Chapter

Assessment of How Users Perceive the Usage of Biometric Technology Applications

Taban Habibu, Edith Talina Luhanga and Anael Elikana Sam

Abstract

Biometrics applications are progressively widespread as a means of authenticating end-users owing to the extensive range of benefits over traditional authentication (token-base-authentication). However, the transaction involves taking into account the perceptions and responses of end-users. If end-users are fearful, hesitant about these biometric technology-applications, misuse and implementation-complications can surely overshadow. The goal of this study is to sightsee the user's-motivation, understanding, consciousness and acceptance towards utilization of biometric technology-applications. A 300-person survey was conducted to evaluate public-opinion on the use and adoption of biometrics. Stratified sample technique was used to administer the surveys. The results presented that perceived ease-of-use, user-motivation and attitude are more important-factors when deciding whether to accept new technology-applications. Although many end-users have become more familiar with biometric technology-applications (e.g., Fingerprints or facial-recognition), many individuals still have a negative-perception of the technology. Concerns regarding confidentiality and security i.e., storing and protecting personal-identification data, the fear of intruding into a person's daily-life and disclosing personal-information remain a major problem. Some end-users claim that despite the potential resilience to biometrics, designers must mentally and psychologically prepare the general public for the new use of biometric technology. This will make it possible to transform negative user-perceptions into a positive-experience. Thus, this study can help end-users and companies understand and make the right decisions to promote the use of biometric-applications and services. The study is expected to be an important research-discovery that will greatly contribute to Uganda's digital-economy.

Keywords: biometric application, user perception, privacy, security, utilization

1. Introduction

Biometric technologies are becoming more ubiquitous in our day-to-day life for a wide variety of applications such as border clearance and immigration, civilian ID cards, mobile banking, police and security, health care labs and many others [1]. The technology is used for authorization and proof of identity as a solution to the

challenges associated with combatting, managing and potentially resolving criminal activity [2, 3]. In fact, mobile companies have increasingly embraced biometric technologies to allow users to connect to their mobile devices by scanning their fingerprints and faces [4]. It is estimated that 100% of mobile devices i.e., smartphones, portable devices and tablets will require biometric protection by 2020 deliberately about preventing fraud. This is quite possible because users are now exposed to biometric technologies and never realize it. Banks and credit unions have used biometrics as part of a multi-level safety means to assist address risk-related concerns. It is expected that many others will move in this direction [3, 5].

Indian, Hindustan Computing Limited (HCL) Technologies reported that e-commerce inventors are discovering the usage of biometrics and smart cards to properly prove the identity of a party to the transaction. Because it can help to reach the security facilities on the handset via voice verification [6, 7]. Since the focus is on what the user is, rather than what the user knows or possesses. The implementation of biometrics is largely dependent on the degree to which system users are willing to accept the technology [8]. User behavior may cause or break the implementation of biometric technology. The process of providing personal data publicly may be offensive to some people. As well, users may associate fingerprints with law enforcement and crime and may be unwilling to use fingerprint systems [9]. Others believe that scanning, iris and retinal systems can be harmful to their eyes. In any event, these positions may potentially contribute to significant public embarrassment to the company that collected the data, regulatory fines or law suits. If DNA scans become prevalent, they can give escalation to an entire new arena of secrecy worries such as exposure of health situations and household relationships [10].

At present, there is not a single piece of legislation that provides a comprehensive overview, addresses legislation or provides standardized guidelines for the usage of biometrics [1]. The lack of a specific document or regulation that obliges as a pre-eminent guide and governs biometric usage leaves organizations to make their own rules about how to handle and use biometric data. The potential for misuse of biometrics is an important concern for users. Consequently, the perception of the user, especially in the field of security and privacy, must be well understood. As reported by Emami et al. user's perception on use of biometric applications are generally tied to their socio-cultural, religious believe, health matters and occasionally the lawful consequence of the subject matter which has to do with delinquency. Researchers found that when applying for biometrics, individuals are unwilling to allow for instance, their faces to be captured as it violates their religious belief. Once again, others are not comfortable entering their fingerprints for fear of a security breach or for health reasons. Chandra et al. reported that while user fear is: belief, user acceptance, secrecy concerns are not taken into consideration, there is a possible threat of system failure. It might be surprising to install biometric applications without assessing the acuity of biometric knowledge [11, 12]. As a result, users must be educated on why the system was introduced and how it can be beneficial to them.

