



# Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:  
[https://semarakilmu.com.my/journals/index.php/applied\\_sciences\\_eng\\_tech/index](https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index)  
ISSN: 2462-1943



## Identity in the Digital Age: An Investigation of Malaysian Perspectives on Technology and Privacy

Faiz Zulkifli<sup>1</sup>, Rozaimah Zainal Abidin<sup>1,\*</sup>

<sup>1</sup> College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA, Perak Branch, Tapah Campus, 35400 Tapah, Perak, Malaysia

### ARTICLE INFO

#### Article history:

Received 22 June 2023  
Received in revised form 24 August 2023  
Accepted 14 February 2024  
Available online 17 April 2024

#### Keywords:

Technology adoption; Online identity management; Trust in technology; Digital identity; Demographic factors

### ABSTRACT

Malaysia is in the process of developing a new identity system to provide citizens and residents with secure and efficient access to digital services. This study aimed to determine the responsiveness of the Malaysian population to new technologies and evaluate their opinions on managing their identity online. The study employed a quantitative research design and collected data through an online questionnaire. A total of 1,014 participants from Malaysia, aged 18 years and above, were included in the study, and the data were analysed using cross-tabulation analysis. The theoretical framework of the study was based on the technology acceptance model, the risk and negative consequences theory of individuals' perceptions, and the organizational trustworthiness theory. The results showed that various demographic characteristics influence individuals' attitudes towards technology adoption and online identity management. Gender, age, ethnicity/race, work status, employment sector, level of education, place of living, household income level, and residence state were all significantly associated with early adoption of emerging technologies, trying out new technologies, and enjoyment of trying out new technologies. Certain demographic factors may also have an impact on people's preferences for specific identity management tools. The study also found significant relationships between various demographic factors and trust levels when it comes to personal data. The study findings have implications for policymakers and practitioners involved in promoting the adoption of new technologies and the management of online identities. The study's findings may assist policymakers in implementing better measures for protecting Malaysians' online identity and privacy. Additionally, the results could also inform future research investigating technology adoption and acceptance among Malaysians.

## 1. Introduction

In recent years, the widespread adoption of new technologies has transformed the way people interact with one another and engage with the world around them. From social media to e-commerce, these technologies have provided new opportunities for communication, commerce, and social interaction. However, with these new opportunities come new challenges, particularly in managing personal information and identity online.

\* Corresponding author.

E-mail address: rozai256@uitm.edu.my

<https://doi.org/10.37934/araset.43.2.120>

The Malaysian context is no exception to this trend. With a population of over 32 million people and a rapidly growing digital economy [1], Malaysia has seen a significant increase in technology adoption in recent years. According to a report by Datareportal, as of January 2022, over 29 million Malaysians are active internet users [2]. This figure represents a penetration rate of over 70% of the total population and is projected to continue growing in the coming years.

Despite the benefits of new technologies, concerns over data privacy and security remain a major challenge in Malaysia, as in many other countries. A survey conducted by the Malaysian Communications and Multimedia Commission (MCMC) found that over half of Malaysian internet users are concerned about online privacy and security issues [3]. Furthermore, recent high-profile data breaches in Malaysia have raised public awareness of the risks of identity theft and data breaches [4].

Given these concerns, it is important to understand how Malaysian people perceive new technologies and manage their identity online. By assessing their receptiveness to new technologies and their views on online identity management, policymakers and practitioners can better address these concerns and ensure that technology adoption is done in a way that is safe, secure, and beneficial for all.

The purpose of this study is to measure Malaysian people's receptiveness to new technologies and assess their views on managing their identity online. We employ cross-tabulation analysis to explore the relationships between various demographic factors and attitudes towards new technologies and online identity management. Our findings will help shed light on the factors that influence technology adoption in Malaysia and inform policies and practices related to online identity management.

## **2. Literature Review**

As new technologies become increasingly pervasive in our daily lives, understanding how people perceive and adopt these technologies has become a topic of interest for researchers and practitioners alike. In particular, researchers have explored the factors that influence individuals' attitudes towards and adoption of new technologies [5], as well as the challenges and opportunities presented by these technologies in the context of identity management online.

One key factor that has been shown to influence individuals' adoption of new technologies is their level of trust in those technologies. According to the Technology Acceptance Model (TAM), which has been widely used to study technology adoption, perceived ease of use and perceived usefulness are two key factors that influence an individual's attitude towards a technology, which in turn influences their intention to use that technology [6]. In the context of identity management online, perceived security and privacy are also important factors in shaping individuals' attitudes towards new technologies [7,8]. Studies have shown that individuals who perceive greater levels of security and privacy in online identity management tools are more likely to adopt those tools [9,10].

Another important factor that has been shown to influence individuals' attitudes towards new technologies is their demographic characteristics [11]. For example, age, gender, and educational level have been found to be significant predictors of technology adoption [12,13]. In particular, younger individuals and those with higher levels of education are generally more receptive to new technologies and more likely to adopt them [14]. However, studies have also found that demographic factors can interact with one another in complex ways, such that the relationship between demographic characteristics and technology adoption may vary depending on the specific technology in question [15,16].

In the Malaysian context, several studies have explored attitudes towards technology adoption and online identity management. For example, a study by Li, [17] found that trust, perceived usefulness, and perceived ease of use were significant predictors of Malaysian consumers' intention to use online banking services. Similarly, a study by Loke *et al.*, [18] found that perceived security and privacy were key factors in shaping Malaysian consumers' attitudes towards mobile payment services.

Despite the growing interest in comprehending individuals' attitudes towards and adoption of new technologies, significant gaps in knowledge remain, particularly in the Malaysian context. While previous studies have examined the factors that influence technology adoption and attitudes towards online identity management in Malaysia, further research is warranted to investigate how Malaysian individuals perceive and manage their online identity and how this correlates with their attitudes towards new technologies. Moreover, while previous studies have acknowledged the importance of demographic factors as predictors of technology adoption, additional research is necessary to comprehend how these factors interact with one another in the Malaysian context and how they may differ based on the technology in question.

As a result, this study aims to gauge the Malaysian population's responsiveness to new technologies and evaluate their opinions on managing their identity online via cross-tabulation analysis. Our specific objective is to determine the demographic variables that impact the attitudes of Malaysian individuals towards new technologies and their adoption of online identity management tools. This research is intended to enhance our understanding of the factors that influence technology adoption and attitudes towards online identity management in Malaysia and provide valuable insights for the development of new technologies and policies in this field.

### **3. Research Objectives (ROs), Research Questions (RQs) and Hypotheses**

The main objectives of this study are:

- i. To measure the receptiveness of Malaysian people to new technologies.
- ii. To assess the views of Malaysian people on managing their identity online.
- iii. To identify the demographic factors that influence Malaysian individuals' attitudes towards new technologies and their adoption of online identity management tools.

