Business & Social Science
IJRBS

Research in Business & Social Science

IJRBS VOL 9 NO 6 ISSN: 2147-4478

Available online at www.ssbfnet.com
Journal homepage: https://www.ssbfnet.com/ojs/index.php/ijrbs

Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks

Hayder M. Kareem Al_Duhaidahawi[(a,b)], *Jing Zhang*[(c)], *Mustafa S. Abdulreza*[(d)], *Meriem Sebai*[(e)], *Sinan Abdullah Harjan*[(f)]

(a,c,e) School of management/ Huazhong University of sciences and Technology (HUST), Wuhan China
(b) Banking and Financial Sciences/ Imam Al-kadhum College (IKC), Baghdad, Iraq
(d) AL-Furat Al-Awsat Technical University / Technical institute of AL.Musaib, Iraq
(f) Department of Banking and Financial science/ Cihan University-Erbil, Erbil, Iraq

ARTICLE INFO

Article history:
Received 09 October 2020
Received in rev. form 19 Oct. 2020
Accepted 22 October 2020

Keywords:
Financial Technology (Fintech), Cybersecurity, Cybercrime, Banking

JEL Classification:
L25, O31

ABSTRACT

In this paper, we investigate the definition of Fintech and measure the extent of the impact of Fintech variables on the Cybersecurity as the dependent variable. The hypotheses developed by the authors which are based on research through the statistical results of the research variables and as all correlation coefficients were a positive relationship and at the level of significance 0.01 which made the authors accept the correlation hypotheses, and for the results of the influence factor between the research variables it also had a positive effect when the level of 0.05 for all sections of the independent variable, as we have also noticed that the influence of the independent variable of financial technology when linked to all of its sections with Cybersecurity. We find the influence of the influence coefficient significantly increased to 0.908, which explains that there is complementarity between the sections of the independent variable.

Introduction

Financial technology, often referred to as FinTech, is the technology and innovation that seeks to compete with traditional financial methods when providing financial services, whereas, it is considered an emerging industry that uses technology to improve financial activities. An example of this technology can be referred to the use of smartphones in banking services or what is known as cellular banks, as well as investment services via mobile phone, and Cryptocurrencies, which aims to make financial services accessible to the general public, Financial technology companies consist of emerging projects, financial institutions, and well-established technology companies that aim to either enhance or replace the use of financial services provided by existing financial companies. Many current financial institutions apply financial technology solutions and technologies to improve and develop their services, and to improve their competitive position (Peters et al., 2015), Therefore, we find that financial technology innovations work hard to improve the efficiency of the financial system for all public and private sectors as well as companies and consumers, which in turn makes financial technology more vulnerable to financial risks and losses. Policymakers, titles, and regulations work to protect all parties involved to promote financial innovation and encourage the development of these services (Philippon, 2016; Shah et al., 2018). .

In recent years, a new generation of financial technology startups supporting financial institutions and providers of digital solutions has emerged, resulting in a reversal of financial market conditions around the world by leveraging technology innovations in finance. In light of this rapid development, it is necessary to adopt methods that guarantee the utilization of the financial technology revolution for the benefit of society and the economy, considering consumer protection and the financial system.

* *Corresponding author. ORCID ID: 0000-0002-4294-9586*

https://doi.org/10.20525/ijrbs.v9i6.914

The field of finance has evolved thanks to technological developments throughout the ages. However, over the past decade, technology-based innovations in finance have enhanced consumer access to many services in the areas of payments, lending, insurance, savings, and investment; This is within their reach, with an unprecedented pace and scope (Kim et al., 2015), But it raises a lot of privacy concerns and whether dealing in technology reveals customer data and is at risk, and will related technologies be used in machine learning and artificial intelligence in risk management in banking (Kareem et al., 2020), Where it is possible and in an unintended or unexpected way or without the knowledge that the customer may fall into the trap of fraud so we see that the process of increasing adoption of cloud computing is assigned to companies that have sufficient experience to deal with modern technology with financial institutions and provide financial services electronically and have the potential to counter cyber-attack The most important thing is that the new world is not only full of opportunities, but also fraught with a set of risks known and unknown risks on several levels, starting with individuals (Sinan Abdullah Harjan et al., 2019), We notice recently the growth of non-bank internet lenders, it has become possible to obtain credit anywhere and anytime, and therefore comes the role of industry watchers in organizing this business, as this system becomes very stressful and it is required to protect consumers (Sadłakowski & Sobieraj, 2017). Because the third party has become the dominant provider of services through electronic control, therefore industry observers discuss the extent to which these companies apply laws and regulations and put in place important security guarantees with electronic security. Increasingly, systems, points of sale, and payment systems for consumers are being developed, and that these systems will be more appropriate and effective. Therefore, concerns arise here about the market power of the dominant companies in providing services and their impact on people who do not have much information to access these services (Sinan A Harjan et al., 2015). At the same time, individual Cryptocurrencies have emerged that allow payments to be made in a completely different way than traditional financial systems. This form allows for greater privacy, but at the same time, it increases the scale of fears, especially money laundering and consumer protection concerns. We see that Fintech offers new and innovative ways to increase the capital of individuals through crowdfunding and currency offers, and introducing new ways of trading securities and managing investments, which leads to increased fundraising. This, in turn, increases the challenges to protect investors, and several laws were passed that regulate and manage the risks resulting from the financial technology industry (Firmansyah & Anwar, 2019; Hayder M. Kareem et al., 2019).

