Author(s): Balogun, Oluwafemi Samson; Sunday, Adewale Olaleye

Title: Demystifying Mobile Banking App Security Through Gender, Education, Privacy, and Trust Intervention

Year: 2022

Version: final version

Please cite the original version:

Balogun, O. S., & Sunday Adewale Olaleye. (2022). Demystifying Mobile Banking App Security Through Gender, Education, Privacy, and Trust Intervention. International Journal of E-Adoption (IJEA), 14(1), 1-18.

DOI: 10.4018/IJEA.294859

URI: http://doi.org/10.4018/IJEA.294859

Demystifying Mobile Banking App Security Through Gender, Education, Privacy, and Trust Intervention

Oluwafemi Samson Balogun, University of Eastern Finland, Finland*
https://orcid.org/0000-0002-8870-9692

Sunday Adewale Olaleye, School of Business, JAMK University of Applied Sciences, Rajakatu, Finland

ABSTRACT

The escalation of mobile banking apps has decongested the banking hall, especially in developing countries, and the penetration of mobile banking apps is crucial for both financial institutions and customers. This study reviewed existing relevant literature from the Web of Science to position this study well and dwelled on a theoretical foundation for the exposition of the interrelation of trust and privacy as an antecedent of mobile banking app security. The quantitative method was employed on banking customers' data using SmartPLS 3.0 version with different data analysis techniques such as structural equation modelling, multigroup data analysis, interaction effects, and importance-performance analysis. This study results show the intervention of gender and education. It also indicates that the orientation and persuasion of banking customers to the point of higher trust is a determinant of security assurance of using mobile banking apps. This study discusses the theoretical and managerial impacts with the limitation of the study and projects into the future.

KEYWORDS

Data, Internet Surfing, Mobile Apps, Privacy, Risk, Security, Tablet, Trust

1. INTRODUCTION

The global digital transformation has renewed many business sectors, but the intervention of mobile banking app has paved the way for the convenience and comfort of mobile banking users during financial operations. The escalating mobile banking app has decongested the banking hall, especially in developing countries, and the penetration of mobile banking app is crucial for both financial institutions and customers. For the banks, the app is a means of intensive engagement with mobile banking app users on the go, and the ubiquitous of mobile banking app is significant for the users as they do inter-banking transfer, pay bills, manage debt, credit cards, and carry out other banking transactions with clicks.

Mobile devices such as smartphones, foldable phones, and tablets, as an antecedent of mobile banking apps, are increasing their capability, functionality, and accessibility. For instance, statistics

DOI: 10.4018/IJEA.294859

*Corresponding Author

show that globally, consumers downloaded 194 billion apps in 2018, spent $101 billion in app stores, and used an average of three hours per day on mobile devices (App Annie, 2019). This outstanding result which is rare in the earlier devices such as desktop and laptop, have a managerial implication in the banking sector as one of the arms that benefits from the solution that mobile banking app proffer to the users and the society at large by turning the traditional banking transaction to paperless transaction. To buttress the growth of mobile banking app, the findings of App Annie (2019) shows that time spent on app grew by 50 percent from 2016 to 2018 while the downloads increased by 35 percent over the same period.

With all the mentioned opportunities comes the risk of mobile banking app insecurity. These security risks could be the need for privacy assurance and trust. The security battle is ongoing because the existing virus is being solidified, and new ones are springing up. The security risk can emanate from the corrupt app, compromised authentication, lost or stolen devices. The banking consumer's response to security and privacy issues could also be fear of the unknown.

According to Kumar and Pandey (2017), understanding consumers' behavior is crucial for a strategic marketing plan. Eraslan, İç, and Yurdakul (2016) also emphasized customers' feelings, expectations, and usability of mobile devices in their study. The trusting issues began in the days of a trade by barter and when the banking customers stored their coins and bill in vaults and persists today.

Today, researchers have examined the security risks from different perspectives. For example, Olkiewicz, Terebecki, and Wolniak (2019) studied the security of information channels in banking services and recommended modern methods to guarantee information security to the stakeholders of a bank. Likewise, Olkiewicz et al. (2019) focussed on the banking stakeholders, and Sundaram, Thomas, and Agilandeeswari (2019) discussed the online security of banking customers that uses smartphones and computers and concluded that security of banking technology did not depend on electronic devices such as smartphone and computers.

Since mobile banking app is a global issue, Merhi et al. (2019) and Abdullaev et al. (2019) carried out a cross-cultural study of the intention and security challenge to use mobile banking in Asian and European countries, and the results of their study identified the influencer of the behavioral intention of mobile banking as perceived privacy, trust, habit, and perceived security. Along the same line, Chin, Harris, and Brookshire (2018) used a bidirectional approach of trust and risk to determine the factors that influence mobile app installation and discovered trust and security to have a significant positive relationship with the intention to install the mobile app while risk and privacy had weak and insignificant relationships.

Gender and education also play a crucial role in mobile banking app use. Alkhaldi (2019) proposed a model that determines the customer's use of mobile banking services and found that two items from the Technology Acceptance Model (TAM) performance expectancy, effort expectancy, and user awareness affect the users' intention to use mobile banking while gender did not make any significant impact. The study of Ojeniyi and Abdulhamid, 2019 confirmed the importance of awareness in mitigating the risk associated with banking customers' passwords in online banking transactions; Nwogu and Odoh (2015) also contribute to the existing literature by emphasizing the importance of user's education.

The existing literature reviewed shows a national gap for an empirical study with a theoretical framework. This study intends to answer the following research questions: (1) How do privacy assurance and trust perception affect mobile banking app security? (2) Why is Gender an essential variable for mobile banking app security? (3) How does education factor contribute to the success of mobile banking app security? Further, the study utilized quantitative methodology and analyzed the data with SmartPLS 3.0 through Structural Equation Modelling (SEM). The first section of the study introduced the mobile banking app. The second section explained in detail what others have done in a mobile banking app. Section three described the methodology employed. Section four showcases the study findings, and the final section discusses the theoretical contribution, managerial implications, study limitations, and future research. The results show that trust and privacy are the determinants of secured mobile banking apps and trust is a higher predictor than privacy in the Nigerian mobile banking context. Also, gender mediates between privacy, trust, and mobile banking app security and interact with privacy and security. This study finally discussed its limitation and proposed future studies.

2. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

2.1 Mobile Banking App Security Threats

Regarding the security threats that exist from the use of the internet, Sundaram, Thomas, and Agilandeeswari (2019) investigate how banks, through the use of the internet, are prone to security risks due to the devices the banking customers use. The study also examined the solutions provided and the factors related to security issues in electronic banking devices in the past six years. They suggested that smartphones and computers do not contribute to the bank's security issues, but rather the users, service providers, and the bank should be up to the task of tackling the issues. In mobile device security study, it is pertinent to understand the views of users on the app risk, and Cen, Kong, Jin, and Si (2015) used the opinion of the actual user to view the risk assessment of an app as a crowdsourcing problem and adopt the ranking model as an evaluation method. A co-training scheme was developed to amalgamate feature learning to rank model.

