Gardan, D.A., State, O., Gardan, I.P., Baicu, C.G., Hristea, A.M., Moise, D. (2024), "Acceptance of Biometric Payment Security Technology among Romanian Consumers", *Transformations in Business & Economics*, Vol. 23, No 2 (62), pp.510-532.

---------TRANSFORMATIONS IN --------
BUSINESS & ECONOMICS

ACCEPTANCE OF BIOMETRIC PAYMENT SECURITY TECHNOLOGY AMONG ROMANIAN CONSUMERS

[1]Daniel Adrian Gardan
Faculty of Economic Sciences
Spiru Haret University
Fabricii Street no 46G
030045 Bucharest
Romania
Tel.: +407 3 7165 996
E-mail: danielgardan@gmail.com

[2]Olimpia State
Faculty of Business and Tourism
Bucharest University of Economic Studies,
Piața Romana 6, Sector 1,
010374 Bucharest
Romania
Tel.: +407 2 3695 011
E-mail: state.olimpia@com.ase.ro

[3]Iuliana Petronela Gardan
Faculty of Psychology and Education Sciences,
Spiru Haret University
Fabricii Street no 46G
030045 Bucharest
Romania
Tel.: +407 2 6456 420
E-mail: petronela.gardan@spiruharet.ro

[4]Claudia Gabriela Baicu
Institute for World Economy,
Romanian Academy,
Casa Academiei, Calea 13 Septembrie No 13, Sector 5,
050711 Bucharest
Romania
Tel.: +407 2 3317158
E-mail: baicuclaudia70@yahoo.ro

[5]Anca Maria Hristea
Faculty of Accounting and Management Information Systems
Bucharest University of Economic Studies
Piața Romana 6, Sector 1,
010374 Bucharest
Romania
Tel.: +407 2 3394 210
E-mail: anca.hristea@cig.ase.ro

[6]Daniel Moise
Faculty of Marketing
Bucharest University of Economic Studies
Piața Romana 6, Sector 1,
010374 Bucharest
Romania
Tel.: +407 2 1530 980
E-mail: moisedaniel@mk.ase.ro

[1]Daniel Adrian Gardan, PhD, is an Associate Professor at the Spiru Haret University and PhD advisor in the field of Marketing at the doctoral School from "Dunărea de Jos" University of Galati. He has extensive experience as a reviewer or editor for various Journals (Frontiers in Nutrition, Journal of Theoretical and Applied Electronic Commerce Research, Energies etc.). His research interests cover topics like consumer behaviour, mobile media marketing, content marketing, technology acceptance models etc.

[2]Olimpia State (*corresponding author*) PhD, is an Associate Professor at Bucharest University of Economic Studies, Vice-Dean in charge of researching activity and international relationships for the Faculty of Business and Tourism, member of the Romanian Association of Journalists in Tourism, co-founder of CACTUS Association - Academic Research in Tourism and Services and of Academic Research Centre in

Tourism and Services within the Bucharest University of Economic Studies. She has research interests in the field of AI applications in business and tourism, human resources management, operational techniques in tourism, and organisational culture.

[3]**Iuliana Petronela Gardan**, PhD, is an Associate Professor at Spiru Haret University, with extensive experience as a reviewer or editor for valuable Journals like Frontiers in Nutrition, Journal of Pacific Rim Psychology, Journal of Financial Services Marketing etc. Her research interests include technology acceptance models, consumer psychology, mobile media marketing etc.

[4]**Claudia Gabriela Baicu**, PhD, is a Scientific Researcher III, at the Institute for World Economy, the Romanian Academy. Her research interests include international payments, international banking, international trade, green finance.

[5] **Anca Maria Hristea**, PhD, is an Associate Professor at Bucharest University of Economic Studies and a member of the Romanian Society of Economic and Financial Analysis, with extensive experience on research projects. Her research interests include global diagnosis of organisation, economic-financial analysis, business valuation, real estate investments analysis, entrepreneurship, business games or quality management.

[6]**Daniel Moise**, PhD, is an Associate Professor at Bucharest University of Economic Studies, Faculty of Marketing. His research interests include events marketing, strategic marketing, international marketing, public relations.

Received: November, 2023
1st Revision: January, 2024
2nd Revision: April, 2024
Accepted: May, 2024

ABSTRACT. ***More than ever the need to assure the security of online channels and the interface between online and offline transactions is very present and very important for business customers and individuals alike. Our paper investigates the validity of a model comprising variables specific to TAM (technology acceptance model) and UTAUT (Unified Theory of Acceptance, and Use of Technology) that explains the complex relationship between factors that can influence the adoption of biometric security technology with direct application in the financial services and payments field. The research made on a final validated sample of 1057 individuals filtered to be active users of biometric security devices and applications shows that performance expectancy along with facilitating conditions and social influence have a pretty well-defined effect on the perceived utility of the biometric technology, effect translated with the help of trust and intention to use towards usage behaviour.***

KEYWORDS: biometric payment security, technology acceptance model, consumer behaviour.

JEL classification: M41, C83, L20.

Introduction

The essential characteristic of what we call in the present time biometric-based technology relies on the technical capacity to automate the use of physiological, biological, genetic and behavioural features that can assess or authenticate the identity of a person, his or her uniqueness (Ceyhan, 2008). The term itself - "biometrics", was coined using two words derived from the Greek "bios" – meaning life and "metrikos" – meaning measurement, measure (Faundez-Zanuy, 2005; Ceyhan, 2008).

One of the first times that we may find referrals to something similar to biometrics can be considered the information according to which in ancient China there has been the use of fingerprints to authenticate individual property (Ceyhan, 2008). Another example is related to the custom of ancient Egyptian pottery makers to use fingerprints to authenticate their work. More recently, in the nineteenth century, biometrics was officially introduced within police activity through the work of Alphonse Bertillon in the field of anthropometrics to help the identification of recidivists' criminals due to their unchanging individual characteristics.

Within this framework of biometric security technology usage, the use of this technology in the field of securing financial transactions has also gained an important role in developing modern financial operations. Nowadays, one of the most preeminent concepts that are influencing also consumption patterns in the field of financial services across the world is the one referring to digital identity. According to Chui *et al*. (2023), digital identity may be considered the sum of digital information that can characterize and distinguish an individual or an entity (Chui *et al*., 2023). To ensure the security of such identities, technologies such as biometrics, devices and authentication applications have been used on a large scale to ensure which information is shared and to whom. Also, technological advancements have made possible the idea of "converged identity" that can bring different dimensions of the identity of a person into a single platform which allows multiple roles for one individual – from employee to customer or business partner (Chui *et al*., 2023).

Biometric payment cards present some advantages for all involved participants: consumers, banks/issuers, and merchants. Consumers benefit from secure and fast contactless payment. Besides, there is no limit on the amount paid. Among others, issuers have the opportunity to get higher transaction fees and to improve their relationship with the clients. Finally, biometric payment cards do not require modification of the POS equipment of the merchants. Also, this innovative method can contribute to reducing queuing time within stores (Smart Payment Association, 2021).

The growing importance of the use of fingerprint authentication for payments is also revealed by a survey performed by Statista in 2021. According to the survey's results, the respondents willing to change the use of PIN codes when paying in stores with the use of fingerprints account for 94 per cent of all respondents from Saudi Arabia and 69 per cent of respondents from the United States (Statista Research Department, 2023). All these represent relevant dimensions of the readiness to use biometric technologies for payments from both the bank's and the client's perspective.

Moreover, the relevance of biometric payment technology is stressed by ARATEK, which considers that it "is quickly becoming the new way to pay" (ARATEK, 2023). In line

with this, Goode Intelligence forecasts that the number of people using biometric payments by 2023 will reach the level of 2.6 billion (Burt, 2018). Acuity Market Intelligence predicts that by 2022 biometrically-enabled mobile devices will allow about one trillion Cloud-based biometric transactions annually. Annual biometric transaction revenue is also projected by Acuity to strongly increase from $474 million in 2017 to $18 billion in 2022 (Acuity Market Intelligence, 2017).

Despite the many advantages that can be pointed out for biometric-based security technologies one of its main drawbacks is that biometric data is not secret and cannot be replaced after being compromised by a third party (Wayman *et al*., 2005; Kravchenko *et al*., 2021) and some barriers can be highlighted when we talk about the adoption of biometric-based devices: physical invasiveness, information invasiveness, ease of use, privacy, and the perceived level of benefit from the device. (Liu, Silverman, 2001; James *et al*., 2006).

Our paper is proposing a study that investigates with the help of a tested conceptual model the effect of different variables upon the adoption and usage of biometric security technology in the field of payment operations or financial-related services. To do so, we have started from the consecrated TAM (technology acceptance model) and UTAUT (Unified Theory of Acceptance, and Use of Technology) approach and we have grounded our proposed model into the specific scientific literature at the level of each advanced hypothesis, and we have empirically tested the validity of the model with the help of a quantitative type of research based on an online survey. The results and discussions present specific information regarding the acceptance of each hypothesis and highlight the effect of variables such as safety perception (SP), facilitating conditions (FC), social influence (SI), expected effort (EE), performance expectancy (PE), anxiety determined by a forced transition to the new technology (ATT) upon usage behaviour (UB), mediated through perceived utility (PU), trust (TR) and intention to use (IU). The conclusions of the paper emphasize the main results and highlight possible limitations of our research and future directions for other such endeavors.

