Turkish Journal of Computer and Mathematics Education *Vol.12 No.6(2021), 56-68*

Research Article

Behavioral Intentions towards adoption of Information Protection and Cyber security (Email Security and Online Privacy): SEM model

Sivarethinamohan R[1], Sujatha S[2]

[1]Department of Professional Studies,
CHRIST (Deemed to be University), Bengaluru, India

*Corresponding author: E-mail: mohan.dimat@gmail.com

[2]Professor, K Ramakrishnan College of Technology, Trichy, Tamilnadu

Article History:Received:11 november 2020; Accepted: 27 December 2020; Published online: 05 April 2021

Abstract : Email security and online privacy have become the hot-spots of discussion during the testing times of the pandemic as most of the communication and transactions take place through email and online respectively. Though the industry of information security claims to have put forth rigorous rules and guidelines to continually ensure and improve the level and quality of Email security and online privacy, the people always have their own doubts and fears about the same. The doubts and the fears appears to have increased with the wide-spread pandemic as the people who are new to email communication and online transactions are compelled to involve in them. With this as the backdrop, the researchers aim to analyze the level of confidence created by the existing Email security and online privacy standards by identifying the people's opinions, their beliefs and their trust towards them. In order to arrive at the above, a survey, using a structured questionnaire, was con-ducted among six-hundred people, residing in the Asia-pacific region, selected using convenient sampling. The data were collected and analyzed. The results indicate that the human intentions, beliefs and trust have a great influence on Cyber defenses (Email Client Security and Online Privacy) in this region. The study also provides information on the outstanding nature of these measurement items and the perception of privacy and security in information sharing as distinctive constructs

Keywords: Human Opinions, Perceived Trust and Beliefs, Perceived Email Security, Perceived Online Privacy, Information Sharing.

1 Introduction

Email, e-commerce and online transactions have become the rulers of the roost today and the existing pandemic has accentuated the need and necessity for those in the collective efforts of the nation's world-wide to bring back some normalcy during this period of abnormality. All communications and transactions that take place between nations, organizations and even common people depend on internet. The rapid development and advancement of internet has made even the most difficult and time-consuming things possible and in a relatively lesser time just with a tap or a swipe of the finger. With all the pros experienced in connection with the use of internet, the question of internet security has always been a nagging question at the back of everyone's mind. Though the industry of information security assures its clients sure security and privacy with the aid of Advanced Analytics, Integrated Technology, Human-Centric Security and Risk-Adaptive Protection, the concept of internet security has always been a matter of topmost concern among the email users [9]. In spite of the concern, the users also trust the Insider Threat Programs, Cloud App Security and Network Security. The positive attitude and good intentions towards the appropriate use of electronic messaging is found to have a tremendous impact on the willingness and desire to use email technology for information sharing.[11] In line with this and on findings from the related literature reviews, the three factors namely Human intention, Trust and security have been identified as the three major forces which greatly influence the sharing of information through email.[28] Based on the popular and frequently used theories and for the purpose of the study, a theoretical model and hypotheses were designed to measure the magnitude of user readiness and inclination to employ email technology for the tasks it is exclusively designed to support and persuade responsible behavior. The study also aims to prove that trust and security are antecedents for transactions through email and recommends an all-inclusive model for email transaction, taking into consideration its direct governing constructs for predict-ing the pre-service users' intentions for using email technology to share information.

2. Review of Literature

Email gives its users the impression that it is personal and is from a reliable source in spite of the fact that it has been mailed from a different place. Modern email systems transmit text, electronic documents, voice, graphics,

*Corresponding author : Sivarethinamohan R[1]
[1]Department of Professional Studies,
CHRIST (Deemed to be University), Bengaluru, India

animations and financial transactions through internet [10]. The threat of duplication, stealing or distorting the data shared is always considered a possibility with the advancements in use of internet. The risk of cyber security cannot be overlooked [1]. However, surmounting Email spoofing, Transport Layer Security and its predecessor, Secure Sockets Layer (TLS /SSL) are useful to enforce authentication. Haider M Al-Mashhadi and Mohammed H Alabiech [20] elucidate about how email works and talk about dissimilar threats in Email Communication and offer quite a lot of Email security solutions. Several models and techniques were also introduced in this paper to fix and enhance the safety of Email systems. Elliptic curve cryptography combined with public key algorithm ensures security of e-mail services proficiently and without much trouble

Fatima Aziz Rawdhan and Mahmood Khalel Ibrahim [18] have attempted to determine that with Confidentiality and Integrity, the asymmetric encryption is employed to sign and encrypt the message and is considered essential for data security. Banday, M.T. (2011). proposed a simple prototype of e-mail security protocol to enhance security services for e-mail clients. [4]. Azeem Aleem (2020) report that highly sensitive information like patient and healthcare information or customer financial records are expected to maintain proper compliance and protect this information as appropriate [3]. Moneer Alshaikh (2020) suggested cyber security behaviors, establishing a 'cyber security champion' network as key initiatives to improve their respective cyber security cultures [24].

Derks, D., & Bakker, A. B (2010). reported that a smart phone surges the flexibility and adaptability of employee in the work place, but enables working long hours with a threat of disturbed work-life balance at the same time [14]. Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra and Amy Ginther [19] studied the role of motivation to evaluate their populations for correlations between individual differences and security behaviors in order to continue developing the security community's understanding of users. Deepak Chawla &Himanshu Joshi [13] conveyed that perceived trust, PEOU, perceived lifestyle compatibility and perceived efficiency were instituted to positively and significantly affect user intention.

