# An Exploratory Study of Mobile App Use by Financial Institutions: Cybersecurity Perspective

Olumide Bashiru Abiola
Beechnet Solutions Limited
2967 Dundas Street West, #724D, Toronto, Ontario M6P 1Z2, Canada

## ABSTRACT

The ability of Internet technology has changed the mode of financial transactions in recent times whereby most bank transactions are now carried out via mobile apps. The nature of the transaction has also changed the financial processes which has led to an unparalleled improvement in the support given by different banks. Nonetheless, considering the volume of digital-related transactions that take place today, particularly with mobile Internet banking systems, cybersecurity vulnerabilities, and privacy are jeopardized using a mobile app for financial transactions, resulting in bank customers' vulnerability. The confidentiality and integrity of bank customers' information while using mobile banking apps are negatively impacted by the effects of cybersecurity threats. Once more, the feeling of cybersecurity vulnerability interferes with users' decision-making over the use of mobile banking apps. In this study, efforts are exerted to explore existing literature on mobile app use by financial institutions and to examine how internet cybersecurity threats may impact customers' belief in the use of mobile apps. The results of this study revealed that bank security management and guidance had a positive impact on financial institutions' staff while using mobile apps for financial transactions. Similarly, it has been found that security management and guidance benefit staff members of financial institutions who use mobile apps for work-related objectives. As a result, it can be inferred that security management and guidance influence behavioral intent to utilize mobile apps. Furthermore, decision-makers at banks should consider these findings when determining how to construct future mobile app infrastructure.

## Keywords

A mobile app, financial institution, cybersecurity.

## 1. INTRODUCTION

For the past ten years, the mobile app market has grown rapidly, with new markets maturing every year [25]. By 2025, mobile app industry revenue is anticipated to increase to $70 billion [16]. However, records from 2018 show that the sector has surpassed this forecast, achieving over $86 billion in consumer expenditure in 2017, an increase of 105% from 2015. With these numbers, mobile app stores are clearly among the fastest-growing e-commerce platforms worldwide [16]. Academics published research papers on mobile app consumer behavior, app business models, app success factors in the market, and other topics because of a surge in interest in the industry [25].

The reasons the mobile application industry is of significance to academics are as follows:

- The developer and customer communities are both extremely sizable. More than 250,000 developers work for consumer app stores, and there are close to 400,000 mobile app downloaders overall. Thus, carrying out research that assists this community in identifying strategies to maximize their profit in the market will provide stakeholders and developers with major financial advantages in the business.
- As a result of the fact that developers selling apps on the same platform share the same business environment, consumer traffic, and platform limitations, study findings and recommendations would be scalable and applicable to the entire community.
- As consumer behavior is a crucial component of sound business modeling [2], study results can be used to create standards that are relevant to hundreds of thousands of developers working in a multibillion-dollar sector.

By examining financial institutions' use of mobile apps from the standpoint of cybersecurity, this study aims to significantly add to the body of knowledge already available in the research area of mobile apps. The goal of the study is to reduce the possibility that financial consumers would be subjected to security risks while transacting on a mobile app platform.