1. Literature Review and Hypothesis Development

In the following, we will briefly investigate a series of relationships that can be established between different variables that have been studied within the scientific literature as being a part of the TAM (technology acceptance model) and UTAUT (Unified Theory of Acceptance, and Use of Technology). The sum of these relationships will be conceptualised into the form of a theoretical model capable of grasping the process of adoption in the case of biometric security technology.

The first variable taken into discussion is the one referring to safety perception (SP) and its possible relationship with the perceived utility (PU).

In research made on a sample of 112 managers from Vietnamese companies, regarding intentions to use cloud-computing software, results have shown that perceived usefulness and perceived ease of use had positive impacts on the enterprises' intentions to use cloud-based accounting software (Le, Cao, 2020). Also, other studies have indicated that the perceived value is a predictor of behavioural intention to use the technology (Popa *et al*., 2023). In another setting, research made by Chen (2015) showed that perceived safety and privacy positively affect perceived usefulness and perceived ease of use of information technology. These results can be completed with results obtained by Ardiansah *et al*. (2020), which have shown the increased intention to use e-payment-specific technology when users have more positive impressions about the software safety and privacy of e-payments (Ardiansah *et al*.,

2020). Different authors, referring to different technology contexts have shown that the modified behaviour toward the acceptance of the new technology is sustained from the point of view of the decisional process to adapt to new requirements, the predicted results by the perception of safety and security offered by the technology that can act as a mediator between ease of use or perceived utility and purchase intentions (McCoy *et al*., 2007; Viehland, Leong, 2007; Kabir *et al*., 2015; Lai, 2017). This means that perceptions about safety offered by the technology are an important factor that influences the perceived utility and in advance the intention to use it. Taking into consideration all the above, we can issue the following hypothesis: ***H.1. Safety Perception (SP) in the case of biometric security technology use positively influence the perceived utility of this technology (PU).***

A second variable that is analysed refers to the facilitating conditions (FC) and the possible relationship with the perceived utility.

Facilitating conditions can be seen from different angles if we take into consideration the specific process of adoption of new technologies at the level of individual consumers and respectively business consumers (Dinu *et al*., 2021; Junsawang *et al*., 2022; Machova *et al*., 2023). At the level of individual consumers, facilitating conditions refer to different elements regarding the capacity of a person to connect with a certain technology and use it. Such elements may refer to financial resources, time and know-how, the usage of other technologies that are facilitating the access to the new one etc. Facilitating conditions may have at the level of individual consumers also the function to influence behaviours and intentions pretty much like the behavioural control encountered within the Theory of Planned Behaviour (Ajzen, 1991).

In the case of business consumers, facilitating conditions can refer to the elements of infrastructure or how the company is organised elements that can help the organisation to use properly the specific technology (standards, logistics, procedures and methodologies, etc.) (Venkatesh *et al*, 2003).

Other authors consider that facilitating conditions, (doesn't matter the type of consumer analysed - individuals and businesses alike), are essential for the adoption process of technology and for the perceived utility at the same time (Ocloo *et al*., 2020; Dvorsky *et al*., 2023). In the same time, facilitating conditions, which can manifest in a particular way at the level of individual consumers and business consumers alike impacts also the degree of the technology adoption and thus the level of utility perceived (Venkatesh *et al*., 2011).

Taking into account the above considerations we may issue the following hypothesis: ***H.2. Facilitating conditions (FC) regarding the use of biometric security technology positively influence the perceived utility of this technology (PU).***

Among variables that are important when we want to assess technology acceptance, we may consider social influence (SI).

Many authors have considered that the adoption of various technologies is influenced directly by the social influence exerted at the level of social groups or social networks (Micu *et al*., 2017). Thus, social influence has been accounted from various perspectives. One of the first is related to the fact that a certain person can be influenced by the degree to which other persons from his or her social network are actively using a specific technology (Venkatesh *et al*, 2003). Another perspective is the one that considers the notion of subjective norms or social factors, a perspective that is encountered within innovation diffusion theory (Clemes *et al*., 2014). The subjective norm was defined as being the perception that can be realised at the level of a person about the fact that he or she has to take into account other people that are important within his or her social group opinion regarding if he or she has to perform a certain

behaviour. Thus, the impact of social influence on technology acceptance can be seen as the outcome of a process through which individuals assess the importance of a new technology taking into account perceptions and approval from others from their inner social circle (Ingham *et al*., 2015; Hu *et al*., 2019; Nagy *et al*., 2023).

In the process of adopting a new technology, the individuals will gain with the help of internalisation a positive perception of the utility of the new technology. A very important distinction can be made from this point of view between the first version of the Technology Acceptance Model (TAM) and the second version of this model. Within TAM 1, the subjective norm was considered to have a clear effect on the intention to use technology in a mandatory setting, while it does not have a strong effect in a voluntary setting. This means that a certain person will have the intention to use or adopt the technology as a result of the opinions and actions of other important people especially within a mandatory setting (like an organisational one for example). In the case of TAM 2, with the help of the internalisation process, compliance will occur not only in a mandatory setting but also in a voluntary one. Thus, the individuals may perceive positively the utility of the new technology as a result of the internalisation of other relevant people's beliefs.

In the case of biometric security technology social influence importance is given by the specificity of the usage of such a technology. Considering all of the above there is another hypothesis that can be issued: ***H.3. Social influence (SI) perceived in the case of biometric security technology positively influences the perceived utility of this technology (PU).***

A fourth important variable will refer to the expected effort (EE) that can be implied by the use of the new technology.

Expected effort or "effort expectancy" is a variable encountered within the UTAUT framework, being related to the previous variable defined within the TAM and TAM2 framework, meaning perceived ease of use. This was referring to the fact that the degree of effort needed for a new technology usage can affect the performance expected from that technology. Actually, within the scientific literature, the perceived ease of use is related to intention and has an impact on the perceived usefulness (or utility). An important detail that can be highlighted is the fact that perceptions about ease of use are differentiated from the ones regarding social influence (Venkatesh, Davis, 2000).

Expected effort is dealing at a basic level with the degree to which a technology can be easily used if the technology gives the user the feeling of simplicity and easiness, different studies assess that when a particular technology is perceived as being simple to use, the adoption process is favourable (Amofah, Chai, 2022).

In the case of biometric security technology, Miltgen *et al*. (2013) highlight that perceived ease of use of biometric methods has a positive effect directly upon the intention to accept the technology and indirectly through perceived usefulness (Miltgen *et al*., 2013).

Effort expectancy can be related to other external variables such as convenience, perceived safety and hygiene (James *et al*., 2006). The same idea stems from the research conducted by Chan *et al*, 2010 in which convenience was an important factor that determined the adoption and use of electronic government services (Chan *et al*., 2010).

Therefore, following all of the above we can issue hypothesis H4 - ***Expected effort (EE) to use biometric security technology positively influences the perceived utility of this technology (PU).***

The fifth variable, which refers to performance expectancy (PE), is one of the variables used on a large scale within studies concerning the intention to use and behaviour (Miltgen *et al*., 2013). Performance expectancy is related to the perception that a certain

individual can have about the degree to which using a certain technology can raise the level of quality of the current activity in which he or she is implied (Venkatesh *et al*., 2003). In the context of biometric security technology usage, we can consider performance expectancy as the degree to which this technology can give substantial benefits to a person (the possibility of authenticating very easily and securely, the possibility prove the identity needed for a financial transaction, possibility to perform various task without the assistance of the banking – financial institution staff etc.).

A study conducted in Nigeria sought to explore the adoption of biometrics by applying a modified UTAUT model. An innovative aspect developed by the authors consisted of addressing the problem from three different contexts: individual, implementation and technological. Their findings show that simpler biometric systems – such as fingerprints- have a higher level of intention to use in comparison with more complex biometric methods (e.g., DNA recognition). In terms of the intention to adopt biometrics, the identified influencing factors were: perceived ease of use (PEU), perceived security, facilitating conditions, self-efficiency and technological compatibility (Akinnuwesi *et al*., 2016).

Taking account of all the above, we may issue hypothesis H5 - ***Performance expectancy (PE) related to biometric security technology positively influences the perceived utility of this technology (PU).***

The usage and adoption of a technology that has an important stake – the one related to the need to secure financial transactions and operations or different settings that imply the preservation of the user identity - has an important connection with the idea of risk perception (Zahrani, 2021). In the scientific literature, the concept of risk has been widely addressed by different studies, even from the 1960s, developed an entire theory about risk to explain the impact of this concept on consumers' decisions (Lin, 2008; Taburchak, *et al*., 2022).

The perceived risk dimension is determined by the type of product or service that is analysed, and the type of risk consists of six different dimensions that can cover the impact of new technology (biometric security one being as well counted) (Lee, 2009; Soto-Beltrán *et al*., 2022): Safety-privacy risk, Financial risk, Social risk, Time risk, Performance risk.

The problem regarding the perceived risk in the case of financial transactions and payments can be strongly connected with the one related to the degree of anxiety determined by the transition to a new technology. This can imply a certain amount of pressure that users can feel because the new technology can reduce the risks and provide a better solution from this point of view than the older one. That means individuals can feel a certain amount of anxiety due to their incapacity to embrace the new technology in a short time. To reduce this anxiety, the utility of the new technology becomes evident, thus the anxiety can be counted among the factors that are emphasising the perceived utility of the biometric security technology.

