Wang, Jen Sheng

Article

Exploring biometric identification in FinTech applications based on the modified TAM

Financial Innovation

Provided in Cooperation with:
Springer Nature

Suggested Citation: Wang, Jen Sheng (2021) : Exploring biometric identification in FinTech applications based on the modified TAM, Financial Innovation, ISSN 2199-4730, Springer, Heidelberg, Vol. 7, Iss. 1, pp. 1-24, https://doi.org/10.1186/s40854-021-00260-2

This Version is available at:
https://hdl.handle.net/10419/237273

Wang *Financ Innov* (2021) 7:42
https://doi.org/10.1186/s40854-021-00260-2

Financial Innovation

RESEARCH Open Access

Exploring biometric identification in FinTech applications based on the modified TAM

Jen Sheng Wang*

*Correspondence:
vincent.mt98g@nctu.edu.tw;
vincentwjs@nycu.edu.tw
Institute of Technology Management, National Yang Ming Chiao Tung University, 1001 Ta-Hsueh Road, Hsinchu 300, Taiwan

Abstract

In recent years, biometric technologies have been widely embedded in mobile devices; these technologies were originally employed to enhance the security of mobile devices. With the rise of financial technology (FinTech), which uses mobile devices and applications as promotional platforms, biometrics has the important role of strengthening the identification of such applications for security. However, users still have privacy and trust concerns about biometrics. Previous studies have demonstrated that the technology acceptance model (TAM) can rigorously explain and predict user acceptance of new technologies. This study therefore modifies the TAM as a basic research architecture. Based on a literature review, we add two new variables, namely, "perceived privacy" and "perceived trust," to extend the traditional TAM to examine user acceptance of biometric identification in FinTech applications. First, we apply the analytic hierarchy process (AHP) to evaluate the defined objects and relevant criteria of the research framework. Second, we use the AHP results in the scenario analysis to explore biometric identification methods that correspond to objects and criteria. The results indicate that face and voice recognition are the two most preferred identification methods in FinTech applications. In addition, there are significant changes in the results of the perceived trust and perceived privacy dominant scenarios.

Keywords: Biometric identification, FinTech applications, AHP, Perceived privacy, Perceived trust

Introduction

The world is changing due to the use of financial technology (FinTech) in both the business and personal lives of people. People around the world connect and interact via FinTech (Milian et al. 2019). People have many electronic devices in their pockets, on their desks, and in their homes, which means that they can send money across the world at any time, purchase products on the Internet from people they have never met, and manage their personal wealth with fast, accessible, and convenient electronic devices (Callen-Naviglia and James 2018). The explosive growth of mobile computer, communication, and consumer (3C) devices and the introduction of mobile payments are forcing traditional retail banks and electronic commerce (e-commerce) retailers to increase the flexibility of their businesses to meet the challenges of new business pipelines and models in the FinTech era (Jonker 2019; Kou 2019). A complex action to balance the interests

of all parties was derived from financial services providers, who attempt to moderate the relationship among privacy, convenience, and security or other latent concerns, and showed that the opinions of financial services providers about security issues had to change (Liébana-Cabanillas and Lara-Rubio 2017; Alhassany and Faisal 2018; Hu et al. 2019; Norma and Farah 2020).

However, it is impossible to protect the security of information assets by using locks and keys. We often trust people and systems that we cannot identify even if face-to-face. High levels of online information exchange and interaction provide opportunities for hackers who are attempting to steal people's identities and credentials for illegal purposes (Costigan 2016; Callen-Naviglia and James 2018). The highly regulated financial services industry has a large amount of sensitive financial and personal information, so it needs to maintain a high level of attention to information security issues. In addition, banks are also driven by technology and are transforming and innovating at an extraordinary rate to meet regulatory requirements and customer expectations (Costigan 2017; Patil et al. 2020; Singh et al. 2020). Almost any certification technology can be destroyed, so financial services providers cannot rely on one method to authorize high-risk activities. In FinTech applications, financial services providers use a variety of identification technologies to improve fraud monitoring and user experience (Wang et al. 2019; Zhu et al. 2020).

Biometric technologies are expected to provide enhanced identification solutions for these problems. From a technological viewpoint, the technical research process of identity verification via people's physical characteristics began with the emergence of computer systems in the second half of the twentieth century (Ogbanufe and Kim 2018; Wang et al. 2019). As an emerging technology concept, biometrics was not widely applied until Apple introduced fingerprint recognition technology as a feature of its electronic devices (Liu et al. 2015; Wu et al. 2018; Murakami et al. 2019). Biometrics could be well applied to application software or devices to enable users to directly utilize these technologies (Liu et al. 2015; Barkadehi et al. 2018). This technique is consistent with the need for intuitive and frictionless certification experiences (Murakami et al. 2019). For mobile device providers, biometrics is an ideal technical solution because it can collect rich data obtained by many sensors in intelligent mobile devices to strengthen not only identification but also security (Ogbanufe and Kim 2018). These results are difficult to achieve in traditional networks. Considering the widespread use of intelligent mobile devices, this technology is particularly suitable for the identification of mobile payments and even the future security of various FinTech applications (Wang et al. 2019; Kim et al. 2019; Dubey 2019).

Based on these two arguments, it is understood that biometrics have gradually been designed in FinTech applications because it is convenient for user login and accessing cloud financial services (Fenu and Marras 2018). Mehrban et al. (2020) also considered biometrics as an alternative to enhance the security of FinTech applications in protecting privacy and trust. Biometrics can apparently reduce the leakage of personal information by simplifying the identification process of FinTech applications. For example, Ant Financial launched face recognition to complete a payment system that took security and the user experience to a new level (Qi and Xiao 2018). Beyond the cybersecurity of FinTech applications, the customer experience has the potential to be changed as a result

of increasing reliance on biometrics (Imerman and Fabozzi 2020). On the other hand, concerns about user acceptance have arisen. Regarding privacy and trust with respect to biometrics, most studies have discussed biometrics penetration from a technical viewpoint (Dubey 2019; Tanimoto et al. 2019; Iyer et al. 2020), but there is less research from the perspective of users.

Therefore, this study applies the research objective to explore customers' acceptance related to biometric identification in FinTech applications. Further, the technology acceptance model (TAM) is utilized to define the possible influence variables and realize their significance. The TAM has been widely employed to examine user acceptance of new technologies (Cheng and Yeh 2011; Rashed and Alajarmeh 2015; Shachak et al. 2019). The TAM can adjust the variables with the research object to further and effectively explain and predict (Wu et al. 2017; Chopdar and Sivakumar 2019). In FinTech, the TAM has been applied to investigate mobile payment (Norma and Farah 2020), cryptocurrency (Singh et al. 2020), and financial service innovations (Hu et al. 2019). Many sophisticated analytical methods identify the best solution for a multi-objective problem, and these methods can also be used for exploratory research. As one of the most widely employed techniques, the analytic hierarchy process (AHP) can evaluate each alternative based on established criteria (Saaty 1980; Kou and Lin 2014; Lee et al. 2018; Galankashi et al. 2020). Thus, the current study applies the AHP to explore the improved TAM to confirm the weights and priorities of criteria that are critical for biometrics in FinTech applications.

Second, the AHP provides quantitative output to use in sensitivity analysis to comprehend the variations in weights or priorities and how these affect the scenarios of the research aim (Srdjevic et al. 2012; Başar 2018; Lin et al. 2020). Sensitivity analysis also increases the reliability of AHP by appropriately answering "what if" questions. This approach is specifically useful for multi-objective decision problems (Wang et al. 2013; Schmidt et al. 2015; Atmaca and Karadaş 2020; Yu et al. 2021). By including scenario construction and analysis via sensitivity analysis, the research contributions of AHP are broadened (Başar 2018). Analysts can construct scenarios to describe situations that may affect the weight of the criterion or the attributes of each choice (Wang et al. 2013; Kou et al. 2014; Zhang et al. 2021). We performed a sensitivity analysis to adjust the weight of every object for simulating practicable biometric identification in FinTech application scenarios. Using these technical evaluation schemes, we can identify the impacts of variables of the modified TAM on the determination for biometric identification in FinTech applications.

This study describes the security used in FinTech applications and then essentially introduces four common biometric technologies. Next, based on the TAM and related literature, we construct a multi-object framework to evaluate biometrics in FinTech applications. The third and fourth parts introduce the AHP and sensitivity analysis methods. Section 5 describes the empirical and sensitivity analyses that are performed by employing the AHP. Based on the results, the conclusion and management implications are discussed in Sect. 6.

Literature review

Identification in FinTech applications

FinTech is often considered a unique combination of financial services and information and communication technologies (ICTs). The 2008 financial crisis was a critical reason for FinTech to subvert tradition and develop new and alternative types of financial services (Arner et al. 2016; Kou 2019). In addition, Mead (2016) suggested that FinTech refers to an economic industry produced by enterprises using technological methods to improve the efficiency of financial services. This definition assumes that FinTech companies would prosper with the transformation of financial services and solve the dilemma of the traditional financial industry in developing financial technology, thereby adding great value to financial services. Kang (2018) determined that FinTech is composed of "financial" and "technology" elements. In the era of the information explosion, as one of the most important international trends since the emergence of the civilian population of the Internet, FinTech refers to various applications of technology that are related to financial applications (Milian et al. 2019).

Many researchers have regarded FinTech as a kind of "financial service innovation" and found that people widely use technologies in the early stage of procuring financial consumer goods. New participants are competing in new areas such as Bitcoin or third-party payments. These researchers also promote digital financial transformation to support sustainable strategies that leverage financial technologies to achieve financial expansion, development, stability, and integrity. Furthermore, FinTech optimizes traditional financial services via technology flipping, and many financial services can be completed directly on the Internet across time and space (Arner et al. 2016; Eagar 2016; Sonea 2016).

