Migration Letters

Volume: 21, No: S4 (2024), pp. 885-900

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Biometric Authentication In Fintech And Its Role In Increasing Security Of Financial Services

MURAD MOHAMMAD ALKASEASBEH[1], BELAL RABAH SHAMMOUT[2] , TALAL ABDUL KAREEM ALQURRAN[3]

Abstract

Purpose: *The current study aimed to examine the role of biometric authentication characteristics "Unique Biological Traits, Multifactor Authentication, Non-Replicable, Continuous Authentication, and Anti-Spoofing Measures" in fintech in increasing security of financial services from perspective of IT managers departments within banking industry in Jordan. The study hypothesized that "biometric authentication can increase security of financial services of fintech from the perspective of IT specialists in Jordanian banking industry".*

Methodology: *Realizing main hypothesis of study was done depending on quantitative methodology. For that, a questionnaire was built and distributed on (63) IT managers within Jordanian banking sector. SPSS was employed in order to mitigate primary data.*

Findings: *Results of study indicated the acceptance of the study main hypothesis and confirmed that "The biometric authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry". Regarding sub-hypotheses, study indicated that (anti-spoofing measures) appeared with a strong correlation of 0.899 and a variance of 80.9%. this meant t[1]hat measures of anti-spoofing is able to support the security of financial services through making sure to prevent all trials and actions that may jeopardize the financial services through hacking, piracy and unauthorized usage of financial accounts. Study recommended increasing individuals and organizational awareness on the importance of authentication and the fact that it is still exposed to malfunctions and errors.*

Significance: *Significance of current study lies in its ability to guide decision makers, IT specialists, customers and regulatory bodies in Jordanian banking sector towards adopting the best and most efficient biometric authentication methods based on their existing security measures and regulatory needs.*

Keywords: *Biometric, Unique Biological Traits, Multifactor Authentication, Non-Replicable, Continuous Authentication, Anti-Spoofing Measures, Iris, Fingerprint, Face, Recognition, Access, Fraud.*

[1]Assistant Professor: The World Islamic Sciences and Education University (W.I.S.E), Faculty of Finance and Business, Department of Banking and Financial Sciences, Amman, Jordan. Orcid: https://orcid.org/0009-0003-0521-2387

[2]Assistant Professor: The World Islamic Sciences and Education University (W.I.S.E), Faculty of Finance and Business, Department of Banking and Financial Sciences, Amman, Jordan. Orcid: https://orcid.org/0009-0009-9017-5173

[3] Associate Professor: The World Islamic Sciences and Education University (W.I.S.E), Faculty of Finance and Business, Department of Banking and Financial Sciences, Amman, Jordan. Orcid: https://orcid.org/0000-0002-0658-8082

1. Introduction

Technology has appeared in many areas of life for individuals and organizations, and reliance on technology has become one of the organization's characteristics that indicates its development and keeping pace with everything new in the field in which it operates (Quintal et al., 2019). Today, financial technology or knowledge of Fintech has emerged as a result of the many developments that have appeared in the world of finance, and many banks and financial organizations have begun to adopt Fintech for the purposes of providing their services in a sophisticated and unique way (AbuHamad et al., 2020).

Alorfi et al. (2023) points out that many organizations working in the financial sector have rushed to adopt technological financial services based on their belief in the effective role that these services will play in terms of time, effort, and improvement of financial services. Zachariadis et al. (2019) He added that technological financial services have contributed significantly to improving the performance of financial organizations and have also led to increasing the agility of these organizations due to their reliance on technology as a means of service delivery.

Ryu et al. (2021) confirms that with the increase in financial organizations adopting technological financial services, and the increasing rush towards fintech, in addition to the spread of the Covid-19 virus, which has enhanced individuals' adoption of these technologies, multiple problems have emerged related to security protection, piracy, and unauthorized access. Xu (2022) added that the increasing reliance on fintech has led to the emergence of what is known today as biometric authentication, which refers to verifying authorized access by relying on a person's biological specifications and characteristics, such as the pupil of the eye, facial features, and/or fingerprint.

In a study by Wang (2021), the researcher discussed the role of biometric authentication in enhancing data security in applications related to fintech and addressed the idea from the standpoint of the TAM model by adding the dimensions of "perceived trust" and "perceived privacy." Previous studies were also relied upon to reach the level of individuals' acceptance of the security issued by biometrics authentication. The study reached the conclusion that there is more acceptance among individuals for biometric authentication based on **"face and voice recognition"** than other methods such as the **iris or fingerprint**.