The following research questions will guide this study:

- i. What is the level of receptiveness of Malaysian people towards new technologies?
- ii. What are the views of Malaysian people on managing their identity online?
- iii. How do demographic factors such as age, gender, and education level influence Malaysian individuals' attitudes towards new technologies and their adoption of online identity management tools?

Based on the literature review and research questions, the following hypotheses will be tested in this study:

H1: Malaysian individuals who perceive greater levels of security and privacy in online identity management tools are more likely to adopt those tools.

H2: Demographic factors such as age, gender, and education level are significant predictors of technology adoption and attitudes towards online identity management in Malaysia.

H3: There is a significant relationship between Malaysian individuals' attitudes towards new technologies and their adoption of online identity management tools.

#### **4. Research Methodology**

This study will employ a quantitative research design to determine the responsiveness of the Malaysian population to new technologies and evaluate their opinions on managing their identity online. The primary data collection method used will be an online questionnaire. This section aims to describe the theoretical framework and procedures involved in developing the research instrument, including the sampling method, data collection, and data analysis.

##### *4.1 Theoretical Framework*

The theoretical framework of this study is based on three prominent theories, namely the technology acceptance model (TAM), the risk and negative consequences theory of individuals' perceptions, and the organizational trustworthiness theory, which have been widely used in previous research investigating technology adoption and acceptance [19,20]. The TAM posits that users' behavioural intentions towards technology adoption and use are influenced by the perceived usefulness and ease of use of the technology. In contrast, the risk and negative consequences theory states that perceptions of risks and negative consequences associated with technology adoption significantly influence the intention to adopt and use technology.

##### *4.2 Research Instrument Design*

The proposed research instrument is based on the theoretical framework outlined above. The instrument consists of two sections: the Innovativeness section aims to measure people's openness to new technologies, while the Data Management section assesses their opinions on managing their identity online.

##### *4.3 Sampling and Participants*

This study will target adults aged 18 years and above residing in Malaysia. A representative sample of the target population will be selected using probability sampling. The sample size will be determined using statistical power analysis based on the research objectives.

##### *4.4 Data Collection and Analysis*

Data will be gathered through an online survey directed towards the designated sample. The questionnaire will undergo a pre-testing phase with a small sample of participants to establish its validity and reliability. The questionnaire has also undergone validation by professionals and stakeholders, including the Malaysian Communications and Multimedia Commission (MCMC). All tests carried out during the analysis were deemed significant. The data collected will be subjected to cross-tabulation analysis using IBM SPSS software.

#### **4.5 Ethical Considerations**

Informed consent will be obtained from all participants before they take part in the survey. Participants will be informed of the purpose of the study, the nature of the questions, and their right to withdraw from the study at any time. Data collected through the survey will be kept confidential and used for research purposes only.

### **5. Results**

#### **5.1 Demographic Factors**

The present study encompassed a total of 1,014 participants, of which the majority (77.2%) identified as female, and the remaining 22.8% identified as male. With respect to age, the largest proportion of participants (52.8%) were in the age group of 30-39, followed by 15-29 (32.8%), 40-49 (9.2%), 50-59 (3.6%), and 60-80 (1.7%) respectively.

Regarding marital status, most participants (54.5%) identified as married, followed by single participants (42.9%). A relatively small percentage of participants (2.6%) identified as divorced. In terms of ethnicity/race, the largest percentage of participants identified as Malay (73.5%), while the smallest percentage identified as Indian (3.5%) and others (0.1%). The sample size for the Chinese and Indian categories was relatively small, with only 52 and 35 participants respectively.

About work status, most respondents identified as having a managerial occupation (57.3%), followed by skilled workers (10.1%) and professionals (11.8%). Only a small percentage of respondents identified as business owners (0.1%), executives (0.1%), or pensioners (1.1%). Most participants in the study worked in the private sector (79.4%), while a smaller percentage worked for the government (15.3%). Only 3% of the participants identified as self-employed, and 2.4% reported that their work was not related to any of the categories listed in the survey.

Concerning the level of education, the highest level of education among the participants was a degree (60.7%), followed by a diploma (20.3%), and a master's degree (12.0%). The remaining participants had either completed their MCE/SPM/SPMV (2.9%), STPM/STPMV/certificate (1.8%), or PhD (2.3%).

Most of the participants (70.8%) in the study were from rural areas, while 29.2% were from urban areas. In terms of income level, 80.4% of the participants reported having a monthly income below RM4,850, with only 3.7% reporting a monthly income of more than RM10,971. Notably, the income distribution observed in our sample aligns with the Malaysian household income distribution categorised into the B40, M40, and T20.

Finally, the distribution of participants' state of residence revealed that the highest percentage of respondents were from Pahang (11.6%), followed by Sarawak (10.6%) and Sabah (10.1%). The states with the lowest representation in the sample were Pulau Pinang (1.3%), WP Kuala Lumpur (2.6%), WP Labuan (2.2%), and WP Putrajaya (2.2%).

#### **5.2 Innovativeness Section**

The Innovativeness section of the study aimed to assess participants' propensity for adopting new technologies. A total of 58.9% of participants agreed that they were early adopters of emerging technologies (item 1), while 61.0% agreed that they try to adopt new technologies when they hear about them (item 2), and 57.4% agreed that they derive enjoyment from trying out new technologies (item 3). These findings suggest that most participants have a positive attitude towards new

technologies and are willing to experiment with them, which could have implications for the future adoption of emerging technologies.

### *5.2.1 Chi-square test*

Significant associations were observed between demographic factors and statements. Pearson chi-square tests were used to determine the significance of these associations. The results revealed that gender, age, ethnicity/race, work status, employment sector, level of education, place of living, household income level, and residence state were all significantly associated with item 1, item 2, and item 3 ( $p < 0.05$ ). However, marital status was only found to be significantly associated with item 3 ( $p < 0.05$ ). In contrast, no significant association was found between the place of living and item 3.

### *5.2.2 Frequency distribution*

#### *5.2.2.1 Gender*

The results of the frequency distribution analysis indicate that, with respect to gender, a higher percentage of females responded and agreed with statements item 1 and item 2 on adopting emerging technologies than males. Additionally, a greater proportion of females reported enjoying trying out new technologies compared to males. These findings suggest that females are more likely than males to adopt new technologies and enjoy experimenting with them.

#### *5.2.2.2 Age*

Concerning statement item 1, most responses fell in the "agree" category (rating of 4), with the highest number of respondents being in the 30-39 age group. Similarly, for statement item 2 and 3, most respondents also gave ratings of 4 or 5 (agree and strongly agree), with the highest number of respondents in the 15-29 and 30-39 age groups. In general, it appears that younger age groups are more inclined to adopt and enjoy new technologies than older age groups.