## 2. LITERATURE REVIEW

The distinctions between mobile applications and conventional software systems were highlighted by [26], the study included usability of mobile app from the perspectives of source code, third-party Application Programming Interfaces (APIs), and historical data. [5] indicated that app updates after downloading occur because of deployment problems or changes to source code. The study discovered that updates most times do not include notification explanations, are infrequently followed by another emergency update, and the ones that come before them often result in customer backlash expressed in unfavorable reviews. [3] evaluated online testing methods for the Android platform and created a comprehensive framework that describes the most prevalent testing methods that can be found online and in the literature. [24] investigated whether mobile apps adhered to European Union data protection laws, which prohibit the export of personal information from European users. They examined 1,498 applications and discovered that 51% of them did not offer any privacy policies to users in Europe and that 16.5% of them transferred user data outside of the European Union. [20] examined Android and BlackBerry micro-apps along the dimensions of source code, code dependencies, and code churn. They discovered that BlackBerry micro-apps are bigger and more dependent on outside libraries. To uncover software engineering issues specific to mobile apps, [20] compared large and tiny desktop programs to mobile apps along two metrics: code size and debugging time. [23] examined software reuse through inheritance or class reuse and discovered that, on average, 61% of classes in every store category appear in multiple apps. [3] created an automated spam app detection mechanism that can identify spam apps with over 95% accuracy; the detection tool was then used on the Mobile App Download Store and discovered that 2.7% of the 180,000 tested applications were potentially spam. Inadvertent personal data disclosure from mobile apps using wireless networks was examined by [7]. Despite Wi-Fi encryption being in place, they discovered that mobile apps can still broadcast information like age, gender, and religion. The market for mobile apps cannot be fully satiated without a change in any part of the hardware that goes into these mobile devices. Among the hardware upgrades required are possibly greater wireless network bandwidth or better, more effective computing power. A mobile app portal, which is crucial in streamlining the process of distributing these mobile apps, is present in the mobile app market [8]. As they play a part in connecting/linking app developers and users, portals are helpful in this course of action. The unquestionable changes they undergo are a constant despite the arguments for and against expanding or contracting the number of gateways. Portals can be either centrally located or dispersed, and both carry out different tasks. Talking about the mobile app market also means talking about the process of distributing mobile apps, which entails developing (or creating) an app, connecting it to the market, selling and buying apps, and then using them on mobile devices. Moreover, If the designers come across as unprofessional, they typically have trouble persuading potential customers to purchase them [8]. Exploring this idea is necessary so that users can understand the fundamental ideas guiding the markets. [9] examined the number of users who are active monthly to draw a correlation between their frequency on the apps and the popularity of these mobile applications. These mobile apps are built, designed, and developed for international markets that aim to draw various consumer demographics [13]. Offering an examination of the reach of in-app advertisements is helpful in comprehending the technology narrative while discussing the importance of these apps in the lives of mobile consumers. Although bothersome and inconvenient, ads are still present, and despite this, consumers continue to buy and use mobile apps, so their position is unaffected [17] These advertisements are helpful since developers have a responsibility to promote advertisers and make sure they have strong connections to their target market (or market). Software Development Kits (SDKs) functions in various mobile app markets guarantee the development of apps that run on the platforms, third-party developers collaborate with these kits. These platforms are intended to provide integrated development environments (IDEs) to speed up the development process and increase exposure to the application markets [10.] Developers are encouraged to experiment with specific features to cover potential challenges with device variability. It is the responsibility of the developer to keep at least one device compatible when dealing with a feature that appears to work with most devices. When considering this range of devices, these foundations suggest more freedom for developers [18]. For instance, capabilities like Bluetooth were included in other devices that fiercely competed with IOS, despite not being present in older iPhone platforms. Even though Apple insist that Bluetooth is a "standard" component of their most recent gadgets, this may be the result of pressure from their rivals. The ease of use of apps and their ability to help users find the material they want are two factors that are particularly related to their adoption. Using a smartphone app, for instance, seems quicker and more efficient when one wants to sign into a website [22]. It could be challenging for users to access all the features and actions while using the website via mobile phones with apps like Facebook. Using a computer or laptop makes more sense if one is going to sign into Facebook utilizing a website. Mobile apps, such as those for banking, shopping, and food delivery, are far more helpful because they make these users' lives easier. The pressure that developers face can be understood by identifying the inevitable competition between various platforms in the mobile app market [6]. There might not be a need to steal or duplicate technologies from other industries if there was only one development platform already in use.

# 3. METHODOLOGY

This study used quantitative research methods. The study focuses on gathering and examining structured data [21]. Surveying bank staff in the financial institutions in Lagos State, Nigeria, is the method used to collect data. The study was able to gather statistics and data on the bank's mobile banking app security, thanks to the data gathering from bank staff. Hence, positivism is the research paradigm employed in the study. The positivist approach begins with the formulation of a theory, followed by the execution of the investigation [19]. The information acquired enables the conceptual model of the financial institution mobile app used to be validated and determines whether the model's construct is supported.