Shappie, A. T., Dawson, C. A., &Debb, S. M. [30] advocate that personality structure is associated with cyber security behaviors and that conscientiousness and openness may be particularly salient to this relationship. Uffen, J., &Breitner, M. H. [32] specify that once executives are confronted with information security standards or guidelines, the personality traits of conscientiousness and openness will have a significant impact on attitude towards managing security measures than without moderators. Most of the past literature concludes that consumers have a zero trust mentality in the era of advanced email security threats [23]. Thus, this study's main interest is to expand previous theory on the subject of email security in work place by investigating trust and security dimensions

3. Materials and Methods

3.1 Theoretical model and Hypotheses Development for the Proposed Model

Figure 1 displays the theoretical model that will be examined, which was constructed based on previous studies. There are two exogenous (independent) variables: Perceived Trust and Beliefs and Human intention and Perception. There are three endogenous variables: Perceived Email security, Perceived Email privacy and Information sharing. The proposed hypotheses states that perceived trust and beliefs, human intention and perception, perceived email security, perceived privacy and Information sharing are the major constructs that influence a user's willingness to share information through an online platform. The researchers also proposed to find the Human Intentions and their Trust and Beliefs towards Email Security and Email privacy and show how they influence the security and privacy in sharing information through Emails. The proposed hypothesis was empirically tested. The following hypotheses are constructed based on the study model exhibited in the Fig.1:

(i). Perceived Trust and Beliefs, as a latent variable, is measured by the observation of Quality antivirus, Backlists and whitelists, Hard to Guess passwords, S/MIME protocol, Cyber security plan and Minimizing risk snooping [22].

(ii). Human intention and Perception, as a latent variable, is measured by observing and protecting malware attacks, minimizing Spam, cutting back email traffic, ensuring sensitive information and Information Exchange

(iii). Perceived Email security, as a latent variable, is measured by the observation of 0.0001% false positives, Zero-day protection, and Targeted Threat protection

(iv). Perceived Email privacy, as a latent variable, is measured by the observation of Server- to- server transport layer security, Enterprise email encryption & layer security, and AES-encrypted archive

(v). Information sharing, as a latent variable, is measured by the observation of Cloud computing landscape and Mobile computing landscape

H1: There is a strong relationship between Human Intention and Perception towards internet services landscape and Email security

(i). Quality antivirus strongly influences Human Intention and Perception towards internet services landscape and information assurance

(ii). Backlists and whitelists applications strongly influences Human Intention and Perception towards internet services landscape and information assurance

(iii). Hard to Guess passwords strongly influences Human Intention and Perception towards internet services landscape and information assurance
(iv). S/MIME (Secure/Multipurpose Internet Mail Extensions) protocols strongly influence Human Intention and Perception towards internet services landscape and information assurance
(v). Cyber security plan strongly influences plan Human Intention and Perception towards internet services landscape and information assurance
(vi). Minimizing risk snooping strongly influences Human Intention and Perception towards internet services landscape and information assurance The World Economic Forum identified blockchain as a mechanism to repair the world's most challenging environmental issues. It is one of the promising technologies currently gaining a lot of attention in environment protection. Blockchain is a decentralized ledger which records transactions in a chronological order on a real time basis and allows any two parties to transact between each other without the need for trusted outsiders.
H2: Users strongly trust and believe email privacy that deals with issues of unauthorized access and inspection of electronic mail.

(i). Users strongly trust and believe email privacy that protect their business from malware attacks
(ii). Users strongly trust and believe email privacy that helps in Minimizing Spam
(iii). Users strongly trust and believe email privacy that can Cut back email traffic
(iv). Users strongly trust and believe email privacy that helps in ensuring sensitive information
(v). Users strongly trust and believe email privacy that helps in Information Exchange

H3: There is a strong relationship between Email security and information sharing through mobile and cloud computing landscape.

(i). 99% email spam protection with 0.0001% false positives SLA has strong influence on email security while sharing the information
(ii). Zero-day protection has strong influence on email security to defend against zero-day attacks while sharing the information
(iii). Targeted Threat protection has strong influence on email security that protects users against targeted social engineering attacks in email (whaling or CEO Fraud) and protects against domain similarity at-tacks.

H4: There is a strong relationship between Email privacy and information sharing or data to be kept private, confidential and secure through mobile and cloud computing landscape.

(i). Server- to- server transport layer security has strong influence on email privacy while encrypting the communication between web applications and servers, such as web browsers loading a website.
(ii). Enterprise email encryption & layer security has strong influence on email privacy that helps stop in-advertent or deliberate data leaks while protecting information in transit.
(iii). AES-encrypted archive has strong influence on email privacy that is used to encrypt data to keep it private and to keep classified data secure

3.2 Sampling, Data collection and Sample size determination

The present study covers the following eleven Asia Pacific locations namely Japan, South Korea, India, Australia, Hong Kong, Taiwan, Singapore, New Zealand, Malaysia, Indonesia and the Philippines. There are numerous companies in these regions. Using convenience sampling, the samples were derived from the Computer Security Division in the companies who develop and advance their innovative security technologies and improve their ability to resolve current and future computer and information security challenges[36]. Therefore, the researchers consider them as appropriate respondents for the present study. Respondents N=600 were selected at convenience sampling in order to get an idea of the opinion of Cyber Defenses mechanism as a whole. The data for the study was collected by conducting an online customized survey questionnaire specifically designed to test the proposed framework. The questionnaire was distributed through emails and search engines. All items of the proposed research framework were measured on a 5-point Likert scale, ranging from 1 (extremely strongly disagree) to 7 (extremely agree). SEM (Structural Equation Modeling) is performed to detect relationships among constructs using AMOS 21.0.