Taking into account all the above implications, we may issue hypothesis H6 - ***Anxiety determined by the forced transition to new technology (ATT) positively influences perceived utility for new biometric security technology (PU).***

Prior studies state that safety perceptions of technology in the financial sector are not based on direct practical use of biometrics, but on other external contexts such as electronic banking (Tassabehji, Kamala, 2009). This idea highlights the fact that within the development of financial banking operations and transactions, the implementation of e-banking was a first challenge, followed by the introduction of biometric technology. This means that safety perception and trust have a special relationship within the biometric security technology field, with studies showing that perceived biometrics effectiveness significantly influenced the

strength of the relationships between both perceived privacy and perceived security with trust (Normalini, Ramayah, 2017).

Recent research shows that nowadays consumers interact on a larger scale day by day with biometric security technology (through their mobile devices) and there is a lack of evidence about safety or performance risks (Soto-Beltrán *et al*., 2022). Such situations can positively influence attitudes and intentions to use this technology because a higher safety perception is provided for the mass of consumers.

Therefore, we may issue hypothesis H7 - ***Safety Perception (SP) in case of biometric security technology positively influence Trust related to the use of this technology (TR)***

One of the most preeminent variables used within technology acceptance models over time is the one referring to the perceived utility or perceived usefulness. From the very beginning of the TAM model definition for the first time in 1987, perceived utility was associated with the idea that a certain technology can have a clear utility for people in relation to a particular situation of consumption. Some studies have evaluated the perceived utility attached to different e-payment technologies (Liébana-Cabanillas *et al*., 2018; Francisco *et al*., 2015; Gefen *et al*., 2003; Pavlou, 2003; Nguyen, Huynh, 2018).

The results of the above studies show a relationship between perceived usefulness and trust in technology that goes in both directions. Trust can be an antecedent for the perceived utility of the technology, and at the same time, the perceived utility has a certain influence on trust in the technology (Dinu *et al*., 2022).

Taking into account these conditions, we may issue hypothesis H8 - ***Perceived utility for biometric security technology (PU) positively influences perceived trust related to the use of this technology (TR).***

One of the focal points that can be found in both TAM models (1 and 2) refers to the positive influence that perceived usefulness can have on the intention to use a new technology.

In the field of biometric technology usage, research made on 583 Chinese tourists showed that perception of trust in the biometric technology and consequently their intention to use it was influenced by perceived ease of use that was also differentiated taking account of the type of biometric technology – with the fingerprint scan technology being the most trusted and accepted (Pai *et al*., 2018). Another research carried out by James *et al*. (2008) has found that both the perceived ease of use and perceived usefulness have had a direct influence on the intention to use biometric devices.

Another research made on bank customers regarding their attitude toward the usage of biometric devices to improve e-banking security has revealed that user perceptions of biometric security positively influenced their attitude and intention to use biometric banking. The perceived utility of biometric security and self-efficacy have a positive influence on the intention to use (Tassabehji, Kamala, 2009). Taking account of all the above, we may issue hypothesis H9 - ***Perceived utility for biometric security technology (PU) positively influences intention (IU) to use this technology.***

Another variable that has a prominent role in the process of technology adoption is the one referring to trust. Trust (TR) is associated with an individual belief that the interaction with another individual is developing responsibly. With a direct reference to biometric security technology, the importance of assessing risks that are related to the disclosure of personal data is a vital one. The perceived risk and the degree of trust are linked to particular decisions, in the field of biometric security technology risks are usually related to privacy and identity (Thiesse, 2007). Research made on a sample of UK respondents demonstrated a

model in which trust in technology and concern for data privacy are influencing perceived risk and the latter influence behavioural intentions (Miltgen *et al*., 2013).

In a certain technology usage context, trust was able to increase the perception of certain information and the fear raised by risks regarding the expected behaviour in the case of e-payments (Kim, Benbasat, 2006). In the research conducted by Nguyen and Huynh (2018), perceived risk and trust have the principal role along with perceived usefulness and ease of use within the structural model of e-payment adoption. Both because of the dominance of trust in the existing literature and because the biometric system demands the cooperation of individuals with little ability to monitor or control those operating it, trust is an important factor when considering biometric technology acceptance. Privacy concerns indicate that people are willing to act to protect it (Cho *et al*., 2009), thus the intention to use a technology that can increase the level of trust is more than conclusive.

Therefore, it can be drawn from hypothesis H10 that trust ***related to the use of this technology (TR) positively influences intention (IU) to use this technology.***

In the majority of studies regarding acceptance of technology, the intention to use the technology is directly linked with the actual usage of the specific technology. The same direct relation can be evaluated within the biometric security technology acceptance setting.

Research made on Australian respondents regarding the application of TAM within the framework referring to the palm vein authentication technology has demonstrated that attitudes towards using have a direct strong influence over the behavioural intention and actual use of the technology (Nakisa *et al*., 2022).

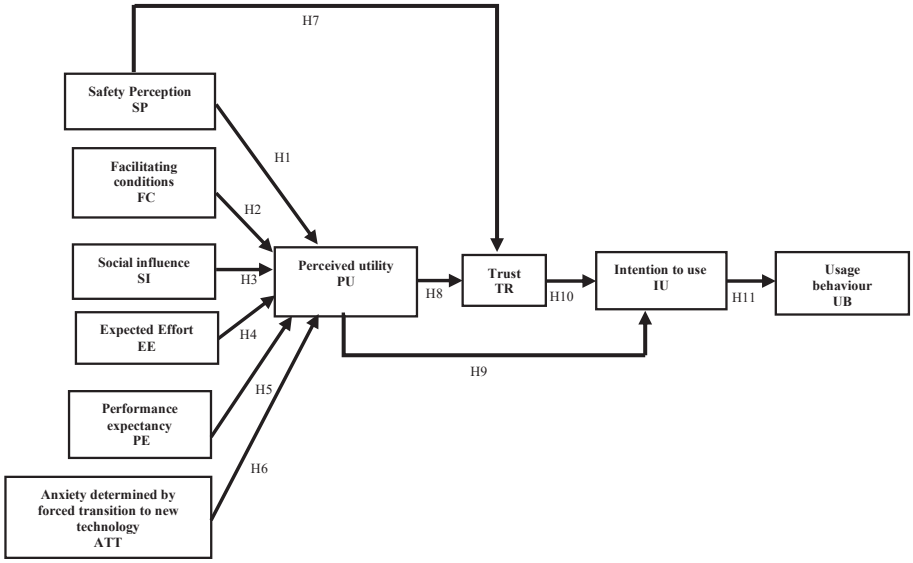
In another research, 751 hotel customers have been tested regarding their behavioural intention to use and adopt devices and applications. The research has shown in the context of TAM implementation that the adoption behaviour was linked to intentions (Kim, 2016).

A study made to investigate the acceptance and use of Behavioural Biometric Continuous Authentication technology (Skalkos *et al*., 2021) has revealed that intention to use the technology has antecedents like perceived vulnerability, perceived severity and perceived response efficacy and goes into the direction of actual usage for this specific technology.

Another context, referring to the adoption of the biometric system within the consumption occasion regarding restaurant guests, showed that customers of restaurant-type services are ready to adopt this technology, their decision being influenced primarily by their perceptions regarding the degree of usefulness and security associated with the biometric-based technology. In their effort to assess the adoption of biometric technology authors have used the TAM model adding variables referring to the perceived security of biometric systems and perceived innovativeness toward information technology (Morosan, 2011; Phonthanukitithaworn *et al*., 2016).

All the ideas above give us the possibility to issue hypothesis H11 - ***Intention (IU) to use biometric security technology positively influences Usage behaviour (UB) regarding this technology.***

The emphasised relationships between variables can be synthesised into the form of a coherent theoretical model that assumes the link between six types of factors on one hand and three mediating variables and usage behaviour variable on the other hand, to explain the acceptance of biometric security technology by users in the field of financial transactions and buying processes. In the figure below, we have represented the proposed conceptual model taking account of all eleven hypotheses, and the effect carried by the corresponding variables.



Source: created by the authors.

Figure 1. **The Proposed Research Conceptual Model**

The proposed model is built on the well-known structure of the TAM model but has also variables very similar to the ones used by the UTAUT 2 model, and two variables – the safety perception (SP) and anxiety determined by forced transition to new technology (ATT) that have been specifically proposed to describe better the factors implied by the biometric security technology acceptance.

The validation of the proposed model can explain satisfactorily the process of adopting a technology that has a lot of implications at the level of nowadays security needs and preferences of individuals toward online transactions.

2. Methods

The present study proposes to explore the background and the process implied by biometric security technology consumption and acceptance by users. Thus, we employed a quantitative type of research based on an online survey methodology. The sample adequacy was assured taking into account the fact that young people have been envisaged as being early adopters of new technologies, implicitly new technologies that are dealing with online and digital security issues (Magis-Weinberg *et al*., 2021; Duleepa *et al*., 2023). Also, the fact that men are more likely to adopt new electronic and IT-related technologies was an important starting point in the construction of the relevant sample. To ensure the adequacy of the sample used for the research we have taken into consideration different sources from the literature review regarding the behaviour of individuals in terms of computer-related technology and electronic-related new technologies comprising biometric security.

Thus, different authors point out that there are gender differences in terms of technology usage, with females being less comfortable than men with computer and electronic-related technologies (Lowe, Krahn, 1989; Frenkel, 1990; Beyer, 2008; Karsten,

Schmidt, 2008; He, Freeman, 2010). In a research made on 461 respondents from the US that tested the degree of acceptance of a camera face detection technology in the workplace, women were significantly less inclined to accept this technology than men (Stark *et al*., 2020). Another research made on a sample of 70 respondents, in the form of a questionnaire survey and testing experiment, shows that male respondents are more aware of biometric technology than female respondents, respondents above 28 years of age consider biometric security based on keystroke more robust than the traditional security in front of attacks, the higher degree of education was related with the positive willingness to use face detection technology and a higher level of trust in this technology. At the same time, a higher degree of education was correlated with a lower degree of concern about privacy (El-Abed *et al*., 2010).