## 3.1 Population and Sample

In this study, financial institutions and bank employees in Lagos State, Nigeria, who use mobile banking applications, are the target population [12]. Targeting this group is being done with the intention of assisting financial institutions in developing a framework that will aid in the design and development of mobile banking applications and lessen customer vulnerabilities. The study also seeks to obtain an understanding of how insecure mobile banking applications are and to safeguard the privacy of financial institution customers [15]. The bank staffs are the target audience in financial institutions. This will allow the study to gather data and information on the financial institution regarding the mobile app security feature incorporated into the app the clients utilize for their financial operations.

## 3.2 Survey Instrument

To gather data for this study, a survey was undertaken, and questionnaires were sent to bank staff [28]. Two distinct sections make up the survey. The first part of the questionnaire is to gather personal information of the staff in the financial institution. The second part of the questionnaire is used to collect data on staff usage of mobile apps and the impact cybersecurity. Cybersecurity threats, guidance, and security management are some of these factors [14]. The measurement items used in this study were taken from a previous study on the impact of cybersecurity threats on mobile banking users.

## 3.3 Data Analysis

For the statistical analysis in this work, SAS/STAT is utilized to run the Structural Equation Modeling (SEM) procedure [4]. Moreover, SEM is regarded as the appropriate methodology for this type of investigation because it is exploratory-based research [4]. To establish the convergent validity of the measurement model, it was advised by [4] that researchers should take into account the outer loadings of the items and the average variance extracted (AVE). Cross-loading and the Fornell-Larcker criterion were two additional measures [27] suggested for proving discriminant validity. As an additional criterion for evaluating the discriminant validity, [1] also recommended looking at the Heterotrait-Monotrait. The path coefficients and the coefficient of determination (R2) are estimated in terms of the structural model [27]. The measurement and structural models can therefore be evaluated using all the criteria.

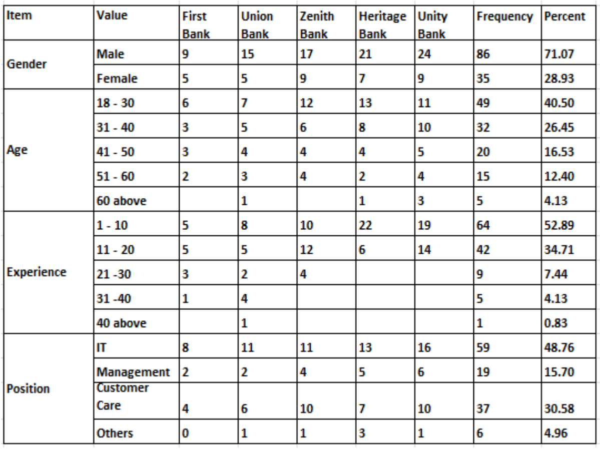
# 4. RESULT

This section of the study discusses the descriptive data analysis, the measurement model, and the structural model assessment.

## 4.1 Descriptive Analysis

The data used in this study were gathered from 163 staff that works in five different financial institutions in Nigeria [11]. However, after eliminating the missing values, the viable responses total 121. The participants' demographic data are shown in Table 1 for convenience.

**Table 1. Frequency distribution**



| Item | Value | First Bank | Union Bank | Zenith Bank | Heritage Bank | Unity Bank | Frequency | Percent |
|---|---|---|---|---|---|---|---|---|
| Gender | Male | 9 | 15 | 17 | 21 | 24 | 86 | 71.07 |
| | Female | 5 | 5 | 9 | 7 | 9 | 35 | 28.93 |
| Age | 18 - 30 | 6 | 7 | 12 | 13 | 11 | 49 | 40.50 |
| | 31 - 40 | 3 | 5 | 6 | 8 | 10 | 32 | 26.45 |
| | 41 - 50 | 3 | 4 | 4 | 4 | 5 | 20 | 16.53 |
| | 51 - 60 | 2 | 3 | 4 | 2 | 4 | 15 | 12.40 |
| | 60 above | | 1 | | 1 | 3 | 5 | 4.13 |
| Experience | 1 - 10 | 5 | 8 | 10 | 22 | 19 | 64 | 52.89 |
| | 11 - 20 | 5 | 5 | 12 | 6 | 14 | 42 | 34.71 |
| | 21 -30 | 3 | 2 | 4 | | | 9 | 7.44 |
| | 31 -40 | 1 | 4 | | | | 5 | 4.13 |
| | 40 above | | 1 | | | | 1 | 0.83 |
| Position | IT | 8 | 11 | 11 | 13 | 16 | 59 | 48.76 |
| | Management | 2 | 2 | 4 | 5 | 6 | 19 | 15.70 |
| | Customer Care | 4 | 6 | 10 | 7 | 10 | 37 | 30.58 |
| | Others | 0 | 1 | 1 | 3 | 1 | 6 | 4.96 |

