacking.

B. Phishing

Phishing is a term that is derived from the word "fishing" in which the cybercriminal sends out spoof emails or calls to a random database of people while deceiving them into providing valuable information that can be used against them [14]. In e-banking cybercrimes, phishing is used to acquire confidential information from customers, which can be used to drain the individual's bank balance financially. One of the key tools of phishing is 'carding'. The term "carding" has been assigned to frauds related to credit cards and can be described as the uncertified use of victims' credit cards and accessing the information present on the card through various techniques which are illegally used by cyber-criminals. Phishing is one of the most common cyber-attack used by hackers to attain valuable information of banking customers as customers are not aware of repercussion of providing valuable information to fake emails and calls and they are unable to distinguish between original and fake calls/emails from banks. Due to the increase in credit card thefts and fraud, the research regarding this has also taken a hit. Downing, Downing Jr, Capriola and Geller [15] studied the techniques that were implicated by these cyber-criminals and emphasized the use of techniques such as data mining to put a hold on such crimes to protect the private data of the account holders, as this technique has proven to be effective for detecting hacking events. Another research has identified various types of techniques in order to overcome phishing, such as anticipation, uncovering, offensive security, etc., which could be used by organizations to mitigate the fraud being conducted[16].

H1: Increasing number of phishing attacks would have a negative impact on the adoption of e-banking services by customers

C. Identity Theft

Identity theft is also one of the rising types of cybercrimes that are prevailing in the world. According to the study by Hille, Walsh and Cleveland [17], identity theft tends to involve the acquisition of data from customers of a bank or any personal information that can be counterfeited by another person, enabling him to misuse it for his own purposes without the acknowledgment of the individual whose identity has been stolen. According to Li, Yazdanmehr, Wang and Rao [18], identity theft is a technique used by criminals to mainly target the least protected area of the banking system, which is the customer end. Many such systems and procedures have been furnished by these cybercriminals to target the customers, who are the end-users of the banking system and the ones who are protected the least. Some of the various techniques used by the cyber criminals for identity theft are highlighted in the table 1 below:

Furthermore, no one way has been developed by financial institutions to overcome these identity theft crimes, and banks still have to use different procedures to fight this risk [18]. In the banking industry, identity theft is a prevalent cybercrime that has resulted in the loss of millions of dollars from the consumer end and has dramatically affected the trust factor of customers in e-banking services.

H2: The threat of losing one's identity along with monetary value would have an adverse impact on the adoption of e-banking services by the existing and potential customers

D. Hacking

Hacking is a globally acknowledged cybercrime, which does not have a singular area of commencement in terms of industry. Hacking is done on the disruption of the social welfare of an individual, in the real estate industry, or in any other company to attain valuable information while getting control of the information system. According to Alsayed and Bilgrami [19], hacking is the attempt to exploit a computer system or cyberspace through digital coding to gain unauthorized access to it so that all personal and confidential information can be extracted, altered, and even deleted as per the nature of the criminal mind for which it is done in the first place. Hacking in e-banking has been a long-reached problem that has contributed to exploiting the valuable information from customers and used as
extortion and/or draining of funds from bank accounts. According to Lawal, Lawal and Akanbi [20], the Nigerian banking system is also threatened by skimming attacks through hacking and argues that this skimming fraud is international in nature and many countries are facing these cybercrimes, and these concerns both the bankers and its stakeholders. Further discussions are made on various aspects of cybercrimes and how to reduce these frauds from happening in the Nigerian banking industry. Both primary and secondary data have been incorporated to figure out these cyberattacks in Nigeria. The research implies that the banks and the customers of the bank play a vital role in order to stop the criminals of ATM fraud in the banking industry. The study also discusses that common practices used by criminals for hacking purposes and acts such as Shoulder surfing, ATM cards that are stolen, and Card jamming make up almost 65% of total ATM frauds that are being carried out in Nigeria. Hence, it was pivotal to assess the significance of hacking on the intention of banking customers in Pakistan towards adopting e-banking services.