Dubey (2019) in their study tried to unravel the mechanism by which fintech relies on biometric authentication in order to ensure a high level of security and privacy for individuals using fintech services. Through a review of previous literature, the study reached the conclusion that biometric authentication had a role in activating individuals' confidence in fintech services, especially with the idea that their biological specifications determine access to their accounts, and this is something that cannot be imitated or stolen.

Meng et al. (2019), researchers pointed out that the rush of individuals and organizations to use fintech gave a lot of space for hackers and cybercriminals to electronically attack unprotected accounts. In addition, the previous traditional methods of textual passwords became easy to break and the need for more effective protection methods emerged. This led to the emergence of many more secure technologies, such as **fingerprint, iris, facial features, or even voice fingerprint**. The most modern of these methods is known as graphical password GPs, which outperforms traditional methods by relying on different schemes such as Passpoint, Ced Click, and DAS. The study confirmed that different authentication methods played a role in enhancing the security of biometric authentication, which increased the confidence of individuals and organizations in fintech.

Ali (2023), the researchers pointed out that financial organizations have adopted many authentication foundations in order to ensure a high level of security and privacy in fintech services. Among these techniques is **two-factor authentication or multifactor authentication**, which includes the password in addition to the OTP one-time password in order to ensure a high level of authentication. For financial data within electronic accounts. In addition to using a password and fingerprint in order to secure authorized access for individuals. The study concluded that multifactor authentication is feasible and provides a higher degree of security. The study also showed that this method of verification was able to provide a higher level of performance compared to other methods such as pattern and password.

Moallem (2021) many emerging organizations and stakeholders prefer biometric authentication methods for many reasons, including that these methods are specific to individuals and can distinguish each individual from another. On the other hand, these biometric methods have advantages that include being **non-transferable and non-replicable**, which increases the level of security of the services provided by fintech. These methods differ from previous techniques based on passwords and codes in that they prevent repetition and prevent repudiation. The study also confirmed that although these techniques are effective, using them alone is not enough and there is a need for **multifactor authentication** in order to ensure a higher level of data and account security.

Dahia et al. (2020) indicated that the shortcomings and insecurities that have arisen as a result of relying on legacy authentication methods have led to the need for continuous authentication. This method is based on requiring **continuous authentication** by individuals' electronic applications in order to identify and reconfirm their identity more than once during the session in order to ensure that there is no unauthorized access. This appears in contrast to traditional authentication, which occurred only once at the beginning of the session. The study reached the conclusion that this method contributed significantly to enhancing efforts towards protecting accounts and ensuring a higher level of security by preventing unauthorized access, as re-authentication more than once requires entering biometric data more than once in order to ensure that the person entering the account is authorized to be inside it.

Gomaa et al. (2022) argued that among the recent authentication approaches in fintech is through depending on **anti-spoofing measures**. This technology played an effective role in combating all forms of impersonation by relying on biometric standards in order to ensure authorized entry. It has also been sensitive to **spoofed biometric authentication**, which involves attempting to trick biometric systems by providing false or manipulated biometric samples, such as fake fingerprints or facial images.

According to the previous studies, and launching from the results accompanied each study. There appeared a literary gap in terms of identifying the rule of biometric authentication and its characteristics and its influence on fintech services. In other words, most of the studies took into perspective aspects of biometric measures or some of its characteristics and applied on the concepts of (account). Such accounts could be financial, academic or even social media accounts. Researcher uncovered that there was a lack in adopting biometric authentication characteristics on fintech services on particular.

Launching from that literary gap, current study aimed to examine the role of biometric authentication in fintech in increasing security of financial services from perspective of IT managers departments within banking industry in Jordan. The characteristics taken into account included “Unique Biological Traits, Multifactor Authentication, Non-Replicable, Continuous Authentication, and Anti-Spoofing Measures”.

In order to unravel that relationship between variables adopted, researcher built the following model from which the study hypotheses were extracted:

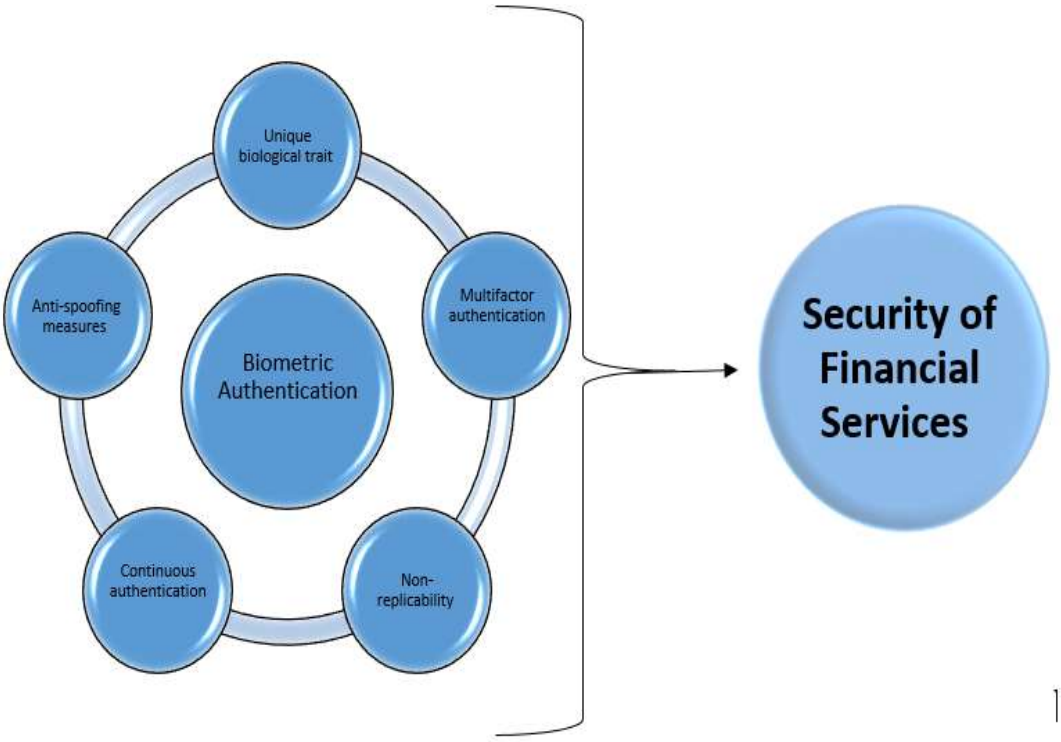

Figure 1. Study Model **Wang (2021); Dubey (2019); Meng et al. (2019); Ali (2023); Moallem (2021); Dahia et al. (2020); Gomaa et al. (2022)**

According to the study model, the following set of hypotheses was reached:

Main Hypothesis:

H: The biometric authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

Sub-Hypotheses:

H1: Unique biological trait can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

H2: Multifactor authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

H3: Non-replicability can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

H4: Continuous authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

H5: Anti-spoofing measures can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

It is worth mentioning that the current study was launched through the underpinning theory of **(Human-Computer Interaction HCI)**. This theory was coined back in (1983) by authors of the renounced book "The Psychology of Human-Computer Interaction" which was presented by Allen Newell, Thomas P. Moran and Stuart K. Card. In the current study, the starting point of the theory is based on the idea of interaction between a computer and a human and how this interaction occurs as a type of biometric authentication between the human and the system in order to ensure an effective, friendly user experience based on privacy and security.

2. Theoretical Referential

2.1. Financial Technologies "Fintech"

Technological development in the world have changed the nature of its operations and service providing. Technology managed to invade every sensitive aspect of life including education, medicine and finance (Tan and Chung, 2023). Now, banks and financial institutions are familiar with presenting their services through the means of technology in in the heist quality that a human has witnessed (Meng et al., 2019). Financial technologies fintech was a results of such development in the financial arena. Fintech refers the process of presenting financial services through technological means such as smart phones applications, online digital payments, online crowdfunding, personal financial management and robo advisors (Manggala et al., 2022; Kumar, 2023).

According to Abbas et al. (2023), the massive orientation towards fintech in financial services has opened the door of piracy and online fraud. Many organizations and individuals started to question the authenticity of data security and the ability of these technologies to protect their money and their privacy when they dealing with their finances online. This has led to the appearance of authentication which is an approach that is used by financial institutions and banks in order to protect the privacy of their clients and secure their financial information and accounts (Khan et al., 2023). Wang (2023) argued that authentication in fintech is a process in which users' identity is verified in real time in order to grant an individual or organization access to financial services.

From the point of view of Gopal et al. (2023) and AlKasasbeh et al. (2023), authentication is actually a process aimed at ensuring that there is a high level of security and sufficient ability to protect consumers in order to ensure financial accounts from fraud and hacking. As indicated by Nigam et al. (2022); Abuarqoub (2019); Bao and Youl (2021); Bukola (2020), there are many types of authentication, including the following:

- Password authentication: It relies on a strong password supported by various computer symbols and forms, and its effectiveness is coupled with constant change.
- Two-factor authentication: a type of authentication that requires the use of more than one security method and authentication process, such as a password and OTP.
- Biometric authentication: type of authentication that relies on the unique characteristics of individuals, such as the iris, fingerprint, facial features, or voiceprint.
- Smart authentication: This type of authentication relies on machine learning and artificial intelligence in order to analyze specific patterns and behaviors that are sufficient to identify individuals.
- Joint authentication: This type of authentication depends on combining more than one verification method, such as a password, a fingerprint, or even the iris and a unique number sequence, and it provides a high level of security and privacy.