FinTech claims to introduce the original financial business to nonfinancial industries under the precondition of risk control; that is, it allows industries, such as the ICT industry, to enter financial industries. Thus, the ICT industry can utilize its research to create highly innovative developments in financial goods and services (Drummer et al. 2017). However, the highly regulated environment of the financial services industry requires secure data protection, strict identity recognition, and verification processes, and the industry relies on existing traditional but critical infrastructure. When FinTech began to change the financial services industry, some aspects were quite threatening to the existing situation (Costigan 2016, 2017). In contrast, biometrics have been on the rise in mobile finance services in recent years. Consider the fingerprint reader on new iPhones, face recognition on Android devices, and voice recognition in many mobile banking applications. Biometrics could strengthen the identification of financial service procedures and eliminate imposter scams in e-payments (Wu et al. 2018).

As FinTech has begun to lead the development trend of future financial services, security identification at the login step has become more important. People are increasingly and frequently logging on to their online bank accounts to quickly check their balance or make payments. If a service provider cannot provide 30 s of automatic identification for 60 s of transactions, then the user will have a sense of distrust and end the interaction (Stewart and Jürjens 2018). Therefore, FinTech developers must carefully consider the security needs of users, who should be given appropriate security protection. Relative to addressing the degree of risk, FinTech must provide sufficient security (Menat 2016).

As financial accounts are increasingly employed in various service scenarios, the implied risks increase; hence, it is necessary to ensure that people are authenticated securely. Another issue that needs special attention is that users' perception of secure identification will become a variable that affects users when they consider how FinTech provides new forms of service. This issue should be regarded as the basis for relying on FinTech services and protecting users (Arner et al. 2017; Kang 2018; Kim et al. 2019).

Biometric identification

According to the research objectives, this study applies the biometric definition provided by the US Department of Defense's Biometrics Management Agency (BIMA) to convey two main concepts of biometric identification (Biometrics Management Agency 2010): "The common term of biometric can alternatively be used to describe a feature or process. As a characteristic: a measure of biological (anatomical and physiological) and/or behavioral biological characteristics that can be used for automatic identification. As a process: an automated method of identifying individuals based on measures of biology (anatomy and physiology) and/or behavioral biological characteristics" (BIMA 2010; Liu et al. 2015; Zhu et al. 2020).

Actual biometric recognition should meet the accuracy, speed, and resource requirements of the designated recognition function (Wu et al. 2018). The system must be harmless and acceptable to the intended users and sufficiently robust to resist most fraud approaches and attacks on the system (Barkadehi et al. 2018). The four most popular forms of biometric identification are face, fingerprint, voice, and iris recognition. All of these technologies can be embedded in mobile devices and FinTech systems for identification (Jain et al. 2016). We briefly introduce these four biometric technologies as follows.

1. Face recognition

   Face recognition is the most widely known and most natural form of biometric identification, but it may lead to problems of increased facial roundness or other distortions. It is often combined with other biometric technologies to enhance security. At this stage, it ranks second in terms of market share. Advanced technologies can enable face recognition that mixes the two- (2D) and three-dimensional (3D) modes, and face recognition needs to regularly update the biometric data to correct for accuracy (Guo et al. 2016). It can replace more utilized monitoring systems (Donohue 2012; Faddis et al. 2013; Breckenridge 2014).
2. Fingerprint recognition
   Undoubtedly, the most pioneering biometric technology that is embedded in mobile devices is fingerprint recognition. The fingerprint uniqueness of individuals is second only to iris recognition. It is easy to input biometric characteristics on mobile devices. However, the false acceptance rate of fingerprint recognition is high, so it is easy to hack. In addition, it has various operating principles, such as optical, capacity, or ultrasonic principles, each of which has pros and cons (Donohue 2012; Faddis et al. 2013; Breckenridge 2014; Jain et al. 2016).
3. Iris recognition

Iris recognition has the highest individual uniqueness, as even twins do not have the same irises. It has previously been applied in access control systems. With the growth of camera pixels in mobile devices and the enhancement of light-emitting diode (LED) light assistance, iris recognition has gradually been embedded in mobile devices, but is still limited by various scenarios. In addition, wearing special contact lenses will decrease the success rate (Donohue 2012; Faddis et al. 2013; Breckenridge 2014; Jain et al. 2016).

4. Voice recognition
   Voice recognition is based mainly on the tone and audio quality of an individual's voice. A voiceprint may differ due to the shape and pronunciation habits of an individual. Recognition errors may also occur due to field noise. In recent years, due to the proliferation of voice assistants and the control functions of mobile devices, as well as the improved performance of microphones, it has become popular to embed voice recognition in mobile devices (Donohue 2012; Faddis et al. 2013; Breckenridge 2014; Jain et al. 2016).

Summary of literature review

According to the previous discussion, we know that biometric identification has been widely employed for many applications. Additionally, biometrics can identify users to meet know-your-customer (KYC) requirements that conventional financial services regulate. In this way, biometrics could help various FinTech applications collect user information per biometric identification (Arner et al. 2019). Biometrics and personal information are also deeply bound, and some information may be sensitive (Fenu and Marras 2018). Biometric identification is expected to be utilized for FinTech applications over networks, such as Internet financial services, network access control, and membership authentication (Murakami et al. 2019; Imerman and Fabozzi 2020).

Obviously, biometrics is usually considered a more effective alternative for identification than other tools in financial services applications, such as passwords, short message services (SMSs), and one-time passwords (Dubey 2019). Biometric identification in FinTech applications has injected one-click onboarding and payment solutions from anyplace at any time (Qi and Xiao 2018). The ease of use and rapidity of technology have made people's lives more comfortable. Biometric identification is a promising replacement for conventional identification approaches and has been employed in many application situations (Fenu and Marras 2018). Such applications generally involve handling queries and searches at scale in a networked environment (Zhu et al. 2020). Hence, this study explores biometric identification in FinTech applications, which are based on the modified TAM to better predict its development.

Modified TAM

Technology acceptance model

Many models have been applied to explain the systematic adoption of emerging technologies. The TAM developed by Davis (1989) is the most commonly employed analytical and representative model (Chau and Hu 2001). Using the relevant variables of user attitudes and behaviors to assess the acceptance of new technologies (Bagozzi 2007; Schierz

et al. 2010), the TAM addresses the most influential arguments in the theory of reasoned action (TRA) and theory of planned behavior (TPB).

The TAM is an advantageous and reliable research method with excellent measurement, simplicity, and empirical stability (Pavlou 2003). Compared to alternative models, it can explain the main differences in usage intentions (Schierz et al. 2010), so it is widely utilized to analyze the introduction of many emerging technologies, such as the application of radio frequency identification (RFID) in specific fields (Cheng and Yeh 2011) or how health-relevant information technologies should be implemented (Shachak et al. 2019). In addition, the TAM is applied to infer the role of new variables in deducing the acceptance of a specific technology (Jeong et al. 2009).

Although the TAM is very useful in explaining behavioral intention, Venkatesh and Davis (2000) suggested that it is relatively simple and that relevant explanatory variables should be added in the study of specific technology assessments. Many studies have successfully validated this argument by modifying the basic model and adding relevant explanatory and mediating variables. In this way, the continuity of the TAM has been maintained in the research field (Venkatesh et al. 2007; Cheng and Yeh 2011; Rashed and Alajarmeh 2015; Shachak et al. 2019).

When the variables of relevant research arguments are integrated, the TAM provides a deeper understanding of the issues related to user acceptance (Jeong et al. 2009). Chopdar and Sivakumar (2019) and Wu et al. (2017) applied the TAM and relevant theories to investigate financial services to predict users' intentions. Priya et al. (2018) measured young Indian consumers' satisfaction levels with mobile financial services and revealed that the TAM included strong determinants of user attitudes and the intention to use technology. Singh et al. (2020) also applied a TAM-based concept and found its significance in evaluating users' adoption of mobile wallet services. The concept of the modified TAM has also been applied in FinTech application studies. Hu et al. (2019) employed the extended TAM to investigate the influence mechanism behind the adoption of FinTech services and attempted to provide comprehensive determinants. Norma and Farah (2020) examined the variables of continuance intention of FinTech payments to further understand the influential factors in users' decisions to use FinTech payment services.

Researchers examined the factors that affect user intention to use emerging financial services and found "perceived trust" was one of the key factors that influence user acceptance (Abhishek and Hemchand 2016; Shaw and Kesharwani 2019). Patil et al. (2020) addressed "perceived trust" that provides a positive guarantee that lets users have a positive experience of financial services. That is, if users perceive trust in FinTech applications, they can be convinced to use these applications and can increase their intention to do so (Cao et al. 2018). Researches supported the positive influence of trust on online finance (Shao et al. 2019; Kang and Namkung 2019). Choi et al. (2020) regarded biometric identification as a major feature to generate users' trust in mobile payment services. The use of biometric identification in FinTech applications amplifies the role of trust because of cybersecurity (Imerman and Fabozzi 2020).

In addition, we considered "perceived privacy" with the TAM, as many scholars have highlighted that this factor could indicate a deeper and more predictable intention to adopt new technologies in financial services industries (Norma and Farah 2020). Considering the sensitivity of FinTech applications, the digitization and virtualization of

financial services has frequently been met with privacy concerns (Merhi et al. 2020). People using FinTech applications can still control any manipulation of their personal information online, and they may worry that it may be lost or stolen (Kalinić et al. 2019). More importantly, studies examining financial services application adoption have provided evidence for this influence (Carranza et al. 2021). Buckley and Nurse (2019) highlighted that users are seemingly more comfortable with biometric identification, which demonstrates privacy protection. Furthermore, "perceived privacy" can specifically measure user attitudes toward the topic (Ghani et al. 2017; Rahia et al. 2018; Hassan and Wood 2020).

