“Security perception of e-banking users in India: an analytical hierarchy process”

AUTHORS	Mahesh Kumar https://orcid.org/0000-0003-4017-4892 Sanjay Gupta https://orcid.org/0000-0002-6590-5025

ARTICLE INFO	Mahesh Kumar and Sanjay Gupta (2020). Security perception of e-banking users in India: an analytical hierarchy process. *Banks and Bank Systems*, *15*(1), 11-20. doi:10.21511/bbs.15(1).2020.02
DOI	http://dx.doi.org/10.21511/bbs.15(1).2020.02
RELEASED ON	Thursday, 13 February 2020
RECEIVED ON	Thursday, 01 August 2019
ACCEPTED ON	Monday, 09 December 2019

LICENSE	This work is licensed under a Creative Commons Attribution 4.0 International License

JOURNAL	"Banks and Bank Systems"
ISSN PRINT	1816-7403
ISSN ONLINE	1991-7074
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
42	2	11

© The author(s) 2026. This publication is an open access article.

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Mahesh Kumar (India), **Sanjay Gupta** (India)

SECURITY PERCEPTION OF E-BANKING USERS IN INDIA: AN ANALYTICAL HIERARCHY PROCESS

Abstract

When choosing online financial transactions, security is a paramount concern of users. Three categories of banks in India, namely public, private and foreign banks, have a completely different focus on technology and capabilities. The study aims at investigating e-banking users' perception with regard to online risk for public, private and foreign banks. Online risk perception for the abovementioned banks was assessed on three major risk parameters, i.e. security aspect, privacy aspect, and trust; using a multiple-criteria decision-making tool, called the Analytical Hierarchy Process (AHP). The outcomes indicate that security risk is paramount among various aspects of perceived risk, followed by privacy and trust concern. Moreover, public sector banks are perceived to be the safest in this aspect. Public sector banks are also considered to be benign in terms of privacy and trust. Given the general user's perception of risk generated by all the three risk parameters taken together, public sector banks are perceived to be the most secure, followed by private and foreign banks. The findings of this study have various implications for both research and practice. Private and foreign banks in India may adopt appropriate marketing strategies to achieve a favorable perception. Various studies have been conducted earlier on these factors and their interrelationship, but limited research has been carried out to demonstrate the importance of each of these factors in relation to the other as perceived by the user. Moreover, the study quantifies factors in order of their importance.

Keywords Analytical Hierarchy Process (AHP), security risk, privacy risk, trust, e-banking

JEL Classification G21, G29, L81

Received on: 1st of August, 2019
Accepted on: 9th of December, 2019

© Mahesh Kumar, Sanjay Gupta, 2020

Mahesh Kumar, MBA, Assistant Professor, Sri Aurobindo College of Commerce and Management, Commerce and Management Department, Panjab University, India.

Sanjay Gupta, M.Com, MBA, CMA (Inter), Assistant Professor, Sri Aurobindo College of Commerce and Management, Commerce and Management Department, Panjab University, India.

This is an Open Access article, distributed under the terms of the Creative Commons Attribution 4.0 International license, which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

There are many types of banks in India, namely public sector banks (most of which are owned by government), private sector banks (owned or controlled by domestic private entities), and foreign entities owned by foreign banks. However, there are still many regional banks and co-operative banks, but public, private, and foreign banks dominate the sector. When it comes to the share of advances and deposits in the country, public sector banks lead with 71.8% in deposits and 68.1% in advances at the end of fiscal 2017. Over the years, public sector banks have been losing share of its private sector counterparts, while foreign banks have marginally lost their share on a smaller basis of about 5% of advances, in the last decade to the end of March 2017. This all is happening at a time when the banking sector is undergoing a transformation phase as a result of the digital era, and the country's central bank is catching most of the public sector banks that are napping on ballooning non-performing assets (NPAs).

The Government of India, led by Prime Minister Narendra Modi, is trying to transform India into a digitally empowered society, and a faceless, paperless, cashless, and knowledge driven economy. Numerous

initiatives have been taken by the government, such as Digital India, free to air channel DigiShala, the cashlessindia.gov.in website, creating a new UPI (Unified Payment Interface) digital payment system, and an app BHIM thereon. Demonetization, an initiative to curb black economy, gave a surge to cashless economy and gave confidence to the government to set a mission of 2.5 billion cashless transactions for 2017–2018.