Taking account of these assumptions, our sample comprised a volume of 1057 individuals, with more than 64% of them males and approximately 35% being at the secondary school level of education followed by 30.2% of master's degree holders and 26.4% undergraduate level. The structure of income categories shows a prevalence of 27.9% of the individuals with monthly income between 2001-3000 lei (approx. 402-603 euros), followed by the ones having a monthly income above 6000 lei (approx. 1206 euros).

In terms of age intervals, the majority are between 18 and 25 years of age (44% of the respondents), followed by the interval between 26 and 35 years of age (23.9% of the respondents). The explicit structure of the final validated sample can be seen in *Table 1*.

Table 1. Research Sample structure

Variable	Items	N	%
Gender	Female	373	35.3%
	Male	684	64.7%
Level of finalised studies	Secondary school	376	35.6%
	Higher education	279	26.4%
	Master degree	319	30.2%
	Doctoral Degree	83	7.9%
The monthly income of the respondent	Under 2000 lei	131	12.4%
	2001-3000 lei	295	27.9%
	3001 – 4000 lei	167	15.8%
	4001-5000 lei	125	11.8%
	5001–6000 lei	102	9.6%
	Above 6000 lei	237	22.4%
Age	18-25 years of age	465	44.0%
	26-35 years of age	253	23.9%
	36 – 45 years of age	168	15.9%
	46 – 55 years of age	152	14.4%
	56-65 years of age	19	1.8%

Notes: * the income groups expressed in euro are: under approx. 402 Euro; approx. 402–603 Euro; approx. 604–804 Euro; approx. 805-1005 Euro; approx.: 1006-1206 Euro; 1206 Euro and over (level of National Bank of Romania exchange course on 28 September 2023).

Source: own calculations.

After the selection of the suitable profile of the selected population, questionnaires have been sent with the help of an online platform toward completion within July 2023. The

number of valid completed questionnaires has consisted of 1057 integral completed questionnaires from an initial number of 1634 questionnaires sent in the first phase.

Within the questionnaire, we have set two filter questions to select the respondents that are presenting the features of active users of biometric security technology (fingertip, retina scan etc.). Only people who own a device capable of interacting with this type of technology and who currently use the technology were considered. The measurement of the variables in the questionnaire was carried out by using the 7-step Likert scale (Jebb *et al*., 2021; Phakiti, 2020).

The questionnaire had a total number of 16 questions, each question corresponding to one of the constructs considered in the proposed model – safety perception (SP), facilitating conditions (FC), social influence (SI), expected effort (EE), performance expectancy (PE), anxiety determined by the forced transition to the new technology (ATT), trust (TR), perceived utility (PE), intention to use (IU), usage behaviour (UB). These constructs and the items corresponding to them from within the questionnaire have been adapted from the relevant scientific literature considering TAM and UTAUT variables.

3. Results

Confirmatory factor analysis was used to assess the validity of the conceptual model proposed (*Figure 1*). The validity and reliability of the constructs from the model were tested through the determination of factor loadings, Cronbach's Alpha for internal consistency reliability of the scale, Kaiser-Meyer-Olkin (KMO) values for sampling adequacy for each variable in the model, the Average Variance Extracted (AVE) values for the convergence validity of the constructs, and the composite reliability (CR) for discriminant validity.

Lower KMO values may indicate that the data are not as suitable for these analyses and that a different approach may be needed (Shrestha, 2021). In the case of the present research, it can be observed that the values fall within the upper limits (*Table 2*), which means that the data set is suitable for factor analysis.

In conclusion, it can be stated that factor analysis can be used since the latent variables determined starting from the initial items are valid from the point of view of the commonality of the items (Kaiser-Meyer-Olkin test) and the consistency of the measurement scale (Cronbach's Alpha).

Following the exploratory factor analysis, a confirmatory factor analysis was performed to assess the relevance of the relationships that exist between the model variables using the IBM-SPSS AMOS 20.0 program.

Table 2. Values of indices regarding the degree of validity and reliability of the constructs from the proposed model

Construct	Item	Factor Loadings	Cronbach's Alpha	KMO	AVE	CR
Safety perception	SP1	0.764	0.902	0.851	0.574	0.843
	SP2	0.764				
	SP3	0.780				
	SP4	0.722				
Facilitating conditions	FC1	0.764	0.894	0.839	0.595	0.854
	FC2	0.775				
	FC3	0.790				
	FC4	0.755				
Social influence	SI1	0.705	0.976	0.859	0.523	0.815

Table 2 *(continuation*). Values of indices regarding the degree of validity and reliability of the constructs from the proposed model

Construct	Item	Factor Loadings	Cronbach's Alpha	KMO	AVE	CR
	SI2	0.740				
	SI3	0.707				
	SI4	0.741				
Expected effort	EE1	0.808	0.977	0.925	0.640	0.899
	EE2	0.809				
	EE3	0.799				
	EE4	0.810				
	EE5	0.777				
Performance expectancy	PE1	0.759	0.976	0.878	0.604	0.859
	PE2	0.785				
	PE3	0.782				
	PE4	0.783				
Anxiety determined by the forced transition to new technology	ATT1	0.782	0.976	0.884	0.644	0.879
	ATT2	0.811				
	ATT3	0.813				
	ATT4	0.803				
Trust	TR1	0.810	0.992	0.950	0.643	0.915
	TR2	0.795				
	TR3	0.785				
	TR4	0.788				
	TR5	0.816				
	TR6	0.816				
Perceived utility	PU1	0.829	0.990	0.893	0.716	0.910
	PU2	0.857				
	PU3	0.845				
	PU4	0.854				
Intention to use	IU1	0.827	0.953	0.777	0.688	0.869
	IU2	0.834				
	IU3	0.827				
Usage behaviour	UB1	0.839	0.983	0.790	0.666	0.857
	UB2	0.811				
	UB3	0.797				

Notes: factor Loadings > 0.7; Cronbach's Alpha> 0.7; KMO > 0.7; AVE>0.5; CR>0.7 (Hair *et al*., 2010; Shrestha, 2021).

Source: own calculations.

Table 3. Values of indices regarding the degree of validity and reliability of the constructs from the proposed model

Model-Fit index	P	CMIN/ DF	NFI	RFI	IFI	TLI	CFI	RMSEA	PNFI	PCFI
Research obtained values	0.000	2,949	0.958	0.954	0.966	0.963	0.966	0.041	0.880	0.887
Accepted fit	< 0.05	< 5	< 0.95	> 0,90	> 0,90	> 0,95	> 0,95	< 0.05	> 0.50	> 0.50

Notes: source for accepted fit: Iacobucci, 2010; Marsh, Hocevar, 1985; Igalla, Edelenbos, van Meerkerk, 2021; Tabachnick, Fidell, 2006; Field, 2013; Hooper *et al*., 2008; Hu, Bentler, 1999.

Source: own calculations.

Test results can be declared eligible by the criteria in the previous *Table 3*, namely the criteria of P, CMIN/DF, NFI, RFI, IFI, TLI, CFI, RMSEA, PNFI, PCFI, and so that all hypotheses proposed in this study can be explained. Thus, in *Table 4*, below you can see the results of the structural model that demonstrate the validity of the advanced hypotheses.

Table 4. The structural model results

Paths	Path Coefficients	S.E.	C.R.	p-value	Hypotheses and decision
SP → PU	0,120	0,049	2,449	0,003	H1—Supported
FC → PU	0,261	0,051	5,096	0,000	H2—Supported
SI → PU	0,274	0,026	10,571	0,000	H3—Supported
EE → PU	0,138	0,048	2,859	0,004	H4—Supported
PE → PU	0,472	0,036	12,972	0,000	H5—Supported
ATT → PU	0,116	0,043	2,699	0,004	H6—Supported
SP → TR	0,177	0,015	11,649	0,000	H7—Supported
PU → TR	0,827	0,015	56,587	0,000	H8—Supported
PU → IU	0,914	0,041	22,568	0,000	H9—Supported
TR → IU	0,143	0,040	3,577	0,002	H10—Supported
IU → UB	1,031	0,016	65,141	0,000	H11—Supported

Notes: C.R. is greater than 1.96, p-value < 0.01.

Source: own calculations.

According to the table, we may consider the advanced hypotheses validated and the conceptual model proposed as being a viable one. This means that variables referring to Safety Perception (SP), Facilitating Conditions (FC), Social Influence (SI), Expected effort (EE), Performance Expectancy (PE), and Anxiety determined by the new technology (ATT) have a positive effect on perceived utility (PU) for biometric security technology. From the above group of listed variables, the Performance Expectancy has the most powerful effect on PU, while anxiety determined by the new technology (ATT) has the weakest effect with a β of 0.116, CR=2.699 The relationship between listed variables and perceived utility highlighted until now, means that hypotheses from H1 to H6 are supported. The effect of safety perception (SP) upon trust (TR) is moderate with a β of 0.177, and CR=11,649, sustaining hypothesis H7 while the effect exerted by perceived utility over trust is very strong with a β of 0.827 and CR=56,587, meaning that also the hypothesis H8 is being supported.

A strong influence is registered in the case of perceived utility (PU) over the intention to use, a correlation that proves the acceptance of hypothesis H9. In contrast, the greatest influence is exerted by intention to use (IU) over usage behaviour (UB) with a β of 1.031 and CR= 65,141, also proving the acceptance of hypothesis H11.