4. Results and Discussion

4.1.1 Cronbach's Alpha test

The first step of analysis is to determine the internal consistency and the reliability of the questionnaire as a research instrument [12]. As it can be seen from the Table 1, Cronbach's alphas of all constructs are within the acceptable values of 0.7 or 0.6 [6]and thus the internal consistency of the measured constructs is acceptable for the study. As the average inter-item correlation increases, the internal consistency and scale reliability increases as well. [25]

4.1.2 Average variance extracted (AVE) and Composite or construct reliability (CR

Average variance extracted (AVE) is a measure of the amount of variance that is captured by a construct in relation to the amount of variance due to measurement error. [24]. Composite or construct reliability (CR) is a measure of internal consistency in scale items [29]. Recommended Thresholds of CR is > 0.6 and AVE is > 0.5

[31]. Average Variances Extracted of Human Intention and Perception = 0.5, Perceived Trust and Beliefs = 0.602, Perceived Email Security = 0.5, Perceived Privacy = 0.605 and Information Sharing = 0.738 are above 0.50, indicating that the reliability of this model is good and suggestive of adequate convergent validity[35]. Moreover, Composite or construct reliability (CR) of Human Intention and Perception = 0.839, Perceived Trust and Beliefs = 0.613, Perceived Email Security = 0.6, Perceived Privacy = 0.606 and Information Sharing = 0.738 are above 0.50 throughout indicating Construct internal consistency in the present study.

4.2. Descriptive statistics to check Scaling and normality assumption

The Table2 includes Descriptive Statistics for each variable and the Analyses N=600. It reports a mean score more than three [26] indicating that there is a strong human intention towards creating and using hard-to-guess passwords (mean score=5.295), then Use the S/MIME protocol for data and use the S/MIME protocol for data (mean score=5.277). End-users have strong trust and beliefs on establishing an organizational and technical infrastructure (mean score= 5.165)[34]. In terms of email security, they have more sensitivity and opinions on Anti-spam protection SLA, with 0.0001% false positives (mean score= 4.877), and Anti-Malware production SLA including zero-day protection (mean score= 4.568). In the view of email privacy, they have more interest on Scanned with email virus protection Enterprise email encryption, using public key infrastructure (mean score=4.923), Enforced server-to-server transport layer security to protect information in transit and stop inadvertent or deliberate data leaks (mean score =4.880) and then Data leak protection technology and stored in a secure AES-encrypted archive (mean score =4.702). By and large, end users prefer Cloud Computing Landscape for sharing the data (mean score =4.920) and then Mobile Computing Landscape (mean score =4.910). Since Values of skewness and kurtosis are within -1 and + 1, Scaling and normality assumption are fulfilled[37]. Therefore, it relies on normal distribution.

4.4 Factor analysis for data reduction and identify latent constructs

Factor analysis is used to serve two purposes, firstly data reduction and secondly to pinpoint latent constructs. Bartlett's test of sphericity inspects the correlation among variables in data set; its value (Approx. Chi-Square=3399.110, df= 171, Sig.=.000) is significant which indicates that variables are correlated. Kaiser-Mayer-Olkin's (KMO) technique checks whether the sample size is appropriate for factor analysis or not. The value of KMO 0.878 which is between 0.8 and 0.9 is very good. Variables having communality value less than 0.5 are deleted and the factors having more than 1.0 eigen-value are retained for further analysis. The results of Rotated Component Matrix are reported in Table 4after Varimax rotation[33]. Highly correlated variables are clustered under one construct. At the end, totally 5 Latent constructs out of 19 indicators viz., Human Intention and Perception, Perceived Trust and Beliefs, Perceived Email Security, Perceived Email Privacy and Information Sharing are extracted to analyze structural relationships using Structural Equation Modeling[38].

4.5. Multivariate Statistical Analysis using Structural Equation Modeling(SEM) [5]

The hypothesized relationships are estimated among the constructs in the Multivariate Statistical Analysis. [8]. It estimates latent variables based on the correlated variations of the dataset. Initially 19 observed variables or indicators were employed based on the research goal [16]. Fig. 2 and 3 put on display of model with the non-standardized estimates and the standardized estimates respectively[39].

4.5.1 Model fit analysis

SEM Analysis is employed to validate the hypothesis about the association of a set of measurement items to their relevant factors.

Model fit summary

Confirmatory factor analysis is used for the model fit of the proposed framework. For structural equation model fit, various fit indices and tests have been developed. [17] These indices and tests, however, can point to conclusions about the extent to which a model actually matches the observed data, known as good model fit, and involves non-experimental research[40]. Let us see the results of model fit indices which are used to validate the model fit:

Tests of Absolute Fit

In the output shown in the Table 5, AMOS divulges that the minimum is achieved with no errors ie., Amos reached a local minimum The value of chi-square test of overall model fit is 458.046with 147 degrees of freedom, returning a probability value of less than 0.001[41]. The null hypothesis is rejected. Therefore, by convention it is conclude that the model fits to the dataset used in the study.

Measuring predictive fit

Values and observations of model fit indices are presented in Table 9 .Dividing $\chi 2$ or CMIN by df is called as Normed chi-square (NC).In the present study, the value of CMIN/df (3.116) is between 3.0 and 5.0indicates the overall fitness of the model[42] .

Measuring Comparative fit

IFI, NFI, CFI, TLI, and RFI evaluate the model of interest with the null or independence model. IFI=0.906, NFI=0.9, CFI =0.905, TLI =0.90, and RFI=0.845 are also above 0.8 and considered adequate based on recommended thresholds. It proves that the default model is correct and is the best fit to the data.