With the spate of government initiatives for the cashless economy, concerns about security also raise. "In India, from 2011 to 2014, there has been a surge of approximately 300 per cent in cybercrime cases registered under the IT Act, 2000," said the Assocham-PwC joint study. A recent Assocham-PwC study reported an increase in Cyber security incidents in 2016 compared to 2014 and 2015. The above figures are disquieting at a time when India is undergoing its digital transformation. Online security becomes the most critical factor when users make transactions involving money online. Various factors influence the adoption of internet banking services, such as perceived ease of use, attitudes, subjective norms, perceived usefulness, security and trust, and awareness of online banking services (Juwaheer, Pudaruth, & Ramdin, 2012).

1. LITERATURE REVIEW

In literature, various factors have been identified that affect consumer perception of risk and security when transacting online. Laforet and Li (2005) have studied users' attitudes with regard to mobile and internet banking in China. Perception of risk, lack of skills, and the culture of cash-carry banking were identified as barriers to online banking. Furthermore, lack of awareness of mobile banking benefits was found to be a deterrent for its adoption. Previous positive banking experience, level of education, and reference group's sway did not affect the acceptance of mobile and online banking in China. Miyazaki and Fernandez (2001) find that perceived risk mediates the impact of the Internet experience on the online purchase behavior. Consumers' perceptions of privacy protection and security protection are regarded as antecedents and having strong influences on trust and risk. Thus, privacy and security technologies provided by the bank for Internet banking are the most important concerns for internet banking. Perceived security and privacy, usefulness, and perceived ease of use significantly affect intention to use internet banking (Lallmahamood, 2007). The impact of perceived security on trust is more significant in comparison to reputation and financial liability in online e-commerce transactions (Chellappa & Pavlou, 2000).

Stone, Gueutal, Gardner, and McClure (1983) conceptualize Information privacy as "the ability of the individual to personally control information about one's self." Smith, Milberg, and Burke (1996) in their study of privacy consider individual's concerns about organizational information privacy practices. Besides, a four-dimension scale was developed to measure this concern: the collection of an extensive proportion of personal information and its illegitimate secondary use – inside or outside the organization, errors – deliberate or accidental, in personal information, and improper access to personal information by outsiders. Based on the communication privacy management (CPM) theory, Petronio (2002), Xu, Teo, Tan, and Agarwal (2012) propose that the privacy concerns of mobile users are based on three dimensions, namely, perceived surveillance of personal information and activities, perceived intrusion, which means that information recipients are able to make independent decisions about users' information, and the secondary use of personal information. Privacy concerns may have an impact on online trust. It may depend upon consumers' attributes like gender, age, education, and their extraversion (Riquelme & Román, 2014). A privacy concern is recognized as a major threat to development of e-commerce and the digital economy (Malhotra, Kim, & Agarwal, 2004).

In addition to the privacy concern, consumer information security has been identified as one of the impediments in the e-commerce development (Gray, 1999). Although security issues are closely related to privacy concerns, this is a distinct construct (Vijayasarathy, 2004; Belanger, Hiller, & Smith, 2002). Román and Cuestas (2008) consider

http://dx.doi.org/10.21511/bbs.15(1).2020.02

security as uncertainty of incurring financial losses while interacting with a website. For instance, this may result from the online credit card fraud (Miyazaki & Fernandez, 2000). As per Román (2007), perceived security means perceptions of consumers about the online transaction security, particularly with regard to safety of the payment options. In addition, it refers to safeguard of financial information from unauthorized access. Privacy concerns focus on the unauthorized use of personal information, while security concerns correspond to the safeguard of shared information. According to Chellappa (2008), security means the concerns about the guarding of private information with three specific objectives: integrity, authentication and confidentiality. Integrity refers to the intactness of the information, i.e. it is not altered or changed during the transmission or storage. Authentication ensures validation of a user's identity and eligibility to information access; and confidentiality means that only authorized users are able to access the information for the authorized purpose. Ackerman (2004) suggests that "security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimize the risk of disclosure, or to reassure users".