#### *5.2.2.3 Marital status*

Regarding marital status, for all statements, the highest percentage of respondents who agreed or strongly agreed that they were early adopters, attempted to adopt new technologies, and enjoyed trying out new technologies, respectively, were single, followed by married, and the lowest percentage were divorced. These results suggest that being single is associated with a higher likelihood of being an early adopter and trying out new technologies compared to being married or divorced.

#### *5.2.2.4 Race / ethnicity*

Based on the data, individuals of Malay ethnicity are more likely to be early adopters of emerging technologies and try to adopt new technologies when they learn about them compared to individuals of other ethnic/racial backgrounds. In addition, individuals of Malay ethnicity also report higher levels of enjoyment in experimenting with new technologies. Conversely,

individuals of Indian ethnicity appear to be less likely to adopt emerging technologies, with lower ratings on all three statements than individuals of other ethnic/racial backgrounds.

#### *5.2.2.5 Work status*

The results show that individuals in managerial positions are the largest group across all three questions, implying that they are more likely to be early adopters of new technologies, attempt to adopt new technologies when they hear about them, and enjoy trying out new technologies. The "Worker/Labour" group is the second largest in all three questions, suggesting that individuals in these positions are also relatively likely to embrace new technologies. Although the "Professional" group is relatively small in all three questions, they tend to give high ratings to emerging technologies, likely because professionals often use specialized software or tools pertinent to their work. The "Pensioner" group is small but has relatively high ratings for emerging technologies, perhaps because they are interested in technologies that aid them in staying connected with family and friends or in improving their quality of life. The "Non-working" and "Business Owner/Executive" groups are relatively small and tend to give lower ratings to emerging technologies. In summary, these findings suggest that individuals in managerial and worker/labour positions are more likely to be early adopters of new technologies and enjoy trying out new technologies, while professionals and pensioners also tend to be interested in emerging technologies. However, there is some variance in attitudes towards emerging technologies among different work status groups.

#### *5.2.2.6 Employment sector*

In all three questions, the "Private" employment sector has the largest group, indicating a higher likelihood of early technology adoption, attempting to adopt new technologies upon hearing about them, and enjoying trying out new technologies among individuals in this sector. The "Government" sector is the second-largest group in all three questions, indicating a relatively higher inclination towards technology adoption among individuals in this sector. Conversely, the "Self-employed" group is the smallest across all three questions but provides high ratings for emerging technologies, possibly due to the use of specialized software or tools relevant to their profession. The "Not Related" group is relatively small and appears to provide lower ratings for emerging technologies compared to the other two groups, indicating that they may not be as receptive to new ideas and innovations as the other two groups.

#### *5.2.2.7 Education level*

In terms of education level, degree holders and those with higher degrees were the most interested in emerging technologies, with a high proportion of them giving ratings of 4 or 5 for all three questions. Diploma and STPM/STPMV/certificate holders also showed a high level of interest in emerging technologies. Additionally, respondents with higher levels of education were more likely to try new technologies when they heard about them and enjoy trying out new technologies.

#### *5.2.2.8 Place of living*

Regarding location, respondents living in urban areas were more likely to be early adopters, try new technologies, and enjoy trying out new technologies. The study found that individuals from cities

had a higher percentage of respondents who indicated a rating of 4 or 5 for all three questions, compared to those from rural areas.

#### *5.2.2.9 Income level*

With regards to income level, respondents from households with higher income levels were more likely to be early adopters, try new technologies, and enjoy trying out new technologies. Individuals from households with income levels of more than RM10,971 had the highest percentage of responses in the "4" and "5" categories for all three questions, indicating that they were more interested in emerging technologies than those from lower income households.

#### *5.2.2.10 Residence state*

When analysing the results based on location, the study found that respondents from all states exhibited a favourable disposition towards adopting new technologies, with a relatively high proportion of respondents expressing agreement or strong agreement for all three questions. The highest scores were consistently from states situated on the east coast of Peninsular Malaysia and from Sabah and Sarawak.

### *5.3 Data Management Section*

This section comprises several questions related to the online information individuals share (item 1), the parties they trust with their personal data (item 2), the activities for which they share personal information (item 3), and their concerns regarding personal information risks (item 4). Respondents are also asked to agree or disagree with several statements related to their ability to keep online activities private (item 5), their comfort level with sharing personal information online (item 6), and their perceptions of the internet's safety for leisure, work, and business transactions (item 7). The survey results indicate that most participants have made their name (73.6%), nationality (54.7%), and pictures of themselves (57.3%) available online, while a smaller proportion have made their IC number (89.3%), bank details (92.5%), and physical appearance (66.6%) available.

The participants' views on the safety of trusting various individuals and entities with their personal data were explored, with most participants expressing uncertainty about whether they could trust family members (4.1%) and friends (10.2%). In contrast, 78.9% of participants indicated that they could trust family members with their personal data. When it came to government entities, a little less than half of the participants (46.8%) expressed distrust towards the federal or state government, while 41.7% stated that they could trust the government. Regarding companies, a larger proportion of participants expressed distrust towards famous companies (73.8%) and known companies (68.8%), with only 11.7% and 21.6% indicating that they could trust these entities, respectively. Finally, most participants did not trust unknown companies with their personal data (96.0%).

The participants' views on sharing personal information for different online activities were also examined. The highest percentage of participants who reported sharing personal information were those who aimed to improve services (61.3%), obtain useful knowledge (61.8%), and socialize (24.2%). On the other hand, the lowest percentage of participants who reported sharing personal information were those who aimed to take advantage of targeted advertising (25.6%), expecting gifts or samples (14.1%), and getting money or discounts (21.9%).



The survey results also show that a vast majority of participants expressed concern about personal information risks, with 97.6% of respondents concerned about their personal details being misused, 94.5% concerned about their online behaviour being monitored, and 96.4% concerned about their personal data being used for marketing purposes.

Furthermore, the participants' views on managing their identity online, online privacy, and internet security were investigated. Most participants agreed (55.4%) with the statement "I know how to keep my online activities private" (item 5). However, a significant number of participants (47.6%) either disagreed or strongly disagreed with the statement "I am comfortable giving my personal information online due to the internet's security" (item 6). Similarly, almost 37% of participants disagreed or strongly disagreed with the statement "The internet is safe for leisure, work, and business transactions" (item 7).

### *5.3.1 Chi-square test*

In the data management section, various questions are analysed through chi-square tests to determine if there are statistically significant relationships among the variables. The results show that there are several significant relationships between factors and items in the personal information question. For example, gender, age, ethnicity/race, work status, and employment sector are all significantly related to various items. Conversely, some factor-item combinations do not exhibit a significant relationship, such as Nationality-IC number, People I regularly interact with, Pictures of myself, and Bank details, and Employment Sector-IC number, People I regularly interact with, Pictures of myself, and Bank details.

Regarding trust levels, the results indicate that there are noteworthy dissimilarities among diverse demographic groups regarding their degree of trust when it comes to personal data. Gender, age, marital status, ethnicity/race, work status, level of education, place of living, household income level, and residence state all play a role in determining trust levels.