The table shows that only 71.07% of the data were male, while females make up the remaining 28.93% of the data. For the age brackets, the staff representation for the age range 18 – 30 years of age is 40.50%. Between 31 – 40 years of age, the staff representation in this age range represents 26.45% and between 41 – 50 years of age, the staff representation in this age range is 16.53%. The age ranges for 51 – 60 years of age, staff representation in this age range is 12.40%, and for 60 years of age and above, the staff representation in this age range represents 4.13%. The usage of mobile apps for a financial transaction was examined, and the findings revealed that 87% of participants have had more than a year's worth of experience using bank apps for transactions. Also, the results showed that 59% of the bank staff chose both banking over the counter and mobile apps for their financial transactions, with 21% of those staff using the mobile banking app for their daily transactions.

## 4.2 Measurement Model Assessment

The factor loading should be calculated to assess each item's reliability. A threshold value for each item's loading that is equal to or higher than 0.7 is regarded as dependable. Moreover, Cronbach's Alpha and composite reliability scores should both be at least 0.7. Table 2 shows the items are valid and meet the established requirements, except for SM5 and SM6, whose factor loadings were less than 0.7, and as a result, they were removed from the construct's structure for the model of mobile app use by financial institutions. A further definition of the average variance extracted (AVE), which is used to quantify convergent validity, is the grand mean value of the squared loadings of the construct-related items. The AVE indicates that a construct explains more than half of the variance of its elements when it has a value of 0.5 or higher. According to Table 2, the AVE values are greater than 0.5, and Cronbach's Alpha and composite reliability values are both over 0.7. It is established that the constructs are convergent.

**Table 2. Model measurement item loading**

| Constructs | Item | Loadings | Cronbach Alpha | Composite Reliability | Average Variance Extracted |
|---|---|---|---|---|---|
| Security Management | SM1 | 0.872 | 0.856 | 0.892 | 0.574 |
| | SM2 | 0.864 | | | |
| | SM3 | 0.841 | | | |
| | SM4 | 0.823 | | | |
| | SM5 | 0.548 | | | |
| | SM6 | 0.680 | | | |
| Guidance | GU1 | 0.851 | 0.914 | 0.920 | 0.723 |
| | GU2 | 0.864 | | | |
| | GU3 | 0.881 | | | |
| | GU4 | 0.769 | | | |
| | GU5 | 0.894 | | | |
| Cybersecurity | CS1 | 0.887 | 0.880 | 0.904 | 0.856 |
| | CS2 | 0.897 | | | |
| | CS3 | 0.924 | | | |
| | CS4 | 0.911 | | | |
| | CS5 | 0.902 | | | |
| | CS6 | 0.882 | | | |
| | CS7 | 0.867 | | | |

The Fornell-Larcker criterion, cross-loadings, and the heterotrait-monotrait ratio should all be looked at to prove the discriminant validity. The present study, as shown in Table 3, satisfies the Fornell-Larcker criterion, which states that the square root of AVE (diagonal value) for each variable should be greater than the correlation of latent variables. Regarding the cross-loadings, each indicator's loading ought to be higher than the loadings of the indicators for the variables to which it corresponds. It can be seen from Table 4 that the cross-loading requirement is met. A result of less than 0.85 for the heterotrait-monotrait ratio (HTMT) should be verified. The HTMT condition is satisfied, signifying that the discriminant validity is demonstrated.

## 4.3 Structural Model Assessment

The level of disagreement between the model's dependent variables is used to gauge the model's explanatory power. The R2 and the path coefficients are the crucial metrics for evaluating the structural model, claims [4]. According to Figure 1, the model's R2 values for Security Management (SM), Guidance (GU), and Cybersecurity (CS) are 59.6%, 47.5%, and 58.4%, respectively.