**H3:** Hacking tends to have a significant impact on customers’ intention to adoption of e-banking services

### IV. IMPACT ON PERCEPTION OF END-USERS OF CYBERCRIMES TOWARDS E-BANKING ADOPTION AND RETENTION

In the technologically driven era of the global market, organizations are working effectively to transform their operations and other business activities towards innovation in terms of technology adaptation and ICT adjustments. The most significant transformation of the industry towards innovation and technology can rightly be identified in the banking sector. However, according to the study by Leukfeldt and Kleemans [13], with every progression in terms of technological adaption, there is always a mind behind the fact that these technologies can be misused negatively. In this regard, the banking sector has seen a more significant loophole in the notion of cybercrime, which is prevalent in the digitalized world of banking operations and customer services. Cybercrime in the banking sector is a growing concern in the global dialect of innovation in the banking sector. According to Malik and Islam [21], the main effect of cybercrime is the monetary loss of banks and their customers. However, the study by Behl, Pal and Tiwari [22] critically argued the fact that it is more than monetary and data loss for the banks. The author, given his research, clarified that cybercrime has a more significant impact on customers' adoption of e-banking services. There have been different cases in recent times with the most notable and market-dominant banks, Habib Bank Limited and Bank Islami, which have crucially been impacted by the cyber-attack. It has been highlighted in print and electronic media that Bank Islami had lost Rs. 2.6 million from cybercrime, whereas the international financial system projects the loss to have been $6 million, which is equal to Rs. 795 million. On the other hand, Rs. 10.2 million is the amount lost by an ATM fraud scam while affecting 559 customers [23]. In the light of the growing cases of cybercrime, customer trust and loyalty towards the banking sector have greatly been affected. The most notable impact it has produced is on their risk perception towards operating on e-forums of the bank. With increasing discomfort in the adoption of e-banking services, the future profitability of banks and their operations is a big question [24]. Hence, investigating the impact of cybercrime on the adoption of e-banking services is of vital notion to be examined in the increasing innovation and technologically driven era. Thus, from the research problems and its objectives, it is clear that the research is subjected to examine the impact of cybercrime on the adoption of e-banking. The significance of this research is pertaining to the gap which is lying in the local market that there is a deficiency of researches which is catering to the adoption of e-banking services by customers from the impact of cybercrime in banking sector. There are many researches which caters to adoption of e-banking services while identifying different factors, due to the implementation of technology. However, there is very less substantial research which has worked its way to determine the impact of cybercrime on e-banking, with the increasing number of cyberattacks in Pakistan and globally.

With the growing concern of cyber threat, it is vital to identify how the customers perceive their views towards e-banking services while keeping in mind the increasing cyber-attacks in the industry [25]. Moreover, it also essential to deduce techniques which can be effectively used by banks to prevent and mitigate the risk, which is about cybercrimes.

### V. CONCEPTUAL FRAMEWORK

The notion of the research being the impact of cybercrime on the adoption of e-Banking shows that cybercrime is the independent variable, whereas e-Banking adoption is the dependent variable of the study. The independent variable, i.e., cybercrime in the banking sector, tends to have different factors of operation through which consumers’ wealth is negatively affected by criminal activities. These factors include phishing, hacking, and identity theft, which ultimately affect the adoption of e-Banking services [16, 26].
The above model can be presented in the following statistical equation:

\[ \text{INTADOP} = \alpha + \beta_\text{hack} + \beta_\text{identity} + \beta_\text{phish} + e \]

Where:
- \( \text{INTADOP} \) = Intention to adopt E-Banking
- hack = Hacking
- identity = Identity Theft
- phish = Phishing
- \( \alpha \) = Constant
- \( \beta \) = Beta coefficient
- \( e \) = Error Term

As discussed in the literature, cybercrime is one of the growing concerns in the banking industry, which not only affects the monetary wealth of banks and their customers but is a blatant anomaly which is affecting the adoption criteria of e-Banking services towards investing and trusting digital banking services. Hence, it was important to analyze different factors prevalent in cybercrime and which are being used by criminals towards cyber theft. The conceptual framework, in this regard, allows the researcher to develop a model to understand the impact of an independent variable on the dependent variable.

VI. RESEARCH METHODOLOGY

The proposed study has used a quantitative research design in order to fulfill the objectives of the research according to the notion of the study, which signifies the fact that numerical data with empirical analysis is a key determinant for analyzing the consumer perception of cybercrime in the banking sector. The numerical data was in form of Likert scale data from the surveys, which was taken from the consumers to extract the relevant data towards their experience, perception, and feeling towards cybercrime in banks and adoption of e-banking services. In order to choose the right target audience while considering the limitation of time to carry out the research and the resilience of the right sample audience, the study used the non-probability sampling method. In relation to this convenience was used. A sample size of 384 respondents was catered in this study following [27] sample size determination. The model was tested through Structural Equation Modeling that Smart PLS 3 was used to perform data analysis.