Furthermore, the results show that there are several significant relationships between factors and activities. All factors (gender, age, marital status, ethnicity/race, work status, and level of education) have a significant relationship with "improving service, for example, education, health, etc." and "obtaining useful knowledge." Other activities that have significant relationships with at least one factor include "securely log into a system," "take advantage of targeted advertising," "expecting gifts or samples," "get money or discounts," "game-playing," and "socializing."

Regarding personal information risks, the results indicate that there are significant associations between age and "Various personal data sources reconstruct my identity." However, none of the risks displayed a significant association with gender. The risks that showed a significant association with other demographic variables include "My personal details are misused," "My online behaviour is monitored," "My personal data online is used for marketing," "My online information may misrepresent my views and behaviours," "Personal information posted online could damage my reputation," "Online identity theft threatens me," and "Online financial fraud may affect me."

Finally, the survey results show that not all individuals agree to the following statements: "I know how to keep my online activities private," "I am comfortable giving my personal information online due to the internet's security," and "The internet is safe for leisure, work, and business transactions." These discrepancies in opinion suggest that there may be a lack of awareness or understanding regarding online privacy and security measures, which highlights the need for increased education and resources in this area. It is important for individuals to take proactive steps to protect their personal information and be aware of potential risks when using the internet for various activities.

Additionally, businesses and organizations should prioritize cybersecurity measures and transparency with their users to ensure a safer and more secure online environment.

### *5.3.2 Frequency distribution*

#### *5.3.2.1 Gender*

In option (name), both female (72%) and male (79%) respondents exhibited willingness to divulge their name online. Similar patterns were discernible in options (Age, Nationality, IC number, Address, Physical appearance, My activities, Opinions, People I regularly interact with, Locations where I frequently visit, Information you provide on social media, Pictures of myself), where the majority of respondents from both genders were disposed towards disclosing the respective personal information online. However, a mere fraction of female (6%) and male (11%) respondents were willing to disclose their IC number online. Likewise, only a small proportion of both female (3%) and male (6%) respondents were willing to disclose their bank details online. The infrequency of the "Not Sure" response category suggested that most respondents were confident about the information they had shared online.

With respect to family members, 599 females and 144 males agreed to entrust personal data, while 40 females and 2 males were uncertain. Concerning friends, 583 females and 158 males expressed distrust towards sharing personal data, while 88 females and 15 males were unsure. In the case of the federal/state government and famous/known companies, a majority of both female and male respondents responded negatively. Unknown companies were not trusted by most respondents. Only one female and one male indicated their willingness to share personal data with unknown companies.

Females were more inclined than males to agree to share personal information for all activities examined. The largest gender difference was observed for obtaining useful knowledge. Similarly, for socializing, taking advantage of targeted advertising, and receiving money or discounts, the number of females responding positively was significantly higher than males. However, for automatic keystroke input and game-playing, there were relatively fewer gender differences in the number of respondents who agreed to share personal information.

For certain personal information risks, such as personal data sources reconstructing one's identity, online information misrepresenting one's views and behaviours, and online financial fraud, females expressed greater levels of concern than males. However, for risks related to personal data being misused, online behaviour being monitored, personal data being used for marketing, online information damaging reputation, and online identity theft, there were no substantial differences in the level of concern between males and females.

Females exhibited greater concern about online privacy and security than males. Regarding item 5, most females disagreed or strongly disagreed with the statement, while most males also disagreed or strongly disagreed. Similar trends were observed for items 6 and 7, with females being more likely than males to strongly agree or agree with the statements and less likely to neither agree nor disagree, disagree, or strongly disagree.

#### *5.3.2.2 Age*

The data reveals that most respondents have disclosed their personal information online, except for their IC number and bank details, which have been disclosed by a smaller percentage of respondents. The age group of 15-29 years exhibits the highest percentage of individuals sharing their personal information, whereas the age group of 60-80 years exhibits the lowest.

Furthermore, there are disparities based on the type of information, with physical appearance being more frequently shared by respondents aged 30-39 years than those aged 15-29 years.

Most respondents exhibit a preference for trusting their family members with their personal data, while they exhibit a lack of trust towards their friends, federal/state government, well-known companies, and unknown companies. Respondents aged 15-29 years are the least confident about trusting their friends, the government, popular companies, and unknown companies.

For automatic keystroke input, most age groups are uncertain about sharing personal information, but a substantial number of individuals agree to disclose personal information to enhance services and gain useful knowledge. Socializing and game-playing are the two activities with a higher percentage of individuals who choose not to share personal information. Securely logging into a system is the activity with the greatest preference for sharing personal information across all age groups.

The age group of 15-29 years exhibited the most anxiety regarding personal information misuse, online behaviour monitoring, online information misrepresenting their views and behaviours, and online identity theft. The age group of 30-39 years expressed the most concern about personal data being used for marketing purposes, multiple sources of personal data reconstructing their identity, personal information posted online harming their reputation, and online financial fraud.

The findings imply that there are differences in attitudes towards online privacy and security based on age. For item 5, respondents aged 30-39 had the greatest proportion of individuals who strongly agreed and agreed, while respondents aged 60-80 had the lowest proportion. For item 6, respondents aged 15-29 had the greatest proportion of individuals who strongly agreed and agreed, while respondents aged 60-80 had the lowest proportion. For item 7, respondents aged 30-39 had the highest proportion of those who strongly agreed and agreed, while respondents aged 60-80 had the lowest proportion.

### *5.3.2.3 Marital status*

Based on the data, it can be inferred that married respondents exhibited greater uncertainty with regards to the disclosure of personal information about their online interactions as compared to divorced or single respondents. Furthermore, a higher percentage of married respondents answered affirmatively compared to their divorced or single counterparts.

The trust levels with regards to personal data varied among respondents belonging to different marital statuses. Among respondents from all marital statuses, family members were generally considered trustworthy with personal data while famous or unknown companies, as well as government, were not. Divorced individuals had the lowest percentage of uncertainty when it comes to trusting family members with their personal data, while married individuals had the highest. Divorced individuals had the highest percentage of uncertainty when it comes to trusting famous and known companies with their personal data, while married individuals had the lowest. Almost all respondents from all marital statuses said "no" when it comes to trusting unknown companies with their personal data, except for two single respondents.

For all activities, most respondents from all marital status groups were willing to share personal information, except for when it comes to expecting gifts or samples where the majority answered "no". However, there were some differences in the proportions of answers between the marital status groups.

Respondents from different marital statuses expressed varying concerns about the risks associated with personal information in different categories. Married respondents had the highest

number of individuals expressing concern about personal information risks across all categories except for "Misuse of my personal details".

In terms of attitudes towards online privacy and security, there were no substantial differences across marital status groups for all three statements. However, it is worth noting that the number of divorced participants was relatively small compared to the other two groups.