Measuring Badness of fit index

RMSEA (0.059) value of < 0.2 and RMR =0.072 indicates that the data do not underfit the model.
[2]. Measuring Comparative fit
PCFI=0.778 closer to 1, GFI =0.924 and AGFI=0.902 >0.9 guarantees perfect model fit. Hoelter's Critical N is 249 at 1%, i.e. sample size is sufficient since Hoelter's N is ≥200.
4.5.2 Significance test of individual parameters: Results of Hypotheses testing for the Proposed Model
Since the structural model evaluation ensured the evidence of reliability and validity, the structural model was inspected to assess the hypothesized relationships among the constructs in the research model [7]. Table5 shows non-standardized Estimate, Standardized Estimate, Standard error, Critical ratio and inferences to study the direct association between the study's constructs[43]. The probability value connected with null hypothesis is presented under the P column. To test hypotheses 1–18, the structural equation model was tested in Table 6. The results show that all hypothesized relationships are supported.
All of the regression coefficients in this model significantly differ from zero beyond the 0.01 level and supported. Let's elucidate one by one the results of latent constructs and their relationship with other latent construct[44].
1) Human intention (H1: Non-standardized Estimate= .261, Standard error =.072 Critical ratio=4.539 and p = ***). Regresses significantly with email security and positively on willingness to Cloud computing landscape and Mobile computing landscape.
2) Internet users positively trust and believe (H2: Non-standardized Estimate= .463, Standard error =.089, Critical ratio=5.944and p = ***) email privacy with good intention.
3) Email security (H3: Non-standardized Estimate= .422, Standard error=.076, Critical ratio=5.895 8 and p = ***) and email privacy (H4: Non-standardized Estimate= .076, Standard error=.076, Critical ratio=5.619and p = ***) are both positively related to information sharing in the internet services platform.
4) Email privacy (H4: Non-standardized Estimate= .076, Standard error=.076, Critical ratio=5.619and p = ***) is both positively related to information sharing in the internet services platform.
Mediation effects

The relationship between human intention and information sharing was fully mediated by perceived email security. Further The relationship between human trust & believe and information sharing was fully mediated by perceived Email privacy
From the above result it could be understand that an email spam checks and multiple layers of malware protection are acting as an email bridgehead in the cloud to stop known and emerging threats before they reach the network. Privacy is essential since, in its absentia, there is a chance to abuse surveillance information for instance, to peep, to sell to marketers and to spy on individual, political and business enemies whoever they happen to be at the time.
Moreover, almost all latent constructs can be measured by indicator items or measurable constructs since their p-values are 0.000 and supported. Let's describe the results of measurable constructs and their relationship with latent construct one by one.
(i). Users have a strong intention to use quality anti-virus to protect their PC and keep them informed as to what threats are attacking and when they're vanquished
(ii). Users have a strong intention to use Backlists and whitelists approach to controlling access to the network as a whole.
(iii). Users have a strong intention to create a password that's easy to remember & Hard to Guess
(iv). Users have a strong intention to accept S/MIME protocols for sending digitally signed and encrypted messages and encrypting emails and digitally sign them
(v). Users have a strong intention to use Cyber security plan that seeks to protect its customers, employees and corporate information
(vi). Users have a strong intention to minimize risk snooping for avoiding unauthorized access to another person's or company's data
(vii). Users have a strong trust to use privacy settings to Protect against Malware attacks when cybercriminals create malicious software that's installed on someone else's device without their knowledge to gain access to personal information or to damage the device, commonly for financial gain
(viii). Users have a strong trust to use privacy settings to minimize Spam and kind of unwanted, unsolicited digi-tal communication that gets sent out in bulk
(ix). Users have a strong trust to use privacy settings to cut back email traffic and email overloading that leads to spend an hour or more a day just dealing with incoming emails
(x). Users have a strong trust to use privacy settings to ensure sensitive information if not protected, lead to a loss of employee trust, confidence and loyalty.
(xi). Users have a strong trust to use privacy settings to create Information Exchange or information sharing done electronically or through certain systems.

(xii). Secure Email Gateway provides an email spam filter with 99% email spam protection with 0.0001% false positives SLA
(xiii). While sharing information, Zero-day protection Mitigate Advanced Threats in Email Spam Targeted Threat protection. Zero-day attacks are often effective against "secure" networks and can remain undetected even after they are launched. The present study believes that the Zero-day protection has the ability to provide protection against the zero-day exploits.
(xiv). Targeted Threat Protection URL builds on user's security gateway services to protect their organization against the growing threat posed by advanced phishing and spear phishing attacks in inbound (xv). Transport Layer Security highly used to encrypt sensitive information sent over the Web
(xvi). Users trusted fully Enterprise email encryption that is essential for sharing sensitive and confidential information with contacts outside your organization.
(xvii). Users understood AES Crypt that can safely secure their most sensitive files using a powerful 256-bit encryption algorithm.
Therefore, Users do trust and believe that the internet services' platforms protect them from Malware attacks, minimize spam, ensure safety of sensitive information, cut down email traffic and maintain AES-encrypted archive, blacklists and white lists. Users are found to have good intention and thought in using Hard-to-Guess passwords, maintaining Backlists and whitelists, installing quality antivirus, planning Cyber security, minimizing spam and ensuring safety of sensitive information. Bearing in mind email security, users breed a positive opinion on 0.0001% false positives, Zero-day protection and means of minimizing risk snooping for information assurance. Cloud computing landscape and Mobile computing landscape are also closely working in sharking the information confidentially. Also, the overall email security and privacy secure the access and content of an email account or service from the view point of users

VI.CONCLUSION

The study has proved its proposed hypothesis by showing how the users in Asia –Pacific perceive and trust that sensitive information is kept safe in email communication and that accounts are protected against unauthorized access, loss or any compromise by way of examining the various Cyber Defenses techniques. On the basis of the structural equation modeling, it shows that email security is an absolutely safe and sound means of sending out information of any high importance. It also shows that email is endowed with protected messaging service, offers users the facility for speedy setup and guarantees continual user safety from email scammers and hackers. It is found that the users are highly comfortable with email privacy as it provides confidentiality against all advanced threats including phishing, impersonation and spam. Karl Pearson's correlation confirms that a significant relationship exists among all the constructs including intention, trust, beliefs towards components of email security and privacy for harmless transmission of information through the Information exchange, Cloud computing landscape and Mobile computing landscape. Model fit indices also confirm the validity of the present model by denoting the robust inter-linkage among the constructs of the study. It can be concluded that the computer security division of high-growth companies in the AsiaPacific region have a strong belief in safety, defend themselves by ensuring protection of information with an appropriate infrastructure and assure to uphold the companies' electronic information and information infrastructures as a matter of primary mission.

