

Digital trust in the workplace: Testing a new instrument on a multicultural sample

MARKUS LAUNER, FATİH ÇETİN, JOANNA PALISZKIEWICZ

Abstract

DOI: 10.23762/FSO_VOL10_N01_2

The theme of digital trust is of the utmost importance during the digital transformation of our workplaces and society. Rapidly changing technological innovations disrupt lives and workplaces. Such a transformation influences an employee's feelings and self-esteem pertaining to their work and life. It changes the way people believe in the ability, reliability, and power of something or someone. This study suggests a new instrument for the measurement of digital trust in the workplace based on three dimensions: technology, people, and processes. We used a worldwide sample consisting of 5575 employees working in different countries and industries, employing a snowball sampling method. An online survey was used to collect data after translating items into different languages. In order to test the proposed model, the factorial structures and internal consistencies were calculated. The results showed that the 50-item questionnaire is a valid and reliable instrument for measuring the core structure of a digital trust model. Moreover, the affirmed 10 subdimensions present a constructional basis for understanding the main drivers of digital trust in the workplace. This study builds and tests a new three-dimensional model of digital trust in the workplace. Focusing on employees' trust perceptions of technologies, people, and processes in the workplace, this study presents three factors which are fundamental to answering the question of what influences employees' digital trust in the workplace. This study proposes a valid and reliable instrument for measuring digital trust in the workplace in different environments.

Key words

digital trust, e-Trust, scale development, validity, reliability.

Markus Launer

e-mail: m-a.launer@ostfalia.de
Ostfalia University of Applied Sciences,
Germany

Fatih Çetin

e-mail: fcetin@ohu.edu.tr
Niğde Ömer Halisdemir University, Turkey

Joanna Palisziewicz¹

e-mail: joanna_paliszkiewicz@sggw.edu.pl
Warsaw University of Life Sciences,
Poland

¹ Corresponding author

Introduction

With the integration of digital technologies into all areas of business, such as Information and Communication Technologies (ICT), the Internet of Things, Artificial Intelligence, Virtual or Augmented Reality, blockchain, robotics, and automation, etc., the need for trust is becoming a fundamental factor for doing business and for people using these technologies as well (Charalambous et al., 2016; Alcazar, 2017; Ejdy, 2018; Amin et al., 2019; Ferrario et al., 2021; Rakowska, 2021; Intalar et al., 2021). From a human point of view, establishing a trusting relationship with others and with these technologies in the digital workplace is the key to individual and organisational cooperation and success (Lankton et al., 2015; Ettlie et al., 2017; Sindwani, 2020). In this respect, the unique characters of digital trust, indicating initiating and maintaining elements of any relationship, raises the fundamental question of our time: what influences employees' digital trust in the workplace?

The article aims to answer this question, present a new model, and test a newly created digital trust instrument. Although previous studies attempted to measure digital trust in Industry 4.0 technologies (Mubarak and Petraite, 2020), trust in people with computer-mediated technologies (Mackenzie, 2010), or human-computer trust (Gulati et al., 2019), we have not come across any study focusing on digital elements of the workplace environment and discussing individual perceptions of digital trust. In this paper, the meaning of trust and digital trust is presented. Next, the model is described as consisting of technology, people, and processes with their sub-dimensions. In the research section, the newly created instrument is tested on a multi-cultural sample. Finally, the discussion, conclusions, limitations, and future directions are presented.

1. Literature review

1.1. The concept of trust and digital trust

The concept of trust is a multidimensional phenomenon with different definitions, such as a personality trait (Rotter, 1967), a feeling (Gibb, 1978), a positive expectation (Rousseau et al., 1998: 395), a state of mind (Sako and Prices, 1992), or a willingness to accept a vulnerable situation (Bos et al., 2002). According to Nikodemowska-Wołowik et al. (2020), trust comprises reliability, longevity, business with a human face, high-quality products, and a commitment to local communities. From the relational perspective, trust is perceived in terms of individuals' expression of the belief that others a) will not act in a way that is harmful to the trusting firm, b) will act in such a way that is beneficial to the trusting firm, c) will act reliably, and d) will behave or respond in a predictable and mutually acceptable manner (Paliszkiewicz, 2014).