The study therefore focuses on the intensity, comprehension, awareness and acceptance of biometric use by end-users. The objective is to provide useful information and benefits of the usage of biometrics technology as well as factors affecting end-users in the usage of related technologies. The author assumes that this study will help stakeholders and policymakers at different levels to differentiate between the capacity of the application of biometrics technology, and user acceptability in the design of robust procedures for deploying biometric technologies that are user-centric. The paper is prearranged into five sections: Section 2 briefly presents several

studies carried out to understand users' perceptions regarding the usage of biometric applications. Section 3 provides an idea of the method used in conducting the study. Section 4 presents the results and discusses their importance, and Section 5 presents the discussion of findings. Finally, the conclusion, limitations and some insights for future research.

2. Related work

The review addresses two main lines of research: (a) the Technology Acceptance Model (TAM) and (b) the user's perception of the usage of biometric technology application. The relevant literature for each of these two areas is discussed below.

2.1 Technology acceptance model (TAM)

To examine the public perception of the usage of biometric technology, the Technology Acceptance Model (TAM) was examined. This is an accepted model for explaining people's acceptance and behavior. Based on its simplicity and understanding [13, 14]. It helps researchers and practitioners distinguish between the reasons why a proposed technology may be acceptable or unacceptable [15]. The model is based on the Theory of Reasoned Action (TRA), a psychological approach that illustrates how the individual's belief application system acts on human behavior [16]. This implies that behavioral intent is closely related to real behavior. In essence, the TAM is based on two basic concepts: perceived usefulness (PU) and perceived ease of use (PEOU). Perceived usefulness is the extent to which a person believes that the usage of a particular technology would enhance their work performance [17]. If the assessed PU results are positive, users will tend to have confidence in the technology. However, perceived ease of use refers to the extent to which an individual believes that using a specific system would be effortless. The extent to which one believes that the usage of technology would exempt a person from conscientious work. In addition to the PU and PEOU, two other variables were expressed: attitude and motivation. Attitude is a general positive or negative assessment of a person's particular behavior. In studies of user behavior, attitude is considered as a predictor of the future inspiration to be used. Thus, the impact of the user's attitude on the intention to usage is universal, which partly explains why the TAM has been widely studied in various areas. Motivation is an indicator in which a system is used to measure subjective intent by users. This has a critical impact on whether a certain type of technology or system is accepted. Therefore, in the present study, the motivation to use was to define the magnitude of the intention of users with respect to the usage of biometric technology. **Figure 1** adds two variables that are proposed for the determinants of relative advantage, attitude and motivation to establish the intent and perception of the end-users to use the biometric technology application. The relative benefit is the level at which an innovation is better discovered than the practice previously employed. Derived from **Figure 1**, perceived usefulness, perceived ease of use, user attitudes, and user motivation are variables dependent on end-users' perception to make effective use of the application of biometric technology. As a result, technology users have greater acceptance and satisfaction. From this perspective, we anticipate the same thing in the case of accepting biometric technology. The greater the perceived usefulness, the greater the intent to accept a biometrics application system. The greater the perceived ease