Table 1 Reliability statistics

Latent variables (Unobserved, endogenous variables)		Cronbach's Alpha score N=600	Cronbach's Alpha Based on Standardized Items N=600	N of Items
Human Intention and Perception	HI	.602	.607	4
Perceived Trust and Beliefs	TB	.622	.611	4
Perceived Email Security	ES	.700	.701	4
Perceived Privacy	EP	.703	.703	4
Information Sharing	IS	.678	.684	3
Score of all variables (for final model)	overall	.850	.856	19

Table 2 Descriptive statistics and normality tests of the constructs in the model

Item description N=600	Observed variables	Items	Sum	Rank	Mean	σ	Skew	Kurtosis
Use strong, hard-to-guess passwords	Hard to Guess passwords	INTEN3	3177	1	5.295	1.208	-1.04	1.617
Use the S/MIME protocol for data	S/MIME protocol	INTEN4	3166	2	5.277	1.198	-1.14	2.132
Protection for information in transit to minimize the risk snooping	Minimizing risk snooping	INTEN6	3131	3	5.218	1.17	-0.92	1.528

Create a cyber security plan	Cyber security plan	INTEN5	3117	4	5.195	1.182	-0.71	0.762
Establish an organization-al and technical infrastruc-ture	Information Ex-change	TB5	3099	5	5.165	1.142	-0.52	0.713
Protecting the system against malware	Protecting from-Malware	TB1	3087	6	5.145	1.253	-1.03	1.403
Minimizing the receiving of spam	Minimizing Spam	TB2	3068	7	5.113	1.248	-0.59	0.621
Protection against unsolic-ited messages and cut back on the amount of email traffic	Cut back email traffic	TB3	3021	8	5.035	1.197	-1.01	1.372
Create email blacklists and whitelists	Backlists &d whitelists	INTEN2	3009	9	5.015	1.29	-0.87	1.139
Ensuring Confidential information.	Ensuring infor-mation	TB4	2959	10	4.932	1.147	-0.66	1.444
Scanned with email virus protection ,Enterprise email encryption, using public key infrastructure	Enterprise email encryption & layer security	PRIV2	2954	11	4.923	1.564	-0.74	0.143
Transmission of data, voice and video thru a computer or wireless ena-bled device	Mobile computing Landscape	SHAR1	2952	12	4.92	1.349	-0.55	0.549
Serving as the IT infra-structure driving new digital businesses.	Cloud computing Landscape	SHAR2	2946	13	4.91	1.404	-0.89	0.806
Enforced server- to- serv-er transport layer security to protect information in transit and stop inadvert-ent or data leaks	Server- to- server transport layer security	PRIV1	2928	14	4.88	1.341	-0.57	0.474
Anti-spam protection SLA	0.0001% false positives	SECR1	2926	15	4.877	1.39	-0.86	0.786
Invest in quality antivirus measures	Quality antivirus	INTEN1	2925	16	4.875	1.279	-0.64	0.255
Data leak protection tech-nology and stored in a secure AES-encrypted archive	AES-encrypted archive	PRIV3	2821	17	4.702	1.466	-0.8	0.419
Anti-Malware production SLA + zero-day protec-tion	Zero-day protec-tion	SECR2	2741	18	4.568	1.505	-0.8	0.34
email security platform and targeted threat protec-tion	Targeted Threat protection	SECR3	2739	19	4.565	1.398	-0.78	0.58

Table3 KMO and Bartlett's test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy..		878
Bartlett's Test of Sphericity	Approx. Chi-Square	3399.110
	df	171
	Sig.	.000

Table 4 Rotated Component Matrix[a]

	Component (latent Construct)				
Construct Items	Human Intention and Perception	Perceived Trust and Beliefs	Perceived Email Security	Perceived Privacy	Information Sharing
INTEN1	.629				
INTEN2	.767				
INTEN3	.581				
INTEN4	.688				
INTEN5	.614				
INTEN6	.745				
TR1		.723			
TR2		.823			
TR3		.530			
TR4		.522			
TR5		.512			
SEC1			.623		
SEC2			.831		
SEC3			.803		
PRI1				.736	
PRI2				.809	
PRI3				.581	
SHAR1					.796
SHAR2					.809

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. a. Rotation converged in 7 iterations.

Table 5 Model fit indices of the model

*Corresponding author: Sivarethinamohan R[1]

[1]Department of Professional Studies,
CHRIST (Deemed to be University), Bengaluru, India

Measures of fit		Indices		Indications of model fit	Measurement Weight	Standard values	Acceptability
Minimum sample discrepancy function	predictive fit	NC	Normed Chi-square	Assess Acceptable fit between hypothetical model and sample data	= 3.116	< 2 (Ullman, 2001)	+
Measures based on the population discrepancy	Badness of fit index	RMSEA	Root Mean Square Error of Approximation	Measures of a construct	0.059	< 0.08 (Hair et al. 2006)	+
		RMR	Root Mean Square Residua	Tells how concentrated the data is around the line of best fit	0.072	< 0.08 (Hair et al. 2006)	+
Comparison of baseline model	Comparative fit	NFI Delta1	Normed Fit Index	Signifies Proportion in the improvement of the overall model	0.867 round off 0.9	> 0.90 (Hu and Bentler, 1999)	+
		TLI rh0 2	Tucker-Lewis index	Compare alternative model against null model	0.889	A value close to 1	+
		CFI	Confirmatory Fit Index	Determine Over all fit of the model	0.905	> 0.90 (Daire et al., 2008)	+
		IFI Delta2	Incremental fit index	Deals with the issue of parsimony and sample size in the model	0.906	A value close to 1	+
		RFI rho1	Relative Fit Index		0.845	A value close to 1	+
Parsimony-Adjusted Measures	Parsimonious fit	PCFI	Parsimony Comparative Fit Index	Assess sensitive to model size	0.778 round off 0.8	A value close to 1 (Mulaik et al., 1989)	+
GFI and related measures	Goodness of fit	GFI	Goodness of Fit	Compute a fit between the hypothesized model and the observed covariance matrix	0.924	> 0.90 (Hu and Bentler, 1999)	+
		AGFI	(Adjusted) Goodness of Fit	Corrects the GFI, which is affected by the number of indicators of each latent variable	0.902	> 0.90 (Hair et al. 2006)	+
Hoelter Index	Test the adequacy of the sample size	HOELTER at 1%	HOELTER	Review if sample size is adequate	249	N≥200, sample size is sufficient	+
		at 5%			231		