According to the interactions between individuals and their digital environment, digital trust is related to expectations, perceptions, and beliefs. Corritore et al. (2003: 740) describe digital trust as "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited." In turn, Wang and Jeong (2018: 163) present it as "general beliefs in online service providers that result in behavioral intentions." Pietrzak and Takala (2021) claim that it is "the measure of confidence which workers, consumers/buyers, partners and other stakeholders have in an organisation's ability to protect data and the privacy of individuals." According to a suggested model (Marcial and Launer, 2019) and our proposition, the definition of digital trust is "the general belief that technology, people, and processes act or are aligned in ways that will fulfill people's digital expectations, such as sense of confidence, security, or control to support the creation of a secure digital environment."

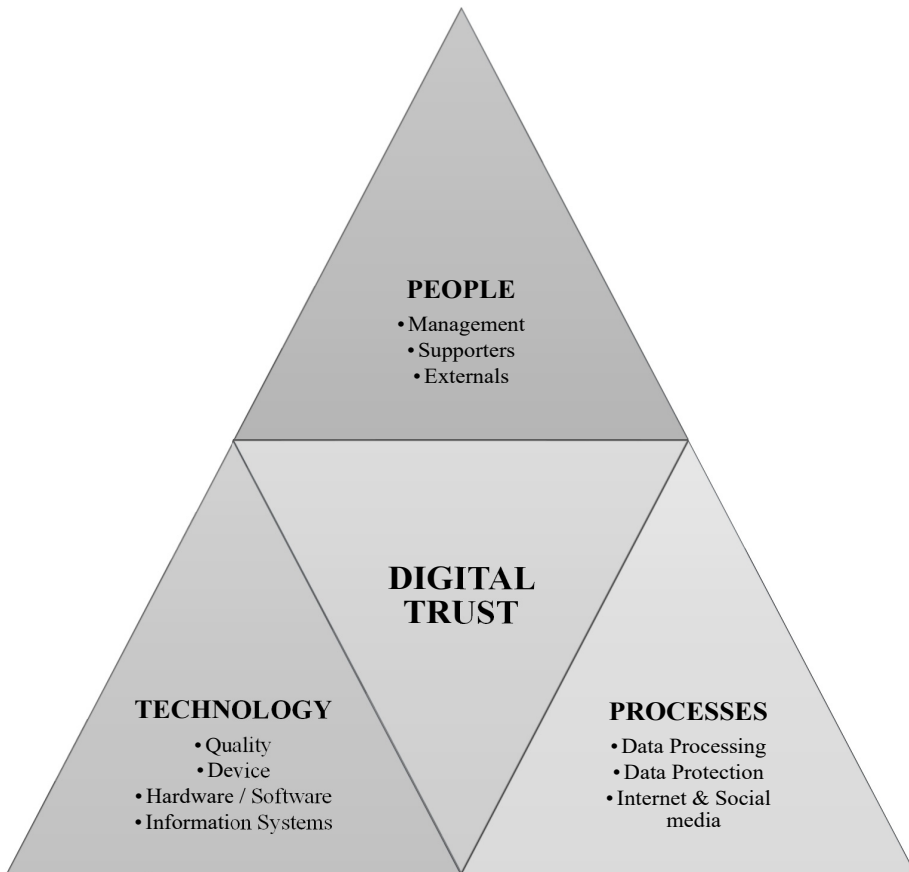
1.2. Digital trust in the workplace

Marcial and Launer (2019) suggest a framework for researching digital trust in the workplace. This framework, based on an input-output model in the principles of information systems, was used as a basis for the formulation of the conceptual framework of this study. For example, the level of trust in digital technology is one of the principles of information systems. Other theories taken into consideration in this study are: Forrester's Social Technographics Ladder, Technology Adoption Theory, Management Theory, Information Systems Theory, the Software Quality model, General Data Protection Regulation Principles, Digital Citizenship Principles, and Caldicott Principles. Thus, the level of digital trust is measured in terms of Technology, People, and Processes (PWC, nd.). Covering key mechanisms of digital trust in the workplace, this model originally proposes different interrelated factors. The distal factors are demographical variables, technological profiles, employment background, technology integration, decision-making styles, and personality. The proximate factors refer to the technology used, people involved, and the digitalisation process in the workplace. These factors cover and structure the key mechanisms of digital

trust in the workplace in a practicable way for practice and provide a well-founded theoretical basis for future research:

- **Technology:** The technology factor is employees' perceived trust in the reliability and effectiveness of the results of performed actions of technological artifacts, such as the quality of technologies, the devices used in the workplace, the hardware and software systems, and the information systems.
- **People:** The people factor is employees' perceived trust in other people in the online platforms in the workplace or environment, such as managers from different managerial levels, co-workers, supporting and technical employees, and also people from the immediate external environment such as customers, suppliers, and stakeholders.
- **Processes:** The processes factor is employees' perceived trust in the accuracy and success of the data collection, processing, and protection systems in the workplace or between companies, such as data processing, data protection, and the Internet and social media.