We therefore use the TAM as the basic research structure and add two explanatory variables "perceived trust" (PT) and "perceived privacy" (PP), which may be highly relevant to this research topic. Accordingly, this study expects to fully explain the concepts of this research, construct new research arguments, and propose advanced research contributions. We believe that based on the modified TAM, some variables that can help us evaluate the behavioral intention and explanatory variables of biometric identification can be extended to FinTech applications. The modified TAM is illustrated in Fig. 1.

Perceived ease of use (PE)

With proper guidance and instruction, users can easily log in to mobile devices and FinTech systems via biometric identification. In the process, the user experience is theoretically simple and fluent and does not cause much confusion or negative feelings for users (Liu et al. 2015; Jain et al. 2016; Ko and Yu 2015; Rashed and Alajarmeh 2015; Morosan 2016; Pai et al. 2018). "Perceived ease of use" (PE) is positively associated with users' attitude and intention to adopt new financial services (Kanak and Sogukpinar 2017; Alhassany and Faisal 2018). Hence, we develop three criteria to evaluate the weight of PE in the research model.

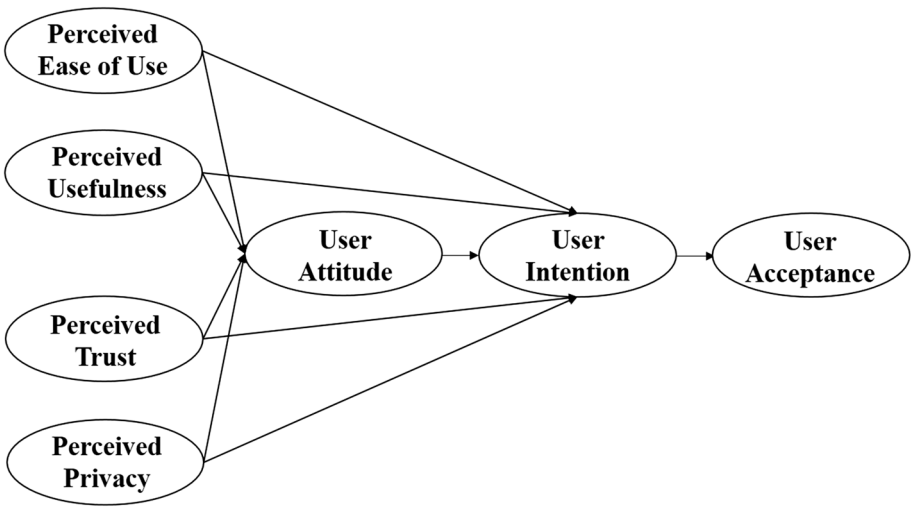

Fig. 1 Modified TAM of Biometric Identification in FinTech applications

1. Users perceive that biometric identification in FinTech applications is convenient to use (PE1).
2. Users perceive that biometric identification in FinTech applications is workable (PE2).
3. Users perceive that biometric identification in FinTech applications is easy to learn (PE3).

Perceived usefulness (PU)

Ideal biometrics provide accurate identification. Although traditional passwords have the same function, biometric characteristics are more natural, and users can intuitively manipulate them (Liu et al. 2015; Jain et al. 2016; Ko and Yu 2015; Rashed and Alajarmeh 2015; Morosan 2016; Kanak and Sogukpinar 2017; Pai et al. 2018). Liébana-Cabanillas and Lara-Rubio (2017) evaluated various studies and determined that, in mobile payment systems, "perceived usefulness" (PU) was a significant predictor of user attitude and intention (Alhassany and Faisal 2018). Hence, we develop three criteria to evaluate the weight of PU in the research model.

1. Users perceive that biometric identification in FinTech applications is effective (PU1).
2. Users perceive that biometric identification in FinTech applications can improve the login success rate (PU2).
3. Users perceive that biometric identification in FinTech applications is helpful for logging in (PU3).

Perceived trust (PT)

Biometrics is based on the uniqueness of individual biometric characteristics. No two people (except for identical twins) have the same biometrics. In addition, most biometric characteristics are permanent, which means that they do not change, even over time. Therefore, biometric technology has higher trust than other identification techniques in FinTech applications (Liu et al. 2015; Jain et al. 2016; Ko and Yu 2015; Rashed and Alajarmeh 2015; Morosan 2016; Lee and Rha 2016; Kanak and Sogukpinar 2017; Pai et al. 2018). "Perceived trust" significantly affects user attitudes and intentions toward adopting FinTech services (Shaw and Kesharwani 2019; Hu et al. 2019). We develop three criteria to evaluate the weight of PT in the research model.

1. Users perceive that biometric identification in FinTech applications is secure (PT1).
2. Users perceive that biometric identification in FinTech applications is reliable (PT2).
3. Users perceive that biometric identification in FinTech applications is safer than other identification methods (PT3).

Perceived privacy (PP)

In general, biometrics provide the user with irrefutable evidence of identification. Therefore, privacy is users' primary concern. Most biometric technologies have been developed with complete solutions for privacy issues. In the future, we believe that these

solutions will be perfected (Liu et al. 2015; Jain et al. 2016; Ko and Yu 2015; Rashed and Alajarmeh 2015; Morosan 2016; Lee and Rha 2016; Kanak and Sogukpinar 2017; Pai et al. 2018). "Perceived privacy" would negatively influence users' attitudes and intentions toward adopting FinTech services (Hu et al. 2019; Hassan and Wood 2020). Hence, we develop three criteria to evaluate the weight of PP in the research model.

1. Users perceive that biometric identification in FinTech applications will not invade privacy (PP1).
2. Users perceive that biometric identification in FinTech applications will strengthen privacy protection (PP2).
3. Users perceive that biometric identification in FinTech applications will not leak personal biometric characteristics (PP3).

Research methodology

AHP

The AHP is an approach used in multi-objective decision-making and planning. The results of an additive weighting process indicates that various related attributes are present based on their comparative priorities (Erkut and Tarimcilar 1991; Kou and Lin 2014; Lin et al. 2020). The AHP has been widely utilized by scholars and researchers and can be employed to systematize complex issues by hierarchical decomposition based on experts' opinions or literature reviews (Yu et al. 2021). The weights among criteria can be calculated to rank the importance of each criterion (Kou et al. 2014; Zhang et al. 2021). The AHP includes a quantitative comprehensive assessment to provide decision makers with information about choosing appropriate solutions or technology evaluations (Schmidt et al. 2015; Lee et al. 2018; Yu et al. 2021). The AHP has also been applied in financial studies. Galankashi et al. (2020) applied the concept to a literature review to establish the main criteria for portfolio selection and finalized a list of criteria for ranking 10 different Tehran Stock Exchange (TSE) portfolios. Atmaca and Karadaş (2020) applied it in decision-making on financial investment using factor weights.

In exploring biometric identifications in FinTech applications, the current study proposes the AHP approach to analyze the causal link and degree of interaction between the TAM variables and evaluate the significance of objects and related criteria of the extended TAM structure. The AHP can be utilized to effectively build a hierarchy of different assessment objects and related criteria to create a quantified process that values the relative importance of each possible criterion and alternative method (Kou et al. 2014; Lin et al. 2020). Based on the relevant literature (refer to Fig. 2), this study constructs an AHP analysis framework for biometric identification in FinTech applications according to the modified TAM. The objects and relative criteria of the AHP are shown here.

The main goal of this research is to explore corresponding biometric identifications from a modified TAM perspective. In addition, we conducted in-depth interviews with researchers from both the biometric and the FinTech application sectors to ensure the effectiveness of this research methodology. This study principally applies the AHP to confirm the feasibility of biometric identification to fulfill the investigated objects and

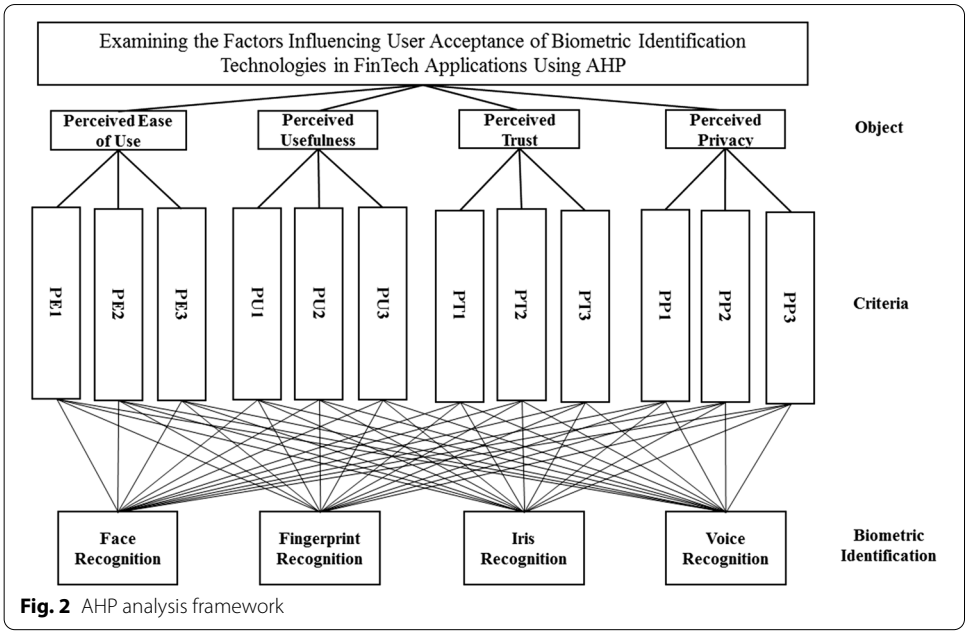

Fig. 2 AHP analysis framework

relative criteria of the model. For an exploratory purpose, it is important to evaluate not only the success of assessing the priority of each object but also whether the substitutes satisfy these objects. Hence, biometric identifications in FinTech applications can be well organized to respond to the priorities of objects. The AHP seems to be a very useful approach that allows users to deliver their judgments, which are either qualitative or subjective. In addition, we can use the AHP results to examine the significance of substitutes in different hypothetical scenarios via sensitivity analysis.