#### *5.3.2.4 Race / ethnicity*

The survey results indicate that a significant proportion of respondents from all ethnicities were unsure if they had made their name available online. Additionally, most respondents from all ethnicities did not make their age, address, physical appearance, or IC number available online. Conversely, most respondents from all ethnicities made their nationality, activities, and opinions available online. Respondents from all ethnicities did not make the people they regularly interact with, the locations they frequently visit, pictures of themselves, or their bank details available online.

Furthermore, the survey findings reveal that most respondents across all ethnicities trusted their family members with their personal data. However, Malay and Bumiputra of Sabah/Sarawak respondents were more uncertain in this regard. On the other hand, most respondents across all ethnicities did not trust their friends with their personal data, with Malay and Bumiputra of Sabah/Sarawak respondents also expressing more uncertainty. Additionally, most respondents across all ethnicities did not trust federal/state government or famous/known companies with their personal data. Malay and Bumiputra of Sabah/Sarawak respondents also showed more uncertainty in this regard. Finally, almost all respondents across all ethnicities did not trust unknown companies with their personal data, except for two respondents (one Malay and one Bumiputra of Sabah/Sarawak) who were single and aged 15-29 and said yes.

Moreover, the survey results indicate that Malays have the highest number of respondents who are unsure if personal information is shared, followed by Bumiputra of Sabah/Sarawak. In contrast, Malays tend to share personal information more frequently than other ethnicities/races for activities such as "Automatic keystroke input," "Improve service, for example, education, health, etc.," "Obtaining useful knowledge," and "Securely log into a system." Chinese respondents tend to share personal information less frequently, especially for activities such as "Automatic keystroke input," "Game-playing," and "Take advantage of targeted advertising." In terms of specific activities, Malays and Bumiputra of Sabah/Sarawak tend to share personal information more frequently for "Expecting gifts or sample" and "Get money or discounts" activities, while Chinese tend to share less. There is no significant difference in personal information sharing among different ethnicities/races for "Socializing" activities.

Finally, the survey revealed that there is a significant concern among all ethnic groups regarding the potential risks of personal information misuse online. Many individuals across all ethnicities expressed concerns about the potential for online identity theft, personal data being used for marketing purposes, and online information misrepresenting their views and behaviours. Concerns about personal information risks varied slightly across ethnic groups, with Malay respondents expressing the highest number of concerns overall. Ultimately, the survey findings suggest that there are differences in attitudes towards online privacy, personal information disclosure, and internet safety among respondents of different ethnicities.

### 5.3.2.5 Work status

The variation in disclosure of online information is significantly dependent on an individual's work status. Individuals belonging to work status groups such as business owners, executives, and non-workers tend to disclose less online information as compared to managerial workers and workers/labourers who share more online information. A categorization of online information reveals that managerial workers have the highest number of respondents who have made their information available online. Skilled workers, professionals, and workers/labourers share most categories of online information, except for IC number, where skilled workers have the highest number of respondents who have made the information available. The lowest number of respondents who have made their physical appearance and activities available online are students, while the highest number of respondents who have made their bank details available online are workers/labourers.

The survey results on the trustworthiness of individuals/parties with personal data based on their work status are presented in the table. The results show that family members and friends are the most trusted with personal data across all work status categories. However, the level of trust in federal/state governments, famous companies, known companies, and unknown companies varies depending on one's work status. Professional and skilled workers show the highest level of trust in federal/state governments, while business owners and executives show the highest level of trust in famous companies. Known companies are generally trusted more than unknown companies. The survey results suggest that trust in different parties with personal data is influenced by one's work status.

The willingness of individuals to share personal information for certain activities may be influenced by their work status. Managerial workers tend to have the most "Yes" responses for several of these activities, such as automatic keystroke input, improving services, obtaining useful knowledge, targeted advertising, and getting money or discounts. Workers/Labourers tend to have the most "Yes" responses for expecting gifts or samples. Skilled workers and professional workers also have significant numbers of "Yes" responses depending on the activity.

Most respondents from the Managerial and Worker/Labour work status answered "Yes" for activities such as "My personal details are misused", "My online behaviour is monitored", "My personal data online is used for marketing", "Various personal data sources reconstruct my identity", "My online information may misrepresent my views and behaviours" and "Personal information posted online could damage my reputation". However, a small number of respondents from these work statuses answered "No." There were also some respondents who were "Not Sure."

The survey results demonstrate that individuals in different work status groups have varying levels of concern when it comes to their online privacy. Managerial workers exhibit the highest level of concern, with 83.4% expressing concern. Skilled workers and professionals also express a high level of concern, with 79.2% and 78.6%, respectively. In contrast, business owners and executives have the lowest levels of concern, with only 71.1% and 70.9%, respectively, expressing concern.

The survey results also indicate that individuals in different work status groups manage their online privacy differently. Business owners and executives are more likely to use privacy settings and limit the information they share online as compared to other groups. Skilled workers and professionals, on the other hand, are more likely to review privacy policies and read terms and conditions before sharing information online. Workers/labourers are less likely to take any action to protect their online privacy.

Based on the survey results, individuals in different work status groups have different motivations for sharing personal information online. Business owners and executives primarily share personal

information to network and establish business connections. Skilled workers and professionals are more likely to share personal information for professional development and learning opportunities. Workers/labourers are more likely to share personal information for entertainment and socialization purposes.

### *5.3.2.6 Employment sector*

The survey revealed that a total of 746 respondents voluntarily provided personal information online. Among these respondents, the majority (570 individuals) were from the private sector. Furthermore, 466 respondents disclosed their age, of which 323 were from the private sector. Similarly, among those who shared their nationality, 436 were from the private sector. With respect to IC number disclosure, only 74 individuals shared this information, the majority of whom were from the private sector. Similarly, the majority of the 194 respondents who shared their address and 261 respondents who disclosed their physical appearance were from the private sector. Additionally, a majority of the respondents who shared their activities (468), opinions (639), list of people they interact with (357), frequently visited locations (254), information shared on social media (377), and pictures of themselves (581) were from the private sector. However, only 35 respondents shared their bank details online, most of whom were from the private sector.

In terms of trust levels for personal data protection, the government and known companies are generally considered more trustworthy than unknown companies. Private sector employees and self-employed individuals are the least trusting of any party with their personal data. However, government employees are more likely to trust all parties with their personal data compared to private sector or self-employed individuals. These findings suggest that trust in personal data protection varies by employment sector, with government employees being more trusting and private sector employees being less trusting.

While the majority of respondents across all sectors do not share personal information for various activities, a higher percentage of individuals in the private sector share personal information for obtaining useful knowledge, game-playing, socializing, targeted advertising, receiving gifts or samples, getting money or discounts, and securely logging into a system compared to the government and self-employed sectors. The self-employed sector has the lowest percentage of individuals who share personal information for these activities overall.