In light of these developments, cyber-attacks continue to evolve and become more and more widespread. Persons specializing in attack operations work to improve their methods to enable them to develop rapidly and faster than security teams can do so that their methods are more sophisticated, so it is important to define the type of threat and understand the risks associated with Cybersecurity and its effects on financial services. This e-crime did not change this, but the greater the speed and the consequences, the more attacks and the more closely notified the regulators, the greater the pressure on workers. By realizing that hackers will find weaknesses, leaders can improve the way they design, deliver services, manage risk, and train their teams, this means that it is essential to understand the changing threat landscape that financial companies face. This blog aims to provide some indications about the state of the land and how banks and insurance companies respond. We don't have room to take a comprehensive look, but we hope to provide sufficient evidence to make CFOs think twice about the effectiveness of their Cybersecurity strategies.

Financial technology (Fintech) has become a modern phenomenon. With the rise in technology and the need for convenience, these applications and programs have revolutionized both banking and personal businesses. Fintech is not new, but what has been discovered is the rise in cyber-attacks on Fintech companies in recent years. Although they have been around since the late 2000s, cyber-attacks on the financial technology industry have been spotted on the rise since 2017 (Sadłakowski & Sobieraj, 2017).

The growth of the financial technology companies (or “financial technology”) and the fundamental changes they have made on a variety of fronts, from how banking works, to how capital is increased, even to the form of money itself. These changes call for a massive reformulation of financial regulation in the era of technology-enabled financing. In particular (Magnuson, 2018).

In light of the developments in technology and in all fields, especially financial ones, where financial technology is expected to play an important role in leading financial services shortly. So as financial technology becomes more important, stronger Cybersecurity mechanisms are needed. As a result, the benefits of financial technology are not lost. This requires a certain level of preparation in many areas, including cyber governance, such as better understanding and analysis of Internet technologies and security facts, security partnerships. For instance, ensuring reliable security partnerships between the various components of the financial system and establishing trust elements. With the use of fully trusted transactions because of the benefits Clear from Fintech, innovation could not continue at the expense of bank safety and durability, as well as at the expense of consumer protection.

The main problem is that with the recent development and high capabilities of financial and banking services, great risks arise as well, and these services are accompanied by fierce attacks that institutions must prepare for since financial institutions are the most vulnerable to these risks. Therefore, the supervision of banking operations and regulatory bodies should oversee oversight mechanisms that are in line with the evolution of electronic banking operations and the resulting risks. So, this study aims to know the reality of financial technology and its impact on Cybersecurity by knowing the extent of the impact of each section identified to measure financial technology and its impact on Cybersecurity.

Literature Review

Theoretical and Conceptual Background

Financial Technology (FinTech)

Financial technology and its abbreviation (Fintech), which is an innovation that aims to create services that compete with traditional services in its style (Lin, 2015), based on the use of technology to improve financial activities (Schueffel, 2018), through the use of financial and banking services via smartphones and tablets in all operations, including borrowing and investment As a multidisciplinary topic that combines finance, technology management, and innovation management. More specifically, working to innovate and improve the quality of financial services by proposing technical solutions according to different work situations (Leong, 2018), and the use of Cryptocurrencies in dealing and making them available for the general public, many companies that work with modern technologies work to enhance the financial services provided by traditional companies and turn them into technology-based companies, and therefore the term technology has gained great importance for researchers to know, so it is necessary to know what financial technology is for the purpose of coherence between texts during a new field of studies. Thus, helping to get inspiration for a scientific health add this field (Schueffel, 2018), one of the definitions that have been researched systematically states: "Fintech is the financial services industry in a new and innovative way through using technology to perform these services where Banks have worked since ancient times to develop their activities, so they cannot be excluded from the definition of technology. On the contrary, these banks have worked to develop digital advocacy systems for years and to invent new financial services in their time. The idea of an ATM was a revolutionary idea at that time and other services where it developed Telephony systems on private computers with modems to access banking applications. In light of the expansion that took place on the Internet in the nineties, banks have developed internet banking outlets for consumers, while MasterCard has provided the latest technologies for online purchases (Nikkel, 2020).

At the same time, Fintech is going up very quickly. Various industries compete in producing services that are favorable to current developments, to disrupt ease for consumers to easily transfer services, as is the case in social networking programs and other programs that provide online services such as Amazon (Wulan, 2017).

It will also be more attractive and impact on the consumer, where these industries have grown significantly in recent years, when Fintech was applied by financial services providers in international stock exchanges, which were identified by specialized institutions in the market and through legal frameworks established by the Financial Supervision Authority, in addition to providing ways to ensure that customers receive on services in online trading platforms (Micu, 2016).

The researchers did not stop at this level, but some tried to understand the level of technology permitted in Islamic law, as long as it complies with the provisions of this law, and the challenges facing Islamic finance were discussed in Indonesia and Singapore, data was collected using the distribution of questionnaires to a group of companies using social media through the internet, the study reached many results, the most important of which is that the prospects of Islamic financial technology are bright and are growing in the study sample countries, and that these developments in Islamic finance are supported by modern technology such as the use of smartphones and other financial, but they face many challenges in Islamic financial technology Like the laws and special frameworks in this financing and the determinants upon which it depends, therefore the regulators of these operations must be in a positive direction to support Islamic finance, and the academic community must explore the practice of Islamic financial technology, and achieve a balance between practice and theory (Firmansyah & Anwar, 2019).