The above-highlighted results show the validity of the conceptual model proposed and are opening the path to extract certain valuable conclusions about the relationship between the considered variables within the model.

The first hypothesis from the model stated that safety perception in the case of biometric security technology use positively influences the perceived utility of this technology. The results show that the hypothesis was accepted, meaning that people who are concerned about the safety of the technology in terms of errors that can appear within online transactions, the possibility that personal information regarding payments can be stolen and the storage of such information or sharing with webservers is not safe are considering that the biometric payment security technology can improve their quality of life or reduce substantially the time spent with payments.

The second hypothesis deals with the relationship between facilitating conditions regarding biometric security technology and the utility attached to this. The positive relationship shows that people having the resources necessary to use the technology (devices capable of using biometric ways to secure payments, access to the internet, etc.) are considering the technology as being useful in everyday life. More and more people have the

means today to access biometric technology with statistics that are showing a general positive trend for the upcoming years as we stated already in the introduction of our paper (https://www.visa.co.th/).

The positive relationship between possible social influence exerted in the case of this technology and the perception of its utility is acknowledged within hypothesis no. 3 and shows that there is a direct link between perceptions that rely on the importance of this technology within social groups of the respondents, and its utility, maybe since more and more people are embracing it. Also, the results show that people consider the opinions of other individuals from their social groups as being positive about biometric technology, with a favourable perception of the utility of the technology.

Hypothesis H4 sheds light on the relationship between the expected effort associated with the usage of biometric technology and the perceived utility. The results are confirming the relation with emphasis on the positive perception of the simple user interface (the item loading of 0.810).

Hypothesis H5 addresses the relationship between performance expectancy and perceived utility. The results show the direct link between these variables, with a strong influence exerted at the level of perception related to the increasing speed of the transactions offered by the new technology (item loading of 0.785). The perception regarding the expected performance was having the strongest influence among the first group of six variables from the model confirming results from other research (Miltgen *et al*., 2013).

In the case of hypothesis H6, the acceptance of this hypothesis leads us to the idea that the pressure exerted by the need to adopt a better, new technology is directly related to such an emotionally driven need – the need for secure actions that are implying money transfer, payments etc. has indeed a direct effect upon the degree in which people are perceiving the intrinsic utility of such a technology. The items with the biggest loading (0.811 and 0.813) refer to the fear of making mistakes when using the technology and the lack of confidence that the technology can be completely understood and used. The latest result goes in the direction of general anxiety caused by the overwhelming rhythm of the latest state-of-the-art technologies development speed (like the ones based on AI's latest implementation in a variety of IT products and services) (Torkzadeh, Angulo, 1992; Harrison, Lucassen, 2019; Hsieh *et al*., 2020; Henderson, Corry, 2021; Meuter *et al*., 2003; Capatina *et al*., 2020; Sejera, Bocarnea, 2022).

Hypothesis H7 moves toward the relationship between safety perception (SP) and trust (TR) regarding biometric security technology. According to the results, the influence is moderate, with a stronger effect exerted at the level of concerns regarding the secure storage of payment information (item loading of 0.780). People are more willing to trust the new biometric technology if they are sure about the possibility of storing securely any information regarding financial transactions. These results are in line with other conclusions from previous research also (Ogbanufe, Kim, 2018).

Hypothesis H8 was concerned about the influence of perceived utility (PU) on trust. Results are showing a strong relationship with a direct influence between the two variables, a stronger effect being measured at the level of perceptions about the degree of usefulness in everyday life and the possibility of reducing the amount of time for payments. If we assume that perception of trust is built with the help of a continuous positive input at the level of repeated usage of a certain technology, also in the case of biometric security technology the sense of utility builds upon consistent positive perception over repeated usage of this

technology seems to be a strong factor for development of trust in the technology (Ogbanufe, Kim, 2018).

Hypothesis H9 has an important degree of similarity with hypothesis H8, being concerned about the influence of perceived utility (PU) on intention to use the technology (IU). Again, our results confirm a strong correlation between these variables, a fact shown in other studies as well (James *et al*., 2006; Miltgen *et al*., 2013; Kanak, Sogukpinar, 2017).

Hypothesis H10 refers to a widely demonstrated relationship in the context of technology adoption in general – the one concerning the influence of the degree of trust on the degree of intention to use a certain technology. Also, in the case of our results, this influence appears to be pretty well represented with a stronger effect measured at the level of willingness to overcome the perceived risk, as a measure of trust in the technology (item loading of 0.816) and at the level of perceptions about the trust in future benefits of the biometric security technology usage (item loading of 0.816). This idea is also sustained by other studies as well (Pai *et al*., 2018; Kanak, Sogukpinar, 2017).

Hypothesis H11 gives a final touch to the tested model, proposing the influence of intention to use biometric security technology over the usage behaviour of this technology. Our results are confirming this relationship, actually being the most powerful effect measured at the level of our model. This means that people who express their intention to use it clearly remain consequent to their decision regarding the effective usage of it. The effect was very clear at the level of the item referring to the effort toward the intention to "always use biometric payment security technology in my daily life" (item loading of 0.834), and frequency of using the technology (item loading of 0.839). Our results are sustained by the previous literature in the field regarding the usage of biometric technologies (James *et al*., 2006; Moriuchi, 2021; Stylios *et al*., 2022; Hizam *et al*., 2021).

Conclusions and Discussion

Biometric security technology represents a complex field that has evolved through time shaped by factors with a social, economic and technological background. As this technology was implying a lot of innovation, it was facing a proportional amount of social, cultural, and legal constraints. The degree of acceptance depends on the social and cultural values that are prevailing within the targeted population.

The future development expected for biometric security technology will imply the full implementation of more robust and safe methods based on 3D image usage technologies, an approach that allows a superior degree of safety for a diversified range of fields like e-commerce, access control, immigration, Internet banking, law enforcement etc. (Dargan, Kumar, 2020). At the same time, specialists appreciate that the development of the degree of AI integration with biometric technology will offer the possibility for different types of biometric security like facial recognition to be used at a very large scale as a viable alternative to the traditional methods (like PIN or cards) for payments in retail chains and service providers (Zhong *et al*., 2021).

The potential of biometric security technology is important as the need to ensure security at different levels and in different settings is a nowadays reality. If we assess the larger picture, the security of individuals, institutions, organisations, states and even modern society as a whole represents a very complex background with a lot of implications at different levels, affected by numerous factors like globalisation, international migration, terrorism, military conflicts etc. If we narrow our analysis only to the potential implications of

the biometric security technology in the field of financial transactions and operations, we still may find a lot of future potential applications, which can optimize these activities and ensure the security of individuals' and organizations' assets, investments and the full plethora of financial operations.

The purpose of our study was to assess the complex process of adoption of biometric security technology in the field of financial services and payments, with the help of a model based on TAM and UTAUT-derived variables, completed with a specific variable defined as "anxiety determined by the forced transition to a new technology".

The results have shown a great deal of influence on performance expectancy, followed by social influence and facilitating conditions over the perceived utility of biometric security technology. The importance of performance expectancy is given by the positive perception of people about the speed that can be obtained for financial transactions using biometric technology. The other variables, meaning social influence and facilitating conditions, complete the picture as they contribute to the effect related to the perceived utility. The aspects related to the means used to access biometric technology – smartphones, devices and software capable of interacting with the capacity of the device to scan the fingerprint or retina of the users-are playing an important role in the construction of the positive perception of people about the utility of the technology. At the same time, positive perceptions of the members from the social groups of the respondents regarding the usage and utility of biometric technology have contributed to the degree of utility perceived by them.

Although the variable that was used to measure aspects regarding the possible anxiety that may occur in front of the impossibility of using any more traditional ways to ensure security (like passwords, email notifications etc.) did not exert the biggest influence in comparison with the other 5 variables considered as factors for the biometric technology perceived utility, there has been a clear effect of the fear not to make mistakes when using the technology and a certain degree of lack of confidence related to the level of understanding the technology.

The influence of safety perception on trust in the technology depends on the perception of the people if the storage of their personal information is safe even of the level of biometric characteristics. Also, the success rate for repeated usage of the technology is a strong factor for trust development. The willingness to overcome perceived risk and the acceptance of future benefits of the technology usage are also important elements within the process of acceptance of the technology. Our model has had a particular approach meaning that was proposes a clear relationship between the perceived utility of the technology and the intention to use both as a direct relation and as a mediated one. The perceived utility will be the base to build a strong intention to use with a superior engagement given by the trust in the technology. We think that the "triangle" consisting of safety perceived utility, trust and intention to use is essential in case of the biometric security technology. In comparison with other new technology acceptance processes, biometric security must deal with a certain specific pressure given by the importance of the need for security that has become more and more common in the last twenty years. In the present time, consumers and businesses alike have a huge dynamic of relationships, and among them, the management of financial assets is a big priority. The new virtual economy and the digitalisation of businesses have imposed models of business that are capable of fully integrating information technologies and online, digital transactions. Therefore, financial operations that come along with e-commerce transactions have to be managed properly with tools and methods capable of offering efficiency and a certain degree of optimisation over time. The security of transactions and

identity information of users is essential for this optimisation. Digitalisation and the virtual online business environment have come with specific challenges regarding the danger that sensible information could be exposed and the finalisation of the transactions to be affected (Dima *et al*., 2023).