Concerns regarding personal information risks also vary among different employment sectors. Individuals in the government sector were the most concerned about personal details being misused and online financial fraud, with 97.4% and 98.7% expressing concern about these risks, respectively. On the other hand, private sector employees exhibited the highest level of concern about various personal data sources reconstructing their identity, with 89.4% expressing concern about this risk. Overall, the data suggests that individuals in different employment sectors have varying levels of concern regarding different personal information risks.

Regarding items 5, 6, and 7, most respondents who agreed were from the private sector, with 805 individuals agreeing with item 5, 319 individuals agreeing with item 6, and 174 individuals agreeing with item 7. The government sector followed with 155 individuals agreeing with item 5, 23 individuals agreeing with item 6, and 28 individuals agreeing with item 7. These findings indicate that individuals in the private and government sectors have relatively higher levels of agreement with these statements compared to those in the not related and self-employed sectors.

### *5.3.2.7 Education level*

Individuals who possess a higher level of education exhibit a greater likelihood of disclosing their personal information online. Specifically, those with a degree level of education had the highest number of individuals who divulged their information, followed by individuals with a diploma and those with a master's degree. Conversely, individuals with a certificate or STPM/STPMV level of education had the lowest number of people who shared their personal information. It is noteworthy that only a small fraction of individuals across all education levels made their bank details available online.

Survey respondents who possess a higher level of education display a higher tendency to trust established institutions, such as governments and well-known companies, with their personal data. A vast majority of respondents in all education levels trust family members with their personal information. As for friends, most respondents answered "yes" across all education levels. In contrast, for famous companies, most respondents answered "no" or "not sure," while for known companies, the majority still answered "yes" across all education levels. Furthermore, most respondents answered "no" when it comes to unknown companies.

Those with higher education levels are more likely to share personal information online for all activities except Automatic Keystroke Input and Targeted Advertising. Individuals with a diploma or higher education level are more inclined to share personal information for activities such as Obtaining Useful Knowledge, Game-playing, Socializing, Getting Money or Discounts, and Securely Logging into a System, in comparison to those with MCE/SPM/SPMV or STPM/STPMV/Certificate education levels. Education level is a critical factor in determining the willingness of individuals to share their personal information online.

Concerns about the risks associated with personal information online are prevalent among all education levels, primarily regarding online identity theft and the misuse of personal data for marketing purposes. Respondents with higher levels of education express greater concern, particularly those with a master's or PhD degree. The level of concern regarding personal information risks is consistently higher among individuals with higher levels of education across all subcategories.

Respondents with higher levels of education tend to concur more with the statement "I know how to keep my online activities private." The proportion of respondents who agree increases as the level of education increases. Conversely, respondents with higher levels of education tend to disagree more with the statement "I am comfortable giving my personal information online due to the internet's security." The proportion of respondents who disagree increases as the level of education increases. Moreover, respondents with higher levels of education tend to agree more with the statement "The internet is safe for leisure, work, and business transactions." The proportion of respondents who agree increases as the level of education increases.

### *5.3.2.8 Place of living*

Rural residents are more likely than urban residents to have made their personal information available online, according to the table provided. The "Yes" responses for most categories are higher for rural areas, while some categories have higher numbers for cities.

The majority of respondents across all groups felt unsure about sharing data with unknown companies, while family and friends were considered safer options. Differences in attitudes towards sharing personal data were observed based on place of living.

Most respondents across all places of living categories answered "No" for all activities listed, but there were some differences between rural and urban areas. Rural respondents were more likely to

be "Not Sure" about sharing data for certain activities, while urban respondents were more likely to answer "Yes" for other activities.

The data indicates that respondents living in cities are more concerned about personal information risks online than those living in rural areas. Although most respondents expressed some level of concern for all listed risks, a higher percentage of city respondents were worried about these risks compared to rural respondents.

The survey results also suggest that respondents from both urban and rural areas generally feel confident about keeping their online activities private, are comfortable giving their personal information online due to internet security, and believe that the internet is safe for leisure, work, and business transactions. However, respondents from urban areas are more likely to agree to these statements than those from rural areas.

#### *5.3.2.9 Income level*

The study's findings indicate that individuals from various income levels generally disclose their nationality online. However, alarming findings emerged regarding the disclosure of IC numbers and bank details. Individuals earning less than RM4,850 were more inclined to share personal information online, such as their address, opinions, pictures, and information about their acquaintances. Additionally, individuals across all income levels revealed information about the locations they frequently visit and shared it on social media.

The outcomes imply that people with higher income levels are more likely to trust their personal data to family members, friends, federal/state government, and established companies. However, people with no or lower income levels are more likely to respond positively to unknown companies.

Most respondents from all income levels were willing to disclose personal information to acquire useful knowledge, while those from lower income levels were more likely to share information for socializing, game-playing, and expecting gifts or samples. In contrast, individuals with higher income levels were less likely to share information for these activities. Moreover, respondents across all income levels were unwilling to provide personal information for automatic keystroke input, but they were willing to share information for securely logging into a system.

Individuals across all income levels expressed apprehensions about the hazards associated with disclosing personal information online, with most expressing concerns about their personal data being utilized for marketing and potential damage to their reputation due to personal information posted online. Respondents with lower income levels expressed greater levels of anxiety about online monitoring, personal data sources reconstructing their identity, and online identity theft.

Individuals with lower income levels were less likely to concur with statements related to online privacy and security. Respondents with no or lower income levels tended to disagree more with item 5, indicating a lack of knowledge in safeguarding their online activities' privacy. Respondents with higher income levels were more comfortable providing their personal information online for item 6, while those with no or lower income levels disagreed more. Finally, respondents with higher income levels had a higher percentage of agreement that the internet is safe for leisure, work, and business transactions for item 7, while those with no or lower income levels had a lower percentage of agreement. These results suggest that income level plays a role in shaping attitudes towards online privacy and security.



### 5.3.2.10 Residence state

The majority of respondents across all states answered questions in the survey as follows: "Yes" for "availability of their name online", "nationality online", "activities, opinions, people they interact with online", "opinions online", "social media information online", and "pictures of themselves online"; "No" for "age online", "IC number online", "address online", "physical appearance online", and "bank details online".

Regarding entrusting personal data, most participants (79%) believed that sharing their data with family members is secure, whereas only 17% believed it was safe to trust friends. Participants were most likely to trust their family members, followed by known companies and the government, with least trust in unknown companies and friends. The level of trust varied significantly across states.

The survey found that respondents' likelihood of engaging in activities varied across states. For example, respondents who answered positively to automatic keystroke input ranged from 9.3% in Pulau Pinang to 34.7% in Terengganu. Respondents who answered affirmatively to game-playing ranged from 1.2% in Perlis to 21.9% in Terengganu. Overall, most respondents across most states were generally reluctant to share personal information for these purposes.