Cybersecurity

After the great spread of the Internet, smart devices and mobile devices, it has become necessary in our time to pay attention to cyber security and how to protect ourselves in the digital space, from home to work and at the state level as a whole, and Cybersecurity is one of the most prevalent topics in our days and learning has become a necessity, Cybersecurity can defined as information security and protection of electronic systems, networks, devices, programs or data from theft or damage (Schatz et al., 2017), Because the whole process is done by computers and smart devices, therefore, you must beware of malicious attacks and electronic attempts with the aim of destroying and stealing systems in order to avoid electronic attacks and malicious attempts to destroy or destroy systems or networks in general (Von Solms & Van Niekerk, 2013), As well as the practice of securing the computer network from intrusive and opportunistic elements, whether targeted attackers, or malware, and focusing on keeping programs and hardware free from threats, as the compromised application can provide access to data designed for protection, and that the successful security concept application begins in the initial design phase before deployment. The program or device for the importance of technological development and increasing reliance on smart devices in all businesses, especially financial businesses and provision of services on the Internet as the assets of the electronic environment require protection from hostile attacks with the aim of intentional damage targeting private organizations, government agencies, banks and other financial institutions at risk (Wang et al., 2015 & Whitley, 2009), Cybersecurity is one of the major challenges in the world today as it is more interconnected than ever. However, for all its advantages, the increasing interconnection has led to an increased risk of theft, fraud, and abuse. As people around the world become more dependent on modern technology, they are more vulnerable to cyber-attacks like breaches of corporate security, phishing, blackmail, fraud, and social media fraud (Stevens, 2018). The high level of insecurity in cyberspace and its basic infrastructure has become vulnerable to a wide range of risks arising from electronic threats and material risks as actors exploit electronically as well as nation-states the weaknesses of their opponents to steal information and funds and develop capabilities to disrupt, destroy or only

threaten the opponent's ability to meet Basic services. There is also a host of traditional crimes now committed across cyberspace, including the production and distribution of child pornography, juveniles, their exploitation plots, banking and financial fraud, intellectual property violations, and other crimes, which have significant human, economic and legal consequences on the Internet (Ayofe & Irwin, 2010), This, in turn, led to great efforts by specialists and researchers to introduce smart technologies such as artificial intelligence and other tools to analyze and know how to counter cyber-attacks before it happens (Kang & Kang, 2016; Rieck et al., 2011), Where smart programs and competent programmers were used to discover and classify malicious programs, stand up and address them, address their implications and set up protocols to prove the user's personality to the program (AL-Maksousy, 2018), For the purpose of introducing people and protecting their files, as well as knowing who is carrying out the attack through its style and style of attack, through the use of language processors and personal files, reports of attack incidents were collected from 2012 to 2018 and five people were trained in them and analyzed how and how to attack during this period, It should be noted that cyber threats have been obtained in a very large percentage (Noor et al., 2019), through what we find that two types of risks are considered the strongest risks, the first on the part of the user and the other on the server-side, where data was stored (Davis, 2017).

Therefore, researchers conducted several studies and models to address Cybersecurity risks because of its importance in practice today, Henrique's started with its model to analyze Cybersecurity risks which was developed by combining two decision and logic theories, regarding the time of data dissemination and the time of data modification, and the time of data loss or damage , The results concluded that the application of the two models showed great benefit and also demonstrated that e-commerce can also be more vulnerable to cyber security attacks than other sites (Henriques de Gusmão et al., 2018). Munk's study explores an understanding of the security and governance strategies presented in the European region. Therefore, the diagnosis of Cybersecurity through the perspective of dogmatic and mental governance allows us to understand Cybersecurity strategies and governance models developed by the European Union and NATO. To diagnose strategies and models of governance, two schools, Copenhagen and Paris, were used, which included different aspects of the security agenda. The study developed a fundamental analytical framework through two case studies, namely Cybersecurity and cyber terrorism. The study concluded a set of results, including the complexity of the contractual system, legislative gaps, reliance on various forms of governance, transparency, and accountability, and types of proactive governance and organizational practices that would reduce cyber-attacks significantly (Munk, 2015). Lee's study focused on the issue of disclosing Cybersecurity risks, especially after the issuance of the Securities Commission's instructions to disclose Cybersecurity risks, so the study aimed to know the determinants and axes of Cybersecurity risks that have been declared and it has become recognized that the presence of these risk factors in a period Before the warning is linked to the reported future Cybersecurity incidents, here we find that the correlation between the Cybersecurity incidents and the reported Cybersecurity risks becomes insignificant unless disclosed, and the study concluded that the decision of the Securities and Exchange Commission regarding the confirmation of disclosure of security risks Cyber. However, the US Securities and Exchange Commission's disclosure directive may inadvertently encourage companies to disclose Cybersecurity risks regardless of the level of risk (Li et al., 2018). As organizations become more interested in developing their information security and protection systems. Despite attempts to secure the information infrastructure, employees within organizations continue to pose the greatest threat to Cybersecurity, so it is necessary to focus on employee behavior within the organization and its relationship to their performance, in addition to these, cyber behaviors that are positive with organizational citizenship behaviors and potentially harmful cyber behaviors And related to negative business behaviors. This research contains the effects of personal use to predict Cybersecurity behaviors and to reduce the internal threat in the workplace (Christine Dreibelbis, 2016). While some studies have focused on identifying security risks, which are difficult to identify to obtain new data to know how technologies have been misused Often. Therefore, this study proposes a fuzzy reasoning model (FIS) to identify cyber risks (Alali et al., 2018)