2.2. Biometric Authentication in Financial Services

Many studies argued that biometric authentication measures are the most suitable and secured in order to protect and secure private data and information. Such measures are based on the accuracy and effectiveness of the programs used in order to use the unique characteristics of people, which cannot be repeated between two people. According to Wang (2021); Dubey (2019); Meng et al. (2019); Ali (2023); Moallem (2021); Dahia et al. (2020); Gomaa et al. (2022) characteristics of biometric measures included:

Unique Biological Traits

Unique biological traits refer to biometric measures which depend on special and inherited aspects of a human like an iris scan, fingerprint, voice recognition and facial features. Those are traits that can't be identical in two persons, even if they were identical twin, they can reach a certain level of similarity but it is impossible for them to be identical especially when it comes to iris scan and fingerprint. Many financial institutions depend on those in order to make sure that there is always a valid access to the financial accounts. Such measures appeared to be highly secured and protective but they have faced many challenges, as they are all human biological aspects that are exposed to change. Such challenges included sickness, swollen in the face or teeth, faded voice, or even inflammation in the iris.

Multifactor Authentication

This type of authentication is based on using dual measures. For example it may depend on asking for more than one authentication process and gathers them to makes sure that the access is valid. Many financial organizations today have used this multifactor authentication to process transactions like a password with an OTP (one time password). They are using also a combination between a fingerprint and an iris scan at the same time. This was proved a very effective methodology in order to guarantee a higher level of accounts' security and validity.

Non-Replicable

One the characteristics of biometric measures is the fact that it is not replicable which makes it hard to mimic of copy. An iris scan or a finger print won't be replicable as they are inherited traits and they are connected to each individual person. The fact that such measures aren't replicable is valid even on identical twins.

Continuous Authentication

Biometrics measures in financial services are based now on continuous authentication. This means that a session is interrupted every once and while in order for the user to re-enter the biometric data again and verify their entrance to the account. Many bank applications are now adopting this approach. It basically gives a user a certain amount of time and them it logs the user out and ask for a verification. This continuous authentication puts into perspective possible hackers and/pirate who are using the internet for fraud.

Anti-Spoofing Measures

The concept of anti-spoofing refers to the software that is able to locate and identify any fake sample of a biometric authentication. Some hackers may depend on a collecting fake sample of authenticating measures like a high definition of an iris scan or a copy of a fingerprint. This is easy to identify by anti-spoofing software which is able to locate the fake samples and prevent the invalid access.

3. Methodology

3.1. Methodological Approach

Quantitative methodology was adopted in realizing the aim of current study. The reason for adopting the quantitative approach is attributed to its ability to depend on a larger sample size. This would help in increasing chances of generalizability of reached results. In addition to that, depending on a questionnaire as a tool eases the process of primary data collection compared to depending on interviews through qualitative approach.

3.2. Tool of Study

Researcher built a questionnaire in order to be the main tool for primary data collection. The questionnaire consisted of two main sections; the first took into perspective demographic of study sample (age, qualification and experience). While the other section consisted of statements related to the study sub-variables as in table 1.Validity of questionnaire items were tested through arbitration from four specialist academics in the field. The accepted statements were left and the noted statements were modified according to requirements.

Table 1. Distribution of Statements on Variables

Variable	**# of Statement**
Biometric Authentication	
Unique Biological Traits	5
Multifactor Authentication	5
Non-Replicable	5
Continuous Authentication	5
Anti-Spoofing Measures	5
Security of Financial Services	8
Total	33

Source: Questionnaire

3.3. Population and Sampling Techniques

Population of study consisted of IT managers within banks in Jordan during the fiscal year 2021-2022. The sample was derived from total of (25) banks in Jordan, including (16) local Jordanian banks, divided into (13) commercial banks and (3) Islamic banks, in addition to (9) foreign banks, including (8) commercial banks, and one Islamic bank. According to the Central Bank of Jordan, banks operate through 818 branches and 76 offices. A convenient sample of (100) IT managers was chosen to represent the study population. After application process, researcher was able to retrieve (63) properly filled questionnaire which indicated a response rate of (63%) as statistically accepted.

3.4. Screening and Analysis

Statistical Package for Social Sciences SPSS was chosen in order to mitigate and screen the gathered primary data. Reliability test was done on study questionnaire in order to test the

reliability and consistency of study questionnaire through identifying Alpha value as according to table 2. Other statistical tests included collinearity test, multiple and linear regression.