Our research has contributed to the assessment of the biometric technology adoption process in the field of financial services by Romanian consumers. There is a very complex process in which the importance of the need for secure financial transactions is translated into specific requirements and factors that express the utility of this technology for users. Thus, the expected performance given by the ease of use and the speed associated with biometric technology, along with the social influence given by the positive opinion of users' social network members about this technology and the importance of facilitating conditions are the main drivers for the perceptions about the degree of usefulness of the technology. Perceived utility constructed by the contribution brought by all the six variables taken into consideration is essential to determine the manifestation of the intention to use biometric technology. In this equation, trust empowered by safety perception about biometric technology has a special role also in the augmentation of the intention to use because of the special nature of the needs that are behind the usage of biometric security technology.

The results of the research may have some practical implications for financial institutions that are willing to promote their products or software capable of offering the possibility to use biometric security technology to ensure the security of their client's transactions. The promotional effort developed to engage clients and to differentiate from the competition may be built on the idea that people rely on their peers' perceptions about the utility of this technology and the net performance gain in making faster financial transactions (Riaz *et al*., 2022).

The research has also a couple of limitations due to the structure of the sample and the need to better assess variables capable of grasping specific aspects of the need for security. In this respect, qualitative research may represent a possible future line of investigation to test more variables that can be taken into consideration when the problem of security is deeply analysed. Another limitation may stem from the fact that our research was not personalised for each type of biometric security method available (facial scan, retina scan, fingerprint scan, palm scan, etc.). It is possible that different methods have different factors that influence their adoption and different perception from the consumers.

References

Acuity Market Intelligence (2017), *Biometrics in The Cloud to Authenticate More Than One Trillion Transactions Annually by 2022, Cision PR Newswire*, 04 December, available at, https://www.prnewswire.com/news-releases/biometrics-in-the-cloud-to-authenticate-more-than-one-trillion-transactions-annually-by-2022-300565686.html, referred on 5/05/2023.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational behavior and human decision processes*, Vol. 50, No 2, pp.179-211, https://doi.org/10.1016/0749-5978(91)90020-T.

Akinnuwesi, B.A., Uzoka, F.M.E., Okwundu, O.S., Fashoto, G. (2016), "Exploring biometric technology adoption in a developing country context using the modified UTAUT", *International Journal of Business Information Systems*, Vol. 23, No 4, pp.482-521, https://doi.org/10.1504/IJBIS.2016.080219.

Amofah, D.O., Chai, J. (2022), "Sustaining Consumer E-Commerce Adoption in Sub-Saharan Africa: Do Trust and Payment Method Matter?", *Sustainability*, Vol. 14, No 14, 8466, https://doi.org/10.3390/su14148466.

ARATEK (2023), *What is biometric payment and what are the benefits?*, 18/2/2023, available at, https://www.aratek.co/news/what-is-biometric-payment, referred on 5/05/2023.

Ardiansah, M., Chariri, A., Rahardja, S., Udin, U. (2020), „The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance", *Management Science*

Letters, Vol. 10, No 7, pp.1473-1480, https://doi.org/10.5267/j.msl.2019.12.020.
Beyer, S. (2008), "Gender differences and intra-gender differences amongst management information systems students", *Journal of Information Systems Education*, Vol. 19, No 3, pp.301-310.
Burt, C. (2018), *Goode Intelligence forecasts 2.6 billion to use biometrics for payments by 2023*, BIOMETRIC UPDATE.COM, October 19, available at, https://www.biometricupdate.com/201810/goode-intelligence-forecasts-2-6-billion-to-use-biometrics-for-payments-by-2023, referred on 5/05/2023.
Capatina, A., Kachour, M., Lichy, J., Micu, A., Micu, A.E., Codignola, F. (2020), "Matching the future capabilities of an artificial intelligence-based software for social media marketing with potential users' expectations", *Technological Forecasting and Social Change,* Vol. 151, February, 119794, https://doi.org/10.1016/j.techfore.2019.119794.
Ceyhan, A. (2008), "Technologization of security: Management of uncertainty and risk in the age of biometrics", *Surveillance & Society*, Vol. 5, No 2, pp.102-123, https://doi.org/10.24908/ss.v5i2.3430.
Chan, F.K., Thong, J.Y., Venkatesh, V., Brown, S.A., Hu, P.J., Tam, K.Y. (2010), "Modeling citizen satisfaction with mandatory adoption of an e-government technology", *Journal of the Association for Information Systems*, Vol. 11, No 10, pp.519-549.
Chen, L.Y. (2015), "Determinants of Software-as-a-Service Adoption and Intention to Use for Enterprise Applications", *International Journal of Innovation and Applied Studies,* Vol. 10, No 1, pp.138-148.
Cho, H., Rivera-Sánchez, M., Lim, S.S. (2009), "A multinational study on online privacy: global concerns and local responses", *New Media & Society*, Vol. 11, No 3, pp.395-416, https://doi.org/10.1177/1461444808101618.
Chui, M., Issler, M., Roberts, R., Yee, L. (2023), *McKinsey Digital Technology Trends Outlook 2023*, available at, http://dln.jaipuria.ac.in:8080/jspui/bitstream/123456789/14260/1/Mckinsey-technology-trends-outlook-2023.pdf, referred on 12/08/2023.
Clemes, M.D., Gan, C., Zhang, J. (2014), "An empirical analysis of online shopping adoption in Beijing, China", *Journal of Retailing and Consumer Services*, Vol. 21, No 3, pp.364-375, https://doi.org/10.1016/j.jretconser.2013.08.003.
Dima, A., Radu, E., Dobrotă, E.M., Oțoiu, A., Săracu, A.F. (2023), "Sustainable Development of E-commerce in the Post-COVID Times: A Mixed-Methods Analysis of Pestle Factors", *Amfiteatru Economic,* Vol. 25, No Special 17, pp.1095-1114, https://doi.org/10.24818/EA/2023/S17/1095.
Dinu, V., Bucur, M., Enache, C., Fratiloiu, B., Cohen-Tzedec, B., Vasiliu, C. (2022), "European consumer trust as a driving force of mobile commerce", *Transformations in Business & Economics*, Vol. 21, No 2A), 419-434.
Dinu, V., Lazăr, S.P., Pop, I.A. (2021), "Factors that influence the adoption of the internet of things in tourism by Romanian consumers", *Amfiteatru Economic,* Vol. 23, No 57, pp.360-375, http://dx.doi.org/10.24818/EA/2021/57/360.
Dargan, S., Kumar, M. (2020), "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities", *Expert Systems with Applications*, Vol. 143, April, 113114, https://doi.org/10.1016/j.eswa.2019.113114.
Duleepa, D., Hasini, J., Ruwan, R. (2023), "Potentials of developing artificial intelligence technology in the Sri Lankan hotel industry with special reference to Colombo district", *Cactus Tourism Journal,* Vol. 5, No 1, pp.36-44, https://doi.org/10.24818/CTS/5/2023/1.04.
Dvorsky, J., Petrakova, Z., Hudakova, M., Bednarz, J. (2023), "National support and legislative change in the business environment of V4 countries: Business sectors view", *Journal of Business Sectors*, Vol. 1, No 1, pp.42-52, https://doi.org/10.62222/EQDP3972.
El-Abed, M., Giot, R., Hemery, B., Rosenberger, C. (2010), "A study of users' acceptance and satisfaction of biometric systems", in: *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, pp.170-178, https://doi.org/10.1109/CCST.2010.5678678.
Faundez-Zanuy, M. (2005), "Biometric recognition: why not massively adopted yet?", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 20, No 8, pp.25-28, https://doi.org/10.1109/MAES.2005.1499300
Field, A. (2013), *Discovering Statistics Using IBM SPSS Statistics*, Thousand Oaks, CA: Sage.
Francisco, L.C., Francisco, M.L., Juan, S.F. (2015), "Payment systems in new electronic environments: Consumer behavior in payment systems via SMS", *International Journal of Information Technology & Decision Making*, Vol. 14, No 02, pp.421-449, https://doi.org/10.1142/S0219622015500078.
Frenkel, K.A. (1990), "Women and computing", *Communications of the ACM,* Vol. 33, No 11, pp.34-46, https://doi.org/10.1145/92755.92756.
Gefen, D., Karahanna, E., Straub, D.W. (2003), "Trust and TAM in online shopping: An integrated model", *MIS Quarterly*, Vol. 27, No 1, pp.51-90, https://doi.org/10.2307/30036519.

Harrison, G., Lucassen, M. (2019), *Stress and anxiety in the digital age: The dark side of technology. Open Learn*, available at, https://www.open.edu/openlearn/health-sports-psychology/mental-health/stress-and-anxiety-the-digital-age-the-dark-side-technology, referred on 5/05/2023.

He, J., Freeman, L.A. (2010), "Are men more technology-oriented than women? The role of gender on the development of general computer self-efficacy of college students", *Journal of Information Systems Education,* Vol. 21, No 2, pp.203-212.

Henderson, J., Corry, M. (2021), "Teacher anxiety and technology change: A review of the literature", *Technology, Pedagogy and Education,* Vol. 30, No 4, pp.573-587, https://doi.org/10.1080/1475939X.2021.1931426.

Hizam, S.M., Ahmed, W., Fahad, M., Akter, H., Sentosa, I., Ali, J. (2021), "User Behavior Assessment Towards Biometric Facial Recognition System: A SEM-Neural Network Approach", in: K. Arai (ed.), *Advances in Information and Communication. FICC 2021. Advances in Intelligent Systems and Computing*, Vol. 1364. Springer, Cham, https://doi.org/10.1007/978-3-030-73103-8_75.