Table 6 Regression Weights (Default model)

Proposed relationship between constructs			Unstandardized Estimate	Standardized Estimate	Standard error	Critical ratio	P	Inferences
Indicator Variables	Relationship	Latent constructs						
ES	<---	HI	0.261	0.247	.057	4.539	**	Supported
EP	<---	TB	0.463	0.407	.078	5.944	***	Supported
IS	<---	ES	0.422	0.373	.072	5.895	***	Supported
IS	<---	EP	0.502	0.399	.089	5.619	***	Supported
INTEN4	<---	HI	1.022	0.653	.076	13.414	***	Supported

Proposed relationship between constructs			Unstandardized Estimate	Standardized Estimate	Standard error	Critical ratio	P	Inferences
Indicator Variables	Relationship	Latent constructs						
INTEN3	<---	HI	0.96	0.608	.076	12.646	***	Supported
INTEN2	<---	HI	1.153	0.684	.083	13.922	***	Supported
INTEN1	<---	HI	1.074	0.843	.081	13.247	***	Supported
TB5	<---	TB	1	0.559				
TB4	<---	TB	1.227	0.683	.103	11.908	***	Supported
TB3	<---	TB	1.271	0.678	.107	11.855	***	Supported
TB2	<---	TB	1.084	0.555	.104	10.414	**	Supported
TB1	<---	TB	1.322	0.674	.112	11.815	***	Supported
SECR1	<---	ES	1	0.581				
SECR2	<---	ES	1.438	0.771	.133	10.840	***	Supported
SECR3	<---	ES	1.174	0.678	.108	10.902	***	Supported
PRIV3	<---	EP	1	0.495				
PRIV2	<---	EP	1.45	0.674	.169	8.562	***	Supported
PRIV1	<---	EP	1.198	0.649	.140	8.549	***	Supported
SHAR1	<---	IS	1	0.687				
SHAR2	<---	IS	1.19	0.788	.132	9.027	***	Supported
INTEN6	<---	HI	1	0.654				
INTEN5	<---	HI	0.987	0.639	.075	13.185	***	Supported

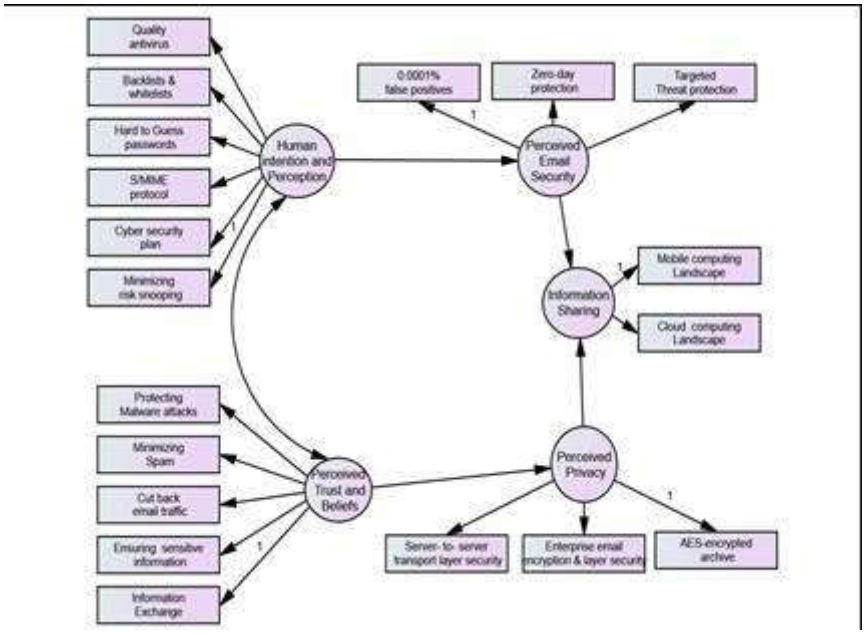

Fig.1 Hypothetical model for the study ((Conceptual model of structural relationships

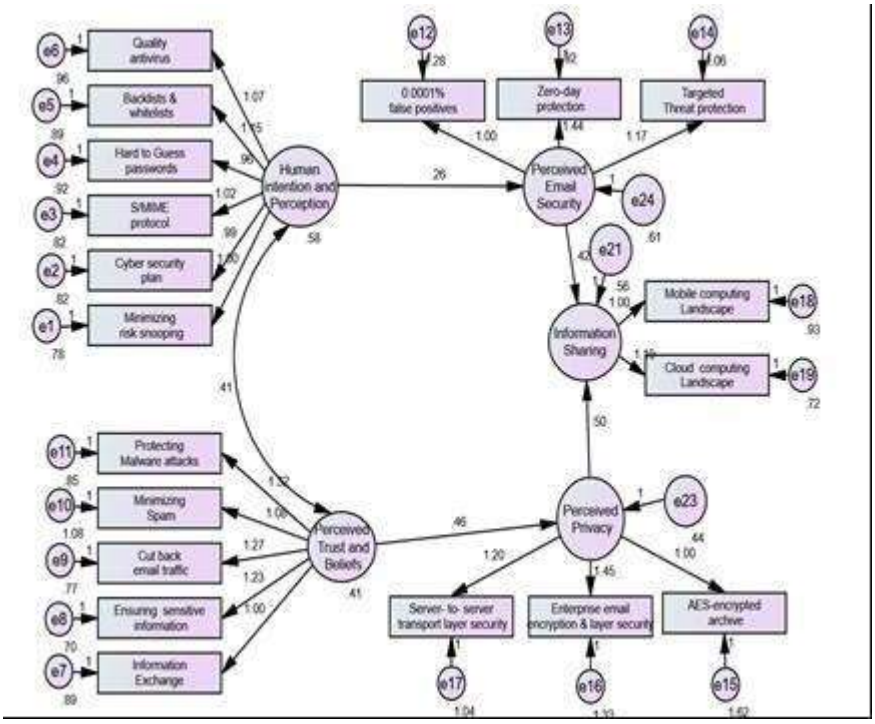

Fig.2 Multiple regression diagram (Non-standardized estimates)