In the conceptual model, three factors were considered: technology, people, and processes. The model is presented in Figure 1.

Figure 1. Model of digital trust in the workplace

Source: own elaboration

1.2.1. Digital trust in technology

Depending on the concept of trust, the technology factor is associated with the capabilities of the technologies to perform a particular action (Castelfranchi and Falcone, 1998; Taddeo, 2010; Corritore et al., 2003; Alsmairat, 2021). In this framework, the capabilities or competencies of technologies construct trust according to certain expectations of individuals. In the workplace, employees' perceived trust is the reliability and effectiveness of the results of performed actions of technological artifacts. For instance, a copier that produces a quality product for a customer is thought of as trustworthy in terms of meeting expectations, or web site fa-

cilities that inspire customers' buying behavior are considered a reliable virtual location for advertising.

The technology components in this study are related to quality, electronic devices provided by the company either for official or personal use, hardware and software systems installed, and information systems implemented in the workplace (Karri et al., 2010; Mcknight et al., 2011; Moldabekova et al., 2020). The quality describes the consumer or client benefits and values, the integrity of processes, control and security, data accuracy, performance, reliability, and business continuity (Tehranipoor and Wang, 2011; Mishra et al., 2017). The devices provided by the company

can be tablets, laptop computers, smartwatches, and other smart wearable devices (Kirs and Bagchi, 2012; Stair and Reynolds, 2021). Hardware and software dimensions are also related to ID systems in daily time recording, doors, gates, and others, entering and exiting the company or organisation, ID systems in printing and duplication services, email tracking (Reed and Jain, 2015) and monitoring systems (Staples, 2014).

1.2.2. Digital trust in people

People are an indispensable element for the effective operation of all electronic systems in the workplace (O'Brien and Marakas, 2011). Individuals use digital technologies to communicate with each other, such as email, chats, and messenger services. Therefore, trust is an important factor when working with colleagues within your own or external organisation, in hierarchical, conventional, or virtual teams – the so-called “trust at the click of a mouse” (Wilson et al., 2006; Ebrahim et al., 2009; Breuer and Hertel, 2017).

The digital trust of people in this study depends on the colleagues they are working with at their workplace, from top-level management to front line managers, employees dealing with IT and data support services (internal department or external services), and managers dealing with external entities from customers and suppliers to service providers and governments. In the meantime, the growing digital collaborative and social nature of digital workplaces is reflected in the development of trusted virtual teams and digital teamwork, which is an important basis for the success and performance of an organisation (Jarvenpaa et al., 2004; Peters and Karren, 2009; Bennett and Bierema, 2010). Furthermore, most employees deal not only with people within the company, but work and communicate with external entities and environments (Dwyer, 2011). According to the supply chain approach, these can be customers, clients and suppliers, logistics

and other service providers (consulting / accounting / IT / taxes), or all kinds of wholesalers working with electronic trading systems or platforms (Launer et al., 2019).

1.2.3. Digital trust in processes

The processes factor is the accuracy and success of the collection, processing, and protection of data in the workplace or between companies. From the evolutionary perspective, digitalised processes are a kind of indicator of how trust has gradually been developed through ongoing digital interactions (Hart and Saunders, 1997). Therefore, all these processes of transforming the data from collection to protection are becoming the building blocks of establishing digital trust. For instance, Enterprise Resource Planning is used to manage and integrate data in business systems, or data protection systems are used to manage privacy concerns or the security of personal or organisational data.

For the processes factor in this study, the level of digital trust is determined as data processing operations, data protection practices, and the use of the Internet and social media. Organisations try to maximise the quality of processes including input-output transformation procedures in the workplace such as automation systems, workflow management, inventory management, etc. The accuracy, timeliness, and quality of these digital applications positively influence users' level of digital trust (Rita et al., 2019; Chakravorti et al., 2021). Another factor for establishing digital trust is online security measures with a high level of data privacy and data protection (Cecere and Rochelandet, 2013; Voigt and von dem Bussche, 2017; Pinkham, 2019). Lastly, the Internet and social media permitting employees to enable knowledge transfer, form virtual social capital, maintain professional networks, reduce uncertainties, etc. are prerequisite factors in building trust for the purposes of organisational communication and collaboration (Valenzuela et al., 2009; Cao et al., 2016).