Mayer, Davis, and Schoorman (1995) suggested an inclusive definition of trust as "the willingness of a trustor party to be vulnerable to the actions of trustee party based on the expectation that the trustee party will perform a particular action important to the trustor party, irrespective of the ability to monitor or control the trustee party." Many researchers from information technology systems have investigated trust in the online context (Gefen, Karahanna, & Straub, 2003; McKnight, Choudhury, & Kacmar, 2002). Trust is found to be an important factor in electronic transaction decision-making (Kim, Ferrin, & Rao, 2008). In online banking, customers are the trustor party, while banks whose online portals are being used are trustee parties. Customers are susceptible to harm since they provide sensitive information, such as debit and credit card information, unique identification numbers, contact number, email ids, when undertaking online transactions. According to Bhattacherjee (2002), trust is a psychological state, and, therefore, is disparate from behavior; rather it is a precursor to the behavior. The author conceptualizes trust as beliefs, having three facets, such as integrity, ability, and benevolence. Integrity refers to the consumers' perception towards online company's commitment to the terms of the online transaction. Ability corresponds to consumer perception towards competencies and knowledge of the online company to handle their transaction faultlessly. Benevolence is the perceived confidence of a consumer in a business that they will not exploit vulnerabilities in an online transaction and will always act for their well-being. In addition, it has a strong negative effect on consumer's risk perception (Kim, Ferrin, & Rao, 2008). Nilsson, Adams, and Herd (2005) concluded that authentication mechanisms, location, and situational awareness have a significant impact on the perceived trust of users in online banking. Online companies can establish trust if they affirm to an online consumer that transactions will take place as anticipated by them (Culnan & Armstrong, 1999). Chellappa and Pavlou (2001) argue that trust is positively influenced by an increase in perception of security and privacy in e-commerce transactions. Gurung and Raja (2016) have also suggested that security concerns, privacy concerns, and trust beliefs have an influence on risk perception. Their study concluded that trust had the highest influence followed by privacy concern, and security concerns.

The review of literature suggested that the perception of consumers towards information security risk is dependent upon three major factors, such as privacy, trust and security (Figure 1). When a consumer carries out online transactions with public, private and foreign banks, his perception on overall information security towards a type of a bank is driven by his assessment based on these three factors. The interrelationship is presented in Figure 1.

2. RESEARCH METHODOLOGY

We often face problems when choosing or prioritizing competing goals. There are various approaches in published texts, but MCDM is considered as one of the most effective and powerful techniques to deal with such ambiguous and unorganized problems with multiple conflicting objectives (Lee & Eom, 1990). Besides, in MCDM,

many approaches are available, such as AHP, fuzzy AHP, TOPSIS, fuzzy TOPSIS, Data Envelopment Analysis (DEA), etc. In all these approaches, all the competing alternatives are compared and decision makers (DMs) give precise ratings based on the preferences or weights to each alternative in comparison to the other competing alternative. In this research, the Analytical Hierarchy Process (AHP) is preferable to others as it is more suited to solving problems with a limited number of alternatives to choose from. Moreover, Sabaei, Erkoyuncu, and Roy (2015) have studied many publications in maintenance management, in the Scopus database, that have used MCDM methods. As a result, it was concluded that AHP is one of the most widely used MCDM methods in research. The analytical hierarchy process, initiated by Saaty (1980), is one of the techniques used to solve complex MCDM problems. The AHP method is often used in analyzing complex problems involving various selection criteria. The AHP analysis is performed in three elementary steps as follows:

1) Arrangement of the evaluation criteria in a hierarchical structure.

2) Evaluation of interest among criteria.

3) Selection of the judgment and the synthesis of interests (Gupta et al., 2018).

AHP has been used extensively in making a range of decisions, such as product screening (Calantone, Di Benedetto, & Schmidt, 1999), plant layout (Abdul-Hamid, 1999; Dweiri & Meirer, 1996), and quality function deployment (Bergquist & Abesysekera, 1996). The AHP contains techniques and ideologies used to prioritize among the criteria and sub-criteria, subsequently for alternative results. It is important to note here that the resulting figures are ratio scale estimates and resemble to numbers (Table 1).

Table 1. Saaty's scale (1-9) for pairwise comparison

Source: Gupta et al. (2018).

Relative significance	Significance intensity
Criteria *i* and *j* are of equal significance	1
Criterion *i* is moderately more significant than *j*	3
Criterion *i* is much more significant than *j*	5
Criterion *i* is very much more significant than *j*	7
Criterion *i* is absolutely more significant than *j*	9
Intermediate values between the two adjacent judgments	2, 4, 6, 8
If criterion *i* has one of the above non-zero numbers allotted to it when compared to criterion *j*, then *j* has the reciprocal value when compared to *i*	Reciprocals of above non-zero numbers

The steps taken in the AHP to arrive at the relative significance of various criteria are as follows:

Step 1: After reviewing the literature, identify an important evaluation criterion, based on which the e-banking user forms the overall perception of security towards particular type of banks.