**Table 3. Cross-loading for the variable measurement**

| | CS | GU | SM |
|---|---|---|---|
| **CS1** | **0.863** | 0.645 | 0.683 |
| **CS2** | **0.917** | 0.667 | 0.642 |
| **CS3** | **0.892** | 0.698 | 0.507 |
| **CS4** | **0.722** | 0.603 | 0.573 |
| **CS5** | **0.941** | 0.674 | 0.597 |
| **CS6** | **0.822** | 0.672 | 0.651 |
| **CS7** | **0.893** | 0.659 | 0.672 |
| **GU1** | 0.569 | **0.884** | 0.527 |
| **GU2** | 0.578 | **0.838** | 0.583 |
| **GU3** | 0.654 | **0.796** | 0.662 |
| **GU4** | 0.662 | **0.820** | 0.669 |
| **GU5** | 0.653 | **0.852** | 0.683 |
| **CM1** | 0.681 | 0.458 | **0.874** |
| **CM2** | 0.619 | 0.457 | **0.846** |
| **CM3** | 0.546 | 0.512 | **0.841** |
| **SM4** | 0.674 | 0.497 | **0.843** |
| **SM5** | 0.682 | 0.490 | **0.862** |
| **SM6** | 0.585 | 0.527 | **0.850** |

Table 3 shows the cross-loading for the variable measurement. All the hypotheses are correct, proving that all the relationships between the independent and dependent variables are significant.

The relationship between perceived ease of use and perceived usefulness is described by H1 (B = 0.766, p 0.05), which shows that the perceived ease of use improves the perceived utility of a mobile app. The relationship between perceived ease of use and behavioral intention is shown in H2 (B = 0.588, p 0.05), indicating that perceived ease of use influences users' intentions to utilize mobile apps.6. H3 (B = 0.199, $p < 0.05$) demonstrates the path between perceived usefulness and behavioral intention; revealing that perceived usefulness positively influences the behavioral intention to use mobile apps. H4 (B = 0.673, $p < 0.05$) describes the path between behavioral intention and actual usage; indicating that behavioral intention is significantly affecting the actual usage of mobile apps. According to the findings of this study, SM and GU have a beneficial influence on financial institution staff when using mobile apps for financial transactions. In a similar vein, it was discovered that SM and GU have a beneficial impact on financial institution staff using mobile apps for work purposes. It is therefore concluded that SM and GU increase the behavioral intention to use mobile apps. Furthermore, while making decisions about building future mobile app infrastructure, banks decision-maker should take these findings into account.