2. Methodology

2.1. Instrument and participants

The questionnaire in this study was part of the EU-funded research project “Digital Trust and Teamwork” based on the definitions by Launer (2014). A follow-up project was conducted with 30 researchers from schools in Europe, the USA, Latin America, Africa, and Asia named “Digital Trust @ the Workplace”, dubbed “eTrust”. Based on the proposed model of digital trust in the workplace, the questions were generated by Marcial and Launer (2019), focusing on the digital environment in the workplace, such as technologies, devices, data processing procedures, people in the workplace, etc. The questions related to individual perceptions of the degree of trust in different factors in the workplace. A total of 103 items were generated for measuring three main digital environmental factors, namely technology, people, and processes. An electronic questionnaire was used to collect data by means of a snowball sampling method through the international personal network of the authors. In order to comply with European data protection rules, individuals were invited to participate in the online questionnaire on a voluntary basis and with a guarantee of confidentiality. The questionnaire was developed in English. The English version of the questionnaire was evaluated by a Teaching English to Speakers of Other Languages (TESOL) expert and was revised based on TESOL standards. Subsequently, qualified bilingual professionals were commissioned to translate the questionnaires into 13 different languages (Simplified Chinese, Traditional Chinese, Japanese, Spanish, Portuguese, Vietnamese, German, Russian, Polish, Romanian, Slovenian, and Thai) by field experts (professors and postdoctoral researchers) from related countries. The questionnaire was pre-tested with the calculation of test-retest reliability coefficients and the internal consistency of the proposed sur-

vey questionnaire. The measurement of the test-retest reliability was done in Germany ($n=51$) and the Philippines ($n=32$). The internal consistency of the questionnaire was measured through the pretesting ($n=376$) of the survey in China, Japan, South Korea, Paraguay, Russia, Brazil, Thailand, USA, and the United Kingdom from June to November 2019 (Marcial and Launer, 2021).

The participants in the study were 5574 employees working in 43 different industries from over 30 countries. Of the participants, 41.2% were female, 8.4% were LGBTQ, and 50.3% were male. Their age group percentage distributions were as follows: 1% were aged 18 or younger, 24.2% were aged between 19 and 28, 24.5% were aged between 29 and 38, 28.7% were aged between 39 and 48, 19% were aged between 49 and 58, and 2.5% were 59 or older. In terms of marital status, 47.8% were single, 43.5% were married, 7.9% were separated or divorced, and 0.8% were widowed. The majority of them had earned a bachelor's degree (36.5%), a master's degree (32%), or a Ph.D. (12.4%). In terms of the distribution of professional experience, 9.3% had less than one year of experience, 19.7% from one to three years, 40.3% from four to 10 years, 18% from 11 to 20 years, 6.6% from 21 to 30 years, 1.3 % from 31 to 40 years, and 0.3% more than 40 years. Their employment status was mostly permanent or regular (85.8%).

The questionnaire originally consisted of 103 items measuring three main factors (48 items for technology, 22 items for people, and 33 for processes) and 10 sub-dimensions. Since most of the responses remained incomplete, six open-ended questions, including the “other” option, were excluded from the questionnaire. The technology factor was formed with the following sub-dimensions: quality (17 items), device (4 items), hardware-software systems (8 items), and information systems (15 items). The people factor was formed with the sub-dimensions of management (6 items), supporters (5 items), and

externals (9 items). The process factor was formed with the sub-dimensions of data processing (15 items), data protection (8 items), and the Internet & social media (10 items). All the questions were measured on a four-point rating scale ranging from 'strongly agree' (1) to 'strongly disagree' (4). Thus, the increasing values show a higher level of trust in the related dimension.