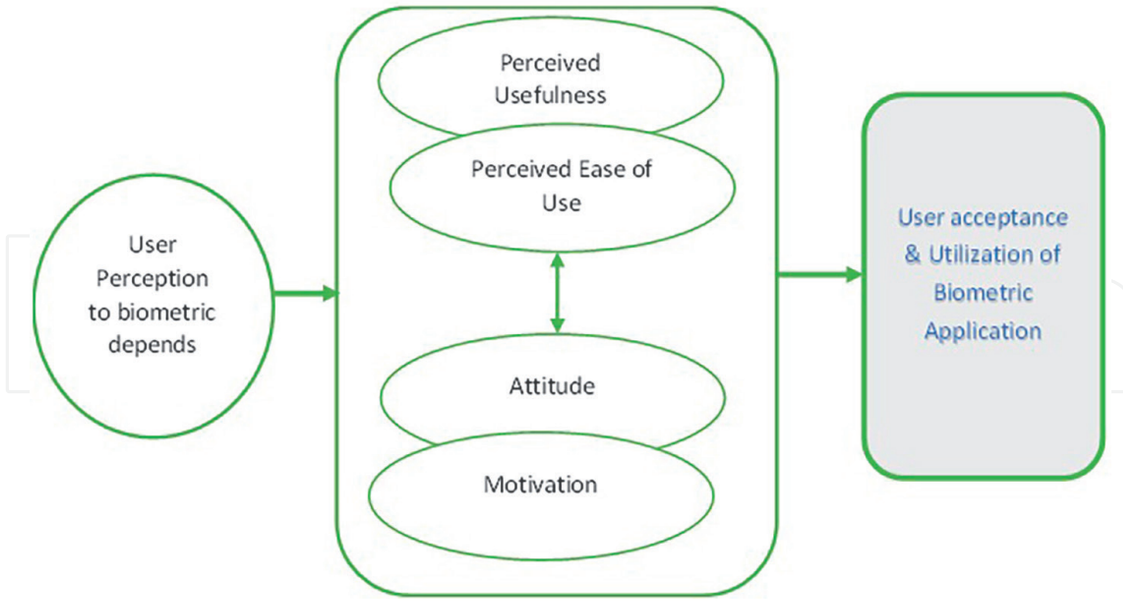

Figure 1.
Framework model for user acceptance of the biometric application.

of use, the greater the intended acceptance of a biometric system. The perceived usefulness of the biometrics system is positively correlated with perceived usability. The greater the attitude towards the use of the biometric application, the greater the likelihood that an end-user will consider a biometric application system to be useful. The higher the motivational factor, the more end users perceive a biometric application system to be easy to use.

2.2 User perception with respect to the usage of biometric applications

Increasingly, biometric technologies are being used in almost all areas of human activities for verification and identification [2, 4]. This technology allows for the collection of personal information and physiological data for identifying purposes. However, the available data is limited. Because users are more likely to have little acceptance or confidence in biometrics due to privacy concerns [18]. As such, it is significant to know the reasons that contribute to user acceptance as well as the need to consider user perception and will associated with biometric technology. As human perception is highly unpredictable in many cases, a greater comprehension of user needs is required.

Study by Habibu et al. [9] conducted a survey of user knowledge and concerns related to biometrics. The study shed light on the user's experience with the usage of biometrics. The findings present that the overall response was optimistic about their prior knowledge of biometric characteristics, but had relatively little practical experience using them. In addition, they noted that many technologies were generally better accepted than others. For example, respondents felt better about the usage of fingerprints and face images than with iris examinations. In fact, fingerprints and faces are used in many national identity systems. For example, inside access control, door pass, and client ID simply required the person to touch the sensor screen or look at the authentication device.

Carpenter et al. [19] presented a study examining workers privacy concerns associated to the organization's use of biometrics. Their findings suggest that

self-determination has played a significant role in formulating privacy protection, perceived accountability, and concerns about perceived vulnerability. The research suggests that, it serve as important indicators of user attitudes to biometric technologies in the workplace.