Hooper, D., Coughlan, J., Mullen, M. (2008), S"tructural Equation Modelling: Guidelines for Determining Model Fit", *Electronic Journal of Business Research Methods,* Vol. 6, No 1, pp.53-60.

Hsieh, Y.C., Tsai, W.C., Hsia, Y.C. (2020), "A Study on Technology Anxiety Among Different Ages and Genders", in: Q. Gao, J. Zhou (eds.), *Human Aspects of IT for the Aged Population. Technology and Society. HCII 2020. Lecture Notes in Computer Science*, Vol. 12209, Springer, Cham, pp.241-254, https://doi.org/10.1007/978-3-030-50232-4_17.

Hu, L., Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", *Structural Equation Modeling,* Vol. 6, No 1, pp.1-55, https://doi.org/10.1080/10705519909540118.

Hu, Z., Ding, S., Li, S., Chen, L., Yang, S. (2019), "Adoption intention of fintech services for bank users: An empirical examination with an extended technology acceptance model", *Symmetry,* Vol. 11, No 3, 340, https://doi.org/10.3390/sym11030340.

Iacobucci, D. (2010), "Structural equations modeling: Fit indices, sample size, and advanced topics", *Journal of Consumer Psychology,* Vol. 20, No 1, pp.90-98, https://doi.org/10.1016/j.jcps.2009.09.003.

Igalla, M., Edelenbos, J., van Meerkerk, I. (2021), "Institutionalization or interaction: Which organizational factors help community-based initiatives acquire government support?", *Public Administration,* Vol. 99, No 4, pp.803-831, https://doi.org/10.1111/padm.12728.

Ingham, J., Cadieux, J., Berrada, A.M. (2015), "e-Shopping acceptance: A qualitative and meta-analytic review", *Information & Management,* Vol. 52, No 1, pp.44-60, https://doi.org/10.1016/j.im.2014.10.002.

James, T., Pirim, T., Boswell, K., Reithel, B., Barkhi, R. (2006), "Determining the intention to use biometric devices: An application and extension of the technology acceptance model", *Journal of Organizational and End User Computing,* Vol. 18, No 3, pp.1-24, https://doi.org/10.4018/joeuc.2006070101.

James, T., Pirim, T., Boswell, K., Reithel, B., Barkhi, R. (2008), "An extension of the technology acceptance model to determine the intention to use biometric devices", in: S. Clarke (ed.), *End user computing challenges and technologies: Emerging tools and applications*, IGI Global, pp.57-78, https://doi.org/10.4018/978-1-59904-295-4.ch005.

Jebb, A.T., Ng, V., Tay, L. (2021), "A review of key Likert scale development advances: 1995–2019", *Frontiers in Psychology,* Vol. 12, 637547, https://doi.org/10.3389/fpsyg.2021.637547.

Junsawang, S., Chaiyasoonthorn, W., Urbański, M., Chaveesuk, S. (2022), "How to Shift Consumer Willingness to Use the Emerging Technologies On Omnichannel", *Montenegrin Journal of Economics*, Vol. 18, No 3, pp.183-196.

Kabir, M.A., Saidin, S.Z., Ahmi, A. (2015), *Adoption of e-payment systems: a review of literature. Proceeding of the International Conference on E-Commerce ICoEC 2015*, 20-22 October 2015, Kuching, Sarawak, Malaysia, pp.112-120, https://aidi-ahmi.com/download/publication/2015_ICoEC_kabir_saidin_ahmi.pdf, referred on 2/06/2023.

Kanak, A., Sogukpinar, I. (2017), "BioTAM: a technology acceptance model for biometric authentication systems", *IET Biometrics,* Vol. 6, No 6, pp.457-467, https://doi.org/10.1049/iet-bmt.2016.0148.

Karsten, R., Schmidt, D. (2008), "Business student computer self-efficacy: Ten years later", *Journal of Information Systems Education*, Vol. 19, No 4, pp.445-453.

Kim, D., Benbasat, I. (2006), "The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's model of argumentation", *Information Systems Research,* Vol. 17, No 3, pp.286-300, https://doi.org/10.1287/isre.1060.0093.

Kravchenko, S.A., Sidorov, N., Draskovic, V. (2021), "New Challenges to Economy Security: the Convergence of Energy and Covid-19 Risks – The Demand for Cosmopolitan Politics", *Montenegrin Journal of*

Economics, Vol. 17, No 2, pp.187-194.

Lai, P. (2017), "The Literature Review of Technology Adoption Models and Theories for the Novelty Technology", *Journal of Information Systems and Technology Management,* Vol. 14, No 1, pp.21-38, https://doi.org/10.4301/S1807-17752017000100002.

Le, O., Cao, Q. (2020), "Examining the technology acceptance model using cloud-based accounting software of Vietnamese enterprises", *Management Science Letters,* Vol. 10, No 12, pp.2781-2788, https://doi.org/10.5267/j.msl.2020.4.032.

Lee, M.C. (2009), "Factors influencing the adoption of internet banking: an integration of TAM and TPB with perceived risk and perceived benefit", *Electronic Commerce Research and Applications,* Vol. 8, No 3, pp.130-141, https://doi.org/10.1016/j.elerap.2008.11.006.

Liébana-Cabanillas, F., Muñoz-Leiva, F., Sánchez-Fernández, J. (2018), "A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment", *Service Business*, Vol. 12, pp.25-64, https://doi.org/10.1007/s11628-017-0336-7.

Liu, S., Silverman, M. (2001), "A practical guide to biometric security technology", *IT Professional,* Vol. 3, No 1, pp.27-32, https://doi.org/10.1109/6294.899930.

Lowe, G.S., Krahn, H. (1989), "Computer skills and use among high school and university graduates", *Canadian Public Policy/Analyse de Politiques*, Vol. 15, No 2, pp.175-188, https://doi.org/10.2307/3551161.

Machova, R., Korcsmaros, E., Csereova, A., Varga, J. (2023), "Innovation activity of Slovak ICT SMEs", *Journal of Business Sectors*, Vol. 1, No 1, pp.32-41, https://doi.org/10.62222/HTPI2054.

Magis-Weinberg, L., Ballonoff Suleiman, A., Dahl, R.E. (2021), "Context, development, and digital media: implications for very young adolescents in LMICs", *Frontiers in psychology*, Vol. 12, 1183, https://doi.org/10.3389/fpsyg.2021.632713.

Marsh, H.W., Hocevar, D. (1985), "Application of confirmatory factor analysis to the study of self-concept: First- and higher order factor models and their invariance across groups", *Psychological Bulletin,* Vol. 97, No 3, pp.562-582, https://doi.org/10.1037/0033-2909.97.3.562.

McCoy, S., Galletta, D.F., King, W.R. (2007), "Applying TAM across cultures: The need for caution", *European Journal of Information Systems,* Vol. 16, No 1, pp.81-90, https://doi.org/10.1057/palgrave.ejis.3000659.

Meuter, M.L., Ostrom, A.L., Bitner, M.J., Roundtree, R. (2003), "The influence of technology anxiety on consumer use and experiences with self-service technologies", *Journal of Business Research,* Vol. 56, No 11, pp.899-906, https://doi.org/10.1016/S0148-2963(01)00276-4.

Micu, A., Micu, A.E., Geru, M., Lixandroiu, R.C. (2017), "Analyzing user sentiment in social media: Implications for online marketing strategy", *Psychology & Marketing,* Vol. 34, No 12, pp.1094-1100, https://doi.org/10.1002/mar.21049.

Miltgen, C.L., Popovič, A., Oliveira, T. (2013), "Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context", *Decision support systems*, Vol. 56, pp.103-114, https://doi.org/10.1016/j.dss.2013.05.010.

Moriuchi, E. (2021), "An empirical study of consumers' intention to use biometric facial recognition as a payment method", *Psychology & Marketing,* Vol. 38, No 10, pp.1741-1765, https://doi.org/10.1002/mar.21495.

Morosan, C. (2011), "Customers' adoption of biometric systems in restaurants: An extension of the technology acceptance model", *Journal of Hospitality Marketing & Management,* Vol. 20, No 6, pp.661-690, https://doi.org/10.1080/19368623.2011.570645.

Nagy, S., Molnar, L., Hajdu, N. (2023), "Understanding the Human Dimensions of the Intention to Use Renewable Energy in Hungary Applying an Extended Model of Theory of Planned Behaviour", *Amfiteatru Economic,* Vol. 25, No 64, pp.830-830, https://doi.org/10.24818/EA/2023/64/830.

Nakisa, B., Ansarizadeh, F., Oommen, P., Shrestha, S. (2022), "Technology Acceptance Model: A Case Study of Palm Vein Authentication Technology", *IEEE Access*, Vol. 10, pp.120436-120449, https://doi.org/10.1109/ACCESS.2022.3221413.

National Bank of Romania (2023), *Exchange course in 28 September 2023*, available at, https://www.bnr.ro/Exchange-rates-1224-Mobile.aspx**,** referred on 29/09/2023

Nguyen, T.D., Huynh, P.A. (2018), "The Roles of Perceived Risk and Trust on E–Payment Adoption", in: L. Anh, L. Dong, V. Kreinovich, N. Thach (eds.), Econometrics for Financial Applications. ECONVN 2018. *Studies in Computational Intelligence,* Vol 760, Springer, Cham, https://doi.org/10.1007/978-3-319-73150-6_68.

Normalini, M.K., Ramayah, T. (2017), "Trust in internet banking in Malaysia and the moderating influence of perceived effectiveness of biometrics technology on perceived privacy and security", *Journal of Management Sciences,* Vol. 4, No 1, pp.3-26, https://doi.org/10.20547/jms.2014.17041.