Table 2. Alpha Value

variable	**α**
Unique Biological Traits	0.791
Multifactor Authentication	0.88
Non-Replicable	0.797
Continuous Authentication	0.80
Anti-Spoofing Measures	0.816
Security of Financial Services	0.845

Source: SPSS

4. Results and Discussion

4.1. Demographic Results

Table 3 indicated that majority of respondents were males forming (81%) of the sample who held BA degree forming 85.7%. in addition to that, table indicated that majority of respondents had an experience in the field that for more than 10 years forming 49.2% of the total sample.

Table 3. Demographic Results

	f	**%**
Gender		
Male	51	81.0
Female	12	19.0
Education		
BA	54	85.7
high studies	9	14.3
Experience		
Less than 5 years	13	20.6
5-9	19	30.2
+10	31	49.2
Total	**63**	**100.0**

Source: SPSS

4.2. Questionnaire Analysis

Mean and standard deviation of responses to questionnaire were calculated. Results in table 4 indicated that all statements were positively received as they all scored a mean that was higher than mean of scale 3.00. The highest variable was (**Anti-Spoofing Measures**) and scored 4.03/5.00 compared to the lowest variables mean 3.87/5.00 and were (Unique Biological Traits and Continuous Authentication) but still positive as it was higher than mean of scale.

Table 4. Questionnaire Analysis

Statement	μ	σ
Unique traits of individuals are used as an authentication tool	3.714	1.099
Biometric traits include iris pattern, fingerprints, and facial features	3.635	1.235
Biometric traits can't be the same in individuals even in identical twins	4.032	.983
Biometric traits can be the similar in twins but not identical	3.873	1.055
Biometric traits are hard to replicate which make them more secure	4.143	.981
Unique Biological Traits	**3.879**	**.793**
Multifactor authentication ensures more than one secure gate to protect data	3.714	1.099
Multifactor authentication include using double security like PINs, voice recognition, tokens, and fingerprints combined	3.984	.942
Multifactor authentication guarantees that one out of multiple security gates are secured	3.968	.983
This approach guarantees a higher level of security for data	4.127	.959
Multiple forms of verifications decreases hacking and piracy efforts	3.968	.983
Multifactor Authentication	**3.952**	**.817**
Even identical twins don't have the same biometric traits	4.063	1.030
Biometric traits can be duplicated or transferred	4.238	1.088
Such traits are inherited and not gained from the environment which makes them hard to replicate	3.857	1.162
Biometric traits can't be stolen, copied, or even mimicked	3.984	1.129
This makes biometric traits the safest tools for accessing financial accounts	3.810	1.045
Non-Replicable	**3.990**	**.734**
The users' session are authenticated multiple times for security	3.619	.958
This prevents the unauthorized accessed, piracy or/and hacking	3.810	.948
Once the safe session is over, the user is logged out electronically	3.825	.890
Multiple wrong trials locks the user outside the account and require another authenticated operations	4.079	.867
Once the user loses control they have to re-authenticate themselves	4.063	.931
Continuous Authentication	**3.879**	**.685**
Anti spoofing means the ability to detect fake biometric samples	3.905	1.011
All e-financial services are supported with multiple Anti spoofing measures	4.111	.882
Complicated software are used in anti spoofing including liveness detection	4.111	.900
Anti spoofing software is able to identify life indicators	4.032	.967
They are able to locate and differentiate between real and fake biometric traits.	4.016	.907
Anti-Spoofing Measures	**4.035**	**.709**
Increased security of financial services influence reputation of banks /financial institution	3.714	1.007
Level of security in financial services is able to influence level of loyalty and satisfaction of clients	3.968	1.015
Adopting smart business approaches means to focus more on security of financial services	4.095	.893
Sensitivity of banking sector increases the need for more secure approaches to financial accounts	4.032	.915
Low security level of financial service negatively impact the performance of the bank/financial institution	3.841	1.066

Low security level of financial service negatively impact market share of the bank/financial institution	4.016	1.024
Financial institution can significantly enhance fintech services through biometric measures	4.000	1.047
Biometric authentication can locate unauthorized access, identity theft, and fraudulent activities.	4.032	.967
Security of Financial Services	**3.962**	**.688**

Source: SPSS

4.3. Multicollinearity Test

In order to assess the existence of multicollinearity among the independent variables, the Variance Inflation Factor (VIF) and Tolerance measures were computed for each variable. The discovered findings were presented in table 5. The table shown above displays data indicating that the Variance Inflation Factor (VIF) values are less than 10, while the Tolerance values surpass 0.10.