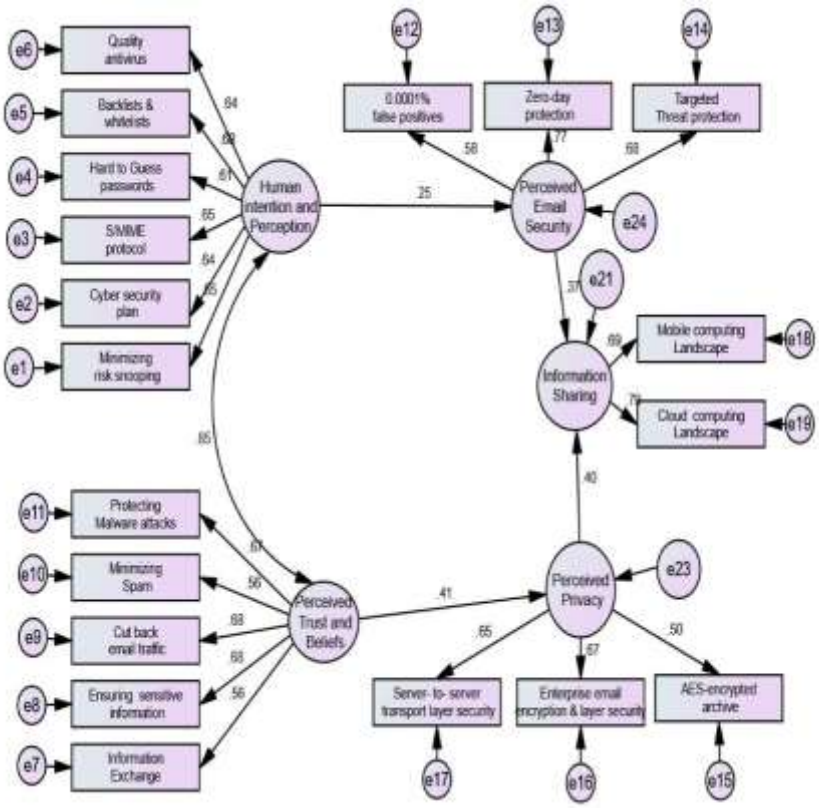

Fig 3 Multiple Regression Diagram (standardized estimates)

References

Al Shidhani, A. A. (2019). Cyber Defense Maturity Levels and Threat Models for Smart Cities. International Journal of Information Security and Privacy, 13(2), 32–46. doi:10.4018/ijisp.2019040103

Angoff, W. H. (1953). Test reliability and effective test length. Psychometrika, 18(1), 1-14.

Azeem Aleem (2020). Adapting security to the new normal, Computer Fraud & Security, 2020(8), 20. https://doi.org/10.1016/S1361-3723(20)30088-9

Banday, M.T. (2011). Effectiveness and limitations of e-mail security protocols. International Journal of Distributed and Parallel systems, 2, 38-49.

Baumgartner, H., & Homburg, C. (1996). Applications of structural equation modeling in marketing and consumer research: A review. International Journal of Research in Marketing, 13(2), 139-161. https://doi.org/10.1016/0167-8116(95)00038-0

Bentler, P. M. (2009). Alpha, dimension-free, and model-based internal consistency reliability. Psychometrika, 74(1), 137–143.

Bentler, P. M; Chou, Chih-Ping (2016). Practical Issues in Structural Modeling. Sociological Methods & Research. 16 (1): 78–117. doi:10.1177/0049124187016001004

Bollen, K.A. (1989). Structural Equations with Latent Variables. New York: John Wiley and Sons.

Butler, K.R., Enck, W., Plasterr, J., Traynor, P., & McDaniel, P.D. (2006). Privacy Preserving Web-Based Email. ICISS.

Chhabra, G. S., & Bajwa, D. S. (2012). Review of E-mail System, Security Protocols and Email Forensics. International Journal of Computer Science & Communication Networks, 5(3), 201–211.

Choukse, D., Singh, U.K., Laddhani, L., & Shahapurkar, R. (2012). Designing secure email infrastructure. 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), 1-9.

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. Journal of Applied Psychology, 78 (1), 98–104.

Deepak Chawla & Himanshu Joshi. (2017). High Versus Low Consumer Attitude and Intention Towards Adoption of Mobile Banking in India: An Empirical Study, Vision, 21(4), 410-424

Derks, D., & Bakker, A. B. (2010). The Impact of E-mail Communication on Organizational Life. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 4(1), Article 4. Retrieved from https://cyberpsychology.eu/article/view/4233

Eunseong Cho. (2016). Making reliability reliable: A systematic approach to reliability coefficients. Organizational Research Methods. 19(4), 651–682.

Fan X, Thompson B, Wang L. (1999). Effects of sample size, estimation methods, and model specification on structural equation modeling fit indexes. StructEqu Modeling 6(1):56–83. (1999). https://doi.org/10.1080/10705519909540119

Fornell, C. &Larcker, D. F (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of marketing research, 39-50. https://doi.org/10.1177/002224378101800104

Fatima Aziz Rawdhan, Mahmood Khalel Ibrahim.: Enhancement of Email Security Services. International Journal of Scientific & Engineering Research .8(1),2090-98 (2017).