Is there anything else to consider when examining the challenges of mobile banking apps besides security? Merhi et al. (2019) used a conceptual framework by extending the Unified Theory of Acceptance and Use of Technology (UTAUT2) to investigate the critical factors that may impede or facilitate the adoption of mobile banking services in a cross-cultural context. The study incorporates trust, security, and privacy, and the results revealed that habit, perceived security, perceived privacy, and trust influenced the behavioral intention towards adopting mobile services for both Lebanon and British consumers. Performance Expectancy was also a significant predictor in their study.

Further, Srinivas, Das, and Kumar (2019) investigated the importance of various cyber defense standards and cybersecurity framework architecture in protecting various organizations' systems and information from cyber-attack in response to this security challenge. They also talked about using the national cybersecurity strategy and government policies to secure and protect cybersecurity. Hackers used Command-and-Control (C & C) servers as a type of mobile malware to gain root-level access and execute instructions from a remote server, posing a significant threat to Homeland security, according to Seo et al. (2014). The authors used DroidAnalyzer to identify potential vulnerabilities in Android apps.

According to Deypir and Horri (2018), antivirus programs on Android can detect malware based on their signature but cannot detect zero-day viruses. The authors developed a new metric for estimating the security risk of untrusted app based on distances to malicious and non-malicious app instances. Using the dataset demonstrates that the new metric has higher detection rates, and it is more effective than previous metrics based on risk score measurement.

2.2 Mobile Banking App Security Benefits

Due to the ubiquitous mobile phone, mobile banking apps have some advantages over conventional banking systems in security and control. Basar et al. (2019) opine that mobile device protection against an intruder is essential for the security and privacy of its users and recommends secure authentication as a viable solution, while Maček et al. (2019) proposed a secure modular authentication framework regarding iris biometrics. Whenever there is more than three times login attempt on a mobile banking app, it will automatically lock the app as a sign of intrusion. This security technique is a benefit of information security for mobile banking users. Also, mobile banking apps pave the way for real-time fraud monitoring and facilitate secure encryption for user information protection. Mobile banking apps benefit from authentication for proper identification of mobile banking users' passwords and devices. Additionally, the user's money protection is possible through firewalls.

2.3 Mobile Banking App Trust

In response to the question of whether behavior plays a significant role in social ties, Bapna, Qiu, and Rice (2016) stated that the researcher seeks a deeper understanding of the fundamental constructs of human behavior such as trust, forgiveness, and their linkage to social ties due to the increasing importance of the online social network. Using data from the Facebook API, the authors measured the social ties that connect the study's intention. The separated instrumental trust from static intrinsic trust revealed how the level of instrument trust and forgiveness and the effects of forgiveness on preventing future defections differed according to the strength of social ties. The findings show that trust in social repeated play is higher than trust level in anonymous play and that forgiveness is essential in facilitating cooperative equilibrium.

By conducting an explanatory study and customizing the Facebook application, Bapna, Gupta, Rice, and Sundararajan (2017) attempt to understand how social ties are linked to an economic measure of trust. They used an investment game to examine the relationship between observed trust and three "revealed preference" tie strength measures and identify latent heterogeneity among the subjects used. The study demonstrates that the traditional measure of dyadic trust, widely used in the physical world and social networks, may not always be an effective predictor of digital trust because not all online social ties are created equal.

Also, Benbasat, Gefen, and Pavlou (2010) extended the emerging trend and identified some ground-breaking perspectives on the study of trust by exploring novel aspects of trust in new and under-researched IS context. Probing the relationship between trust and satisfaction of customers, Fang et al. (2014) mentioned the initial online purchase context used to understand the effects of institutional e-commerce mechanisms of trust and online purchase traditionally. The authors extended the work done in literature by introducing an essential moderator Perceived Effectiveness of Institutional E-commerce Mechanism (PEEIMS), to the relationship between trust, satisfaction, and repurchase intention. The findings show that PEEIMS negatively moderates the relationships between trust in an online vendor and online customer repurchase intention while positively moderating the relationship between customer satisfaction and trust.

Still, Dimoka (2010) observes the location, timing, and level of brain activity that underpins trust and distrust, as well as their underlying dimensions, when it comes to trust. The author supplemented a psychometric measure of trust and distrust with a functional neuroimaging (fMRI) tool. The findings indicate that trust and distrust activate different brain areas and have different effects, which explains why trust and distrust have distinct constructs associated with different neurological processes.

Given that gender can serve as a basis for trust, Riedl, Hubert, and Kenning (2010) used functional magnetic resonance imaging to investigate why women and men differ in their trust decisions (fMRI). The results show that women's brain areas are more activated than men's, indicating that gender differences predict neural information processing modes. It also demonstrates the implications for information systems research and management.

Examining whether online shopping is dependent on online trust, Gefen, Karahanna, and Straub (2003) examined the factors that build online trust in an environment devoid of typical human interaction by integrating an actual e-vendor and its IT website interface, which is at the heart of online shopping. This investigation leads to confidence in understanding these constructs and their connections to behavior. The findings indicate that online trust is based on the belief that the vendor has nothing to gain by cheating and that a safety mechanism is built into the website, with a standard interface and an easy-to-use interface. This study hypothesized, based on the discussion of trust issues, that:

H1: There is a positive relationship between Trust and Security of Mobile Banking Apps.

2.4 Data Privacy for Mobile Banking App

Given the relationship between anonymity and profit maximization, is it possible for the firm to maintain anonymity while increasing profits? Contizer, Taylor, and Wagman (2012) responded to this question and used a model that can assist the firm in recognizing and pricing discrimination against its former customers while the consumers maintain their anonymity at some cost. They also demonstrated that firms can earn a high profit when consumers can maintain their anonymity for free and that consumers can be better off up to the point where maintaining their anonymity is costly.

What are the benefits of customers disclosing personal information? White (2004) attempts this question and investigates consumers' motivations for disclosing personal information to relationship-seeking marketers, the impact of consumers' perception of the relationship, the benefit offered to them by marketers in exchange for such information, and the type of information requested from consumers. According to the findings, consumers find privacy-related information for customized benefits offering appealing but embarrassing information unappealing.

Lowry, Cao, and Everard (2011) stated in the same vein that most users find it challenging to reveal personal information to others. To investigate and validate the relationships between Self-disclosure technology use and culture, the authors proposed a model based on social exchange theory. They also investigated the effects of culture on information concerning privacy and the desire for online interpersonal awareness, which can influence attitudes toward an actual use of self-disclosure technology. The results show that the cross-cultural dimension is essential for information with privacy concerns and the desire for online awareness, which also serve as factors for attitudes toward its usage and actual use of instant messaging.