Cybersecurity and law enforcement capabilities are important to protect and ensure cyberspace. The law plays a fundamental role in achieving the goals of Internet security, by investigating a wide range of cybercrime, ranging from theft and fraud to the exploitation of children, and the arrest and trial of those responsible. Among the duties of the ministries of the interior and justice of different countries highlight the importance of adopting criminal investigations and effective measures to disrupt and deter cybercriminals, prioritize the employment and training of technical experts, develop standardized methods, and exchange best practices and tools related to electronic response on a large scale. Criminal investigators and network security experts - who have a deep understanding of the technologies used by evil actors and the specific vulnerabilities they target - are working to effectively respond to and investigate cyber incidents (Borghard & Lonergan, 2017), while Dawson has focused on the growing concerns of critical infrastructure, which is increasingly exposed to sophisticated electronic penetration, which poses new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is an increased risk of large-scale or high-impact events that could cause damage or disrupt the services that the economy and daily life depend on millions in the contemporary world in light of the risks and potential consequences of electronic events. Thus, enhancing the security and resilience of cyberspace has become an important work of national security for various countries and has also focused on the role of education, technology, and politics in Cybersecurity. The study concluded with developing training environments to teach real Cybersecurity events, and creating an educational environment everywhere to teach Cybersecurity concepts, Policies based on the safe use of modern systems and the study of effects on national and international security (Dawson, 2017).

However, securing cyberspace is particularly difficult due to many factors: the ability of evil actors to operate from anywhere in the world, the existence of links between cyberspace and physical systems, and finally the difficulty of reducing vulnerabilities and consequences in complex information networks.

Research and Methodology

Method

Quantitative methods emphasize objective measurements and the statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys, or by manipulating pre-existing statistical data using computational techniques. Quantitative research focuses on gathering numerical data and generalizing it across groups of people or to explain a particular phenomenon.

Data collection, Study population & sampling

The questionnaire will be collected by means of questionnaire for the sample banks where at least 250 questionnaires will be distributed to the sample customers. The WhatsApp program can also be used to collect data and take opinions from the persons involved in this field. There are three variables for this study, the independent variable will be financial technology (FINTECH) and dependent variables will be financial risks management and banking and financial services. The sample in Iraqi and Lebanese banks consumers working in the field of technology.

Data analysis

The data are analyzed by the statistical package for social sciences (Smart PLS 3) by means of the relevant analysis tools for the purpose of testing hypotheses.

Research Instrument

The questionnaire was designed according to the five-item Likert paragraphs containing (Strongly agree -5- agree -4- neutral -3- disagree -2- strongly disagree -1-)

Research Variables

The independent variable (FINTECH) which can be measured by some of the sup variables assumed by self-efficacy (SE), information security experiment (IS), technology culture (TC), and Competence and skill (CS), and dependent variable (Cybersecurity).

Research Model

Figure (1) shows the proposed model for the study, which shows the relationships between independent and dependent variables.

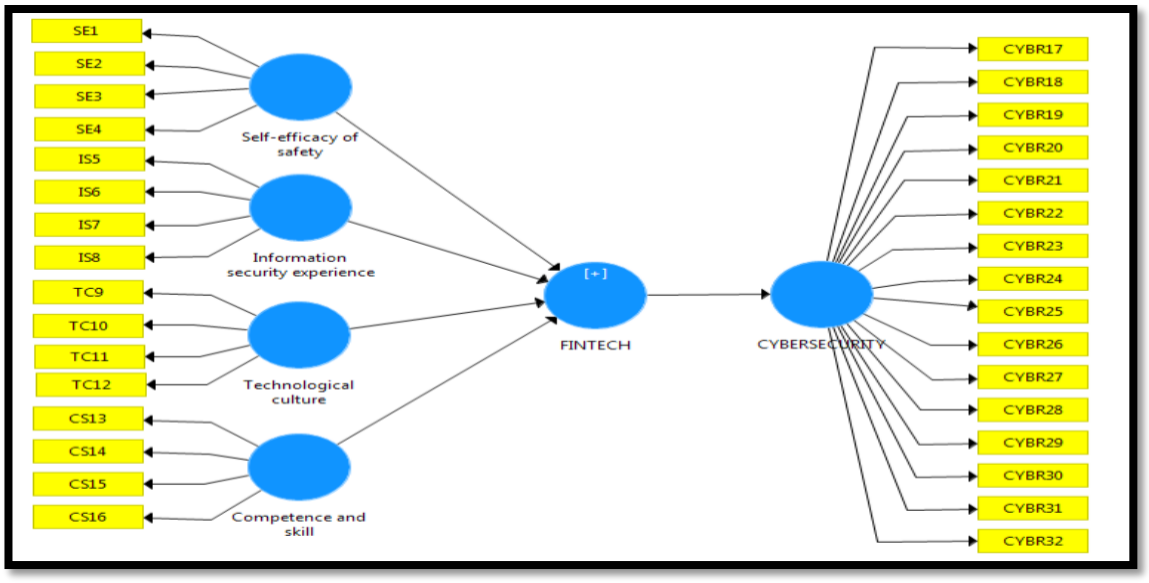

Figure 1: research proposed model

Result and Discussion

Normal Distribution of The Studied Data

Table (1) shows the results of the normal distribution of the adopted data in the study according to the number of observations that reflect the sample size (50). It turns out that the values of the Flatness and Sprain coefficients are close to zero, which indicates the study of the data distributed naturally concerning the variable (Fintech).:

Table 1: The results of the normal distribution of the financial technology variable

No	Coding	Valid	Missing	Skewness	Kurtosis	Std deviation	Mean	Median
Self-efficacy of safety								
1	SE1	50	0.00	-0.259	-1.235	1.064	3.740	4.000
2	SE2	50	0.00	0.328	-1.243	0.767	3.840	4.000
3	SE3	50	0.00	0.497	-1.161	0.770	3.600	4.000
4	SE4	50	0.00	-0.071	-1.040	0.821	3.740	4.000
Information security experience								
1	IS5	50	0.00	-0.441	0.247	0.705	3.820	4.000
2	IS6	50	0.00	-0.153	-0.749	0.890	3.960	4.000
3	IS7	50	0.00	-0.011	-0.777	0.775	3.560	4.000
4	IS8	50	0.00	-0.136	-1.145	0.900	3.900	4.000
Technological culture								
1	TC9	50	0.00	-0.528	-0.574	0.603	4.240	4.000
2	TC10	50	0.00	-0.687	0.011	0.756	3.860	4.000
3	TC11	50	0.00	-0.324	-0.625	0.907	3.850	4.000
4	TC12	50	0.00	-0.744	-0.608	0.693	3.960	4.000
Competence and skill								
1	CS13	50	0.00	-0.654	-0.507	0.635	3.980	4.000
2	CS14	50	0.00	-0.165	-0.006	0.877	3.680	4.000
3	CS15	50	0.00	-1.298	3.448	0.608	3.300	3.000
4	CS16	50	0.00	-1.227	2.094	0.733	3.880	4.000

Source: Statistical Program Outputs

The Normal Distribution of The Cybersecurity Variable

Table (2) shows the results of the normal distribution of the adopted data in the study according to the number of observations that reflect the sample size (50). It turns out that the values of the Flatness and Sprain coefficients are close to zero, which indicates the study of the data distributed naturally concerning the variable (Cybersecurity).

Table2: The results of the normal distribution of the Cybersecurity variable

NO	Coding	Valid	Missing	Skewness	Kurtosis	Std deviation
1	CYBR17	50	0.00	0.034	-0.863	0.873
2	CYBR18	50	0.00	-1.045	1.855	0.660
3	CYBR19	50	0.00	-1.385	1.844	0.775
4	CYBR20	50	0.00	-0.068	-1.084	0.950
5	CYBR21	50	0.00	-0.735	-0.414	0.574
6	CYBR22	50	0.00	-1.011	-1.021	0.449
7	CYBR23	50	0.00	-0.421	-1.900	0.490
8	CYBR24	50	0.00	-0.792	-0.669	0.721
9	CYBR25	50	0.00	-0.510	-1.814	0.485
10	CYBR26	50	0.00	-0.390	-0.626	0.596
11	CYBR27	50	0.00	-0.893	1.838	0.646
12	CYBR28	50	0.00	-1.292	2.195	0.670
13	CYBR29	50	0.00	-1.360	1.202	0.866
14	CYBR30	50	0.00	-1.371	1.913	0.700
15	CYBR31	50	0.00	-0.217	-0.525	0.601
16	CYBR32	50	0.00	-0.653	-0.523	0.574

Source: Statistical Program Outputs

Correlation Test

This section aims to identify the strength of the relationship of dimensions and variables of the study, as this study examines the relationship of the independent variable (FINTECH) with the dependent variable (Cybersecurity). Moreover, through this section, we investigate the nature or direction of the relationship between the variables: whether they are inverse or negative, and five hypotheses that assume a positive correlation relationship between the study variables will be tested. Table (3) shows the correlation matrix between study variables, which are as follows:

Table 3: Matrix of the correlation coefficient between research variables

Variable	SE	IS	TC	CS	CYBR
SE	1.000				
IS	0.046	1.000			
TC	0.235**	-0.169	1.000		
CS	0.303**	-0.058	0.644**	1.000	
CYBR	0.234**	0.091**	0.359**	0.394**	1.000

Source: Statistical Program Outputs

In the table (3), the hypotheses will be tested, as follows:

The First Sub-Hypothesis

This hypothesis Assume that there is a positive correlation between (Competence and skill) in (Cybersecurity) it turned out that there was a correlation between the two variables and it reached (0.234), which is a positive trend correlation and it is also significant relationship, which is acceptable at (0.01) level. According to these results, this hypothesis will be accepted at the level of this study.

The Second Sub-Hypothesis

This hypothesis Assume that there is a positive correlation between (Information security) in (Cybersecurity), It turned out that there was a correlation between the two variables and it reached (0.091), which is a positive trend correlation and It is also significant relationship, which is acceptable at (0.01) level. According to these results, this hypothesis will be accepted at the level of this study.