A. Data Analysis Plan

Partial Least Square (PLS) was developed from the work of an econometrician named Herman World in the late 1970s [28]. It tends to include the alternating least square algorithms, which have been the extended canonical correlation and principal component. There are two sets of paths of linear equation models which are applied in PLS, i.e., the structural model and the measurement model [29]. The application of a structural model specifies the relationship between the manifest and the latent variables (i.e., the inner model), whereas the measurement model specifies the relationship between the unobserved or latent variables (i.e. the outer model). Similarly, in this dissertation, the same principals are applied in order to validate that the study meets the criteria of quality empirical research.
VII. RESULTS

A. Demographic Analysis

The descriptive table 1 highlights the demographics of the data showcasing gender, age, education, profession, and other personal information vital for the research. From table 1 it can be highlighted that out of 372 respondents 314 were males (84.4%), whereas 58 of the total respondents were females (15.6%). The appropriate division of male and female respondents highlights the fact that the study is free from any kind of gender biases and the study equally takes into account the responses of both male and female bank customers. Similarly, it shows that research consists of bank customers who are mainly from the age group of under 25 to 45 having 91.9% of the total age group in the study (372 respondents in total). This shows that most of the bank customers are coming from the age group of youngsters or young adults and this research mainly showed the results of these individuals. Other important data is also assembled from the table consisting of the Profession, Salary, Invested amount, and the pursued usage of electronic payment channels from respondents.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Label</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male</td>
<td>314</td>
<td>84.4%</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>58</td>
<td>15.6%</td>
</tr>
<tr>
<td>Age</td>
<td>&gt;25</td>
<td>144</td>
<td>38.7%</td>
</tr>
<tr>
<td></td>
<td>26-45</td>
<td>198</td>
<td>53.2%</td>
</tr>
<tr>
<td></td>
<td>45-65</td>
<td>22</td>
<td>5.9%</td>
</tr>
<tr>
<td></td>
<td>&lt;65</td>
<td>8</td>
<td>2.2%</td>
</tr>
<tr>
<td>Education</td>
<td>Intermediate</td>
<td>6</td>
<td>1.6%</td>
</tr>
<tr>
<td></td>
<td>Bachelor</td>
<td>250</td>
<td>67.2%</td>
</tr>
<tr>
<td></td>
<td>Post Graduate</td>
<td>116</td>
<td>31.2%</td>
</tr>
<tr>
<td>Profession</td>
<td>Student</td>
<td>31</td>
<td>8.3%</td>
</tr>
<tr>
<td></td>
<td>Salaried Person</td>
<td>209</td>
<td>56.2%</td>
</tr>
<tr>
<td></td>
<td>Businessman/woman</td>
<td>132</td>
<td>35.5%</td>
</tr>
<tr>
<td>Monthly Salary</td>
<td>&gt;25,000</td>
<td>45</td>
<td>12.1%</td>
</tr>
<tr>
<td></td>
<td>25,001-60,000</td>
<td>140</td>
<td>37.6%</td>
</tr>
<tr>
<td></td>
<td>60,001-100,000</td>
<td>101</td>
<td>27.2%</td>
</tr>
<tr>
<td></td>
<td>&lt;100,001</td>
<td>86</td>
<td>23.1%</td>
</tr>
<tr>
<td>Invested Amount</td>
<td>&gt;50,000</td>
<td>170</td>
<td>45.7%</td>
</tr>
<tr>
<td></td>
<td>50,000-100,000</td>
<td>62</td>
<td>16.7%</td>
</tr>
<tr>
<td></td>
<td>100,001-1,000,000</td>
<td>73</td>
<td>19.6%</td>
</tr>
<tr>
<td></td>
<td>&lt;1,000,000</td>
<td>67</td>
<td>18%</td>
</tr>
<tr>
<td>Usage of EPC</td>
<td>Daily</td>
<td>44</td>
<td>11.8%</td>
</tr>
<tr>
<td></td>
<td>Weekly</td>
<td>178</td>
<td>47.8%</td>
</tr>
<tr>
<td></td>
<td>Monthly</td>
<td>143</td>
<td>38.4%</td>
</tr>
<tr>
<td></td>
<td>Annually</td>
<td>7</td>
<td>1.9%</td>
</tr>
<tr>
<td>Pursued EPC</td>
<td>Credit/Debit Card</td>
<td>119</td>
<td>32%</td>
</tr>
<tr>
<td></td>
<td>ATM</td>
<td>113</td>
<td>30.4%</td>
</tr>
<tr>
<td></td>
<td>Internet Banking</td>
<td>74</td>
<td>19.9%</td>
</tr>
<tr>
<td></td>
<td>Mobile Application</td>
<td>66</td>
<td>17.7%</td>
</tr>
</tbody>
</table>