Source: Authors' development

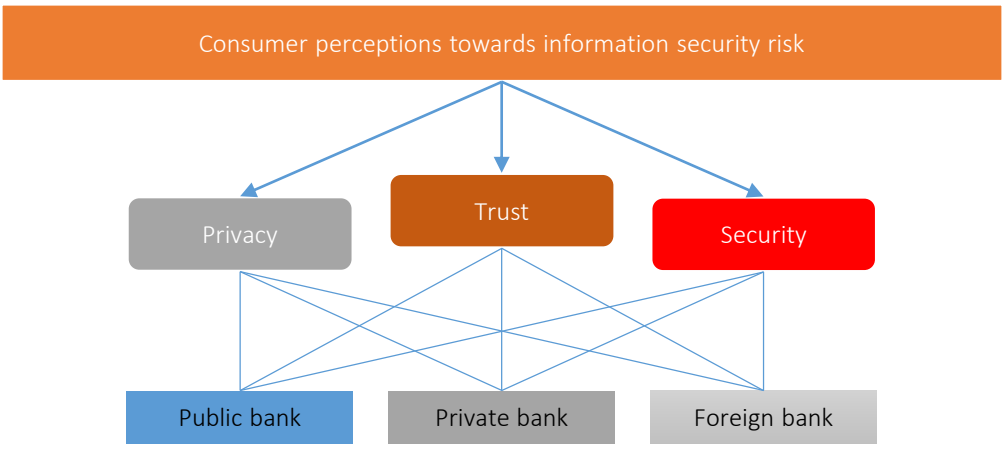

Figure 1. Consumer perceptions towards information security risk for public, private and foreign banks

http://dx.doi.org/10.21511/bbs.15(1).2020.02

Step 2: Data were collected from assessors in the pairwise judgment matrix of substitutes at the qualitative scale defined in the Saaty scale (see Table 1).

Step 3: The average of all the answers given by respondents in the pair-wise comparison matrix (Table 2) was organized into a square matrix.

Step 4: The priority vector (Weight) and the principal eigenvalue (λ) of an evaluation criterion were computed (Table 7).

Step 5: The consistency of judgement of the decision maker was calculated using the principal eigenvalue (λmax) to calculate CI. The consistency index can be calculated using the following formula:

$$CI = \frac{\max - n}{n-1},$$

$$\lambda \max = \sum_{i=1/n}^{n} \left(Principal\ Eigenvalue\right) i,$$

$$i = 1, 2, \ldots\ldots\ldots, n,$$

where λ max is the average of all the principal eigenvalues (λ) of criteria, and *n* is the number of criteria being compared.

CR is calculated using the following formula:

$$CR = \frac{CI}{RI} < 0.10.$$

The value of the random index (*RI*) depends on n. *RI* was taken from the table of the random consistency index, given by a number of experts. A sample of random consistency index is presented in Table 2.

Table 2. Random inconsistency indices for *n* = 10 (Saaty, 1980)

n	1	2	3	4	5	6	7	8	9	10
RCI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

A pairwise judgment matrix is reliable if the consistency ratio is less than 10%. According to Singh et al. (2018), if the significance of the consistency ratio is greater than 10%, the researcher should recalculate the pairwise judgments due to inconsistencies.

Table 3. Pairwise comparison matrix of various aspects of security risk

Indicators	Privacy concern	Security concern	Trust concern
Privacy concern	1.00	0.92	3.73
Security concern	1.09	1.00	7.30
Trust concern	0.27	0.14	1.00
Total	2.35	2.06	12.03

Table 4. Pairwise comparison matrix of various aspects of privacy

Privacy concern	Public bank	Private bank	Foreign bank
Public bank	1.00	2.42	4.40
Private bank	0.41	1.00	4.58
Foreign bank	0.23	0.22	1.00
Total	1.64	3.64	9.98

Table 5. Pairwise comparison matrix of various aspects of security

Security concern	Public bank	Private bank	Foreign bank
Public bank	1.00	2.33	3.31
Private bank	0.43	1.00	3.40
Foreign bank	0.30	0.29	1.00
Total	1.73	3.63	7.71

Table 6. Pairwise comparison matrix of various aspects of trust

Trust concern	Public bank	Private bank	Foreign bank
Public bank	1.00	4.92	6.12
Private bank	0.20	1.00	3.28
Foreign bank	0.16	0.30	1.00
Total	1.37	3.63	7.71

After applying Step 2, the average of all the reactions/responses given by the decision/judgement makers was organized into a Pairwise Comparison Matrix (Tables 4, 5 and 6). After that, the values in each cell of the above matrix was divided by the sum of the respective columns to yield its normalized weighted score. The normalized weighted score so imitative was then put in the Normalization Matrix, i.e. Tables 7, 8, 9, and 10.