Ocloo, C.E., Xuhua, H., Akaba, S., Shi, J., Worwui-Brown, D.K. (2020), "The determinant factors of business to business (B2B) E-commerce adoption in small-and medium-sized manufacturing enterprises", *Journal of Global Information Technology Management,* Vol. 23, No 3, pp.191-216, https://doi.org/10.1080/1097198X.2020.1792229.

Ogbanufe, O., Kim, D.J. (2018), "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment", *Decision Support Systems*, Vol. 106, pp.1-14, https://doi.org/10.1016/j.dss.2017.11.003.

Pai, C.K., Wang, T.W., Chen, S.H., Cai, K.Y. (2018), "Empirical study on Chinese tourists' perceived trust and intention to use biometric technology", *Asia Pacific Journal of Tourism Research,* Vol. 23, No 9, pp.880-895, https://doi.org/10.1080/10941665.2018.1499544.

Pavlou, P.A. (2003), "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model", *International Journal of Electronic Commerce*, Vol. 7, No 3, pp.101-134, https://doi.org/10.1080/10864415.2003.11044275.

Phakiti, A. (2020), "Likert-type scale construction", in: P. Winke, P. Brunfaut (eds.), *The Routledge handbook of second language acquisition and language testing*, New York: Routledge, pp.102-114, https://doi.org/10.4324/9781351034784.

Phonthanukitithaworn, C., Sellitto, C., Fong, M.W.L. (2016), "A Comparative Study of Current and Potential Users of Mobile Payment Services", *SAGE Open,* Vol. 6, No 4, https://doi.org/10.1177/2158244016675397.

Popa, I., Cioc, M.M., Popa, Ş.C., Botez, D., Pantea, M.I. (2023), "Aligning Public Policy with REPowerEU Program Objectives by Adopting EESS Solutions: A Technology Acceptance Model Approach", *Amfiteatru Economic,* Vol. 25, No 64, pp.660-675, https://doi.org/10.24818/EA/2023/64/660.

Riaz, H., Davidaviciene, V., Ahmed, H., Meidute-Kavaliauskiene, I. (2022), "Optimizing customer repurchase intention through cognitive and affective experience: An insight of food delivery applications", *Sustainability,* Vol. 14, No 19, 12936, pp.1-22, https://doi.org/10.3390/su141912936.

Sejera, S.G., Bocarnea, M. (2022), "The Nature of Leadership in Artificial Intelligence Environments: Reconceptualizing Human and Machine Collaboration", *Revista de Management Comparat International,* Vol. 23, No 2, pp.264-283, https://doi.org/10.24818/RMCI.2022.2.264.

Skalkos, A., Stylios, I., Karyda, M., Kokolakis, S. (2021), "Users' privacy attitudes towards the use of behavioral biometrics continuous authentication (BBCA) technologies: A protection motivation theory approach", *Journal of Cybersecurity and Privacy,* Vol. 1, No 4, pp.743-766, https://doi.org/10.3390/jcp1040036.

Smart Payment Association (2021), *Biometric payment cards. The next evolution in secure cantactless transactions*, December, available at, https://www.smartpaymentassociation.com/index.php/liste-documents/public-resources/position-papers/895-21-12-01-spa-biometric-payment-cards-paper-final-1/file, referred on 5/05/2023.

Soto-Beltrán, L.L., Robayo-Pinzón, O.J., Rojas-Berrio, S.P. (2022), "Effects of perceived risk on intention to use biometrics in financial products: evidence from a developing country", *International Journal of Business Information Systems,* Vol. 39, No 2, pp.170-192, https://doi.org/10.1504/IJBIS.2022.121432.

Stark, L., Stanhaus, A., Anthony, D.L. (2020), ""I don't want someone to watch me while I'm working": Gendered views of facial recognition technology in workplace surveillance", *Journal of the Association for Information Science and Technology,* Vol. 71, No 9, pp.1074-1088, https://doi.org/10.1002/asi.24342.

Statista Research Department (2023), *Readiness to use fingerprint instead of PIN code for payments in 2021, by country*, Mar 31, available at, https://www.statista.com/statistics/1338830/payment-in-store-fingerprint-authentication-instead-pin-code-worldwide/#statisticContainer, referred on 15/06/2023.

Stylios, I., Kokolakis, S., Thanou, O., Chatzis, S. (2022), "Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research", *Information & Computer Security,* Vol. 30, No 4, pp.562-582, https://doi.org/10.1108/ICS-08-2021-0124.

Tabachnick, B.G., Fidell, L.S. (2006), *Using Multivariate Statistics*, 5th edition, Boston: Allyn & Bacon.

Taburchak, A.P., Bychkova, S.M., Butina, A.A. (2022), "Analysis of risk factors for applied projects in a digital economy", *Entrepreneurship and Sustainability Issues*, Vol. 9, No 3, pp.152-172, http://doi.org/10.9770/jesi.2022.9.3(10).

Tassabehji, R., Kamala, M.A. (2009), "Improving e-banking security with biometrics: modelling user attitudes and acceptance", *3rd International Conference on New Technologies, Mobility and Security, NTMS 2009*, pp.1-6, https://doi.org/10.1109/NTMS.2009.5384806.

Thiesse, F. (2007), "RFID, privacy and the perception of risk: A strategic framework", *The Journal of Strategic Information Systems*, Vol. 16, No 2, pp.214-232, https://doi.org/10.1016/j.jsis.2007.05.006.

Torkzadeh, G., Angulo, I.E. (1992), "The concept and correlates of computer anxiety", *Behaviour & Information*

Technology, Vol. 11, No 2, pp.99-108, https://doi.org/10.1080/01449299208924324.
Venkatesh, V., Davis, F.D. (2000), "A theoretical extension of the technology acceptance model: Four longitudinal field studies", *Management Science,* Vol. 46, No 2, pp.186-204, https://doi.org/10.1287/mnsc.46.2.186.11926.
Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol. 27, No 3, pp.425-478, https://doi.org/10.2307/30036540.
Venkatesh, V., Thong, J.Y., Chan, F.K., Hu, P.J.H., Brown, S.A. (2011), "Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context", *Information Systems Journal*, Vol. 21, No 6, pp.527-555, https://doi.org/10.1111/j.1365-2575.2011.00373.x.
Viehland, D., Leong, R.S.Y. (2007), „Acceptance and Use of Mobile Payments", in: *ACIS 2007 Proceedings*, pp. 665-671, available at, http://aisel.aisnet.org/acis2007/16**,** referred on 5/05/2023.
VISA (2022), *Consumer Payment Attitudes Study 2022. Navigating a new era in payments*, available at, https://www.visa.co.th/dam/VCOM/regional/ap/documents/visa-cpa-report-smt-2022.pdf, referred on 5/05/2023.
Wayman, J., Jain, A., Maltoni, D., Maio, D. (2005), „An introduction to biometric authentication systems", in: J. Wayman, A. Jain, D. Maltoni, D. Maio (Eds.), *Biometric systems: Technology, design and performance evaluation*, London: Springer London, pp.1-20, https://doi.org/10.1007/1-84628-064-8_1.
Zahrani, A.A. (2021), „Consumers' perceptions of intention to use a credit card: perceived risk and security", *Entrepreneurship and Sustainability Issues*, Vol. 9, No 2, pp.37-49, http://doi.org/10.9770/jesi.2021.9.2(2).
Zhong, Y., Oh, S., Moon, H.C. (2021), "Service transformation under industry 4.0: Investigating acceptance of facial recognition payment through an extended technology acceptance model", *Technology in Society*, Vol. 64, 101515, https://doi.org/10.1016/j.techsoc.2020.101515**.**

RUMUNIJOS VARTOTOJŲ PRITARIMAS BIOMETRINIO MOKĖJIMO SAUGUMO TECHNOLOGIJAI

Daniel Adrian Gârdan, Olimpia State, Iuliana Petronela Gârdan, Claudia Baicu, Maria Anca Hristea, Daniel Moise

SANTRAUKA

Šiuolaikinės finansinės operacijos reikalauja plataus įvairių technologijų naudojimo. Dėl sudėtingų finansų įstaigų ir jų klientų santykių ir apimties atsirado didžiulis informacijos kiekis ir didėjantis poreikis šią informaciją apdoroti greičiau. Šiuolaikinės telekomunikacijos, internetas ir elektroninės prekybos bei sandorių technologijos yra tik šios dėlionės dalys, kuriomis galima itin dideliu mastu tvarkyti konfidencialią informaciją. Sykiu vis labiau auga poreikis apsaugoti pačią informaciją, jos perdavimą ir kaupimą. Poreikis užtikrinti internetinių kanalų ir internetinių bei ne internetinių operacijų sąsajos saugumą yra kaip niekada aktualus ir labai svarbus tiek verslo klientams, tiek privatiems asmenims. Straipsnyje nagrinėjama, ar modelis, kurį sudaro TAM (ang. *Technology Acceptance Model*, technologijų priėmimo modelis) ir UTAUT (angl. *Unified Theory of Acceptance, and Use of Technology*, vieninga technologijų priėmimo ir naudojimo teorija) būdingi kintamieji, aiškinantis sudėtingą ryšį tarp veiksnių, galinčių daryti įtaką biometrinių saugumo technologijų, tiesiogiai taikomų finansinių paslaugų ir mokėjimų srityje, pritaikymui, galioja.

REIKŠMINIAI ŽODŽIAI: biometrinių mokėjimų saugumas; technologijos priėmimo modelis; vartotojų elgsena.