B. PLS-SEM (Measurement Model)

- Outer loadings

The measurement model describes the relationship between an unobserved or latent variable and another unobserved or latent variable (i.e., the outer model). The initial model of PLS reflects all the items with their outer loading, which is the estimated relationship between the latent variables and their indicators. From the model mentioned below, it can be assessed that all the items in the outer loading have a value of over 0.6 and so are acceptable for further studies and results.

- Convergent Validity

In Partial Least Square, the convergent validity is analyzed through the Average Variance Extracted (AVE) value. Purwanto [32], as portrayed in Table 2 below. Convergent validity is achieved if the AVE value is at least 0.5 or greater. In this case, all the constructs have an AVE value well over 0.5, extending from 0.7331 for the intention to adopt e-banking to 0.8708 for phishing. According to the study of [31], discriminant validity is used to differentiate the constructs of measure from one another for different items and measures the degree to which there is a difference in overlapping constructs. For this process, two test measures are taken into action, namely Fornell-Larcker’s criterion and Cross Loading. The tables below show the results of convergent and discriminant validity. All the values meet the minimum benchmark.

C. Hypothesis Testing

The table below shows the path coefficient of the relationships provided in the hypotheses of the study along with the p-values showing the significance of the
the relationship. The same can be seen in the PLS Structural Model provided below.

<table>
<thead>
<tr>
<th>Relationship</th>
<th>Direct Effect (β)</th>
<th>T Statistics</th>
<th>P Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking -&gt; Intention to Adopt E-Banking</td>
<td>-0.2321</td>
<td>4.0307</td>
<td>0.0001</td>
</tr>
<tr>
<td>Identity Theft -&gt; Intention to Adopt E-Banking</td>
<td>-0.2770</td>
<td>3.9299</td>
<td>0.0001</td>
</tr>
<tr>
<td>Phishing -&gt; Intention to Adopt E-Banking</td>
<td>-0.2613</td>
<td>3.6958</td>
<td>0.0002</td>
</tr>
</tbody>
</table>

The above table shows that all three hypotheses of the study are found to be supported as all coefficients are negative and significant. Hence, it can be concluded that hacking, identity theft, and phishing have a significant and negative impact on e-banking adoption. Moreover, the value of R Square was 0.42, which indicates that the overall variance explained by the model is 42%. The relationship is also depicted in the figure below.

**VIII. DISCUSSION**

The objective of developing countries is to gauge economic growth, which is only promised by the mobilization of money in terms of investments and savings. However, people in developing countries like Pakistan are more inclined to use other mediums of saving rather than banks because of a lack of trust and increased threat of cyber security. Moreover, people in rural areas have a lesser understanding of cyber security threats, risks, and lack financial literacy, which makes them reluctant to use banks for transactions.

The study aimed to find out the impact of cybercrimes on banking customers’ risk perception of electronic mediums of payments. With the help of a literature review the study came up with the main dominant factors of cybercrime in the banking industry Phishing, Hacking, and Identity theft are the most prevalent factors.

Through the research, it can duly be concluded that Cybercrime does significantly impact consumers
through the process when using electronic modes of payment. Customers still lack trust and question the banking sector when it comes to safety and security.

The result was extracted through the application of the Structural Model where the variables were analyzed providing the facts towards the acceptance of hypotheses. The Coefficient of Determination was extracted through Smart PLS Tool showcasing the R Square value of 0.4212. This provided the insight that the holistic findings towards the impact of cybercrime on intention to adopt e-banking services were approved and showcases the finding that each latent variable has a significant impact on the dependent variable of the study. This is also justified by the study of Safeena, Kammani and Date [33], which stated that Cybercrimes tend to impact customer trust and loyalty towards the banking sector and has a significant impact on their risk perception towards operating on e-forums of the bank.