When building a hierarchical structure, the designer can use literature reviews, brainstorming, and Delphi methods to search for criteria. If there are n criteria, the criteria are compared with each other once. We adopt the 9-point scale suggested by Saaty (1980) to survey the opinions of professionals and give equal, medium, strong, very strong, or extreme preferences with pair weights of 1, 3, 5, 7, and 9, respectively, while 2, 4, 6, and 8 serve as median values for the preference levels. Matrix $\boldsymbol{I}$ is formulated to process pairwise comparisons in Eq. 1:

$$\left\{ I = \left[i_{xy} \right] = \begin{bmatrix} 1 & i_{12} & \cdots & i_{1n} \\ i_{21} & 1 & \cdots & i_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ i_{n1} & i_{n2} & \cdots & 1 \end{bmatrix} = \begin{bmatrix} 1 & i_{12} & \cdots & i_{1n} \\ 1/i_{12} & 1 & \cdots & i_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/i_{1n} & 1/i_{2n} & \cdots & 1 \end{bmatrix} \right\} \tag{1}$$

where i_{xy} represents the geometric mean of the comparison between criterion x and criterion y on behalf of the professional group. We can compare the priority of the criteria based on estimating the relative weights of the criteria in this matrix by calculating the eigenvectors and eigenvalues according to Eq. 2:

$$I \cdot d = I \cdot \beta_{max} \tag{2}$$

In Eq. 2, the eigenvector of Matrix $\boldsymbol{I}$ is defined as $\boldsymbol{d}$, and the largest eigenvalue of Matrix $\boldsymbol{I}$ is defined as β_{max}. We can use Eq. 3 to obtain the eigenvector $\boldsymbol{d}$.

$$d = \left(\prod_{y=1}^{n} i_{xy}\right)^{1/n} \Big/ \sum_{x=1}^{n} \left(\prod_{y=1}^{n} i_{xy}\right)^{1/n} \tag{3}$$

In Eq. 3, n represents the number of criteria that we compare in Matrix $\boldsymbol{I}$. We estimate the largest eigenvalue β_{max} of Matrix $\boldsymbol{I}$ with Eq. 4:

$$\beta_{max} = \frac{1}{n} \sum_{x=1}^{n} \frac{(Id)_x}{d_x} \tag{4}$$

We use Eq. 5 (CI = consistency index) and Eq. 6 (CR = consistency ratio) to establish the consistency of the matrix so that we can examine the reliability of the judgments in the pairwise comparison. In Eq. 6, the random indexes (RI) are defined as a set of random indexes by Saaty (1980) according to the values of n. In the current study, there are four objects and three relative criteria for each object. Therefore, we adopt the suggested values of RI (i.e., 0.9 for four objects and 0.58 for three relative criteria) to process Eq. 6.

$$\mathrm{CI} = \frac{\beta_{\max} - \mathrm{n}}{\mathrm{n} - 1} \tag{5}$$

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{6}$$

Sensitivity analysis

Sensitivity analysis usually manipulates research model parameters to determine the extent to which they affect the feasible outputs of the research model (Ho and Chen 2009). This specific research approach is very effective because it permits people to understand the different results that can occur despite divergences in the assumptions of the research model (Winebrake and Creswick 2003). In the AHP, the outcome depends on decision makers' subjective understanding of the relative importance of these factors (Erkut and Tarimcilar 1991). This study integrates the AHP with sensitivity analysis to establish hypothetical scenarios and offers decision makers more information for identifying how dissimilar situations determine decisions by altering their initial considerations. Numerous studies on technology evaluations have employed sensitivity analysis to examine the effects caused by variations in weights (Barin et al. 2009; Wang et al. 2013; Başar 2018).

A sensitivity analysis is performed to explore corresponding scenarios and how the modified TAM affects the biometric identification in FinTech applications. The procedure is described in the following equations (Erkut and Tarimcilar 1991; Srdjevic et al. 2012). Equation 7 for the final score of the solution represented in z is as follows:

$$z_k = \sum_{x=1}^{n} d_x f_{xk} \tag{7}$$

where the weight with respect to criterion x is defined as d_x, and the principal eigenvector of the comparison matrix under criterion x is defined as vector f_x. We can use vector f_x to determine the corresponding values of the k solutions related to criterion x.

Assume that the researcher enters the original weights of the pairwise comparisons, which are (d_1, d_2, d_3, d_4) of four objects. Equation 8 represents the score of solution k:

$$z_k = f_{1k}d_1 + f_{2k}d_2 + f_{3k}d_3 + f_{4k}d_4 \tag{8}$$

If the researcher wishes to vary d_1 and if $q_1 = d_2/d_3$ and $q_2 = d_4/d_3$, Eq. 9 can be derived as follows:

$$d_1 + d_2 + d_3 + d_4 = d_1 + q_1d_3 + d_3 + q_2d_3 = 1 \tag{9}$$

Equation 9 implies the following relations:

$$d_2 = q_1(1 - d_1)/1 + q_1 + q_2 \tag{10}$$

$$d_3 = 1 - d_1/1 + q_1 + q_2 \tag{11}$$

$$d_4 = q_2(1 - d_1)/1 + q_1 + q_2 \tag{12}$$

Equations 10, 11, and 12 can be substituted into Eq. 8 to obtain Eq. 13 as follows:

$$z_k = f_{1k}d_1 + f_{2k}q_1(1 - d_1)/(1 + q_1 + q_2) + f_{3k}(1 - d_1)/(1 + q_1 + q_2) + f_{4k}q_2(1 - d_1)/(1 + q_1 + q_2) \tag{13}$$

This study employs this procedure to graphically display the z_k scores; in this way, we can vary the value of d_1 from 0 to 1 (Erkut and Tarimcilar 1991; Srdjevic et al. 2012).

Empirical results

The constructed research framework is utilized to evaluate four common biometric recognitions that have been commercialized to recommend potential biometric identification in FinTech applications based on different perspectives of the modified TAM. The weights for each criterion are obtained using the AHP, as shown in Table 1. In addition, competitive biometric identification methods were assessed using a sensitivity analysis approach to meet the evaluation objects and relative criteria. The five evaluation object conditions constructed via sensitivity analysis are the general, perceived ease of use dominant, perceived usefulness dominant, perceived trust dominant, and perceived privacy dominant scenarios. The results are discussed in the following sections.

AHP analysis

The respondents are all international students who often use FinTech applications to process cross-border money transfers, e-payments, student loans, insurance, and even some investments online. Their age distribution ranges from 22 to 33 years old. For research purposes, 361 respondents were surveyed via a paper-based questionnaire, but only 264 respondents had user experience in the four biometric technologies. In this way, we can confirm that respondents have a certain level of knowledge about both the biometric technologies and FinTech applications. The survey period is from August 1, 2019, to October 31, 2019.

Table 1 AHP analysis results

Object and criteria	AHP weights	Final weights	Recognitions			
			Face	Fingerprint	Iris	Voice
Perceived ease of use	0.276		0.279	0.254	0.206	0.260
PE1	0.369	0.102	0.282	0.196	0.233	0.289
PE2	0.334	0.092	0.253	0.347	0.155	0.245
PE3	0.298	0.082	0.305	0.223	0.231	0.241
Perceived usefulness	0.257		0.261	0.253	0.188	0.298
PU1	0.395	0.102[a]	0.264	0.268	0.137	0.331
PU2	0.285	0.073	0.262	0.244	0.223	0.271
PU3	0.320	0.082	0.256	0.244	0.218	0.282
Perceived trust	0.184		0.222	0.252	0.299	0.227
PT1	0.306	0.056	0.190	0.243	0.352	0.215
PT2	0.317	0.058	0.246	0.285	0.205	0.264
PT3	0.378	0.070	0.225	0.233	0.337	0.205
Perceived privacy	0.283		0.272	0.240	0.257	0.231
PP1	0.374	0.106	0.294	0.238	0.241	0.227
PP2	0.284	0.080	0.295	0.220	0.280	0.205
PP3	0.342	0.097	0.229	0.260	0.254	0.257
Final scores			0.262	0.250	0.233	0.255
Rank			1	3	4	2

Saaty (1980) considered that the CI measurement of the AHP analysis is consistent with the CR measurement below 0.1. Thus, the objects and criteria of this study are consistent with the consistency test and have validity

[a] Larger at the fifth decimal digit

The questionnaire is used to evaluate the biometrics in FinTech applications according to the modified TAM. As suggested by Saaty (1980), we verify the consistency of 264 questionnaires and that the valid questionnaire's CI and CR values are less than 0.1 to meet the requirement. As a result, the final standard weight of the evaluation framework was obtained using the AHP.

As shown in Table 1, the PP object (0.283) is the most emphasized object when using the modified TAM to explore biometric identification in FinTech applications, followed by the perceived ease of use (0.276), PU (0.257), and PT (0.184) objects. Nevertheless, PP, perceived ease of use, and PU were over 0.25, but PT did not exceed 0.25. This finding indicates that when exploring this research topic, the particular aspects of how users perceive trust should be considered (Hassan and Wood 2020).

Within the perceived privacy object, PP1 ("Users perceive that biometric identification in FinTech applications will not invade privacy" (0.374)) was highlighted as the most critical criterion. According to some studies, the major expectations of biometric identification development and popularization should include the protection of personal privacy during commercialization (Ogbanufe and Kim 2018; Wang et al. 2019). In compliance with the first criterion of the analysis, not invading privacy is the first PP object to further accentuate the effort to realize and promote biometric identification in FinTech applications.