Moreover, Anderson (2017) stated that organizations operate in a highly interconnected environment and are primarily faced with balancing the protection of information resources. The authors proposed an information security control theory to explain and manage this tension adequately. As a result, there is a conflict between the expected benefits and the security risks associated with the information sharing process in many domains, including business, healthcare, law enforcement, and the military. The study found that the theory provides a good framework for developing information security policies and reconciling the tension between information sharing and protection in various business domains.

Martin, Borah, and Palmatier (2017) used a conceptual framework based on gossip theory to link customer vulnerability to adverse performance effects. According to the study's findings, transparency and control in the firm's data management practices can mitigate the adverse effects of customer data vulnerability. Using real-life data demonstrates a consistent effect across some types of a customer's data vulnerability, confirming that violation and trust mediate the effects of data vulnerabilities on outcomes.

Many factors influence mobile banking customers, but can a data breach affect their loyalty? Janakiraman, Lim, and Rishika (2018) examine the effects of a multi-channel retailer's Data Breach Announcement (DBA) on customer behavior using a natural experiment and individual customer transaction data from the retailer to obtain a comprehensive and systematic empirical examination of the effects of DBA on customer spending and channel migration behavior. The author compared the treatment groups and control groups' changes in customer behavior (before and after DBA). Customers with higher retailer patronage forgive the most, according to the study, because the negative effect of the DBA is lower for customers with higher patronage. These privacy discussions emphasized how privacy can make or break a bank's excellent relationship with its customers. This study hypothesized, based on the privacy argument of transparency, that:

H2: There is a positive relationship between Privacy and Security.

2.5 Gender

Using age and gender differences to bridge the gap, Lian and Yen (2014) investigated older consumers' motivations and barriers to online shopping. To determine if younger consumers tend to shop online for performance expectations, or social influence, they investigated the online shopping habits of different age groups. It was also found that there were no gender differences regarding older adults' drivers and barriers.

To understand how online consumers make decisions about repurchase, Fang, Wen, George, and Prybutok (2016) look to investigate the impact of gender and age on perceived value. It was discovered that both age and gender affect the intention to return an item online; this relationship was moderated by how much-perceived value there was. A plausible inference is that trust propensity and gender influence perceived benefits and risks on user behavior, as shown by Chen, Yan, Fan, and Gordon (2015). Trust propensity and gender appear to have a significant effect on the strength of intentions to purchase.

Are there gender-based differences in the online shopping attitudes of consumers? Shuman (2010) applied gender differences in attitudes towards online shopping to identify the factors that influence online shopping behavior. The study revealed that females place a higher value on shopping online than males. The moderating effects of inconsistent product reviews on gender attitudes were studied by Zhand, Cheung, and Lee (2014), who examined the theory of reasoned action, trust, and information processing research as it applies to gender differences. Consumers exposed to inconsistent reviews exhibited a more significant influence on purchase intentions for females relative to males.

Social norms, perceived enjoyment, and relationships moderate the impact of gender on adopting the e-commerce system. In the female group, the influence of social norms was more substantial, and in the male group, enjoyment was more robust. Taipale, Kuoppamaki, and Wilska (2017) study the role of mobile technologies in online shopping and entertainment. The findings show that mobile-based online shopping works best with specific demographics such as age, higher education, and household type, while age and gender can predict what one may wish to purchase.

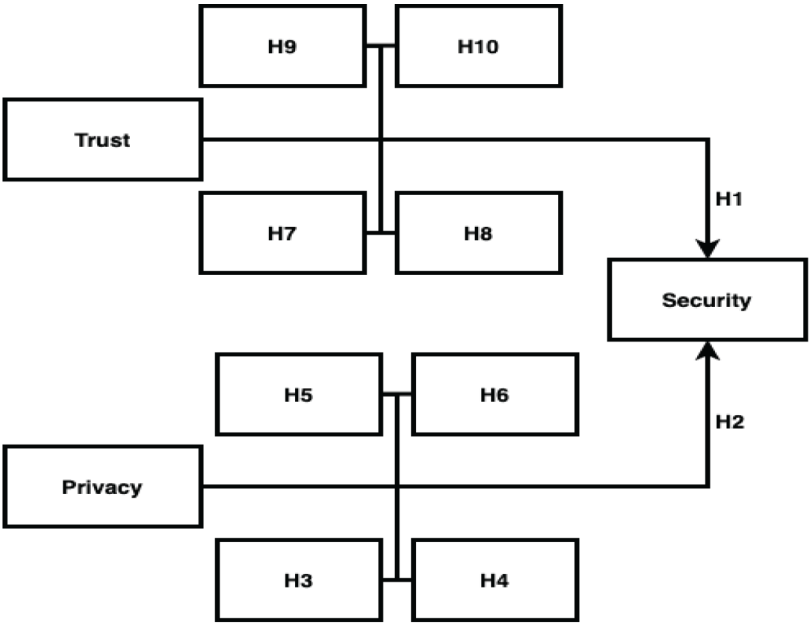
Davis, Smith, and Lang (2017) estimated the effects of people's perception of their online and offline gender behaviors on online shopping motivation and purchase intentions, which, in turn, affect the number of people who engage in online shopping. The results showed that the consumers' perception of their gendered behavior on online shopping motivation significantly impacted determining whether there was a significant effect on purchase intentions. This relationship is mediated by gender. In other words, females' online behaviors play a more significant role in their everyday lives than males'. Many scholars are actively engaged in a lively academic debate on whether gender is a critical control variable, and their findings show that gender does not affect the mediator or moderator variables in their studies. Their study demonstrated that males and females see privacy, trust, and security issues differently. Based on the synthesized literature, this study hypothesized that:

H3: Male perception on Privacy is positively related to Security of mobile banking apps.
H4: Female perception on Privacy is positively related to Security of mobile banking apps.
H7: Male perception on Trust is positively related to Security of mobile banking apps.
H8: Female perception on Trust is positively related to Security of mobile banking apps.

2.6 Education

Customer education is critical for quick response to security issues in online banking, especially when using a mobile banking app. For communication flow, customer enlightenment is directly related to education level. There is a lot of security information out there these days, and to keep customers from becoming confused, security, privacy, and trust orientation, and regular communication are crucial. Tschanz et al. (2013) discovered that the impact of stressful life events (SLE) on cognition varies by education and age, but education did not moderate the body mass index and mental disorders in

Figure 1. Mobile banking app security framework and hypotheses



the study of McCrea Berger and King (2012). Their study, however, established the age and gender differences.

The problem of customer ignorance is solved by relevant knowledge and exposure to the right information at the right time. According to Ukpabi, Karjaluoto, Olaleye, and Abass (2019), mobile banking service providers should plan for customer education attainment. In addition, Jo Bitner, Faranda, Hubbert, and Zeithaml (1997) present the role of customers in creating and ensuring quality and productivity in service experiences via managerial decision making and provide a guide to enable good research on customer participation in service.