Furthermore, Path Coefficient was extracted which analyzed individual variables and justified the hypotheses of the study. According to the results, identity theft is a major threat to the customers as the path coefficient for the variable was 0.277 towards the intention to adopt e-banking services in the bank which is the reason why customers use conventional payment channels rather than electronic. This was also emphasized in the literature review in the study of Li, Yazdanmehr, Wang and Rao [18] that phishing crime through identity theft is the most vulnerable form of cyberattack, which still is not being able to completely eradicated through any means possible and is a potential threat to customers. All the results support the hypothesis and suggest true reasons for the low adoption rate in Pakistan. Customers believe that there is a threat to their personal security when they put all their personal account details.

Also, the study analyzed the impact of hacking as the main factor that generates and evokes negative feelings about safety and security. This was proven through the path coefficient, displaying a value of 0.232 towards the intention to adopt e-banking services in the bank. Moreover, the increasing incidents of cybercrime make customers more doubtful and reluctant to use electronic payments. According to the study by Lawal, Lawal and Akanbi [20], hacking has become a common crime in the banking sector, which is discouraging customers from using Fintech, which is a cutting-edge development in technological advancement in the banking industry.

Lastly, the other independent variable was subjected to an assessment to assess the impact of phishing on the increasing resilience towards using e-banking services in Pakistan. The hypothesis was accepted based on the Path coefficient depicting a value of 0.261, showing the fact that customers have become more resilient to using e-banking services due to the increasing phishing attacks they are facing. It was also argued in the study of Behl, Pal and Tiwari [22], that increasing cybercrime in banking from phishing is increasing the fear in customers to quit the use of e-banking services, as there is a threat of losing important monetary value to the threat of these frauds.

IX. RESEARCH LIMITATIONS

The researcher faced various limitations during the research, including time, area and access limitations. Due to deficiency of resources, limited budget and time the researcher was unable to get the data from the whole population. Hence, the researcher trusted on the convenience method to collect the data. Moreover, the data collection was done only in Karachi as the researcher cannot assemble the data from other cities due to limited time and accessibility issues. Conclusively, the researcher also cannot use specialized tools for analysis of data. Therefore, the context of this study is quantitative, and the researcher only used a questionnaire to understand the phenomena and empirically test the relationships.

X. FUTURE IMPLICATIONS

From the results it was assessed that the coefficient of determination was 0.4212 which showcased the fact that 42.12% variance in customers’ intention had a contribution effect from the factors like phishing, hacking and identity theft. However, it also highlights that 57.88% variance is due to the unknown variables which are not highlighted and examined within the study. Hence, there is a future scope for researchers to analyse these missing factors to develop a more concrete research, which complements this study. This provides banks a holistic view of the areas wherein they can work effectively towards mitigating the risk of losing customers from digital banking and improve their cyber structures to prevent cyber-attacks.

XI. CONCLUSION

The objective of developing countries is to gauge economic growth, which is only promising by the mobilization of money in terms of investments and saving. However, people in developing countries like Pakistan are more inclined to use other mediums of saving rather than banks because of lack of trust and increased threat of cyber security. Moreover, people in rural areas have lesser understanding of cyber security threats and risks and lack of financial literacy, which makes them reluctant to use banks for transactions.

It can be noted that the results of this research are useful to financial institutions, mainly for the banking sector, including the central bank, because it gives the standard operating procedure and guidelines to further enhance safety and financial literacy. The research holds utmost importance for the banking sector because they can develop a plan for the improvement of their payment
strategies to converge them towards electronic modes of payments, which are less time-consuming and cost-effective at the same time. Conclusively, the financial and banking sectors should look at the bigger picture and go the extra mile to protect the privacy of banking customers.

REFERENCES
[31] Fornell, C., and Larcker, D.F.: ‘Structural equation models with unobservable variables and measurement error: Algebra and statistics’, in Editor (Ed.) (Eds.): ‘Book Structural equation models with unobservable variables and measurement error: Algebra and statistics’ (Sage Publications Sage CA: Los Angeles, CA, 1981, edn.), pp.