Regarding privacy concerns, the state of Terengganu had the highest percentage of respondents expressing concern over the potential misuse of personal details, followed by Pahang and Kelantan, with Perlis having the lowest percentage of concern. The highest percentage of respondents expressing concern over their online behaviour being monitored was in Kelantan, followed by Terengganu and Pahang, with Perlis having the lowest level of concern. Pahang had the highest percentage of respondents expressing concern over the use of their personal data for marketing purposes.

## 6. Discussion

The present study aimed to measure the receptiveness of Malaysian people to new technologies, assess their views on managing their identity online, and identify the demographic factors that influence their attitudes towards new technologies and their adoption of online identity management tools. To achieve these objectives, a survey was conducted among 1,014 participants in Malaysia.

The results showed that demographic factors have a significant association with the adoption of new technologies. Gender, age, ethnicity/race, work status, employment sector, level of education, place of living, household income level, and residence state were all significantly associated with early adoption of emerging technologies, trying out new technologies, and enjoyment of trying out new technologies. On the other hand, marital status only significantly influenced the enjoyment of trying out new technologies. These results are consistent with previous research, which has shown that various demographic characteristics can influence individuals' attitudes towards technology adoption [21,22]. For example, previous studies have found that younger people are more likely to adopt new technologies than older individuals [23,24], and that males tend to have more positive attitudes towards technology adoption than females [25,26].

The study also found that there were significant relationships between various demographic factors and items related to personal information management, indicating that certain factors may have an impact on people's preferences for specific identity management tools. However, some factor-item combinations did not exhibit a significant relationship, such as nationality-IC number, people regularly interacted with, pictures of oneself, and bank details.

Moreover, the study revealed noteworthy dissimilarities among diverse demographic groups concerning their trust levels when it comes to personal data. Gender, age, education level, work status, and employment sector were found to be significantly related to trust levels. This result aligns with previous research, which has demonstrated that demographic factors such as age, gender, and education can affect individuals' trust in technology [27,28]. For example, younger individuals tend to have higher levels of trust in technology than older individuals, and individuals with higher levels of education tend to have more trust in technology than those with lower levels of education.

The findings of this study have implications for policymakers and practitioners involved in promoting the adoption of new technologies and the management of online identities. The study results can help policymakers understand the demographic factors that influence people's attitudes towards technology adoption and online identity management [29], and tailor policies accordingly. For instance, policymakers can develop targeted campaigns to promote technology adoption among specific demographic groups that exhibit lower receptiveness to new technologies.

Practitioners involved in developing new technologies and identity management tools can use the study findings to ensure that their products cater to the specific needs and preferences of different demographic groups. For example, if a tool is designed to manage bank details, it may be more effective if tailored to suit the preferences of certain demographic groups based on their income level or work status.

However, there are some limitations to this study that must be considered when interpreting the results. Firstly, the study sample may not be representative of the entire Malaysian population, as it included only those who had access to the internet and were willing to participate. Secondly, the study relied on self-reported data, which may be subject to response biases. Finally, the study did not explore the reasons behind the observed associations, which could be a topic for future research.

## **7. Conclusion**

In conclusion, the findings of this study shed light on the attitudes of Malaysian individuals towards new technologies and online identity management. The study has identified several demographic factors that significantly influence these attitudes, including age, gender, education level, and income. These insights are particularly relevant for policymakers, practitioners, and researchers who are interested in developing effective policies, strategies, and technologies to promote the adoption of new technologies and manage online identities in Malaysia.

The study highlights the importance of considering the diversity of Malaysian individuals when developing policies and technologies related to new technologies and online identity management. Policymakers and practitioners must be aware of the varying levels of trust that different demographic groups have when it comes to managing their personal data. They should strive to develop policies and technologies that cater to the needs of all individuals and ensure that no one is left behind.

Moreover, the study's findings provide important guidance for researchers who are interested in further exploring the factors that influence attitudes towards new technologies and online identity management in Malaysia. Future research should examine how these attitudes and perceptions evolve over time, especially in response to external factors such as economic, social, and political changes. This can help policymakers, practitioners, and researchers to anticipate future trends and develop effective strategies to promote the adoption of new

technologies and manage online identities in Malaysia. By considering the diversity of individuals and their varying levels of trust, policymakers and practitioners can develop more effective policies and technologies that cater to the needs of all individuals in Malaysia.

### Acknowledgement

We express our gratitude to the Malaysian Communications and Multimedia Commission (MCMC) for their kind provision of the Digital Society Research Grant 2022, Cycle 2, which was granted under RMC file no. 100-TNCP/GOV 16/6/2 (070/2022). This funding was of great significance in supporting our research endeavours and in successfully concluding our project. Additionally, we would like to extend our appreciation to Universiti Teknologi MARA (UiTM) for furnishing us with the essential resources and facilities needed to carry out this study.