Furthermore, a study by Jones et al. [20] explaining the purpose of users to use biometrics as an authentication tool with young Arabs were studied. The findings revealed that, perceived ease and usefulness are the most decisive factor influencing user's perception to accept or reject new technology. Therefore, the key to increasing the acceptability of any technology is to work out how the negative perceptions can be lessened.

A study presented by Chan and Elliot [21] updated biometrics secrecy perceptions with two investigations. The first investigation, carried out amongst 200 participants, asked participants of their knowledges and insights of biometrics. Another investigation, observed to measure variations in perception over time. The study suggested a level of disbelief around the safety and secrecy of the biometric data. For example, forty-five percent (45%) of participants were not able to trust their data from a public company. Because the findings revealed that there was more support for the usage of biometrics in the fight against terrorism and the banking sector.

Furthermore, El-Abed et al. [22] claimed that the major drawback in the general satisfactoriness of biometric application is the lack of general assessment method that appraises performance, users' acceptance and satisfaction, data quality and security. Such evaluation methodology assists system designer to be able to ascertain suitability of the technology being designed and aid in making necessary adjustment to the design, in the early stage, to improve the satisfactoriness level.

Study by Elliot et al. [23] reviewed technique to identify and inspect the citizen's perceptions, opinions and fears of biometrics technology. The issues such as security and privacy concerns of users are asked in the review. The findings indicated that people are pro biometrics i.e., they accept the biometrics utilization as a way to enhance security, but they have fears about their privacy (who can utilize that information). The mainstream of the individuals accepted the biometric technology, but also, have security anxieties of using biometric technology. In short, the individuals are eager to utilize the biometrics technology, but they lack hope with approximately legislative organizations. The prerequisite to teach individuals about biometrics in order to eliminate users' greatest concerns is paramount.

One common theme that comes out of the studies is that users are concerned about the privacy and security of their personal data. This is an area that requires further study as part of the proposed research, which explores the concerns of participants and the contextual nature of those concerns.

3. Materials and methods

This study involved a questionnaire survey to assess user's perception in the usage of biometric technology applications. The surveys enable to gather information to be statistically analyzed. It consisted of three sections (A, B and C). Section A was designed to capture demographic, experiential and behavioral characteristics that may affect the use of biometrics or relate to the views of participants. The participant demographic information included age, gender, the education background, the experience level about biometric technology application. The common biometric features listed in the questionnaire were fingerprint, face, iris, voice, retina, gait, signature

and palm print. The analysis of the respondent's descriptive distribution is shown in **Table 1**. Section B considered questions to ascertain the participant intention, willingness and general perception with respect to the use of biometric technology applications. The five-point Likert scale from Strongly Agree (5), Agree (4), Neither (3), Disagree (2) to Strongly Disagree (1) is used. This was aimed to understand users' acceptance and utilization of biometric application. Section C considered questions to ascertain users fears in use of the biometric technology, the technique required for securing the biometric data and the strategies aimed at regulating and protecting the biometric technology information.

3.1 Analysis of the data

Data analysis involved a mixture of quantitative and qualitative techniques. Author applied Statistical method (SPSS) version 25 and presented findings using descriptive statistics in the form of frequency, percentage, mean and standard deviation to analyze responses to close-ended questions. Compared the mean independent t-test results across some aspects for instance, between user willingness and non-user willingness. A total of 300 participants (students, academic staffs and employees) from two selected institutions Muni University and IUIU University were collected. This is largely due to the fact that they are associated with a greater affinity, understanding and acceptance of new technologies, which would be necessary to transmit biometric concepts. The participants were given a consent form to notify them of

Variables	Item	Frequency	Percentage (%)
Age	21–30	94	31.3
	31–40	154	51.3
	41–50	36	12.1
	50 and above	16	5.3
Gender	Male	200	66.7
	Female	100	33.3
Education level	BSc	134	44.7
	MCs	94	31.3
	PhD	72	24.0
Role	Students	138	46.0
	Staff	98	32.7
	Employee	64	21.3
Biometric feature User experience	Fingerprint	106	35.3
	Facial	98	32.7
	Iris	30	10.0
	Retina	12	4.0
	Voice	26	8.7
	Signature	28	9.3