PE1, "Users perceive that biometric identification in FinTech applications is convenient to use" (0.369), was expressed as the highest priority factor in perceived usability objects. Compared with passwords or other methods, people are increasingly concerned about

convenience, so the demand for reliable user identification technology has increased. Therefore, biometrics is considered an effective tool for logging into FinTech applications (Mead 2016). In some cases, biometrics can be used in conjunction with the interface of FinTech applications to reduce the login time provided by system mechanisms. Therefore, biometrics can be utilized to not only improve user convenience but also enhance security. This implies that perceived ease of use has helped promote the popularity of biometrics and FinTech applications (Costigan 2017).

PU1, "Users perceive that biometric identification in FinTech applications is effective" (0.395), was the main criterion for exploring the perceptually useful objects of this research topic. It is necessary to examine the setting of thresholds of a recognition system for effective matching because both registration and acquisition failures (in recognition processes) mean that the system cannot "extract" and distinguish the appropriate feature characteristics of the user's biometrics. Failure to register and/or obtain access indicates that a person's biometrics may not be of sufficient quality for identification; however, the user would then consider the biometric technology to be useless. Alternatively, auxiliary applications, software, or mechanisms can be adjusted to provide a better user experience while increasing login success rates. As a result, users will be more likely to accept biometrics in FinTech applications (Stewart and Jürjens 2018).

PT3 of the perceived trust object, "Users perceive that biometric identification in FinTech applications is safer than other identification methods," ranks first. PT3 plays the most important role in being perceived as trustworthy by users (Jain et al. 2016). With the competition of various types of identification methods, biometric technologies that have been developed can gain user trust (Menat 2016). However, trust needs to be established over a long period; this need may explain why PT has less weight in the model. The weights of the other two criteria within this object are also lower than those of other objects. However, by separately reviewing the criteria, we can still comprehend the strengths of biometric identification in FinTech applications. When users perceive trust as time passes, the advantages of biometric identification will become one of the important core competencies of these technologies. Regarding the results of this study, there is still room for improvement in PT, which could then increase use intention.

General scenario

This scenario represents the user's opinion on the evaluation object related to the corresponding biometric method in the FinTech application. The combined results indicate how to simultaneously achieve all four assessment goals. After completing the modified TAM via the AHP, our interviewees evaluated these four biometric technologies to determine the most recommendable and more potential biometric technology. Respondents compared the performance of each biometric technology in pairs. As shown in Table 1, face recognition (0.262) is the most recommended, followed by voice recognition (0.255), fingerprint recognition (0.250), and iris recognition (0.233).

In addition, a score for every solution according to the criteria is calculated in each column in Table 1. These scores represent a performance distribution of the particular assessment of biometric methods. Several important explanations of the general condition can be made based on the results. Because face recognition may meet the requirements of the perceived ease of use object and PP object, this technology performs best

among the four biometric technologies. Fingerprint recognition is the most commonly employed and stably performing technology in every object (refer to Fig. 3). In addition to meeting the requirement of perceived ease of use, face and voice recognition also work well in terms of PU; these originate from biometric characteristics in human behaviors. This finding explains why face and voice recognition received higher scores on the AHP. However, fingerprint recognition does not rank as well as most people predicted possibly because it is more familiar to people, so the respondents could not clearly recognize its specialty. The results suggest that iris recognition can be improved.

Perceived ease of use dominant scenario

By varying the weights assigned to the four analysis objects, this study confirms the preference of biometric recognition methods in FinTech applications with specific conditions. In this case, it is assumed that easy-to-use objects are predominant. As illustrated by Fig. 4, the weight of perceived ease of use increases from the original weight of 0.276 to a maximum weight of 1, while the weights of the other three objects decrease proportionally to zero, as shown in Eqs. 9–13.

When the perceived ease of use weight is 1, we note that the score of face recognition is ranked first (0.279), followed by voice recognition (0.260), fingerprint recognition (0.254), and iris recognition (0.206). Although the ranking was consistent, the face recognition score increased, the iris recognition score decreased, and the other two scores underwent minimal changes. Face recognition was ranked second in the current biometric technology market (Wu et al. 2018). Initially, face recognition scored higher in easy-to-use criteria, but iris recognition was weaker in the object's criteria. Therefore, as the weight of perceived ease increases, face recognition scores better. The obvious conclusion is that the biometrics evaluated in different situations will produce different results. In this case, face recognition is undoubtedly the preferred biometric recognition

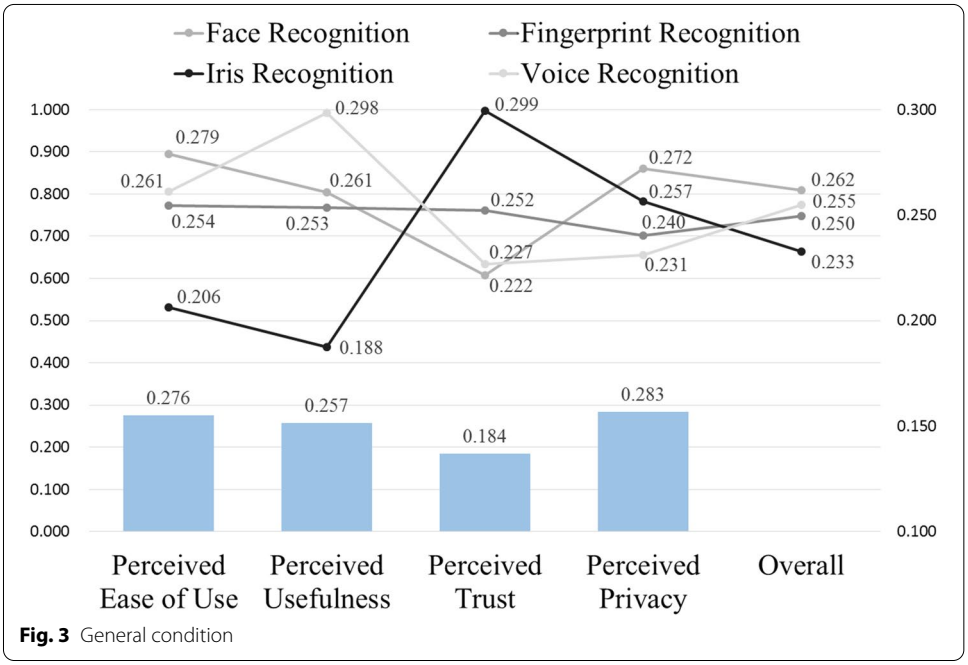

Fig. 3 General condition

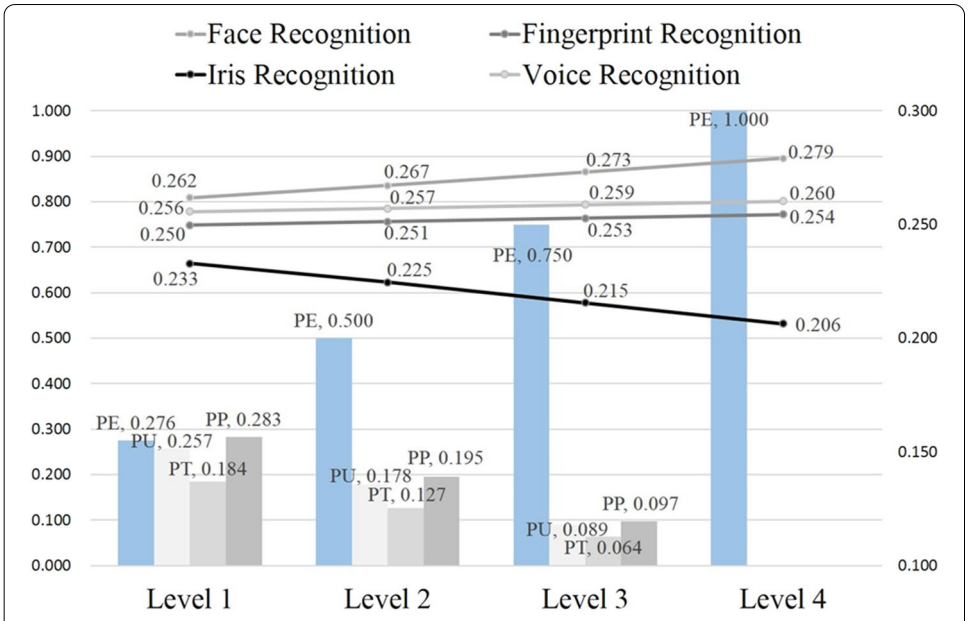

Fig. 4 Perceived ease of use dominant scenario

method to meet this object requirement. In commercialization, fingerprint recognition identification is most commonly adopted in current applications. However, due to user behavior, face recognition and voice recognition may become popular in future FinTech applications.

Perceived usefulness dominant scenario

In the PU dominant scenario, its weight gradually increases to be the dominant evaluation object in the same way as in the previous scenario. As shown in Fig. 5, voice recognition (0.298) is the most advantageous biometric identification, but iris recognition is still disadvantageous. This scenario is relevant when discussing the benefits of utilizing biometric usefulness, and voice recognition performs well compared to the other technologies due to its high performance with the criteria for this object. According to this result, voice recognition can be developed and its rank improved given its high level of usefulness. Unsurprisingly, voice recognition has attracted attention because of the recent increase in artificial intelligence (AI) voice assistants (Sriwati et al. 2019). Assuming that there is a desire for one form of biometric identification to better facilitate its usefulness, the odds of amplifying its penetration and popularity in FinTech applications can be overcome. Voice recognition is applied not only in identification but also in machine or application control. Such functions have recently been embedded in some FinTech applications (Li and Mills 2019).