Gratian, Margaret & Bandi, Sruthi & Cukier, Michel & Dykstra, Josiah & Ginther, Amy. (2017). Correlating Human Traits and Cybersecurity Behavior Intentions. Computers & Security. 73. 345–358. 10.1016/j.cose.2017.11.015.

Haider M Al-Mashhadi and Mohammed H Alabiech (2017). A Survey of Email Service; Attacks, Security Methods and Protocols. International Journal of Computer Applications, 162(11), 31–40. https://doi.org/10.5120/ijca2017913417

Hair J.F., Black W.C., Babin B.J., Anderson R.E., and Tatham R.L. (2006). Multivariate data analysis 6th Edition. Pearson Prentice Hall. New Jersey.

Hung-Min Sun, Bin-Tsan Hsieh and Hsin-Jia Hwang (2005). Secure E-mail protocols providing perfect forward secrecy, in IEEE Communications Letters, 9(1), 58-60, doi: 10.1109/LCOMM.2005.01004.

Levi, A., & Koç, Ç.K. (2001). Inside risks: Risks in email security. Communications of the ACM, 44, 112.

Moneer Alshaikh (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective, Computers & Security ,98, https://doi.org/10.1016/j.cose.2020.102003

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). Scaling procedures. Thousand Oaks, CA: SAGE Publications, Inc. doi: 10.4135/9781412985772

Nick T.G. (2007) Descriptive Statistics. In: Ambrosius W.T. (eds) Topics in Biostatistics. Methods in Molecular Biology™, Humana Press, 404. https://doi.org/10.1007/978-1-59745-530-5_3

Pearson, K. (1895) Notes on Regression and Inheritance in the Case of Two Parents, Proceedings of the Royal Society of London, 58, 240-242. https://doi.org/10.1098/rspl.1895.0041

Rawdhan, F. A., & Ibrahim, M. K. (2017). Enhancement of Email Security Services. International Journal of Scientific & Engineering Research (IJSER), 8(1), 2090–2095. https://www.ijser.org/onlineResearchPaperViewer.aspx?Enhancement-of-Email-Security-Services.pdf

Raykov, T. (2004). Behavioral scale reliability and measurement invariance evaluation using latent variable modeling. Behavior Therapy, 35 (2), 299–331.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. Psychology of Popular Media Culture. Advance online publication. https://doi.org/10.1037/ppm0000247

Shelley, Mack C (2006). Structural Equation Modeling. Encyclopedia of Educational Leadership and Administration. doi:10.4135/9781412939584.n544.

Uffen, J., &Breitner, M. H. (2013). Management of technical security measures: An empirical examination of personality traits and behavioral intentions. International Journal of Social and Organizational Dynamics in IT(IJSODIT). 3(1), 14–31. https://EconPapers.repec.org/RePEc:igg:jsodit:v:3:y:2013:i:1:p:14-31

Ganesh Babu Loganathan, Praveen M., Jamuna Rani D., "Intelligent classification technique for breast cancer classification using digital image processing approach" IEEE Xplore Digital Library 2019, Pp.1-6.

Dr.Idris Hadi Salih, Ganesh Babu Loganathan, "Induction motor fault monitoring and fault classification using deep learning probablistic neural network" Solid State Technology(2020), Volume 63, Issue 6, PP No. 2196-2213.

Ganesh Babu Loganathan "Design and analysis of high gain Re Boost-Luo converter for high power DC application", Materials Today: Proceedings(2020), Volume 33, Part 1, PP 13-22.

M. Viswanathan, Ganesh Babu Loganathan, *and* S. Srinivasan, "IKP based biometric authentication using artificial neural network", AIP Conference Proceedings (2020), Volume 2271, Issue 1, pp 030030.

Mohammed Abdulghani Taha and Ganesh Babu Loganathan, "Hybrid algorithms for spectral noise removal in hyper spectral images" AIP Conference Proceedings (2020), Volume 2271, Issue 1, pp 030013.

G Sharma, A Rajesh, L Ganesh Babu, E Mohan, "Three-Dimensional Localization in Anisotropic Wireless Sensor Networks Using Fuzzy Logic System", Adhoc & Sensor Wireless Networks, (2019) Vol.45 Issue No.1, P.No. 29-57.

B.K. Patle, Ganesh Babu L, Anish Pandey, D.R.K. Parhi, A. Jagadeesh,"A review: On path planning strategies for navigation of mobile robot", Defence Technology, Volume 15, Issue 4, August 2019, Pages 582-606.

Dr.A.Senthil Kumar, Dr.Venmathi A R ,L.Ganesh Babu, Dr.G. Suresh, "Smart Agriculture Robo With Leaf Diseases Detection Using IOT", European Journal of Molecular & Clinical Medicine, Volume 07, Issue 09, PP 2462-2469.

Qaysar Salih Mahdi, Idris Hadi Saleh, Ghani Hashim, Ganesh Babu Loganathan, "Evaluation of Robot Professor Technology in Teaching and Business", Information Technology in Industry, Volume 09, Issue 01, PP 1182-1194.

Mr.Manikandan Ganesan, Mrs.Ishwarya K. R, Mr. Demoz Lisanework, Mr.Ayenachew Hailu Mengiste, "Investigation On Autonomous Pesticide Spraying Robotic Vehicle In Agriculture Field", International Journal of Modern Agriculture, Volume 10, No.1, 2021 pp 382-386.

Ellappan Mohan, Arunachalam Rajesh , Gurram Sunitha , Reddy Madhavi Konduru , Janagaraj Avani-ja, Loganathan Ganesh Babu, "A deep neural network learning-based speckle noise removal technique for enhancing the quality of synthetic-aperture radar images", Concurrency And Computation-Practice & Experience, https://doi.org/10.1002/cpe.6239.