Table 1.
Respondents distribution frequency.

the theme and take their consent to respond in the survey. The questionnaires were provided to the participants who were comfortable in completing the survey by themselves. Stratified random sample was utilized to draw the target population. The formula $S = \frac{X^2 . P(1-P)}{d^2}$ was deployed for the sample size [24]. By using this approach to find the sample size, it is anticipated that the degree of bias can be fixed and the measurements of sampling error becomes low.

4. Results

4.1 Social demographic information

Out of the 300 survey participants, most of the participants were male with 66.7% and female with 33.3% respectively. The majority of participants to the survey were aged between 31 and 40 with 51.3%. Thirty-one-point-three percent (31.3%) were between 21 and 30 ages old. Twelve-percent (12%) were between 41 and 50, and 5.3% were over 51 years old. Nevertheless, this distribution of the participants' ages means that most of respondents will have either grown up with technology from an early age or been early adopters of new technologies.

In terms of education, a majority of participants had at least a high-level degree equivalent with 44.7% having at least a Bachelor's degree, 31.3% with a Master's degree, and 24% of the respondents held a doctoral degree. This is likely to be influenced by the researchers' personal and professional networks. Finally, in regards to respondent's categorical level, 46% of the participants were students, 32.7% were academic staffs, and 21.3% were employees. **Figure 2** presents the investigation of the social demographical information.

4.2 Biometrics feature utilization

The respondent's experience towards the usage of biometric technology were examined. Participants were asked about the biometric features that should be used in each of the physical and behavioral characteristics. It was used to better understand which technologies participants liked most and which ones they liked least. Participants were generally knowledgeable about a numeral of physical biometrics technologies. Thirty-five-point-three percent (35.3%) of the respondents had shared knowledge of how fingerprints are used. Thirty-two-point-seven percent (32.7%) were vast in facial scan. This is not surprising considering their commonness in personal devices and in our everyday lives (e.g., smartphones or migration at an airport). Both of these technologies have been used to protected personal devices and is increasingly become common in our daily lives. For example, the vast widely held of personal devices (e.g., smartphones and tablets) now make use of fingerprint and facial recognition so such a common usage is expected. Ten percent (10%) were having knowledge in Iris, 4% were vast in Retina.

In terms of possibly classified as behavioral biometrics technology, 8.7% were experienced in Voice, and 9.3% were vast in Signature scan. This is actually predictable in that traditionally behavioral biometrics do not require the user to interact with any specific hardware directly. Instead, their behaviors are normally monitored remotely. These analyses were pointed to the user's experience in the usage of biometric application and getting to know whether new biometric technology devices such as