Every market's primary goal is to meet the needs of its customers. As a result, Alt et al. (2018) identified customer orientation as a key for companies to be competitive in the market by implementing concepts such as personalization, one-to-one marketing, mass customization, and co-creation to meet the demands of customers' demands the offerings of companies.

Eisingerich and Bell (2006) presented a model based on education that examined the relationship between customer education, participation, and problem management in driving customer loyalty. According to their findings, customer education is the most powerful predictor of client loyalty.

It is critical to understand the factors influencing customer satisfaction. Hult, Sharma, Morgeson III, and Zhang (2019) demonstrate significant purchase-channel differences in the antecedents of customer satisfaction and their subsequent effects on customer loyalty using the American Customer Satisfaction Index (ASCI) model. They also discovered that some customer demographics and broader product categories influence the differences. The education argument emphasized its effectiveness in terms of privacy, trust, and security. As a result, the following hypothesis was proposed in this study:

H5: Less-educated perception on Privacy is positively related to Security of mobile banking apps.
H6: Well-educated perception on Privacy is positively related to Security of mobile banking apps.
H9: Less-educated perception on Trust is positively related to Security of mobile banking apps.
H10: Well-educated perception on Trust is positively related to Security of mobile banking apps.

3. METHODOLOGY

3.1 Study Sampling

This study used a convenience sampling method to reach the group of tablet users. In Nigeria, 244 questionnaires were distributed to banking customers who use tablets. Out of 244 questionnaires, 194 were returned, and five were removed during the data cleaning process with Microsoft Excel for missing and incomplete values.

This quantitative study employs various data analysis techniques, including structural equation modeling, multigroup data analysis, interaction effects, and importance-performance analysis. This study focuses on Nigerian banking customers who use the app for transactions. The survey was carried out in the Western part of Nigeria because there are more mobile commerce merchants and vendors there than in other geopolitical zones. The study employs a paper questionnaire rather than an online survey because of the erratic power supply and low Internet availability in Nigeria. The western part became an option due to the literacy of the zone's residents, which allows for accessible communication in English.

The data collected has a response rate of 79.5 percent. Among the questionnaires distributed, n=189 responses were related to the study's objectives: customers who use mobile banking apps on their tablets. The previous study taught us that each mobile channel is distinct (Olaleye, Sanusi, Mark, and Salo, 2019). The demographics of the responses there are 123 (65%) male and 66 (35%) female respondents, as well as 89 (47%) Less Educated and 100 (53%) respondents from the study (see table 6). This study used structural equation modeling with SmartPLS 3.0 to analyze the data from mobile banking apps. The current study validated SmartPLS's utility for Partial Least Square Structure Equation Modeling (Hair, Ringle, and Sarstedt, 2011).

3.2 Adapted Instrument

This study used questions from previous studies to achieve good reliability and validity results. The study adopts four items from Flavián and Guinalu's (2006) study on "consumer trust, perceived security, and privacy policy: three essential elements of web loyalty" for the latent variable of Trust. With four items, it also adapts Flavián and Guinalu's (2006) privacy and security questions. The study used two dependent variables: Trust and privacy, with security as the independent variable. Also, Gender and education are the moderating variables. All the items were loaded correctly in their respective constructs (Table 3). The total sample size for Gender was divided into two groups of male and female. Likewise, education was divided into two groups of less and well educated through the multigroup feature of SmartPLS (Table 1).

4. RESULT

The degree of reliability in this study's assessment methods remains constant and steady. The results from the reliability analysis can be trusted. In Cronbach Alpha and Composite Reliability, the

Table 1. Demography statistics

Items (*n*=189)	Freq.	%
Male	123	65
Female	66	35
Less Educated	89	47
Well Educated	100	53

Note: This table shows the demography statistics of mobile banking app security participants.

Table 2. Constructs and items used for the study

Trust	Flavián and Guinalíu (2006)
TR1	The company providing the banking mobile app would be trustworthy in handling my information.
TR2	The company providing the banking mobile app would tell the truth and fulfill promises related to the information provided by me.
TR3	I trust that the company providing the banking mobile app would keep my best interests in mind when dealing with my information.
TR4	The company providing the banking mobile app is in general predictable and consistent regarding the usage of my information.
Privacy	**Flavián and Guinalíu (2006)**
PR1	I think this banking mobile app shows concern for the privacy of its users.
PR2	I feel safe when I send personal information to this banking mobile app.
PR3	I think that this banking mobile app will not provide my personal information to other companies without my consent.
PR4	I think this banking mobile app abides by personal data protection laws.
Security	**Flavián and Guinalíu (2006)**
SE1	I think this banking mobile app has mechanisms to ensure the safe transmission of its user's information.
SE2	I think this banking mobile app shows great concern for the security of any transactions.
SE3	I think this banking mobile app has sufficient technical capacity to ensure that no other organization will supplant its identity on the internet.
SE4	When I send data to this banking mobile app, I am sure that they will not be intercepted by unauthorized third parties.

Table 3. Factors loadings of Constructs and their items measurement

	Privacy	Security	Trust
PR1	0.85		
PR2	0.90		
PR3	0.89		
PR4	0.88		
SE1		0.90	
SE2		0.93	
SE3		0.93	
SE4		0.92	
TR1			0.88
TR2			0.92
TR3			0.94
TR4			0.88

Note: This table illustrate the factors and their loadings. All the items loaded under their latent variables had conformed to the threshold of 0.5.

consistency of the items is demonstrated. The authors of Hair Jr, Sarstedt, Hopkins, and Kuppelwieser (2014) stated that composite reliability, which assumes varying indicator loadings within a population, is a better method for evaluating reflective outer models for internal model consistency reliability than Cronbach alpha, as it considers the number of items in a scale. Witjaksono and Saputra (2019) also discovered that accurate, valid test items are essential.

The threshold for every item loading is reached, which is 0.5 (see table 3). Conforming to the verdict of 0.7 is the reliability test of Cronbach's alpha, which explains the relationship between latent variables and manifest indicators (Hair, Ringle, and Sarstedt, 2011; Witjaksono and Saputra 2019). Additionally, the rho A shows that the latent variables are more significant than the threshold of 0.7 and the Average Variance Extracted for Privacy, Security, and Trust (see table 4). A positive correlation is demonstrated in the discriminant table when determining how trustworthiness relates to privacy, security, and security (see table 5).

There is a positive relationship between Trust and Security, that is, Trust -> Security with t = 3.798, the result is significant with p < 0.01 (see figure 3). For *f*, a moderate effect exists between trust and security with the threshold (0.15 - 0.35), while for *q*, a weak effect exists between Trust and Security with the threshold (0.02 - 0.15). There is a positive relationship between Privacy and Security, that is, Privacy -> Security with t = 3.014, the result is significant p < 0.01. For *f*, a weak effect exists between Privacy and Security with the threshold (0.02 - 0.15), and for *q*, a weak effect exists between Privacy and Security with the threshold (0.02 - 0.15). Regarding importance-performance analysis results of trust and privacy to security, the result shows that the perception of the respondents on privacy is more important (74%) than trust (72%), while trust performed better (0.51) than privacy (0.43), according to the respondents' perception. Overall, the dependent security variable was important (71%); see table 7 and figure 4.