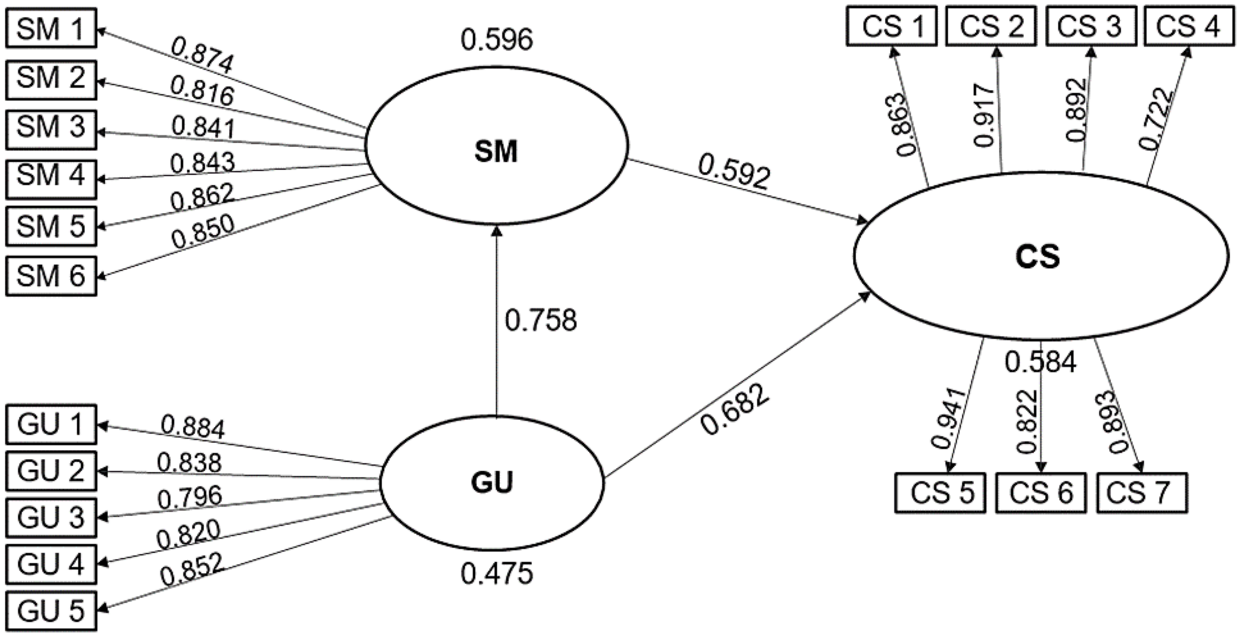


**Fig 1: Structural equation modeling showing path analysis**

## 5. CONCLUSION

This study intends to significantly add to the body of knowledge already available in the growing field of mobile apps by investigating financial institutions' use of mobile applications from the perspective of cybersecurity. The study's objective is to lessen the likelihood that financial consumers may face security threats when transacting on a mobile app platform. The sample used in the study was drawn from 163 staff of five different financial organizations in Nigeria. The results of this study show that SM and GU have a positive effect on employees of financial institutions that use mobile apps for financial transactions. In a similar vein, SM and GU have a positive effect on staff members of financial institutions who use mobile apps for work-related activities. So, it can be inferred that SM and GU promote behavioral intention to use mobile apps. It was therefore suggested in this study that decision-makers at banks should consider these findings when deciding the mobile app infrastructure that will support the successful use of mobile apps in financial institutions.

## 6. ACKNOWLEDGMENTS

Many thanks to families and friends for the support and inspiration all these years in this endeavor.

## 7. REFERENCES

[1] Ab Hamid, M.R., Sami, W. and Sidek, M.M., 2017, September. Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. In Journal of Physics: Conference Series (Vol. 890, No. 1, p. 012163). IOP Publishing.

[2] Alam, A., 2022. Platform Utilizing Blockchain Technology for eLearning and Online Education for Open Sharing of Academic Proficiency and Progress Records. In Smart Data Intelligence: Proceedings of ICSMDI 2022 (pp. 307-320). Singapore: Springer Nature Singapore.

[3] Alkahtani, H. and Aldhyani, T.H., 2022. Artificial intelligence algorithms for malware detection in Android-operated mobile devices. Sensors, 22(6), p.2268.

[4] Al-Maroof, R.A.S. and Al-Emran, M., 2018. Students' acceptance of google classroom: An exploratory study using PLS-SEM approach. International Journal of Emerging Technologies in Learning (Online), 13(6), p.112.

[5] Araujo, F. and Taylor, T., 2020, November. Improving cybersecurity hygiene through JIT patching. In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (pp. 1421-1432).

[6] Barlow, M.A., Verhaal, J.C. and Angus, R.W., 2019. Optimal distinctiveness, strategic categorization, and product market entry on the Google Play app platform. Strategic Management Journal, 40(8), pp.1219-1242.

[7] Bećirović, S., 2023. Privacy and Personal Data Protection in Digital Pedagogy. In Digital Pedagogy: The Use of Digital Technologies in Contemporary Education (pp. 83-96). Singapore: Springer Nature Singapore.

[8] Benner, D., Schöbel, S.M., Janson, A. and Leimeister, J.M., 2022. How to Achieve Ethical Persuasive Design: A Review and Theoretical Propositions for Information Systems. AIS Transactions on Human-Computer Interaction, 14(4), pp.548-577.

[9] Can, U. and Alatas, B., 2019. A new direction in social network analysis: Online social network analysis problems and applications. Physica A: Statistical Mechanics and its Applications, 535, p.122372.