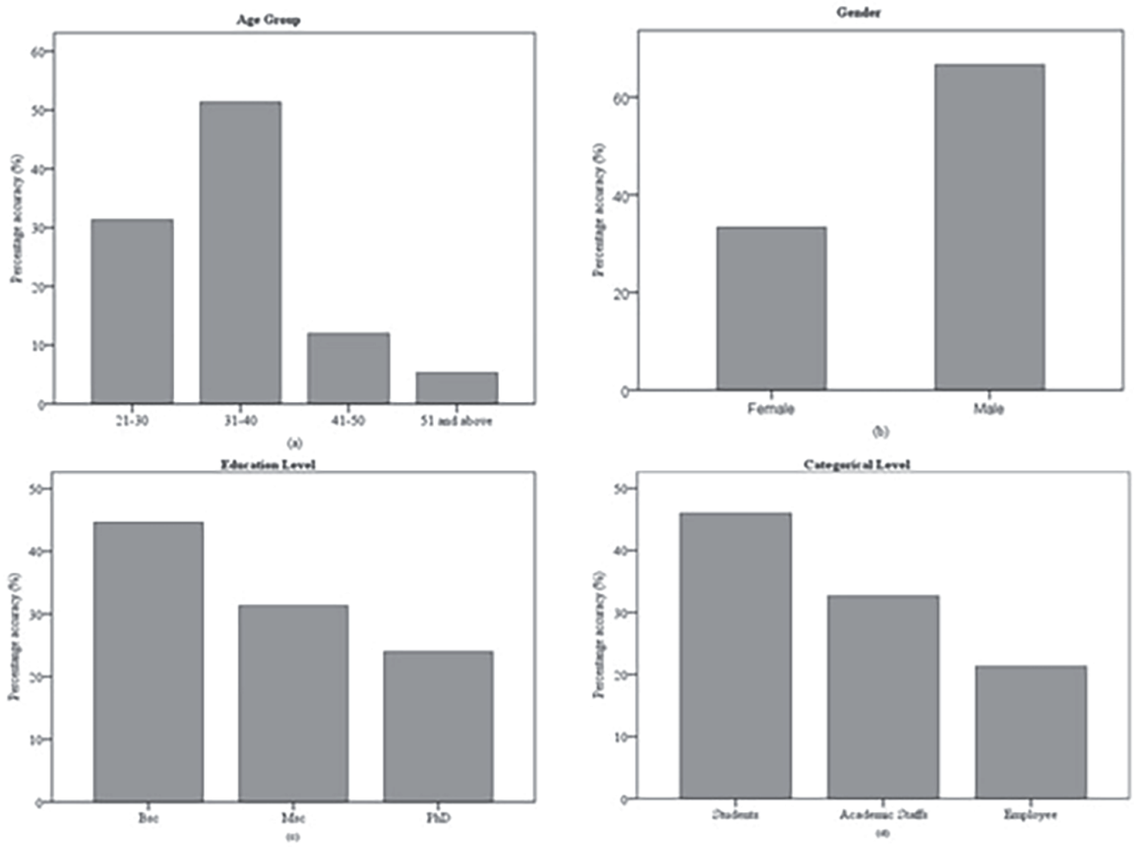

Figure 2.
Social demographic information, (a) age group, (b) gender, (c) education level, (d) categorical level.

smartphones, tablets, or laptops can either be accepted or not. Therefore, developers need to consider actual user willingness and acceptance in the utilization of these new technologies embedded with biometrics devices when designing a biometric security application, and make an effort to promote the use in a positive way. The findings from the analysis are shown in **Figure 3**.

4.3 Usefulness of biometric technology applications

Three hypotheses were verified by multiple regression analysis. Perceived ease of use (PEOU), perceived usefulness (UP), and perceived enjoyment (ENJ), with participants' attitudes towards the usage of biometric technology (ATT) as a dependent variable. Three general questions related to satisfaction with biometric technology were also raised. Sixteen quantitative questions were asked on a five-point Likert scale, ranging from strongly agree to strongly disagree. **Table 2** presents the analytical descriptive statistics for the constructions of each survey question. All three of the PEOU statements ranked highly with an average of 3.70 out of 5.00. "I would find biometric technology easy to use during workplace" scored highest with a mean of 3.73. Most of the survey statements related to perceived usefulness also ranked highly at an average of 3.66. However, respondents ranked the statement, "Biometric technology enables me to have more convenience at workplace," the lowest at 3.07. "Using biometric technology increases security level of an individual data at workplace," the highest at 4.42. With respect to