The Third Sub-Hypothesis

This hypothesis Assume that there is a positive correlation between (Technology Culture) in (Cybersecurity), it turned out that there was a correlation between the two variables and it reached (0.359), which is a positive trend correlation and It is also significant relationship, which is acceptable at (0.01) level. According to these results, this hypothesis will be accepted at the level of this study.

The Fourth Sub-Hypothesis

This hypothesis Assume that there is a positive correlation between (Self-efficacy) in (Cybersecurity), It turned out that there was a correlation between the two variables and it reached (0.394), which is a positive trend correlation and It is also significant relationship, which is acceptable at (0.01) level. According to these results, this hypothesis will be accepted at the level of this study.

Testing of The Model

To test the study model, the main hypothesis was developed which indicated that there is an effective relationship between the independent variable (FINTECH) in the dependent variable (Cybersecurity). To test this hypothesis, simple regression analysis, and path analysis were used in testing this effect relationship. This means that (Cybersecurity) is a real function (FINTECH). To test these relationships, four hypotheses have been assumed from the main Hypotheses which is there is a significant effect between FINTECH and Cybersecurity, as following

H1: Self-efficacy will positively affect Cybersecurity.

H2: Information security experience will positively affect Cybersecurity.

H4: Competence and skill will positively affect Cybersecurity.

H4: Technological culture will positively affect Cybersecurity.

The results extracted using (SMART PLS) program as shown in Figure (2) and Table (4), as shown below:

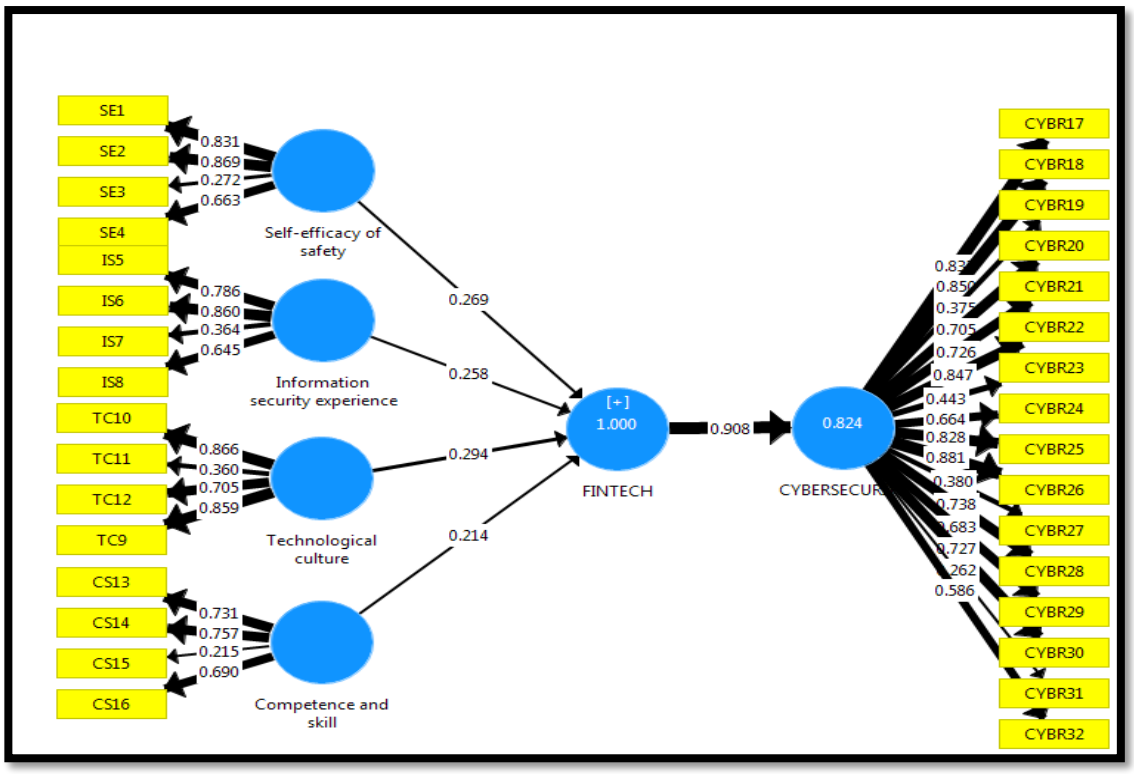

Figure 2: simple direct regression analysis the model variables

Table 4: Analysis of simple direct and indirect regression between the model variables

Direct effect					
Hypothesis test	Original Sample (O)	Standard Deviation (STDEV)	R^2	T Statistics (|O/STDEV|)	P Values
Competence and skill> Cyber security	0.269	0.021	1.000	9.079	0.000
Information security EX> Cyber security	0.258	0.017		13.948	0.000
Technology Culture > Cyber security	0.294	0.022		12.398	0.000
Self-efficacy> Cyber security	0.214	0.019		12.583	0.000
Indirect effect or (Total effect)					
FINTECH -> Cyber security	0.908	0.060	0.820	15.221	0.000

Source: Statistical Program Outputs

The results of the hypothesis test are as follows

First hypothesis assumes that there is an impact relationship (Competence and skill) in (Cybersecurity) and it turns out that there is an impact relationship (Competence and skill) in (Cybersecurity) and the impact ratio has reached (0.269), which is a positive impact relationship, which means when an increase of one unit of (Competence and skill) will lead to an increase in (Cybersecurity) of (0.269). It is also significant because the achieved level of significance (0,000) is lower than the level of significance assumed by the researcher (0.05). According to these results, this hypothesis will be accepted at the level of this study.