Table 5. Multicollinearity

variable	**Tolerance**	**VIF**
Unique Biological Traits	.265	3.778
Multifactor Authentication	.169	5.907
Non-Replicable	.200	4.998
Continuous Authentication	.379	2.639
Anti-Spoofing Measures	.286	3.501

Source: SPSS

4.4. Hypotheses Testing

Multiple regression was used in order to test the realization of the main hypothesis argued "**The biometric authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry".** It was seen that correlation coefficient of r = 0.906, suggested a strong and statistically significant relationship between the independent and dependent variables. Moreover, empirical evidence has shown that the independent factors account for **82%** of the observed variability in the dependent variable. Furthermore, the investigation demonstrated that the F value exhibits statistical significance at a significance level of 0.05. This discovery suggests that biometric authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

Table 6. Main Hypothesis Testing

Coefficients

	Unstandardized Coefficients		Standardized Coefficients				
Model	B	Std. Error	Beta	t	Sig.	R	R Square

1	(Constant)	.245	.247		.995	.324	.906[a]	.820
	Unique Biological Traits	.012	.095	.013	.122	.904		
	Multifactor Authentication	-.022	.115	-.026	-.193	.848		
	Non-Replicable	.103	.118	.110	.878	.384		
	Continuous Authentication	.118	.092	.117	1.285	.204		
	Anti-Spoofing Measures	.716	.102	.738	7.026	.000		

Source: SPSS

Linear regression was used in order to test sub-hypotheses presented in the study. Findings of analysis were as follows:

The first hypothesis scored a correlation coefficient of r = 0.691 with a strong and statistically significant relationship between the independent and dependent variables. Empirical evidence has shown that the independent variable accounts for **47.8%** of the observed variability in the security of financial services variable. F value has statistical significance at a significance level of 0.05. The present discovery suggests that Unique biological trait can increase security of financial services from the perspective of IT specialists in Jordanian banking industry.

In the second hypothesis, correlation coefficient of r = 0.673 was scored and there was a strong and statistically significant relationship between the independent and dependent variables. The independent variable accounts for **45.4%** of the observed variability in the security of financial services variable. F value has statistical significance at a significance level of 0.05. The present discovery suggests that Multifactor authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry.

In the third hypothesis correlation coefficient of r = 0.711 appeared with a strong and statistically significant relationship between the independent and dependent variables. Empirical evidence has shown that the independent variable accounts for **50.6%** of the observed variability in the security of financial services variable. F value has statistical significance at a significance level of 0.05. The present discovery suggests that Non-replicability can increase security of financial services from the perspective of IT specialists in Jordanian banking industry.

The fourth hypothesis scored a correlation coefficient of r = 0.74, and there was a strong and statistically significant relationship between the independent and dependent variables. Empirical evidence has shown that the independent variable accounts for **54.7%** of the observed variability in the security of financial services variable. F value has statistical significance at a significance level of 0.05. The present discovery suggests that Continuous authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry.

The fifth hypothesis indicated a correlation coefficient of r = 0.899, it suggested a strong and statistically significant relationship between the independent and dependent variables. Empirical evidence has shown that the independent variable accounts for **80.9%** of the observed variability in the security of financial services variable. F value has statistical significance at a significance level of 0.05. The present discovery suggests that Anti-spoofing measures can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

Table 7. Sub-Hypotheses Testing

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients				
		B	Std. Error	Beta	t	Sig.	R	R Square
1	(Constant)	1.636	.318		5.147	.000	.691[a]	.478
	Unique Biological Traits	.600	.080	.691	7.468	.000		

H1: Unique biological trait can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients				
		B	Std. Error	Beta	t	Sig.	R	R Square
1	(Constant)	1.721	.322		5.352	.000	.673[a]	.454
	Multifactor Authentication	.567	.080	.673	7.116	.000		

H2: Multifactor authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients				
		B	Std. Error	Beta	t	Sig.	R	R Square
1	(Constant)	1.300	.342		3.799	.000	.711[a]	.506
	Non-Replicable	.667	.084	.711	7.906	.000		

H3: Non-replicability can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients				
		B	Std. Error	Beta	t	Sig.	R	R Square
1	(Constant)	1.079	.341		3.165	.002	.740[a]	.547
	Continuous Authentication	.743	.087	.740	8.583	.000		

H4: Continuous authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry

Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients				
	B	Std. Error	Beta	t	Sig.	R	R Square

1	(Constant)	.439	.222		1.975	.053	.899[a]	.809
	Anti-Spoofing Measures	.873	.054	.899	16.073	.000		
H5: Anti-spoofing measures can increase security of financial services from the perspective of IT specialists in Jordanian banking industry								