4.1 Results of Hypotheses Testing

There is a positive relationship with the male perception of Privacy concerning Security, that is, Privacy*Male-> Security, t = 2.63; the result is significant with p < 0.01. There is a positive relationship with the female perception of Privacy to Security, that is, Privacy*female-> Security, t = 2.56, the result is significant with p < 0.01. There is a positive relationship with the male perception of Trust with Security, that is, Trust*Male-> Security, t = 2.56, the result is significant with p < 0.01. There is a positive relationship with the female perception on Trust to Security, that is, Trust*Female->

Table 4. Model quality metrics

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Privacy	0.90	0.90	0.93	0.77
Security	0.94	0.94	0.96	0.84
Trust	0.93	0.93	0.95	0.82

Note: The table shows the quality criteria of the latent variables. All their values reach the threshold of 0.5 and 0.7.

Table 5. Construct correlations

	Privacy	Security	Trust
Privacy	**0.877**		
Security	0.790	**0.918**	
Trust	0.864	0.803	**0.905**

Note: Bolded diagonal values represent the square root of Average Variance Extracted (AVE) and latent variable correlations

Figure 2. Result tested hypothesis of Mobile banking app (Note: This shows the result of the hypothesis of mobile banking apps theoretical framework)

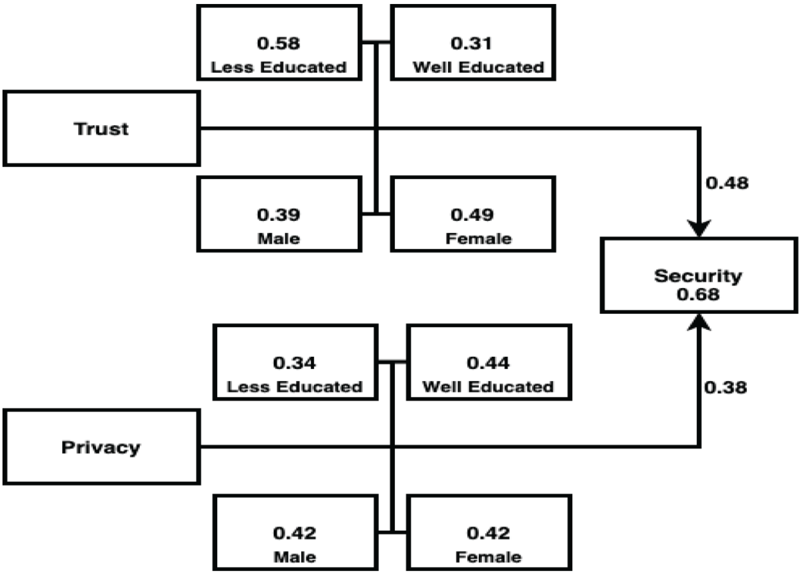


Table 6. Mobile banking app path coefficient and hypotheses results

Hypotheses	Path Coefficient	*f*	Q	STD Mean	STD	T Values	P Values	Status
H1	Trust -> Security	0.18	0.09	0.476	0.125	3.798	0.000	Yes
H2	Privacy -> Security	0.11	0.05	0.381	0.126	3.014	0.003	Yes

Note: Two-tailed significance levels (***p<0.001; **p<0.01)
f and Q Thresholds: 0.02 - 0.15 weak; 0.15 - 0.35 moderate effect; >0.35 strong effect

Table 7. Gender and education moderation analysis

Hypotheses	Path Coefficient	t-Values	p-Values	Status
H3	Privacy*Male-> Security	2.63	0.01	Accepted
H4	Privacy*Female-> Security	2.56	0.01	Accepted
H5	Privacy*Less Educated-> Security	3.86	0.00	Accepted
H6	Privacy*Well Educated-> Security	2.16	0.03	Accepted
H7	Trust*Male-> Security	2.56	0.01	Accepted
H8	Trust*Female-> Security	2.87	0.00	Accepted
H9	Trust*Less Educated-> Security	6.06	0.00	Accepted
H10	Trust*Well Educated -> Security	1.67	0.10	Not Accepted

Two-tailed significance levels (***p<0.001; **p<0.01; *p<0.05)
Note: this table shows the hypothesis decision

Security, t = 2.87, the result is significant with $p < 0.01$. There is a positive relationship with the Less Educated perception on Privacy about Security, that is, Privacy*Less Educated-> Security, t = 3.86, the result is significant with $p < 0.01$. There is a positive relationship with the Well-Educated perception on Privacy concerning Security, that is, Privacy*Well Educated-> Security, t = 2.16; the result is significant with $p < 0.01$. There is a positive relationship with the Less Educated perception on Trust to Security: Trust*Less Educated-> Security, t = 6.06; the result is significant with $p < 0.01$. There is a negative relationship with the Well-Educated perception on Trust with Security: Trust*Well Educated-> Security, t = 1.67; the result is not significant with $p > 0.10$, see table 8 and figure 1-2.

Gender does not moderate Security, that is, Gender -> Security, t = 0.676, the result is not significant with $p > 0.01$. Privacy moderates Security, that is, Privacy -> Security, t = 15.699, the result is significant with $p < 0.01$. Also, the Gender moderate Privacy and Security, that is, Privacy*Gender -> Security, t = 2.381, the result is significant with $p < 0.05$, see table 9.

5. DISCUSSION

Security has become an issue of consideration while using a mobile banking app. The consequence of unsecured mobile apps has become a racking pain for all banking stakeholders. This study developed a model to investigate the relationship between mobile banking app trust, privacy, and security. In a developing country context, trust and privacy as antecedents of security serve as independent variables

Table 8. Moderation result

Path Coefficient	STD. Mean	STDEV	T Statistics	P Values
Gender -> Security	-0.031	0.046	0.676	0.499
Privacy -> Security	0.752	0.048	15.699	0.000
Privacy*Gender -> Security	0.114	0.048	2.381	0.017

Two-tailed significance levels (***p<0.001; **p<0.01; *p<0.05)
Note: this table shows results from the moderation result

Figure 3. Interaction effects (Note: this shows the interaction effects between Men and Women on the perception of low and high privacy of mobile banking app security)