Perceived trust dominant scenario

When the PT object emphasizes its related importance in this scenario as the dominator, as shown in Fig. 6, iris recognition has the highest score (0.299) and is the most significant identification in this scenario, fingerprint recognition (0.252) remains stable,

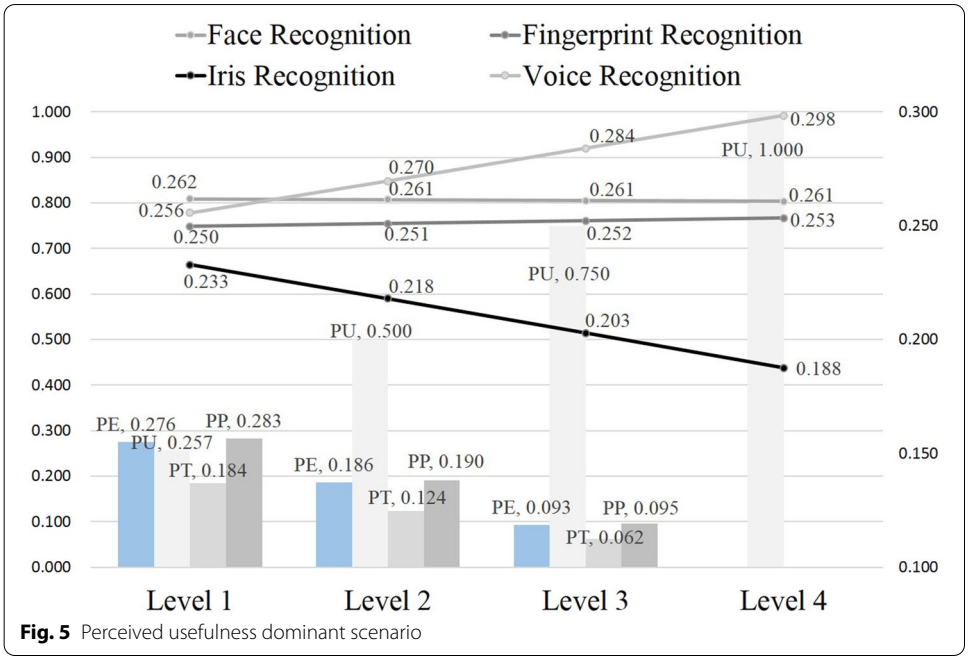

Fig. 5 Perceived usefulness dominant scenario

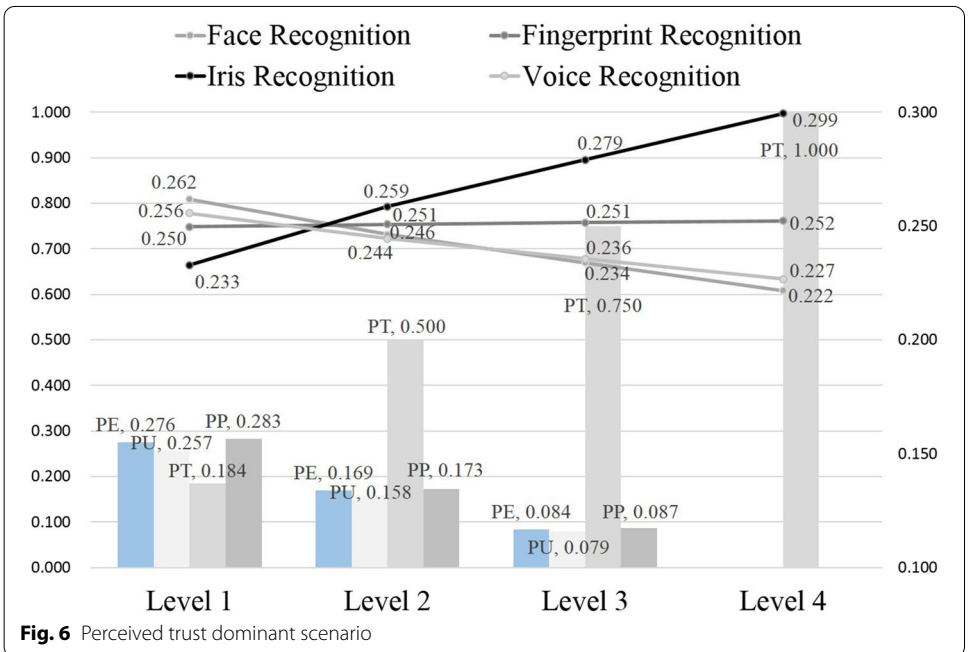

Fig. 6 Perceived trust dominant scenario

followed by voice recognition (0.227), and face recognition (0.222). Compared with other biometric identification methods, the biometric characteristics of iris recognition are more special and difficult to imitate (Ross 2010); thus, it gains a higher degree of trust. However, owing to limited ease of use and usefulness, the application of iris recognition is not as popular as the other three types of recognition. Although fingerprint recognition does not stand out for each object, it balances every requirement of each

object. Therefore, fingerprint recognition is still the more popular biometric identification in all kinds of applications (Ogbanufe and Kim 2018). We believe that fingerprint recognition will not be absent in FinTech applications.

Perceived privacy dominant scenario

In the PP dominant scenario, PP is emphasized as the main evaluation target. As illustrated in Fig. 7, face recognition (0.272) ranks first, followed by iris recognition (0.257), fingerprint recognition (0.240), and voice recognition (0.231). Because every biometric has a specific principle and mechanism, it is hard to assess which is more prominent corresponding to each criterion of the PP object. Therefore, the difference between any two scores is slight. Unsurprisingly, based on the perspective of user behavior, face recognition still ranks first and completely demonstrates its competitiveness in biometrics in FinTech applications. It should be highlighted that faces are easy to see; therefore, face recognition involves minor privacy issues (Trivikram et al. 2017). The integrity of a biometric identifier in all objects will lead to its prosperity in FinTech applications.

Conclusion

In recent years, biometric technology has been vigorously promoted globally to enhance security in information technology (IT) and promote the development of emerging industries (Wang et al. 2019). Although biometric technologies have been employed in particular fields for a long time, they have gradually gained popularity to enhance the security of consumers and consumer electronics (Jain et al. 2016; Dubey 2019). To meet the various needs of FinTech applications, since user experience has an important role in FinTech applications, each form of biometric recognition should be carefully reviewed based on user perception (Milian et al. 2019). The current study identifies how different evaluation objects of the improved TAM determine the corresponding biometrics

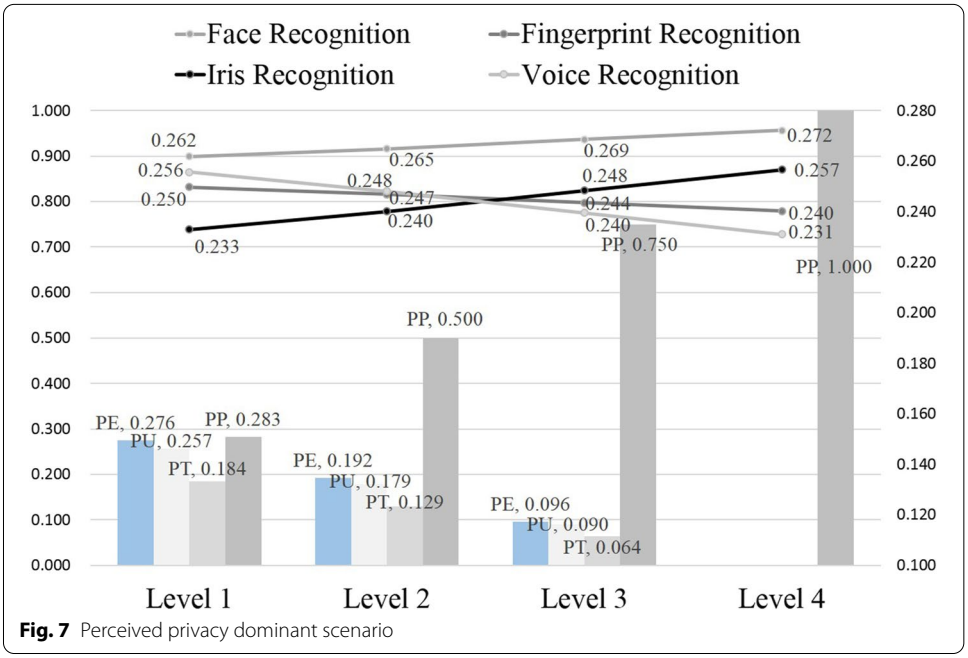

Fig. 7 Perceived privacy dominant scenario

in FinTech applications. The AHP was applied to assess evaluation objects and confirm their relative importance. In addition, the results generated by the AHP were applied to collect corresponding biometrics in the FinTech applications for five different evaluation target scenarios via sensitivity analysis. A total of five conditions are obtained by separately adjusting the weights of the four evaluation objects. In this way, we deduce which biometrics can perform better and the corresponding conditions. These findings can help readers understand how users view biometrics in FinTech applications.