Source: SPSS

4.5. Discussion

Current study aimed at shedding the light on the role of biometric authentication in increasing security of fintech services within banking sector in Jordan. Quantitative methodology was used and an online questionnaire was distributed on a sample of (63) IT managers within banks in Jordan operating during the fiscal year 2021-2022. Characteristics of biometric authentication used in the study included (Unique Biological Traits, Multifactor Authentication, Non-Replicable, Continuous Authentication, and Anti-Spoofing Measures). SPSS was employed to mitigate gathered primary data. Results of study accepted the main hypothesis which argued, "Biometric authentication can increase security of financial services from the perspective of IT specialists in Jordanian banking industry" with a correlation coefficient of (0.906) and a variance of (82%).

Concerning the chosen sub-variables of study which included (Unique Biological Traits, Multifactor Authentication, Non-Replicable, Continuous Authentication, and Anti-Spoofing Measures). It was seen that they all scored a high correlation and a variance with the dependent variables and they all had an influence on security of financial services. The highest influence was scored by the variable (anti-spoofing measures) which appeared with a strong correlation of 0.899 and a variance of 80.9%. This indicated that the anti-spoofing measures that are adopted by banks had the ability to support the security of financial services through making sure to prevent all trials and actions that may jeopardize the financial services through hacking, piracy and unauthorized usage of financial accounts. This came in agreement with Gomaa et al. (2022) who argued that Anti-Spoofing plays a crucial role in protecting customers and sensitive financial data in digital banking services. It contributes to maintaining security and trust, reducing the risks of fraud and counterfeiting, and enhancing customers' experience in using online banking services.

In the second rank there appeared the concept of continuous authentication which scored a correlation of 0.74 with a variance that reached **54.7%** with the dependent variable. This indicated that the process of continuous authentication and the ongoing demand for an authentication when a person is inside a financial accounts puts a limit to unauthorized usage and controls the session in which a person can use a financial account. This came in agreement with Dahia et al. (2020).

The variable of non-replicability came in the third rank with a correlation of r = 0.711 explaining a variance of 50.6%. This result agreed with Moallem (2021) and Wang (2021) non-transferable and non-replicable / multifactor authentication who argued that the non-transferable and non-replicable characteristic of biometric authentication make it hard to mimic and control the fraud in financial services. This is based on the fact that there wouldn't be an approach to replicate or transfer a code of a pass order that is based on a biometric element like fingerprint, voice recognition and facial features.

In the fourth and fifth rank came both sub-variables of uniqueness with a correlation of r = 0.691 and an explained variance of **47.8%**, multi-factor authentication scored a slightly lower

influence with r = 0.673 and variance of **45.4%** but still highly influential. Such results agreed with Meng et al. (2019) and Ali (2023) and Gomaa et al. (2022).

5. Conclusion

Results of study indicated what is taken for granted in data security field, depending on biometric measures for authentication is based on a high level of security and safety as science and medicine proved before "there is no identical biometric trait between two people at all. The trait may be somewhat similar, but it is impossible for it to be identical". However, given that study managed to prove and accept its hypothesis, one question might be raised under the circumstances of biometric authentication. This question revolves around what if meaning that, what if a certain person loses their biometric trait, how this can be resolved?

5.1. Practical and Theoretical Implications

Carrying out the current research and realizing its aim was based on theoretical and practical implications. From a theoretical perspective, the research was able to shed the light on the ability of biometric authentication to be a valid tool for protecting and securing financial data and information. It also ensured the importance of IT specialists in figuring out the best and most secured biometric authentication to be used within the Jordanian banking sector.

As for the practical implication, the study can guide both clients and decision makers to choose the most suitable biometric authentication according to their needs and preferences.

5.2. Limitations of Study

The study was limited to the following

- Banks operating in Jordan (national and foreign) during the fiscal year 2021-2022
- Only IT department point of view were subjected to the questionnaire
- Study was limited to opinion and there were not financial reports, data or information involved in carrying out analysis and results

5.3. Recommendations

Launching from results and conclusion presented above, researcher recommended:

- Increase individuals' and organizational awareness on the importance of authentication and the fact that it is still exposed to malfunction and errors
- Increase the measures used in order to protect financial accounts by both individuals and organization by using dual-authentication

5.4. Future Studies

According to what was mentioned in the study, researcher suggested:

- Carrying out a research that examines the factors and drivers that encourages individuals to adopt biometric authentication measures.
- Examining the challenges that accompany the adoption of biometric authentication among individuals like exposure to accidents that affects fingerprints, voiceprints and facial features.