Second hypothesis assumes that there is a relationship of effect (Information security EX) in (Cybersecurity), it turns out that there is an effect relationship (Information security EX) in (Cybersecurity), and the impact ratio has reached (0.258), which is a positive impact relationship, which means that when increasing one unit of (Information security EX) it will lead to an increase in (Cybersecurity) by (0.258). It is also significant because the achieved level of significance (0,000) is lower than the level of significance assumed by the researcher (0.05). According to these results, this hypothesis will be accepted at the level of this study.

Third hypothesis assumes that there is a relationship of (Technology Culture) in (Cybersecurity) and shows that there is a relationship of (Technology Culture) in (Cybersecurity) and the impact ratio has reached (0.294) and it is a positive impact relationship where when increasing the unit One of (Technology Culture) will lead to an increase in (Cybersecurity) by (0.294). It is also significant because the achieved level of significance (0,000) is lower than the level of significance assumed by the researcher (0.05). According to these results, this hypothesis will be accepted at the level of this study.

Fourth hypothesis assumes that there is a relationship of (Self-efficacy) in (Cybersecurity) and shows that there is a relationship of (Self-efficacy) in (Cybersecurity) and the impact ratio has reached (0.214) and it is a positive impact relationship where when increasing the unit One of (Self-efficacy) will lead to an increase in (Cybersecurity) by (0.214). It is also significant because the achieved level of significance (0,000) is lower than the level of significance assumed by the researcher (0.05). According to these results, this hypothesis will be accepted at the level of this study.

The main hypothesis: This hypothesis assumes that there is a relationship of effect (FINTECH) in (Cybersecurity)), according to the results of the statistical program (Smart pls v.3). The results showed that the overall effect of the model has reached (0.908). The impact ratio was positive that means if (FINTECH) increases by one unit it will increase (Cybersecurity). It is also a moral relationship because the achieved level of significance (0.000) is less than the level of significance assumed by the researcher (0.05), and according to these results, this hypothesis will be accepted at the level of this study.

Conclusions

It is clear from the above, and according to the extracted statistical results that there is acceptance of all the statistical results of the study variables, as it was found that there is a state of correlation between the receiver variable with its four axes and the dependent variable, and this correlation ranged between the average and the strong, as the independent variable occurred with its second axis, information security with the dependent variable Cybersecurity at the highest correlation rate compared to the other three axes, which confirms that the sample members agree that there is a state of correlation between information security and Cybersecurity risks in a way that made the extracted results be substantially realistic, and that all correlation coefficients were positive and at a significant level of 0.01 which made researchers accept the hypotheses of correlation, but as for the results of the effect factor among the study variables also were of positive and significant effect at the level of 0.05 for all axes of the independent variable and they were all at an intermediate level as the axis of culture got the highest impact rate with a positive relationship between it and Cybersecurity. This is a realistic result and indicates that the bank's customers have a very high electronic culture of what they can face from the cybersecurity risks that occur continuously and the need to develop their skills continuously to achieve the required goal which is to mitigate the risks of Cybersecurity. As we also noted that the influence of the independent variable of financial technology when linked to the relationship with the total of one-off dialogue with Cybersecurity, we find the impact factor to a large degree high which reached 0.908, which explains that there is integration between the independent variable axes.

Acknowledgement

This research is sponsored by the National Natural Science Foundation of China under Grant No. 71672068.

References

AL-Maksousy, H. H. L. (2018). Applying Machine Learning to Advance Cyber Security: Network Based Intrusion Detection Systems. Doctor of Philosophy (PhD), dissertation, *Computer Science*, *Old Dominion University*, DOI: 10.25777/8w8w-sa92.

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers and Security*, *74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

Ayofe, A. N., & Irwin, B. (2010). Cyber Security: Challenges And The Way Forward. *Georgian Electronic Scientific journal, Computer Science & Telecommunications*, *29*(6). Https://Www.Researchgate.Net /Publication/265121167_Cyber_Securıty_Challenges_And_The_Way_Forward.

Borghard, E. D., & Lonergan, S. W. (2017). The Logic of Coercion in Cyberspace. *Security Studies*, *26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

Christine Dreibelbis, R. (2016). It' s More Than Just Changing Your Password: Exploring the Nature and Antecedents of Cyber-Security Behaviors, *University of South Florida* .http://scholarcommons.usf.edu/etdhttp: //scholarcommons.usf.edu/etd/6083

Davis, J. J. (2017). Machine Learning and Feature Engineering for Computer Network Security. *Thesis*. https://eprints.qut.edu.au/106914/1/Jonathan_Davis_Thesis.pdf

Dawson, M. (2017). Hyper-connectivity : Intricacies of national and international cyber securities Hyper-connectivity : Intricacies of national and international cyber securities . *London Metropolitan University Maurice Dawson Submitted in partial fulfillment of the award of Doctor of Philosophy by Prior*. *January*. https://www.researchgate .net/publication /314230510_Hyper-connectivity_Intricacies_of_national_and_international_cyber_securities

Firmansyah, E. A., & Anwar, M. (2019). Islamic Financial Technology (Fintech): Its Challenges and Prospect. *Atlantis Press is a professional publisher of scientific. 216*(Assdg 2018), 52–58. https://doi.org/10.2991/assdg-18.2019.5

Faaeq, M. K., Thabit, T. H., & Harjan, S. A. (2015). Technology Innovation Usage in Public Services Among Employees in Republic of Iraq. In 7th International Conference on Information Technology, Al-Zaytoonah University of Jordan, Amman, Jordan..