Research contributions

This research makes several contributions as follows:

1. The research results indicate that face recognition generally received higher scores than the other types of recognition; voice and fingerprint recognition received the next highest scores. Face recognition also performed the best in the perceived ease of use dominant scenario. Voice recognition became a much more recommendable biometric identification in the PU dominant scenario and significantly outperformed the other three technologies. In the PT dominant scenario, iris recognition was regarded as the best form of identification owing to its biometric competence. In the last scenario, the PP dominant scenario, face recognition still ranked first and completely demonstrated its competitiveness based on user behavior perspectives. According to these scenarios, the ranking of biometric identifications in the suggested list for FinTech applications, from most to least beneficial, is face recognition, voice recognition, fingerprint recognition, and iris recognition.
2. In all scenarios, we observe that fingerprint recognition has relatively stable performance, thus explaining why it has a greater market share. However, the results indicate that most people consider that face recognition will have more merit in the future. Therefore, developers should consider strategic approaches to expand FinTech applications with embedded face recognition and then increase the penetration of this technology.
3. The research results indicate that voice recognition scored the highest in the PU scenario. This finding is consistent with those of other reports, which indicate that voice recognition has ranked second in multi-biometric systems (Trivikram et al. 2017). Since AI voice assistant devices, such as Amazon Echo, have become popular, voice recognition has become the most noticeable biometric because it demonstrates the best usefulness of identification (Sriwati et al. 2019).
4. The future of biometric identification in FinTech applications demands rigorous identification of individuals in high-security environments. However, this study concludes with some considerations, such as those of the PT and PP objects, as presented in Table 1. When biometric identification has obtained more working credit, these considerations of the PT object may decrease.
5. Finally, researchers have focused on the criteria for predicting which biometric identification to evaluate so that they can utilize it. Nevertheless, technologies that they predicted may be different from biometric approaches but less applicable to commerce and the market continue to be applied in FinTech. This study not only constructs a modified TAM but also suggests strategies for developing biometric

forms of identification in FinTech applications. Developers of biometric identification methods should take the advantages or disadvantages discovered from research results into account in the future for strengthening, improving, or even eliminating other potential technologies. For instance, face recognition should address its weakness in the criteria of the PT object.

The results indicate that face recognition, voice recognition, and fingerprint recognition can simultaneously achieve all four object requirements. While face recognition is regarded as the best form of biometric identification for FinTech applications, fingerprint recognition is a stable alternative, and voice recognition is a potential alternative.

Research limitations and future work

This study has some limitations. First, most of the respondents are international students, so the results may not represent the overall opinions of users. Those performing further research may consider conducting studies worldwide. Second, we did not categorize the participants by demographic segmentation, thus possibly affecting the generalizability of the results. Hence, future research may include demographic segmentation to proceed with a typical structural equation modeling analysis. The third limitation is the hypothetically stated criteria. Although all participants were experienced in all four biometric identification methods, the results may be affected if some participants did not clearly remember their previous user experience. Hence, future research could examine whether frequency influences user perception.

Received: 2 October 2020 Accepted: 24 May 2021
Published online: 08 June 2021

References

Abhishek A, Hemchand S (2016) Adoption of sensor-based communication for mobile marketing in India. J Indian Business Res 8(1):65–76. https://doi.org/10.1108/JIBR-08-2015-0091
Alhassany H, Faisal F (2018) Factors influencing the internet banking adoption decision in North Cyprus: an evidence from the partial least square approach of the structural equation modeling. Financ Innov. https://doi.org/10.1186/s40854-018-0111-3
Arner DW, Barberis J, Buckley RP (2016) The evolution of fintech: new post-crisis paradigm. Georget J Int Law 47(4):1271–1320
Arner DW, Barberis J, Buckey RP (2017) Fintech, regtech, and the reconceptualization of financial regulation. Northwest J Int Law Bus 37(3):371–414
Arner DW, Zetzsche DA, Buckley RP, Barberis J (2019) The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. Eur Bus Organ Law Rev 20:55–80
Atmaca S, Karadaş HA (2020) Decision making on financial investment in Turkey by using ARDL long-term coefficients and AHP. Financ Innov. https://doi.org/10.1186/s40854-020-00196-z
Bagozzi RP (2007) The legacy of the technology acceptance model and a proposal for a paradigm shift. J Assoc Inf Syst 8(4):243–254
Barin A, Canha LN, da Rosa Abaide A, Magnago KF (2009) Selection of storage energy technologies in a power quality scenario—the AHP and the fuzzy logic. In: Paper presented at the industrial electronics, 2009. IECON '09. 35th annual conference of IEEE. https://doi.org/10.1109/IECON.2009.5415150
Barkadehi MH, Nilashi M, Ibrahim O, Fardi AZ, Samad S (2018) Authentication systems: a literature review and classification. Telemat Inform 35(5):1491–1511
Başar A (2018) Aligning business and IT strategies in banking: a case study. J Glob Strat Manag 12(1):5–16
Biometrics Identity Management Agency (BIMA) (2010) Biometrics glossary version 4.0. Software Engineering Center CECOM Life Cycle Management Command. https://www.marines.mil/Portals/1/MCRP%203-33.1J%20BIOMETRICS%201.pdf. Accessed 23 June 2019
Breckenridge K (2014) Biometric state the global politics of identification and surveillance in South Africa, 1850 to the present. Cambridge University Press, Cambridge
Buckley O, Nurse JCR (2019) The language of biometrics: analysing public perceptions. J Inf Secur Appl 47:112–119

Callen-Naviglia J, James J (2018) FinTech, RegTech and the importance of cybersecurity. Issues Inf Syst 19(3):220–225
Cao X, Yu L, Liu Z, Gong M, Adeel L (2018) Understanding mobile payment users' continuance intention: a trust transfer perspective. Internet Res 28(2):456–476
Carranza R, Díaz E, Sánchez-Camacho C, Martín-Consuegra D (2021) e-Banking adoption: an opportunity for customer value co-creation. Front Psychol. https://doi.org/10.3389/fpsyg.2020.621248
Chau PYK, Hu PJH (2001) Information technology acceptance by individual professionals: a model comparison approach. Decis Sci 32(4):699–719
Cheng YH, Yeh YI (2011) Exploring radio frequency identification technology's application in international distribution centers and adoption rate forecasting. Technol Forecast Soc Change 78:661–673
Choi H, Park J, Kim J, Jung Y (2020) Consumer preferences of attributes of mobile payment services in South Korea. Telemat Inform. https://doi.org/10.1016/j.tele.2020.101397
Chopdar PK, Sivakumar VJ (2019) Understanding continuance usage of mobile shopping applications in India: the role of espoused cultural values and perceived risk. Behav Inf Technol 38(1):42–64
Costigan N (2016) Behavioural biometrics—a new era of security. In: Chishti S, Barberis J (eds) The Fintech book: the financial technology handbook for investors, entrepreneurs and visionaries. Wiley, pp 116–117
Costigan N (2017) Assessing the impact of advanced sensors and behavioural biometric authentication technology on the reach of financial institutions. J Digit Bank 2(2):163–170
Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q 13:319–340
Donohue LK (2012) Technological leap, statutory gap, and constitutional abyss: remote biometric identification comes of age. Minn Law Rev 97(2):407–559
Drummer D, Feuerriegel S, Neumann D (2017) Crossing the next frontier: the role of ICT in driving the financialization of credit. J Inf Technol 32(3):218–233
Dubey V (2019) Fintech—digital way of ID verification and biometric verification in 2020. Int J Innov Appl Stud 27(4):896–901
Eagar M (2016) FinTech þ digital currency—convergence or collision? In: Chishti S, Barberis J (eds) The Fintech book: the financial technology handbook for investors, entrepreneurs and visionaries. Wiley, pp 212–216
Erkut E, Tarimcilar M (1991) On sensitivity analysis in the analytic hierarchy process. IMA J Math Appl Bus Ind 3(1):61–83
Faddis NK, Matey RJ, Stracener J (2013) Improving tactical biometric systems through the application of systems engineering. IET Biom 2(1):1–9
Fenu G, Marras M (2018) Controlling user access to cloud-connected mobile applications by means of biometrics. IEEE Cloud Comput 5(4):47–57
Galankashi RM, Rafiei FM, Ghezelbash M (2020) Portfolio selection: a fuzzy-ANP approach. Financ Innov. https://doi.org/10.1186/s40854-020-00175-4
Ghani MA, Rahi S, Yasin NM, Alnaser FM (2017) Adoption of internet banking: extending the role of technology acceptance model (TAM) with E-customer service and customer satisfaction. World Appl Sci J 35(9):1918–1929
Guo G, Wechsle H, Shan S, Poh N (2016) Guest editorial special issue on mobile biometrics. IET Biom 5(1):1–2
Hassan HE, Wood VR (2020) Does country culture influence consumers' perceptions toward mobile banking? A comparison between Egypt and the United States. Telemat Inform 46:101312. https://doi.org/10.1016/j.tele.2019.101312
Ho CJ, Chen JS (2009) Forecasting VoWLAN technology for the Taiwan mobile telecommunication industry. Technol Anal Strateg Manag 21(2):213–232
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. https://doi.org/10.3390/sym11030340
Imerman MB, Fabozzi FJ (2020) Cashing in on innovation: a taxonomy of FinTech. J Asset Manag 21:167–177. https://doi.org/10.1057/s41260-020-00163-4
Iyer AP, Karthikeyan J, Khan RH, Binu PM (2020) An analysis of artificial intelligence in biometrics—the next level of security. J Crit Rev 7(1):571–576
Jain AK, Nandakumar K, Ross A (2016) 50 years of biometric research: accomplishments, challenges, and opportunities. Pattern Recogn Lett 79:80–105
Jeong N, Yoo Y, Heo TY (2009) Moderating effect of personal innovativeness on mobile-RFID services: based on Warshaw's purchase intention model. Technol Forecast Soc Change 76:154–164
Jonker N (2019) What drives the adoption of crypto-payments by online retailers? Electron Commer Res Appl 35:100848. https://doi.org/10.1016/j.elerap.2019.100848
Kalinić Z, Marinković V, Djordjevic A, Liebana-Cabanillas F (2019) What drives customer satisfaction and word of mouth in mobile commerce services? A UTAUT2-based analytical approach. J Enterp Inf Manag 33(1):71–94
Kanak A, Sogukpinar I (2017) BioTAM: a technology acceptance model for biometric authentication systems. IET Biom 6(6):457–467
Kang J (2018) Mobile payment in Fintech environment: trends, security challenges, and services. Hum-Cent Comput Inf Sci. https://doi.org/10.1186/s13673-018-0155-4
Kang JW, Namkung Y (2019) The role of personalization on continuance intention in food service mobile apps. Int J Contemp Hosp Manag 31(2):734–752
Kim M, Kim S, Kim J (2019) Can mobile and biometric payments replace cards in the Korean offline payments market? Consumer preference analysis for payment systems using a discrete choice model. Telemat Inform 38:46–58
Ko CH, Yu CC (2015) Exploring employees' perception of biometric technology adoption in hotels. Int J Organ Innov 8(2):187–199
Kou G (2019) Introduction to the special issue on FinTech. Financ Innov. https://doi.org/10.1186/s40854-019-0161-1
Kou G, Lin C (2014) A cosine maximization method for the priority vector derivation in AHP. Eur J Oper Res 235(1):225–232. https://doi.org/10.1016/j.ejor.2013.10.019
Kou G, Ergu D, Shang J (2014) Enhancing data consistency in decision matrix: adapting Hadamard model to mitigate judgment contradiction. Eur J Oper Res 236(1):261–271. https://doi.org/10.1016/j.ejor.2013.11.035