Table 7. Normalized weighted scores of various aspects of security risk

Indicators	Privacy concern	Security concern	Trust concern	Priority vector (weight)	Principal eigenvalue (λ)
Privacy concern	0.42	0.45	0.31	39%	3.04
Security concern	0.46	0.49	0.61	52%	3.06
Trust concern	0.11	0.07	0.08	9%	3.01
λ_{max} = 3.04, *CI* = 0.019, *RI* = 0.58, *CR* = 0.03					

Table 8. Normalized weighted scores of various aspects of privacy

Privacy concern	Public bank	Private bank	Foreign bank	Priority vector (weight)	Principal eigenvalue (λ)
Public bank	0.61	0.67	0.44	57%	3.16
Private bank	0.25	0.27	0.46	33%	3.11
Foreign bank	0.14	0.06	0.10	10%	3.03
λ_{max} = 3.10, *CI* = 0.048, *RI* = 0.58, *CR* = 0.08					

Table 9. Normalized weighted scores of various aspects of security

Security concern	Public bank	Private bank	Foreign bank	Priority vector (weight)	Principal eigenvalue (λ)
Public bank	0.58	0.64	0.43	55%	3.14
Private bank	0.25	0.28	0.44	32%	3.09
Foreign bank	0.17	0.08	0.13	13%	3.03
λ_{max} = 3.09, *CI* = 0.043, *RI* = 0.58, *CR* = 0.07					

Table 10. Normalized weighted scores of various aspects of trust

Trust concern	Public bank	Private bank	Foreign bank	Priority vector (weight)	Principal eigenvalue (λ)
Public bank	0.73	0.79	0.59	70%	3.22
Private bank	0.15	0.16	0.32	21%	3.08
Foreign bank	0.12	0.05	0.10	9%	3.02
λ_{max} = 3.11, *CI* = 0.054, *RI* = 0.58, *CR* = 0.09					

Source: Authors' calculation.

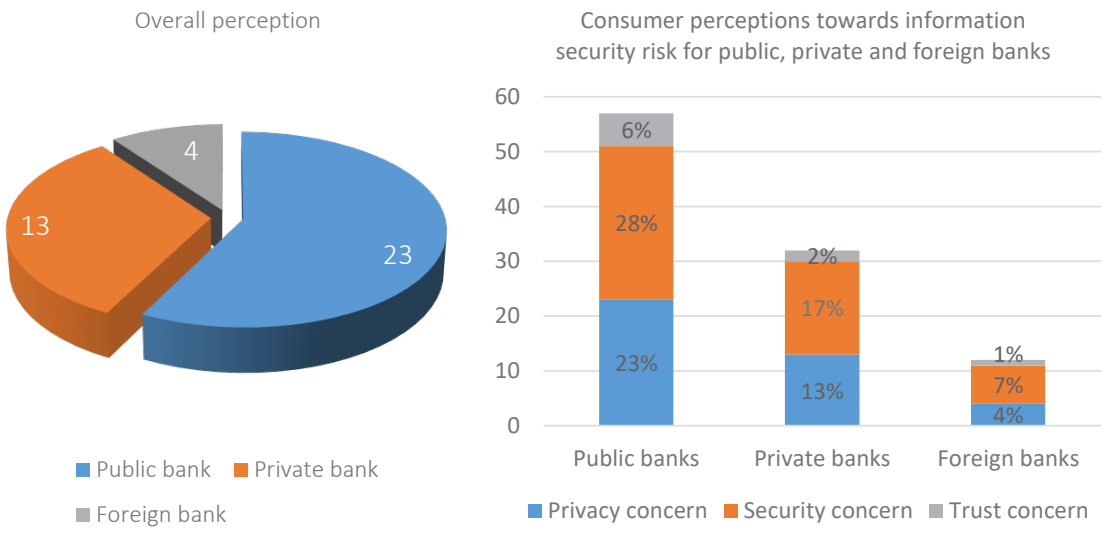

Figure 2. Weighted scores of consumer perceptions towards information security risk for public, private and foreign banks

http://dx.doi.org/10.21511/bbs.15(1).2020.02

3. RESULTS AND ANALYSIS

E-banking user perceptions of risk while transacting online with public, private and foreign banks are measured using a multiple-criteria decision-making technique, namely the Analytical Hierarchy Process (AHP). The sample of carefully selected 25 respondents was taken for the study. Users, who frequently used e-banking, had a good understanding of it, and had several bank accounts, were selected to participate in the study sample. The details of the research, such as objectives, selected factors affecting risk perception, and factors pairwise comparison scale, were explained to users before responding. To avoid any inconsistency, respondents were also provided with an opportunity to interpret and understand each of the factors (security, privacy and trust) in accordance with their intended connotation, and in the similar manner.

Three factors, security, privacy, and trust were identified to significantly influence the formation of a user's perception of online risk after reviewing the literature. In the first stage, respondents were asked to make pairwise comparison of each of the factors and assign weights according to their subjective preference of a factor over the other on a scale of 1 to 9 (Table 1). From three such comparisons – Security vs Privacy, Security vs Trust, and Privacy vs Trust – the importance of each factor relative to the other is quantified by calculating a weighted score of each factor (Table 7). Among the three factors, security risk was considered as the most important factor, getting a priority vector weight of 52% followed by privacy and trust, with 39% and 9%, respectively. It means, users are more concerned about the security parameter for the transaction and least concerned for trust.