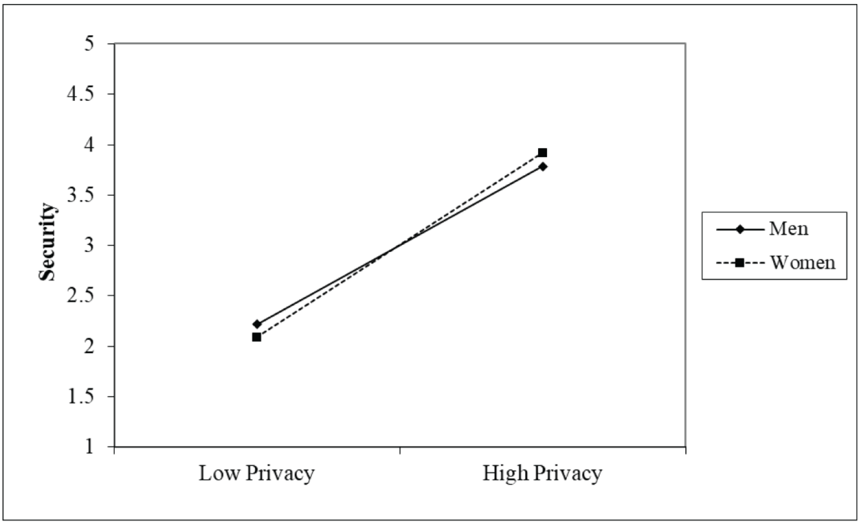
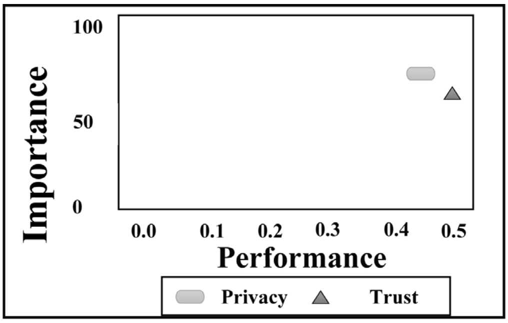


Figure 4. This figure shows the performance analysis (Note: this shows the importance and performance of Privacy and Trust of mobile banking app security)



that predict mobile banking apps' security (dependent variable). Aside from the direct relationship of trust, privacy, and security, the study also looked at the group relationship of gender, education, and the proposed framework of trust, privacy, and security, as well as gender interaction effects.

The combination of Privacy, Trust, and Security (PTS) in this study aligns with the study of Akram et al. (2017) as they suggest a user-centric ecosystem for devices through PTS as a present and future solution to emerging technologies challenges. This study showcases a simple direct relationship model of confidence factors: trust and privacy (Olaleye, Oyelere, Sanusi, and Agbo, 2018) and the security of mobile banking apps.

5.1 Theoretical Contribution

This study contributes to the security literature in four ways. First, the study contributes to the literature by showing the relationship of confidence factors of trust and privacy relationship with the security of mobile banking app, and all the path coefficients were significant. The trust variable is more pronounced than privacy in the context of the table banking app. Privacy and trust were used as independent variables and security as a dependent variable, unlike the study of Munyoka and Maharaj (2019), where they used PTS as independent variables that predicted perceived risk negatively. Second, the study contributes to the literature by showing the difference between the effect size of the trust-security relationship and the privacy-security relationship. The trust-security relationship has a moderate effect size, while privacy-security has a weak effect size. Third, the study shows the impact of categorical variables on continuous variables and their differences. The multigroup relationships were all significant except for mediation of well-educated between trust and security. Based on the original model, there is a slight difference between males and females regarding privacy relationship with security. Concerning trust and security, the difference is a little bit higher than the privacy and security relationship. There is a difference between the intervention of less educated and well educated irrespective of privacy and security. For trust and security, the reverse was that the less educated was significant while the well-educated was insignificant. This study offers an interesting insight as less educated mobile banking app users are more aware of threats due to their limited knowledge of mobile banking app. Lastly, the study contributes to the literature by showing the interaction effects of gender-based on privacy and security. There was a slight interaction effect between men and women, while women had high privacy concerns than men.

5.2 Managerial Contribution

This study provides three managerial implications for banking stakeholders. First, the study suggests that banking managers should pay close attention to gender divergence issues when formulating or reforming their privacy policy. This policy is necessary for building trust and privacy assurance for their customers. Two, it is assumed that well-educated banking mobile app users are well informed of the danger of being careless with their mobile banking app passwords and other banking credentials that are mandatory for transactions due to their high education profile. This study suggests that the banking managers should segment their customers into well-educated and less-educated customers so that they render services to the two proposed customer segments based on their needs. The banking managers should engage these segments with emotion-appealing videos via mobile banking apps on different social media platforms. Third, since the perception of mobile banking app users indicates high importance of privacy issues and high performance of trust element, this insight suggests to the banking managers to boost their privacy strategy on privacy by embarking on more online adverts that can lead to behavioral privacy change and to inculcate some trust elements into their app. Such profound statistics that explain their excellent services, financial penetration, and breakthroughs in terms of awards and social responsibilities will catch the banking customers' attention.

5.3 Summary and Conclusion

Technology is advancing, and mobile apps are gaining more visibility in different business sectors. The companies adopting mobile apps save space and time and could render satisfying business services to their customers. There is a need to allay the customers of the fear of mobile app insecurity to reach a height in the banking sector. Many customers are yet to have a foretaste of emerging technology, such as a mobile app. The growing insecurity of mobile app use has mandated the banking business to create a seamless mobile platform of secured mobile apps for banking transactions. This study results indicate that the orientation and persuasion of banking customers to the point of higher trust is a determinant of security assurance of using a mobile banking app. Also, the study shows that banking customers are sensitive to their privacy issues. There is a need for higher assurance of their privacy to be consistent in using a mobile banking app. To the best of our understanding, the study examines security issues on mobile banking apps in developing nations.

5.4 Limitation of the Study and the Proposed Future Study

Emerging technology security issues are not limited to a single country but are a global phenomenon; however, this study was limited to West Africa, specifically Nigeria. This future researcher should challenge this missing link and broaden the scope of mobile app security issues to include more African countries and possibly developed countries. Furthermore, the sample size is relatively small because the study focuses on the mobile banking app as a distinct mobile channel. However, future researchers should collect data across boundaries and use machine learning techniques to analyze large datasets from mobile banking apps to make necessary predictions about security issues. The future researcher can also use a mixed methodology to shed more light on the security issues with the mobile banking app. The banking stakeholders will be interested in examining different tablets with different operating systems as a channel for mobile apps.

REFERENCES

Abdullaev, A., Al-Absi, M. A., Al-Absi, A. A., Sain, M., Lee, Y. S., & Lee, H. J. (2019, February). Security Challenge and Issue of Mobile Banking in Republic of Uzbekistan: A State of Art Survey. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 249-255). IEEE. doi:10.23919/ICACT.2019.8701952

Akram, R. N., Chen, H. H., Lopez, J., Sauveron, D., & Yang, L. T. (2017). Security, privacy and trust of user-centric solutions. *Future Generation Computer Systems*, *80*, 417–420.