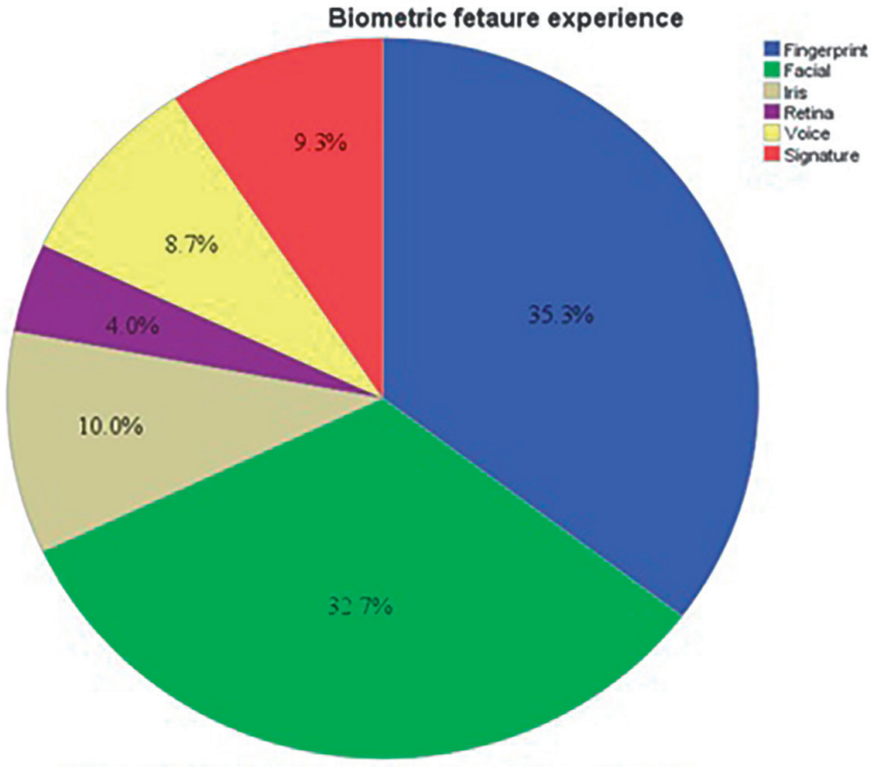

Figure 3.
Biometric feature utilization.

participants' enjoyment using the biometric technology, this category scored the lowest with an average of 2.83. "I have fun when using biometric technology" scored the lowest at 2.30 and "The actual process of using biometric technology is pleasant" scored the highest at 3.59.

Respondents' attitude towards the biometric technology was strong with an average of 3.79 out of 5.00 over the three statements. "I like the idea of using biometric technology at workplace" scored at the lowest with 3.72, while "Biometric technology makes work environment more interesting and "Using biometric technology at workplace is a good idea" were the strongest at 3.83 and 3.81 respectively. In regards to the participants' overall satisfaction with the biometric technology in general, this category scored a very high average of 3.91 over the three statements. The most highly ranked statement was, "As a whole, I am happy with the usage of biometric technology," and scored a 4.01. The results from the statistical analysis are shown in **Table 2**.

In order to gain additional insights, two open-ended questions were asked: (1) "What did you like about the biometric technology?" and (2) "What did you not like about the biometric technology?". A greater percentage 66% responded with optimistic response about the likeness of the biometric technology, while 34% of the biometric users responded with negative feedback. Of the biometric technology user group, 40% mentioned that the biometric technology was easy to use, 28% indicated greater security, while 32% showed conveniences and user friendly. Regard the negative feedback of the dis-likeness of biometric technology, 34.7% mentioned risks of personal data, 45.3% indicated that the biometric data can be stolen, while 20% mentioned insecurity of personal data.