References

Abbas, N. N., Ahmad, R., Qazi, S., & Ahmed, W. (2023). Investigation of Trust Models to Alleviate the Authentication Challenge in FinTech. In Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications (pp. 174-191). IGI Global.

Abuarqoub, A. (2019). D-FAP: Dual-factor authentication protocol for mobile cloud connected devices. Journal of Sensor and Actuator Networks, 9(1), 1.

Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2020). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. IEEE Internet of Things Journal, 8(1), 65-84.

Al_Kasasbeh, O., Khasawneh, O., & Alzghoul, A. (2023). The Real Effects of Fintech on the Global Financial System. International Journal of Professional Business Review, 8(3), e01725-e01725.

Ali, G. (2023). Development of a secure multi-factor authentication algorithm for mobile money applications (Doctoral dissertation, NM-AIST).

Alorfi, A. S., Yonbawi, S., Alahmari, S., Bozorboevich, A. A., Arumugam, M., & Huy, P. Q. (2023). Biometric authentication integrated with wireless communication malicious activity detection in a cyber physical system-based Fintech banking. Optik, 272, 170294.

Bao, D., & You, L. (2021). Two-factor identity authentication scheme based on blockchain and fuzzy extractor. Soft Computing, 1-13.

Bukola, A. (2020). Development of an anti-theft vehicle security system using gps and gsm technology with biometric authentication. Int. J. Innov. Sci. Res. Technol.

Dahia, G., Jesus, L., & Pamplona Segundo, M. (2020). Continuous authentication using biometrics: An advanced review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(4), e1365.

Dubey, V. (2019). Fintech-Digital way of ID Verification and Biometric Verification in 2020. International Journal of Innovation and Applied Studies, 27(4), 896-901.

Gomaa, A., Rashed, O., Refaey, A., Mohamed, A., Sayed, M., & Rashwan, M. (2022, October). A new framework for an eKYC system. In 2022 20th International Conference on Language Engineering (ESOLEC) (Vol. 20, pp. 11-18). IEEE.

Gopal, S., Gupta, P., & Minocha, A. (2023, May). Advancements in Fin-Tech and Security Challenges of Banking Industry. In 2023 4th International Conference on Intelligent Engineering and Management (ICIEM) (pp. 1-6). IEEE.

Khan, H. U., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2023). Role of authentication factors in Fin-tech mobile transaction security. Journal of Big Data, 10(1), 138.

Kumar, H. (2023). A Study on Role of Fintech Services Impact of Business Growth Selected a Public Sector Bank in Punjab. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 8(5), 5.

Manggala, M. P., Wahidah, I., & Hanuranto, A. T. (2022, March). Security And Usability of User Authentication for Fintech Data Protection in Indonesia. In 2022 International Conference on Decision Aid Sciences and Applications (DASA) (pp. 546-550). IEEE.

Meng, W., Zhu, L., Li, W., Han, J., & Li, Y. (2019). Enhancing the security of FinTech applications with map-based graphical password authentication. Future Generation Computer Systems, 101, 1018-1027.

Moallem, A. (2021). Understanding Cybersecurity Technologies: A Guide to Selecting the Right Cybersecurity Tools. CRC Press.

Nigam, D., Patel, S. N., Raj Vincent, P. M., Srinivasan, K., & Arunmozhi, S. (2022). Biometric authentication for intelligent and privacy-preserving healthcare systems. Journal of Healthcare Engineering, 2022.

Quintal, K., Kantarci, B., Erol-Kantarci, M., Malton, A., & Walenstein, A. (2019). Contextual, behavioral, and biometric signatures for continuous authentication. IEEE Internet Computing, 23(5), 18-28.

Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous multimodal biometric authentication schemes: a systematic review. IEEE Access, 9, 34541-34557.

Suryono, F., & Sara, R. (2022, January). Application of Authentication in Peer to Peer Lending Fintech Transactions to Maintain the Confidentiality of Personal Data. In Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia.

Tan, S. F., & Chung, G. C. (2023). An Evaluation Study of User Authentication in the Malaysian FinTech Industry With uAuth Security Analytics Framework. Journal of Cases on Information Technology (JCIT), 25(1), 1-27.

Wang, J. S. (2021). Exploring biometric identification in FinTech applications based on the modified TAM. Financial Innovation, 7(1), 42.

Wang, J. S. (2023). Verification techniques in FinTech compared from user perspectives. Social Science Computer Review, 41(4), 1438-1455.

Xu, J. (2022). Biometrics in FinTech: A Technological Review. Future and FinTech, The: Abcdi and Beyond, 361.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization, 29(2), 105-117.