[10] De Cremer, P., Desmet, N., Madou, M. and De Sutter, B., 2020. Sensei: Enforcing secure coding guidelines in the integrated development environment. Software: Practice and Experience, 50(9), pp.1682-1718.

[11] Etim, O., Fidelis, O. and Archibong, E., 2022. Spiritual Accounting and Corporate Financial Reporting: A Study of Micro Finance Banks in Delta State, Nigeria. Journal of Accounting and Financial Management, 8(4), pp.173-180.

[12] Festus, A.F., Kazeem, K.O. and Ayodeji, O.B., 2020. Information and communication technology and sustainable performance of selected listed deposits money banks in Lagos State, Nigeria. Int. J. Sustain. Manag. Inf. Technol, 6(1), p.18.

[13] Florido-Benítez, L., 2022. International mobile marketing: A satisfactory concept for companies and users in times of pandemic. Benchmarking: An International Journal, 29(6), pp.1826-1856.

[14] Fonseca-Herrera, O.A., Rojas, A.E. and Florez, H., 2021. A model of an information security management system based on NTC-ISO/IEC 27001 standard. IAENG Int. J. Comput. Sci, 48(2), pp.213-222.

[15] Hanif, Y. and Lallie, H.S., 2021. Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. Technology in Society, 67, p.101693.

[16] Hintemann, R., 2020. Efficiency Gains are Not Enough: Data Center Energy Consumption Continues to Rise Significantly. Borderstep Inst. für Innovation und Nachhaltigkeit gGmbH.

[17] Karanfiloğlu, M, Sağlam, M. and Topsumer, F., Advertisement Perception and Generations: Comparison between X, Y, and Z Generations. İletişim Kuram ve Araştırma Dergisi, 2022(58), pp.38-56.

[18] Kolasinski, S.L., Neogi, T., Hochberg, M.C., Oatis, C., Guyatt, G., Block, J., Callahan, L., Copenhaver, C., Dodge, C., Felson, D. and Gellar, K., 2020. 2019 American College of Rheumatology/Arthritis Foundation guideline for the management of osteoarthritis of the hand, hip, and knee. Arthritis & Rheumatology, 72(2), pp.220-233.

[19] Kumatongo, B. and Muzata, K.K., 2021. Research paradigms and designs with their application in education. Journal of Lexicography and Terminology (Online ISSN 2664-0899. Print ISSN 2517-9306)., 5(1), pp.16-32.

[20] Kuttal, S.K., Bai, Y., Scott, E. and Sharma, R., 2020. Tug of Perspectives: Mobile App Users vs Developers. International Journal of Computer Science and Information Security (IJCSIS), 18(6).

[21] Lerner, A., 2021. Analyzing Holocaust archives through a quantitative lens. In The Routledge Handbook of Religion, Mass Atrocity, and Genocide (pp. 443-459). Routledge.

[22] Rogers, Y., Sharp, H. and Preece, J., 2023. Interaction design: beyond human-computer interaction. John Wiley & Sons.

[23] Sandhu, A.K. and Batth, R.S., 2021. Software reuse analytics using integrated random forest and gradient boosting machine learning algorithm. Software: Practice and Experience, 51(4), pp.735-747.

[24] Sharma, S., 2019. Data privacy and GDPR handbook. John Wiley & Sons.

[25] Stonehouse, G.H. and Konina, N.Y., 2020, February. Management challenges in the age of digital disruption. In 1st International Conference on Emerging Trends and Challenges in the Management Theory and Practice (ETCMTP 2019) (pp. 1-6). Atlantis Press.

[26] Weichbroth, P., 2020. Usability of mobile applications: a systematic literature study. IEEE Access, 8, pp.55563-55577.

[27] Yusoff, A.S.M., Peng, F.S., Abd Razak, F.Z. and Mustafa, W.A., 2020, April. Discriminant validity assessment of religious teacher acceptance: The use of HTMT criterion. In Journal of Physics: Conference Series (Vol. 1529, No. 4, p. 042045). IOP Publishing.

[28] Zewude, B. and Habtegiorgis, T., 2021. Willingness to take COVID-19 vaccine among people most at risk of exposure in Southern Ethiopia. Pragmatic and observational research, pp.37-47.