Alkhaldi, A. N. (2019). A Proposed Model for Determining the Customer's Use of Mobile Banking Services in Saudi Arabia: Toward the Differential Role of Gender. *International Journal of Business & Information*, *14*(1).

Alt, R., Ehmke, J. F., Haux, R., Henke, T., Mattfeld, D. C., Oberweis, A., Paech, B., & Winter, A. (2019). Towards customer-induced service orchestration-requirements for the next step of customer orientation. *Electronic Markets*, *29*(1), 79–91. doi:10.1007/s12525-019-00340-3

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems*, *34*(4), 1082–1112. doi:10.1080/07421222.2017.1394063

Annie, A. (2019). *App Annie Releases Annual State of Mobile 2019 Report.* https://www.appannie.com/en/about/press/releases/app-annie-releases-annual-state-of-mobile-2019-report/

Bapna, R., Gupta, A., Rice, S., & Sundararajan, A. (2017). Trust and the Strength of Ties in Online Social Networks: An Exploratory Field Experiment. *Management Information Systems Quarterly*, *41*(1), 115–130. doi:10.25300/MISQ/2017/41.1.06

Bapna, R., Qiu, L., & Rice, S. C. (2016). Repeated interactions vs. social ties: Quantifying the economic value of trust, forgiveness, and reputation using a field experiment. *Forthcoming*. *Management Information Systems Quarterly*, 14–07.

Basar, O. E., Alptekin, G., Volaka, H. C., Isbilen, M., & Incel, O. D. (2019). Resource Usage Analysis of a Mobile Banking Application using Sensor-and-Touchscreen-Based Continuous Authentication. *Procedia Computer Science*, *155*, 185–192. doi:10.1016/j.procs.2019.08.028

Benbasat, I., Gefen, D., & Pavlou, P. A. (2010). Introduction to the special issue on novel perspectives on trust in information systems. *Management Information Systems Quarterly*, *34*(2), 367–371. doi:10.2307/20721432

Cen, L., Kong, D., Jin, H., & Si, L. (2015, June). Mobile app security risk assessment: A crowdsourcing ranking approach from user comments. In *Proceedings of the 2015 SIAM International Conference on Data Mining* (pp. 658-666). Society for Industrial and Applied Mathematics. doi:10.1137/1.9781611974010.74

Chen, Y., Yan, X., Fan, W., & Gordon, M. (2015). The joint moderating role of trust propensity and gender on consumers' online shopping behavior. *Computers in Human Behavior*, *43*, 272–283. doi:10.1016/j.chb.2014.10.020

Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management*, *39*, 49–59. doi:10.1016/j.ijinfomgt.2017.11.010

Conitzer, V., Taylor, C. R., & Wagman, L. (2012). Hide and seek: Costly consumer privacy in a market with repeat purchases. *Marketing Science*, *31*(2), 277–292. doi:10.1287/mksc.1110.0691

Davis, R., Smith, S. D., & Lang, B. U. (2017). A comparison of online and offline gender and goal directed shopping online. *Journal of Retailing and Consumer Services*, *38*, 118–125. doi:10.1016/j.jretconser.2017.02.011

Deypir, M., & Horri, A. (2018). Instance based security risk value estimation for Android applications. *Journal of Information Security and Applications, 40*, 20-30.

Dhami, A., Agarwal, N., Chakraborty, T. K., Singh, B. P., & Minj, J. (2013, February). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 465-469). IEEE.

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *Management Information Systems Quarterly*, *34*(2), 373–396. doi:10.2307/20721433

Eisingerich, A. B., & Bell, S. J. (2006). Relationship marketing in the financial services industry: The importance of customer education, participation and problem management for customer loyalty. *Journal of Financial Services Marketing*, *10*(4), 86–97. doi:10.1057/palgrave.fsm.4760022

Eraslan, E., İç, Y. T., & Yurdakul, M. (2016). A new usability evaluation approach for touch screen mobile devices. *International Journal of Business and Systems Research*, *10*(2-4), 186–219. doi:10.1504/IJBSR.2016.075745

Fang, J., Wen, C., George, B., & Prybutok, V. R. (2016). Consumer heterogeneity, perceived value, and repurchase decision-making in online shopping: The role of gender, age, and shopping motives. *Journal of Electronic Commerce Research*, *17*(2), 116.

Fang, Y., Qureshi, I., Sun, H., McCole, P., Ramsey, E., & Lim, K. H. (2014). Trust, satisfaction, and online repurchase intention: The moderating role of perceived effectiveness of e-commerce institutional mechanisms. *Management Information Systems Quarterly*, *38*(2), 407–427. doi:10.25300/MISQ/2014/38.2.04

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy. *Industrial Management & Data Systems*, *106*(5), 601–620. doi:10.1108/02635570610666403

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *Management Information Systems Quarterly*, *27*(1), 51–90. doi:10.2307/30036519

Hair, J. F. Jr, Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–151. doi:10.2753/MTP1069-6679190202

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. doi:10.2753/MTP1069-6679190202

Hair, J. F. Jr, Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM). *European Business Review*.

Hasan, B. (2010). Exploring gender differences in online shopping attitude. *Computers in Human Behavior*, *26*(4), 597–601. doi:10.1016/j.chb.2009.12.012

Hult, G. T. M., Sharma, P. N., Morgeson, F. V. III, & Zhang, Y. (2019). Antecedents and Consequences of Customer Satisfaction: Do They Differ Across Online and Offline Purchases? *Journal of Retailing*, *95*(1), 10–23. doi:10.1016/j.jretai.2018.10.003

Hwang, Y. (2010). The moderating effects of gender on e-commerce systems adoption factors: An empirical investigation. *Computers in Human Behavior*, *26*(6), 1753–1760. doi:10.1016/j.chb.2010.07.002

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85–105. doi:10.1509/jm.16.0124

Jing, Y., Ahn, G. J., Zhao, Z., & Hu, H. (2014). Towards automated risk assessment and mitigation of mobile applications. *IEEE Transactions on Dependable and Secure Computing*, *12*(5), 571–584. doi:10.1109/TDSC.2014.2366457

Jo Bitner, M., Faranda, W. T., Hubbert, A. R., & Zeithaml, V. A. (1997). Customer contributions and roles in service delivery. *International Journal of Service Industry Management*, *8*(3), 193–205. doi:10.1108/09564239710185398

Kakkar, K., Shah, R., & Kakkar, M. (2013). *Risk analysis in mobile application development*. Academic Press.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369–400. doi:10.1080/07421222.2017.1334467

Kim, H., Cho, T., Ahn, G. J., & Yi, J. H. (2018). Risk assessment of mobile applications based on machine learned malware dataset. *Multimedia Tools and Applications*, *77*(4), 5027–5042. doi:10.1007/s11042-017-4756-0

Kumar, S., & Pandey, M. (2017). The impact of psychological pricing strategy on consumers' buying behaviour: A qualitative study. *International Journal of Business and Systems Research*, *11*(1-2), 101–117. doi:10.1504/IJBSR.2017.080843

Kuoppamäki, S. M., Taipale, S., & Wilska, T. A. (2017). The use of mobile technology for online shopping and entertainment among older adults in Finland. *Telematics and Informatics*, *34*(4), 110–117. doi:10.1016/j.tele.2017.01.005

Lian, J. W., & Yen, D. C. (2014). Online shopping drivers and barriers for older adults: Age and gender differences. *Computers in Human Behavior*, *37*, 133–143. doi:10.1016/j.chb.2014.04.028

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163–200. doi:10.2753/MIS0742-1222270406

Maček, N., Adamović, S., Milosavljević, M., Jovanović, M., Gnjatović, M., & Trenkić, B. (2019). Mobile Banking Authentication Based on Cryptographically Secured Iris Biometrics. *Acta Polytechnica Hungarica*, *16*(1).