### References

- [1] Dwivedi, Yogesh K., Anuj Sharma, Nripendra P. Rana, Mihalis Giannakis, Pooja Goel, and Vincent Dutot. "Evolution of artificial intelligence research in Technological Forecasting and Social Change: Research topics, trends, and future directions." *Technological Forecasting and Social Change* 192 (2023): 122579. <https://doi.org/10.1016/j.techfore.2023.122579>
- [2] Shahin, Saif. "David Atkin, Professor, Department of Communication, University of Connecticut, USA."
- [3] Statistics and Data Intelligence Department MCMC. "Internet Users Survey 2020," (2020).
- [4] Hazelah, Alias, Nur Nadia Ismail, and Rugayah Hashim. "Identity Theft Awareness among City Dwellers in Malaysia." *Journal of Information Assurance & Cybersecurity* 11 (2011): 1-9. <https://doi.org/10.5171/2011.274080>
- [5] Zulkifli, Faiz, Zainal Abidin, Rozaimah, Mohamed Ariff, Mohamed Imran, Ahmad, Nahdatul Akma, Arshad, Noreen Izza, Ependi, Usman, and Razak, Mohamad Sharmizi. "National digital identity: current landscape, emerging technologies and future directions." *International Journal of Academic Research in Business and Social Sciences* 13, no. 3 (2023): 1225-1242. <https://doi.org/10.6007/IJARBS/v13-i3/16603>
- [6] Arunwatanamongkol, Pensri, Natawut Nupairoj, and Uthai Tanlamai. "Innovative Delegation Application in Thai National Digital Identity Platform." *International Journal of Interactive Mobile Technologies* 15, no. 14 (2021). <https://doi.org/10.3991/ijim.v15i14.22055>
- [7] Udwan, Ghadeer, Koen Leurs, and Amanda Alencar. "Digital resilience tactics of Syrian refugees in the Netherlands: Social media for social support, health, and identity." *Social Media+ Society* 6, no. 2 (2020): 2056305120915587. <https://doi.org/10.1177/2056305120915587>
- [8] Third, Allan, Kevin Quick, M. Bachler, and John Domingue. "Government services and digital identity." *Knowledge Media Institute of the Open University* (2018).
- [9] Kó, Andrea, Enrico Francesconi, Gabriele Anderst-Kotsis, A. Min Tjoa, and Ismail Khalil, eds. *Electronic Government and the Information Systems Perspective: 8th International Conference, EGOVIS 2019, Linz, Austria, August 26–29, 2019, Proceedings*. Vol. 11709. Springer, 2019. <https://doi.org/10.1007/978-3-030-27523-5>
- [10] Varela, Jimena Hernández, Matías Jackson Bertón, and Jorge Prego Acosta. "Building a framework for Trust Services in Uruguay." In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, pp. 489-491. 2019. <https://doi.org/10.1145/3326365.3326436>
- [11] Tammpuu, Piia, and Anu Masso. "Transnational digital identity as an instrument for global digital citizenship: The case of Estonia's E-residency." *Information Systems Frontiers* 21 (2019): 621-634. <https://doi.org/10.1007/s10796-019-09908-y>
- [12] Chan, Yee Kiu, Yuk Ming Tang, and Long Teng. "A comparative analysis of digital health usage intentions towards the adoption of virtual reality in telerehabilitation." *International Journal of Medical Informatics* 174 (2023): 105042. <https://doi.org/10.1016/j.ijmedinf.2023.105042>
- [13] Yuan, Mengqi, Zhongfu Li, Xiaodong Li, Xiaowei Luo, Xianfei Yin, and Jin Cai. "Proposing a multifaceted model for adopting prefabricated construction technology in the construction industry." *Engineering, Construction and Architectural Management* 30, no. 2 (2023): 755-786. <https://doi.org/10.1108/ECAM-07-2021-0613>
- [14] Blaskovits, Farriss, Imaan Bayoumi, Colleen M. Davison, Autumn Watson, and Eva Purkey. "Impacts of the COVID-19 pandemic on life and learning experiences of indigenous and non-Indigenous university and college students in Ontario, Canada: A qualitative study." *BMC Public Health* 23, no. 1 (2023): 96. <https://doi.org/10.1186/s12889-023-15010-5>

- [15] Frishammar, Johan, Anna Essén, Frida Bergström, and Tilda Ekman. "Digital health platforms for the elderly? Key adoption and usage barriers and ways to address them." *Technological Forecasting and Social Change* 189 (2023): 122319. <https://doi.org/10.1016/j.techfore.2023.122319>
- [16] Ekman, Björn, Hans Thulesius, Jens Wilkens, Anna Lindgren, Olof Cronberg, and Eva Arvidsson. "Utilization of digital primary care in Sweden: descriptive analysis of claims data on demographics, socioeconomics, and diagnoses." *International journal of medical informatics* 127 (2019): 134-140. <https://doi.org/10.1016/j.ijmedinf.2019.04.016>
- [17] Li, Zhangzhi. "The marketing prospects of consumer trust in banking services to reduce perceived financial risk and enhance intention to use internet banking." *International Journal of e-Collaboration (IJeC)* 18, no. 3 (2022): 1-13. <https://doi.org/10.4018/IJeC.307128>
- [18] Loke, Siew-Phaik, Norlida Mohd Noor, and Khalizani Khalid. "Customer satisfaction towards internet banking services: Case analysis on a Malaysian bank." In *2012 IEEE Colloquium on Humanities, Science and Engineering (CHUSER)*, pp. 159-163. IEEE, 2012. <https://doi.org/10.1109/CHUSER.2012.6504302>
- [19] Ilyas, Muhammad, Arif ud din, Muhammad Haleem, and Irshad Ahmad. "Digital entrepreneurial acceptance: an examination of technology acceptance model and do-it-yourself behavior." *Journal of Innovation and Entrepreneurship* 12, no. 1 (2023): 15. <https://doi.org/10.1186/s13731-023-00268-1>
- [20] Alshurideh, M., Amal Abuanezh, B. Kurdi, Iman Akour, and Ahmad AlHamad. "The effect of teaching methods on university students' intention to use online learning: Technology Acceptance Model (TAM) validation and testing." *International Journal of Data and Network Science* 7, no. 1 (2023): 235-250. <https://doi.org/10.5267/ij.dns.2022.10.009>
- [21] Kanojia, Palak, and Madan Lal. "Moderation effect of demographic factors in adoption of electronic payments." *International Journal of Management Practice* 16, no. 1 (2023): 18-37. <https://doi.org/10.1504/IJMP.2023.10052014>
- [22] Mitra, Sharmili, Anshita Singh, Sambath Rajendran Deepam, and Manish Kumar Asthana. "Information and communication technology adoption among the older people: A qualitative approach." *Health & Social Care in the Community* 30, no. 6 (2022): e6428-e6437. <https://doi.org/10.1111/hsc.14085>
- [23] Rha, Jong-Youn, Youngwon Nam, Sun Young Ahn, Jihye Kim, Youchung Chang, Jisu Jang, Keiko Kurita *et al.*, "What drives the use of wearable healthcare devices? A cross-country comparison between the US and Korea." *Digital Health* 8 (2022): 20552076221120319. <https://doi.org/10.1177/20552076221120319>
- [24] Yap, Yee-Yann, Siow-Hooi Tan, and Shay-Wei Choon. "Elderly's intention to use technologies: A systematic literature review." *Heliyon* (2022). <https://doi.org/10.1016/j.heliyon.2022.e08765>
- [25] Nouraldeen, Rasha Mohammad. "The impact of technology readiness and use perceptions on students' adoption of artificial intelligence: the moderating role of gender." *Development and Learning in Organizations: An International Journal* 37, no. 3 (2023): 7-10. <https://doi.org/10.1108/DLO-07-2022-0133>
- [26] Wang, Kun, and Danan Gu. "Reciprocal associations between social media use and self-perception of aging among older adults: Do men and women differ?." *Social Science & Medicine* 321 (2023): 115786. <https://doi.org/10.1016/j.socscimed.2023.115786>
- [27] Alshari, Hussein Ahmed, and M. A. Lokhande. "The impact of demographic factors of clients' attitudes and their intentions to use FinTech services on the banking sector in the least developed countries." *Cogent Business & Management* 9, no. 1 (2022): 2114305. <https://doi.org/10.1080/23311975.2022.2114305>
- [28] De Santis, Karina Karolina, Tina Jahnel, Elida Sina, Julian Wienert, and Hajo Zeeb. "Digitization and health in Germany: cross-sectional nationwide survey." *JMIR public health and surveillance* 7, no. 11 (2021): e32951. <https://doi.org/10.2196/32951>
- [29] Wang, Dan, Terh Jing Khoo, and Zhangfei Kan. "Exploring the application of digital data management approach for facility management in Shanghai's high-rise buildings." *Progress in Energy and Environment* (2020): 1-15.