2.2. Statistical procedures

The internal structure of a measurement instrument indicates information about the validity of the observed scores. The observed level in a certain sub-dimension of digital trust shows the relationship between items and theoretical factors (e.g. technology, people, or processes). Factor analysis is the most frequently used method for collecting evidence of an instrument's internal structure to assess factorial pattern and validity. In general, Explanatory Factor Analysis (EFA) presents *a priori* information to identify the latent factorial structures and construct validity. In most cases, the goal is simply to take a large set of variables and decrease them to a more manageable number while preserving the original variances to the greatest possible extent. In terms of the existing research, one of the purposes is to test the multidimensionality of the instrument (Digital Trust Scale). The EFA is based on three main decisions: (1) the factor extraction model, (2) the number of factors retained, and (3) the method used to rotate factors. When it comes to exploring the components, Principle Component Analysis (PCA) is the most popular technique for understanding the latent variables that explain the relations among the measured variables. We have selected the criteria of "eigenvalues greater than one" for determining the number of factors since it provides the most interpretable solution in terms of explained variance in a particular structure. Lastly, the more interpretable solution requires rotation analysis based on the relations among factorial patterns. While the

orthogonal rotation assumes that factors are uncorrelated, the oblique rotation assumes correlated factors. The varimax, as one of the orthogonal rotation techniques, attempts to maximise the variance of squared loadings on a factor. Accordingly, we first used EFA with PCA, eigenvalue criteria, and varimax rotation analysis to reduce the number of items, explore latent structures, and reach the most variance explained by assuming uncorrelated factors by employing the SPSS v24 programme.

However, once the items are primarily determined, a Confirmatory Factor Analysis (CFA) is needed to support the measurement model and also provide evidence of the convergent and discriminate structure of the instrument. The CFA is based on latent variable structures that explain the variation and covariation among observed variables. The normality, a sufficient sample size, and a correct prior model are the main assumptions of the CFA. After providing these assumptions, the maximum likelihood model estimation method was used to estimate parameters that best explain the observed data by using the AMOS v23 programme. Furthermore, the following fit indices were employed to evaluate the goodness of the models: the ratio of chi-square to degrees of freedom (χ^2/df , as low as 2 or as high as 5 to indicate a reasonable fit), Comparative Fix Index (CFI, higher than 0.9 or close to 0.95 indicates a good fit), the Tucker-Lewis Index (TLI, higher than 0.9 or close to 0.95 indicates a good fit), and Root Mean Square Error of Approximation (RMSEA, less than or equal to .05 indicates a good model) (Marsh and Hocevar, 1985; Hu and Bentler, 1999; Hooper et al., 2008).

3. Research results

In order to explore the factorial pattern of the instrument, an EFA was conducted on the entire sample ($n = 5574$) using SPSS software (Table 1). The criteria for factor selection included $> .30$ as the minimum

consideration level in the analysis. In the first analysis (see Model 1), 11 factors were extracted from 97 items, explaining a 57.6% variance of the structure by ranging factor loadings from .32 to .73. Since many items were cross-loaded on more than one factor, we excluded inconsistent items one by one and reanalysed the model until an admissible result was reached. After exclud-

ing 47 inconsistent items, 10 factors were extracted from 50 items, explaining 67.2% of the variance of the structure by ranging factor loadings from .37 to .79 (see Model 2). The first modelling approach aimed to identify an acceptable factor pattern and decrease the number of items by excluding the inconsistencies.