While undertaking the e-banking transactions, users are perceived to have more concern among the three given parameters in the following order.

Security concern (52%) > Privacy concern (39%) > Trust concern (9%).

When respondents judge their subjective preferences with reference to various factors by making their pairwise comparison, there are chances of making inconsistent judgements, e.g., if a respondent judges factor one as twice (2 times) as important to factor two. And, in the second comparison, he judges factor two as 4 times as important to factor three, then mathematically, we can say that factor one is 8 times (2*4) important than factor three. However, in the AHP, since a respondent makes the third comparison and judge the importance of factor three subjectively with respect to one, as done previously for other factors, there is a likelihood of inconsistency in subjective judgment and the results drawn mathematically for the third comparison (favors one over factor three in this case). The consistency ratio (*CR*) becomes handy here to check the results for consistency. In the AHP, the consistency ratio is defined as *CR*, where $CR = CI/RI$. Saaty (1980) has shown that the consistency ratio (*CR*) of 0.10 or less is acceptable to continue the AHP analysis. Since three factors are compared the consistency index of the randomly generated comparison matrix value is measured as 0.58, and the Consistency ratio (*CR*) of the above results is 0.03. This is within the acceptable range of 10% or 0.10.

In addition, users compared all types of banks – public, private, and foreign – for all three parameters of risk, namely. Security concern, Privacy concern and Trust concern. The analysis of the responses showed that public sector banks are considered to be the safest on all three concerns. The weighed score of public sector banks for the three parameters was the highest; it was 55%, 57% and 70% for security, privacy and trust, respectively. *CR* consistency ratio of the aforementioned weights was 0.07, 0.08, and 0.09. These are all within the acceptable range of 10% or 0.10, which confirms the accuracy of the results.

Thus, according to the overall online risk perception by users, public banks had the highest weight of 57% followed by private and foreign banks (Table 11 and Figure 2). The results suggest that public sector banks are ranked the safest among major three types of banks followed by private and foreign banks. Moreover, it is interesting to note that private and foreign banks are far behind public sector banks in terms of safety rating as perceived by online banking users – almost 50% to 80%. Public sector banks are considered the safest by all three valuation factors having a weighted score of 28% by the security aspect, 23% by the privacy aspect and

Table 11. E-banking users' perception for various types of banks based on weighted score of selected criteria

	Original score				Weighted score		
Criterion	**Weight**	**Public bank**	**Private bank**	**Foreign bank**	**Public bank**	**Private bank**	**Foreign bank**
Privacy concern	39%	57%	33%	10%	23%	13%	4%
Security concern	52%	55%	32%	13%	28%	17%	7%
Trust concern	9%	70%	21%	9%	6%	2%	1%
Overall perception					57%	31%	11%

6% by the trust constituting a total weighted score of 57% (Figure 2). The online security risk procedure is based on the overall rating of various banks, which is assessed and perceived by online banking users by specified risk factors.

4. DISCUSSION

Among the three aspects of security perceptions considered in this study, namely security concern, privacy concern and trust concern, users are more concerned about security followed by privacy and trust. The results contradict Gurung and Raja's (2016) findings, where trust is seen as having the highest impact on risk perception followed by privacy and security. In addition, the results of this study illustrate that e-banking users in India consider public sector banks as the most secure followed by private and foreign banks. No studies have yet been conducted to evaluate and compare security perceptions of e-banking users with regard to different types of banks, including public, private and foreign banks in India. However, these results appear to be because users in India are more exposed to the public sector banks than private and foreign banks. Although, private sector banks have existed in India since 1899, but after the nationalization of major private banks in 1969 by the Government of India, public sector banks dominate the Indian banking sector. Private sector only became entrenched after the 1990s, and foreign banks after 2005, when government allowed their entry. This has been drawn from Gurung and Raja's (2016) findings, which show that user concerns and beliefs about security are not indestructible but keep evolving over a period of time, as their experience, awareness and conversancy with internet change. Over time, they become more confident in making transaction online. More experience of Indian e-banking users with public sector banks followed by private and foreign banks seems to increase their perception of security.