Malleswari, D. N., Dhavalya, A., Sai, V. D., & Srikanth, K. (2018). *A Detailed Study On Risk Assessment Of Mobile App Permissions*. Academic Press.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58. doi:10.1509/jm.15.0497

McCrea, R. L., Berger, Y. G., & King, M. B. (2012). Body mass index and common mental disorders: Exploring the shape of the association and its moderation by age, gender and education. *International Journal of Obesity*, *36*(3), 414–421. doi:10.1038/ijo.2011.65 PMID:21427699

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, *59*, 101151. doi:10.1016/j.techsoc.2019.101151

Mohd Thas Thaker, M. A. B., Allah Pitchay, A. B., Mohd Thas Thaker, H. B., & Amin, M. F. B. (2019). Factors influencing consumers' adoption of Islamic mobile banking services in Malaysia: An approach of partial least squares (PLS). *Journal of Islamic Marketing*, *10*(4), 1037–1056. doi:10.1108/JIMA-04-2018-0065

Munyoka, W., & Maharaj, M. S. (2019). Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. *South African Journal of Information Management*, *21*(1), 1–9. doi:10.4102/sajim.v21i1.983

Nwogu, E., & Odoh, M. (2015). Security issues analysis on online banking implementations in Nigeria. *International Journal of Computer Science and Telecommunications*, *6*(1), 20–27.

Ojeniyi, J. A., & Abdulhamid, S. M. (2019). Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study. *International Journal of Education and Management Engineering*, *9*(2), 1. doi:10.5815/ijeme.2019.02.01

Olaleye, S. A., Oyelere, S. S., Sanusi, I. T., & Agbo, F. J. (2018). Experience of Ubiquitous Computing Technology Driven Mobile Commerce in Africa: Impact of Usability, Privacy, Trust, and Reputation Concern. *International Journal of Interactive Mobile Technologies*, *12*(3), 4–20. doi:10.3991/ijim.v12i3.7905

Olaleye, S. A., Sanusi, I. T., Mark, F. S., & Salo, J. (2019). Customers' loyalty to tablet commerce in Nigeria. *African Journal of Science, Technology, Innovation and Development*, 1–13.

Olkiewicz, M., Terebecki, M., & Wolniak, R. (2019). The Security of Information Channels in Banking Services. *System Safety: Human-Technical Facility-Environment*, *1*(1), 112–119. doi:10.2478/czoto-2019-0014

Riedl, R., Hubert, M., & Kenning, P. (2010). Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of eBay offers. *Management Information Systems Quarterly*, *34*(2), 397–428. doi:10.2307/20721434

Seo, S.-H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. *Journal of Network and Computer Applications*, *38*, 43–53. doi:10.1016/j.jnca.2013.05.008

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. doi:10.1016/j.future.2018.09.063

Sundaram, N., Thomas, C., & Agilandeeswari, L. (2019). A Review: Customers Online Security on Usage of Banking Technologies in Smartphones and Computers. *Pertanika Journal of Science & Technology*, *27*(1).

Tschanz, J. T., Pfister, R., Wanzek, J., Corcoran, C., Smith, K., Tschanz, B. T., & Norton, M. C. (2013). Stressful life events and cognitive decline in late life: Moderation by education and age. The Cache County Study. *International Journal of Geriatric Psychiatry*, *28*(8), 821–830. doi:10.1002/gps.3888 PMID:23037866

Ukpabi, D., Karjaluoto, H., Olaleye, S. A., & Abass, S. M. (2019). *Factors influencing mobile banking continuous use in Sub-Sahara Africa: A study of mobile banking users in Nigeria*. Routledge Studies in Marketing.

White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology*, *14*(1-2), 41–51. doi:10.1207/s15327663jcp1401&2_6

Witjaksono, R. W., & Saputra, M. (2019, November). Reliability and usability analysis of the implementation ERP in host to host payment system: A case study. *Journal of Physics: Conference Series*, *1367*(1), 012003. doi:10.1088/1742-6596/1367/1/012003

Zhang, K. Z., Cheung, C. M., & Lee, M. K. (2014). Examining the moderating effect of inconsistent reviews and its gender differences on consumers' online shopping decision. *International Journal of Information Management*, *34*(2), 89–98. doi:10.1016/j.ijinfomgt.2013.12.001

Oluwafemi Samson Balogun is a Lecturer at the Department of Statistics and Operations Research, Modibbo Adama University of Technology, Yola, Adamawa State, Nigeria, and he is currently a Post-Doctoral Researcher at the School of Computing, University of Eastern Finland. He holds a Ph.D. in Statistics from the Department of Statistics, University of Ilorin, Kwara State, Nigeria. He is a Senior Research Fellow at Centre for Multidisciplinary Research and Innovation (CEMRI) and He is a member of International Biometric Society (IBS), International Statistical Institute (ISI), Nigerian Statistical Association (NSA), Nigerian Mathematical Society (NMS). He has several conference and journal papers in reputable international bodies, and he is also served as guest reviewers for several journals. His research interest is data science, machine learning, Data Mining, biostatistics, categorical data analysis, modeling, and probability distribution models.

Sunday Adewale Olaleye got his Doctor of Science (D.Sc) in Economics and Business Administration from the University of Oulu, Oulu Business School (AACSB), Finland. He received his Masters of Science in Information Systems from Abo Akademi University, Turku, Finland, MBA from the Lapland University of Applied Sciences, Tornio, Finland, NMS iICT Certificate, Innovation and Entrepreneurship from the Nordic Master School of Innovative ICT, Turku Centre for Computer Science (TUCS), Turku, Finland and Certificate of Leadership and Management in Health from the University of Washington, USA. He is currently doing his post-doctoral research at the University of Oulu, Finland, and he is a visiting Professor at Universidad de las Américas Puebla (UDLAP), Mexico. He has presented papers at conferences and published in academic journals. His research interests are emerging mobile technologies, e-Health, mobile commerce, circular economy, and mobile apps.