Harjan, Sinan Abdullah, Teng, M., Shah, S. S. H., & Mohammed, J. H. (2019). Political Connections and Cost of Debt Financing: Empirical Evidence from China. *International Journal of Economics and Financial Issues*, *9*(1), 212. DOI: https://doi.org/10.32479/ijefi.7561.

Hayder M. Kareem, A.-D., Zhang, J., Abdulreza, M. S., Harjan, S. A., & Shah, S. S. H. (2019). the Role of Financial Inclusion and Competitive Advantage: Evidence From Iraqi Islamic Banks. *International Journal of Economics and Financial Issues*, *9*(3), 193–199. https://doi.org/10.32479/ijefi.8080

Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, *43*(January), 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Kang, M. J., & Kang, J. W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. *PLoS ONE*, *11*(6), 1–17. . https://doi.org/10.1371/journal.pone.0155781

Kareem, H. M., Duhaidahawi, A., Zhang, J., Abdulreza, M. S., & Sebai, M. (2020). An efficient model for financial risks assessment based on artificial neural networks; Evidence from Iraqi Banks (2004-2017), *Journal of Southwest Jiaotong University*. https://doi.org/10.35741/issn.0258-2724.55.3.8. *55*(3).

Kim, Y., Park, Y.-J., Choi, J., & Yeon, J. (2015). An Empirical Study on the Adoption of "Fintech" Service: Focused on Mobile Payment Services. December, *Advanced Science and Technology Letters*, *114*(26), *2015*, 136–140, https://doi.org/10.14257/astl.2015.114.26

Leong, K. (2018). FinTech (Financial Technology): What is It and How to Use Technologies to Create Business Value in Fintech Way? *International Journal of Innovation, Management and Technology*, *9*(2), 74–78. https://doi.org/10.18178/ijimt.2018.9.2.791

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*(June), 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Lin, T. C. W. (2015). Infinite Financial Intermediation. *Wake Forest Law Review*, *50*(643), Temple University Legal Studies Research Paper No. https://ssrn.com/abstract=2711379

Magnuson, W. (2018). Regulating fintech. *Vanderbilt Law Review*, Available at: https://scholarship.law.vanderbilt.edu/vlr/vol71/iss4/2*71* (4), 1167–1226.

Micu, A. (2016). Financial Technology (FinTech) and its Implementation on the Romanian Non-Banking Capital Market. *SEA – Practical Application of Science*, *IV*(11), 379–384.

Munk, T. H. (2015). Cyber-Security in the European Region: Anticipatory Governance and Practices. *PQDT- The University of Manchester (United Kingdom) & Ireland*, 287. . https://search.proquest.com/docview/1784057545?accountid=9645

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, *xxxx*, 200908. https://doi.org/10.1016/j.fsidi.2020.200908

Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, *96*, 227–242. https://doi.org/10.1016/j.future.2019.02.013

Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. *SSRN Electronic Journal*, *3*(3). https://doi.org/10.2139/ssrn.2646618

Philippon, T. (2016). The Fintech Opportunity. *National Bureau Of Economic Research*, *8*(3), 6–10. http://www.nber.org/papers/w22476

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic analysis of malware behavior using machine learning. *Journal of Computer Security*, *19*(4), 639–668. https://doi.org/10.3233/JCS-2010-0410

Sadłakowski, D., & Sobieraj, A. (2017). The development of the FinTech industry in the Visegrad group countries. *World Scientific News*, *85*, 20-28.https://doi. WSN% 2085%20 (2017) % 2020-28.pdf

Schatz, D., Wall, J., Schatz, D., & Wall, J. (2017). Security and Law Towards a More Representative Definition of Cyber Security Towards A More Representative Definition Of Cyber Security. *Journal of Digital Forensics 12*(2). https://doi. 10.1080/ 09636412.2017 .1306396

Schueffel, P. mname. (2018). Taming the Beast: A Scientific Definition of Fintech. *SSRN Electronic Journal*, *April*. https://doi.org/10.2139/ssrn.3097312

Shah, S. S. H., Xinping, X., Khan, M. A., & Harjan, S. A. (2018). Investor and manager overconfidence bias and firm value: Micro-level evidence from the Pakistan equity market. *International Journal of Economics and Financial Issues*, *8*(5), 190.

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. *Politics and Governance*, *6*(2), 1–4. https://doi.org/10.17645/pag.v6i2.1569

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and Software-Defined Networking. *Computer Networks*, *81*, 308–319. https://doi.org/10.1016/j.comnet.2015.02.026

Whitley, E. A. (2009). Informational privacy, consent and the "control" of personal data. *Information Security Technical Report*, *14*(3), 154–159. https://doi.org/ 10.1016/j.istr .2009.10.001

Wulan, V. R. (2017). Financial technology (fintech) a new transaction in future. *Journal Electrical Engineering and Computer Sciences*, *2*(1), 177–182. Corpus ID: 170052661.