CONCLUSION

The study estimates and compares how e-banking users perceive online risk for public, private and foreign banks in India. The study reveals that among the three factors considered, security (Weighted Score = 52%) is perceived as most critical by e-banking users. And further analysis revealed that public sector banks are the safest among major three types of banks followed by private and foreign banks. Moreover, it is interesting to note that private and foreign banks are far behind public sector banks in terms of safety rating as perceived by online banking users – almost 50% to 80%. Although public sector banks are continuously losing market share measured in deposits and advances, they are still strong when it comes to online banking user's perception of risk and trust. When it comes to technology adoption, public sector banks lag behind their peers in digitizing their business processes and implementing digital technologies in their operations (Rishi & Saxena, 2004; Soni, 2019). So, the results of the study seem counterintuitive. This may be due to the years of familiarity, relationship, and experience with public banks that have given rise to such perception. Therefore, besides continuing to develop and modernize the existing security infrastructure, private and foreign banks need to educate and emphasize their safety aspects in an effort to persuade customers. Moreover, they should be more responsive to their existing customers' security concerns if any.

http://dx.doi.org/10.21511/bbs.15(1).2020.02

REFERENCES

1. Abdul-Hamid, Y. T. (1999). An analytical hierarchy process approach to the choice of manufacturing plant layout. *Journal of Engineering Manufacture, 213*(4), 397-406. https://doi.org/10.1243/0954405991516868
2. Ackerman, M. S. (2004). Privacy in pervasive environments: next generation labeling protocols. *Personal and Ubiquitous Computing, 8*(6), 430-439. https://doi.org/10.1007/s00779-004-0305-8
3. Babu, N., & Rajini, P. (2017). Comparative Study between Private Sector and Public Sector Banks in the Adoption of Technology in Banking Services – Twin Cities. *Journal of Business and Management, 1,* 64-69. Retrieved from http://www.iosrjournals.org/iosr-jbm/papers/Conf.17037-2017/Volume-1/12.%2064-69.pdf
4. Bansal, G., & Zahedi, F. M. (2014). Trust-Discount Tradeoff in Three Contexts: Frugality Moderating Privacy and Security Concerns. *Journal of Computer Information Systems, 55*(1), 13-29. Retrieved from http://www.business.uwm.edu/gdrive/Zahedi_M/Temp/Talk%20papers/BansalZahedi-Frugality-JOCIS-2014.pdf
5. Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in Electronic Commerce: the Role of Privacy, Security, and Site Attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.460.6616
6. Bergquist, K., & Abesysekera, J. (1996). Quality function deployment (QFD) – a means for developing usable products. *International Journal of Industrial Ergonomics, 18*(4), 269-275. https://doi.org/10.1016/0169-8141(95)00051-8
7. Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems, 19*(1), 211-241. https://doi.org/10.1080/07421222.2002.11045715
8. Calantone, R. J., Di Benedetto, C. A., & Schmidt, J. B. (1999). Using the analytical hierarchy process in new product screening. *International Journal of Production and Innovation Management, 16*(1), 65-76. https://doi.org/10.1111/1540-5885.1610065
9. Chellappa, R. K. (2008). *Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security* (Unpublished paper). Emory University, Atlanta, GA. Retrieved from https://pdfs.semanticscholar.org/7e2f/bad4fa4877ea3fd8d197950e335d59ebeedf.pdf
10. Chellappa, R. K., & Pavlou, P. A. (2000). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358-368. https://doi.org/10.1108/09576050210447046
11. Chellappa, R. K., & Pavlou, P. A. (2001). *The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions* (eBizLab Working Paper). Marshall School of Business, University of South California, Los Angeles, CA.
12. Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104
13. Dweiri, F., & Meirer, F. A. (1996). Application of fuzzy decision-making in facility lay out planning. *International Journal of Production Research, 34*(11), 3201-3225. https://doi.org/10.1080/00207549608905085
14. Gefen, D. E., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly, 27*(1), 51-90. https://doi.org/10.2307/30036519
15. Gray, P. (1999). *Protecting Privacy and Security of Personal Information in the Global Electronic Marketplace.*
16. Gupta, S., Dawar, V., & Goyal, A. (2018). Enhancing the Placement Value of Professionally Qualified Students in Marketing: An application of the Analytic Hierarchy Process. *Academy of Marketing Studies Journal, 22*(3). Retrieved from https://www.abacademies.org/articles/enhancing-the-placement-value-of-professionally-qualified-students-in-marketing-an-application-of-the-analytic-hierarchy-process-7535.html
17. Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security, 24*(4), 348-371. https://doi.org/10.1108/ICS-05-2015-0020
18. Juwaheer, T. D., Pudaruth, S., & Ramdin, P. (2012). Factors influencing the adoption of internet banking: a case study of commercial banks in Mauritius. *World Journal of Science, Technology and Sustainable Development, 9*(3), 204-234. https://doi.org/10.1108/20425941211250552
19. Kim, D., Ferrin, D., & Rao, H. A. (2008). Trust-based Consumer Decision-making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and their Antecedents. *Decision Support System, 44*(2), 544-564. https://doi.org/10.1016/j.dss.2007.07.001
20. Laforet, S., & Li, X. (2005). Consumers' attitudes towards online and mobile banking in China. *International Journal of Bank Marketing, 23*(5), 362-380. https://doi.org/10.1108/02652320510629250
21. Lallmahamood, M. (2007). An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce : Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce, 12*(3), 1-26. Retrieved from https://www.researchgate.net/publication/284054593_An_Examination_of_Individual's_Perceived_Security_and_Privacy_of_the_Internet_in_Malaysia_and_the_Influence_of_This_on_Their_Inten-