Lee JM, Rha JY (2016) Personalizatione-privacy paradox and consumer conflict with the use of location-based mobile commerce. Comput Hum Behav 63:453–462
Lee S, Kim BS, Kim Y, Kim W, Ahn W (2018) The framework for factors affecting technology transfer for suppliers and buyers of technology in Korea. Technol Anal Strateg Manag 30(2):172–185
Li X, Mills M (2019) Vocal features: from voice identification to speech recognition by machine. Technol Cult 60(2):129–160
Liébana-Cabanillas F, Lara-Rubio J (2017) Predictive and explanatory modeling regarding adoption of mobile payment systems. Technol Forecast Soc Change 120:32–40
Lin C, Kou G, Peng Y (2020) Aggregation of the nearest consistency matrices with the acceptable consensus in AHP-GDM. Ann Oper Res. https://doi.org/10.1007/s10479-020-03572-1
Liu CH, Wang JS, Peng CC, Shyu JZ (2015) Evaluating and selecting the biometrics in network security. Secur Commun Netw 8(5):727–739
Mead W (2016) Banking and the E-book moment. In: Chishti S, Barberis J (eds) The Fintech book: the financial technology handbook for investors, entrepreneurs and visionaries. Wiley, pp 7–9
Mehrban S et al (2020) Towards secure FinTech: a survey, taxonomy, and open research challenges. IEEE Access 8:23391–23406. https://doi.org/10.1109/ACCESS.2020.2970430
Menat R (2016) Why we're so excited about fintech. In: Chishti S, Barberis J (eds) The Fintech book: the financial technology handbook for investors, entrepreneurs and visionaries. Wiley, pp 10–12
Merhi M, Hone K, Tarhini A, Ameen N (2020) An empirical examination of the moderating role of age and gender in consumer mobile banking use: a cross-national, quantitative study. J Enterp Inf Manag. https://doi.org/10.1108/JEIM-03-2020-0092
Milian EZ, de Spinola M, de Carvalho MM (2019) Fintechs: a literature review and research agenda. Electron Commer Res Appl 34:100833. https://doi.org/10.1016/j.elerap.2019.100833
Morosan C (2016) An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports. J Air Transp Manag 55:120–128
Murakami T, Fujita R, Ohki T, Kaga Y, Fujio M, Takahashi K (2019) Cancelable permutation-based indexing for secure and efficient biometric identification. IEEE Access 7:45563–45582. https://doi.org/10.1109/ACCESS.2019.2908456
Norma D, Farah ML (2020) Factors affecting continuance intention of FinTech payment among Millennials in Jakarta. Eur J Bus Manag Res. https://doi.org/10.24018/ejbmr.2020.5.4.444
Ogbanufe O, Kim DJ (2018) Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decis Support Syst 106:1–14
Pai CK, Wang TW, Chen SH, Cai KY (2018) Empirical study on Chinese tourists' perceived trust and intention to use biometric technology. Asia Pac J Tour Res 23(9):880–895
Patil P, Tamilmani K, Rana NP, Raghavan V (2020) Understanding consumer adoption of mobile payment in India: extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. Int J Inf Manag 54:102144. https://doi.org/10.1016/j.ijinfomgt.2020.102144
Pavlou PA (2003) Consumer acceptance of electronic commerce. Integrating trust and risk with the technology acceptance model. Int J Electron Commer 7(3):101–134
Priya R, Gandhi AV, Shaikh A (2018) Mobile banking adoption in an emerging economy: an empirical analysis of young Indian consumers. Benchmark Int J 25(2):743–762
Qi Y, Xiao J (2018) AI powers financial services to improve people's lives. Commun ACM 61(11):65–69
Rahia S, Ghani MA, Alnaser FM, Ngah AH (2018) Investigating the role of unified theory of acceptance and use of technology (UTAUT) in internet banking adoption context. Manag Sci Lett 8:173–186
Rashed A, Alajarmeh N (2015) Towards understanding user perceptions of biometrics authentication technologies. Int J Comput Sci Inf Secur 13(6):25–33
Ross A (2010) Iris recognition: the path forward. IEEE Comput 43(2):30–35
Saaty TL (1980) The analytic hierarchy process. McGraw-Hill
Schierz PG, Schilke O, Wirtz BW (2010) Understanding consumer acceptance of mobile payment services: an empirical analysis. Electron Commer Res Appl 9:209–216
Schmidt K, Aumann I, Hollander I, Damm K, von der Schulenburg JMG (2015) Applying the analytic hierarchy process in healthcare research: a systematic literature review and evaluation of reporting. BMC Med Inform Decis Mak 15:112–139
Shachak A, Kuziemsky C, Petersen D (2019) Beyond TAM and UTAUT: future directions for HIT implementation research. J Biomed Inform 100:103315. https://doi.org/10.1016/j.jbi.2019.103315
Shao Z, Zhang L, Li X, Guo Y (2019) Antecedents of trust and continuance intention in mobile payment platforms: the moderating effect of gender. Electron Commer Res Appl. https://doi.org/10.1016/j.elerap.2018.100823
Shaw B, Kesharwani A (2019) Moderating effect of smartphone addiction on mobile wallet payment adoption. J Internet Commer 18(3):291–309
Singh N, Sinha N, Liébana-Cabanillas FJ (2020) Determining factors in the adoption and recommendation of mobile wallet services in India: analysis of the effect of innovativeness, stress to use and social influence. Int J Inf Manag 50:191–205
Sonea A (2016) So, you think the innovation lab is the answer? In: Chishti S, Barberis J (eds) The Fintech book: the financial technology handbook for investors, entrepreneurs and visionaries. Wiley, pp 181–186
Srdjevic Z, Samardzic M, Srdjevic B (2012) Robustness of AHP in selecting wastewater treatment method for the coloured metal industry: Serbian case study. Civ Eng Environ Syst 29(2):147–161
Sriwati S, Eruinsyah E, Karim S, Rahman F (2019) Control of electronic devices using smartphone-based voice identification. IOP Conf Ser Mater Sci Eng 662:022004. https://doi.org/10.1088/1757-899X/662/2/022004
Stewart H, Jürjens J (2018) Data security and consumer trust in FinTech innovation in Germany. Inf Comput Secur 26(1):109–128

Tanimoto S, Toriyama S, Iwashita M, Endo T, Chertchom P (2019) Secure operation of biometric authentication based on user's viewpoint. In: 2019 IEEE international conference on big data, cloud computing, data science and engineering (BCD), Honolulu, HI, USA, 2019, pp 166–171. https://doi.org/10.1109/BCD.2019.8885177
Trivikram C, Samarpitha S, Madhavi K, Moses D (2017) Evaluation of hybrid face and voice recognition systems for biometric identification in areas requiring high security. I-Manag J Pattern Recogn 4:9–16
Venkatesh V, Davis FD (2000) A theoretical extension of the technology acceptance model: four longitudinal field studies. Manag Sci 46(2):186–204
Venkatesh V, Davis FD, Morris MG (2007) Dead or alive? The development, trajectory and future of technology adoption research. J Assoc Inf Syst 8:267–286
Wang JS, Liu CH, Shyu JZ (2013) Biometrics technology evaluating and selecting model building. Technol Anal Strateg Manag 25(9):1067–1083
Wang X, Xue H, Liu X, Pei Q (2019) A privacy-preserving edge computation-based face verification system for user authentication. IEEE Access 7:14186–14197
Winebrake JJ, Creswick BP (2003) The future of hydrogen fueling systems for transportation: an application of perspective-based scenario analysis using the analytic hierarchy process. Technol Forecast Soc Change 70(4):359–384
Wu J, Liu L, Huang L (2017) Consumer acceptance of mobile payment across time: antecedents and moderating role of diffusion stages. Ind Manag Data Syst 117(8):1761–1776
Wu SC, Chen PT, Swindlehurst AL, Hung PL (2018) Cancelable biometric recognition with ECGs: subspace-based approaches. IEEE Trans Inf Forensics Secur 14(5):1323–1336
Yu D, Kou G, Xu Z, Shi S (2021) Analysis of collaboration evolution in AHP research: 1982–2018. Int J Inf Technol Decis Mak 20(1):7–36. https://doi.org/10.1142/S0219622020500406
Zhang J, Kou G, Peng Y, Zhang Y (2021) Estimating priorities from relative deviations in pairwise comparison matrices. Inf Sci 552:310–327. https://doi.org/10.1016/j.ins.2020.12.008
Zhu Y, Li X, Wang J, Li J (2020) Cloud-assisted secure biometric identification with sub-linear search efficiency. Soft Comput 24:5885–5896. https://doi.org/10.1007/s00500-019-04401-9

Publisher's Note