Measurement questions	Mean	Std. Dev.	Min	Max	N	Variance
Perceived Ease of Use (PEOU) I know how to use biometric technology	3.69	1.248	1	5	300	1.551
I would find biometric technology easy to use during workplace	3.73	1.443	1	5	300	2.082
Learning to use biometric technology is easy for me	3.67	1.438	1	5	300	2.067
Perceived Usefulness (PU) I find biometric technology useful at workplace	3.18	1.278	1	5	300	1.633
Biometric technology enhances the personal security information	3.95	1.442	1	5	300	2.078
Biometric technology enables me to have more convenience at workplace	3.07	0.958	1	5	300	0.919
Using biometric technology increases security level of an individual data at work	4.42	1.043	1	5	300	1.087
Perceived Enjoyment (ENJ) I find using biometric technology is enjoyable	2.61	1.556	1	5	300	2.420
The actual process of using biometric technology is pleasant	3.59	1.369	1	5	300	1.875
I have fun when using biometric technology	2.30	1.538	1	5	300	2.365
Attitude (ATT) Using biometric technology at workplace is a good idea	3.81	1.316	1	5	300	1.731
I like the idea of using biometric technology at workplace	3.72	1.441	1	5	300	2.075
Biometric technology makes work environment more interesting	3.83	1.201	1	5	300	1.441
Overall satisfaction Overall, I am satisfied with the usage of biometric technology	3.81	1.498	1	5	300	2.243
As a whole, I am happy with the usage of biometric technology	4.01	1.168	1	5	300	1.364
I believe by attending any biometric technology conference will enhance my profounder understanding of the technology	3.91	1.430	1	5	300	2.046

Table 2.
Descriptive statistics.

4.4 User willingness vs non-user unwillingness with respect to the usage of biometric applications

In order to compare the overall user willingness vs. non-user unwillingness satisfaction levels in the usage of biometric technology, a t-test was run in SPSS. Statistical measurement of two intact groups using an independent samples t-test is

appropriate to evaluate the variance amongst the two groups [24]. The results were statistically significant between user willingness vs. non-user unwillingness. The user willingness to use biometric technology mean was 4.39 and non-user unwillingness to use biometric technology mean was 3.33. This result shows that both users and non-users willingness rated their overall usage of biometric satisfaction at virtually different level. **Table 3** presents the comparison of the sample independently of the t-test results.

4.5 Security of the biometric technology

The security issues were intended to measure the extent to which subjects felt the application of biometric technology would improve the security of the end-user. Participants were asked to comment on biometric security versus other traditional methods [24]. Ninety-two percent (92%) of participants agreed with the statement that biometrics were more secure because it involves a personal presence during the verification process. Participants were also asked about the ability of biometrics to offer the same level of security as two-factor authentication. The majority 84.7% of respondents concur with this statement. Lastly, respondents were asked if they were of the opinion that biometrics could easily be compromised. Forty-eight percent (48%) of participants explained that biometrics might be compromised. While 52% stated that biometrics cannot be easily compromised, which was not surprising. This is particularly true when seeing that most respondents indicated that biometrics was as secure as two-factor authentication.

One of the key findings of this study was that participants were generally knowledgeable about the usage of fingerprints and face. This emphasizes that exposure to these technologies assists in generating support for the desired methods.

4.6 Users fear in usage of biometric technology

Another area was the level of concern of subjects about privacy issues associated with the implementation of biometric technology. The issues of willingness to provide personal biometric information for collection, use and storage were addressed. While biometric technology offers highly compelling proof of identity and individual confirmation solutions. Participants voiced concern about the usage of biometric technology, as biometrics can easily be hacked and the consequences of their mismanagement could be incredibly dangerous. Thirty-two-point-seven percent (32.7%) expressed the selling of the information to 3rd party. The danger of identity stealing is greater because, unlike a credit card, biometrics cannot be canceled or superseded if it is entered by a third party. With fingerprints all over the place and faces in full view. Forty-eight percent (48%) indicated misuse or abuse of personal data. This is because a compromised biometric data stored in the database cannot be revoked. For instance,

Comparison sample	**Mean**				
User willingness vs non-user unwillingness to use biometric technology?	Willingness (102)	Unwillingness (198)	Mean difference	t-value	Sig.
	4.39	3.33	1.059	7.610	0.000

Table 3.
Independent samples of t-test results.