tion_to_Use_E-Commerce_Using_An_Extension_of_the_Technology_Acceptance

22. Lee, A. H. I., Kang, H.-Y., Hsu, C.-F., & Hung, H.-C. (2009). A green supplier selection model for the high-tech industry. *Expert Systems with Applications, 36*(4), 7917-7927. https://doi.org/10.1016/j.eswa.2008.11.052

23. Lee, S. M., & Eom, H. B. (1990). Multiple-criteria decision support systems: the powerful tool for attacking complex, unstructured decisions. *Systems Practice, 3*(1), 51-65.

24. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355. Retrieved from https://pdfs.semanticscholar.org/7307/1a056403ed5f9fd5b16b9dd70a93e9a4e375.pdf

25. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-34. Retrieved from https://www.jstor.org/stable/258792?seq=1#metadata_info_tab_contents

26. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *Journal of Strategic Information Systems, 11*(3-4), 297-323. https://doi.org/10.1016/S0963-8687(02)00020-3

27. Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: an examination of online retailer disclosures. *Journal of Public Policy and Marketing, 19*(1), 54-61. https://doi.org/10.1509%2Fjppm.19.1.54.16942

28. Miyazaki, A. D., & Fernandez, A. N. A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping All use subject to JSTOR Terms and Conditions AND for Online Shopping of Privacy and Security Risks. *The Journal of Consumer Affairs, 35*(1), 27-44. Retrieved from https://www.jstor.org/stable/23860070

29. Nilsson, M., Adams, A., & Herd, S. (2005). Building security and trust in online banking. *Proceedings Conference on Human Factors in Computing Systems* (pp. 1701-1704). https://doi.org/10.1145/1056808.1057001

30. Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure.* Albany: State University of New York Press.

31. Riquelme, I. P., & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of Is the influence of privacy and security on online trust the same for all type of consumers? *Electron Markets, 24,* 135-149. https://doi.org/10.1007/s12525-013-0145-3

32. Rishi, M., & Saxena, S. C. (2004). Technological innovations in the Indian banking industry: the late bloomer. *Accounting, Business & Financial History, 14*(3), 339-353. https://doi.org/10.1080/0958520042000277801

33. Román, S. (2007). The ethics of online retailing: a scale development and validation from the consumers' perspective. *Journal of Business Ethics, 72*(2), 131-148. https://doi.org/10.1007/s10551-006-9161-y

34. Román, S., & Cuestas, P. J. (2008). The perceptions of consumers regarding online retailers' ethics and their relationship with consumers' general internet expertise and word of mouth: a Preliminary analysis. *Journal of Business Ethics, 83*(4), 641-656. https://doi.org/10.1007/s10551-007-9645-4

35. Saaty, T. L. (1980). *The Analytic Hierarchy Process.* McGraw-Hill: New York.

36. Sabaei, D., Erkoyuncu, J., & Roy, R. (2015). A review of multi-criteria decision making methods for enhanced maintenance delivery. *Procedia CIRP, 37,* 30-35. https://doi.org/10.1016/j.procir.2015.08.086.

37. Singh, T., Patnaik, A., Chauhan, R., & Chauhan, P. (2018). Selection of brake friction materials using hybrid analytical hierarchy process and vise kriterijumska optimizacija kompromisno resenje approach. *Polymer Composites*, *39*(5), 1655-1662.

38. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196. Retrieved from https://www.jstor.org/stable/249477

39. Soni, S. (2019, May 12). *Banks in India Ready for Tech-Revolution* (Interview). Retrieved from https://bfsi.eletsonline.com/banks-in-india-ready-for-tech-revolution/

40. Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology, 68*(3), 459-468. https://doi.org/10.1037/0021-9010.68.3.459

41. Vijayasarathy, L. R. (2004). Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model. *Information and Management, 41*(6), 747-762. https://doi.org/10.1016/j.im.2003.08.011

42. Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of Individual Self-Protection, Industry Self- Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research, 23*(4), 1342-1363. https://doi.org/10.1287/isre.1120.0416

http://dx.doi.org/10.21511/bbs.15(1).2020.02