Table 1. EFA analyses

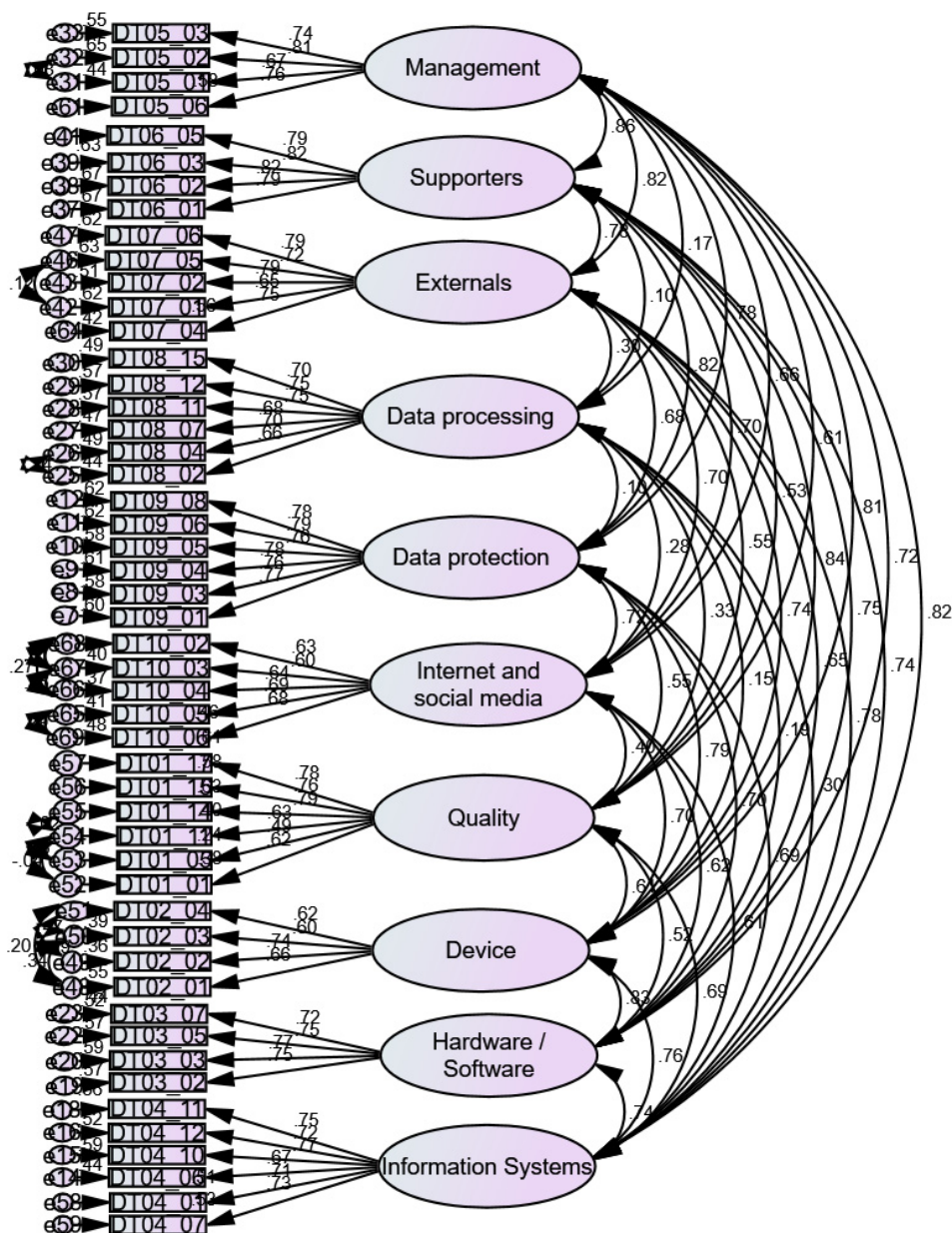
	Analy- sis	Number of items	Number of factors	Factor loadings	Communalities	Eigenvalues	Explained variances
Model 1	EFA	97 items *	11	from .32 to .73	from .57 to .86	from 1.12 to 30.81	57.6%
Model 2	EFA	50 items **	10	from .37 to .79	from .61 to .89	from 1.02 to 18.70	67.2%

Source: own elaboration

After determining the items and factors, CFA was used to confirm the measurement model and test the convergent and discriminant structure using the programme Amos (Table 2). The explored 10 sub-dimensions with 50 items were included as latent and observed variables in the model (see Model 3). The results of this model presented an unacceptable fit with producing a higher level of chi-square divided by degree of freedom, even though other values were acceptable ($X^2/df=8.12$, CFI=.95, TLI=.94, RMSEA=.036). In this situation, the items

that create inconsistency were explored with the help of modification suggestions of the statistical programme. Then, starting from the higher values and testing the model at every turn, these item error variances in the same factor were correlated to decrease the chi-square value. Ultimately, the acceptable fit indices were found after generating 14 paired item error variances in Model 4 ($X^2/df=4.99$, CFI=.97, TLI=.97, RMSEA=.027). This result confirmed the 10-factor structure of the measurement instrument (Figure 1).

Figure 1. The CFA results



Source: own elaboration

Further to these results, we tested the confirmed structure on three different sub-samples from the entire sample to increase

the generalisability. For this purpose, three different samples (approximately 33% of the total sample) were randomly selected.

The confirmed structure was tested on each sample (Models 5, 6, and 7) and found acceptable fit indices (the values ranged from: $X^2/df=2.51$ to 2.63 , $CFI=.96$ to $.97$, $TLI=.96$ to $.97$, $RMSEA=.029$ to $.030$). All these findings supported the measurement model and also provided evidence of the structure of the instrument.

Table 2. CFA analyses

	Sample (n)	Analysis	Number of items	Number of factors	Factor loadings	Fit indices
Model 3	Total Sample-edited (5574)	CFA	50 items	10	from 52 to .82	$X^2/df=8.12$, $CFI=.95$, $TLI=.94$ $RMSEA=.036$
Model 4	Total Sample-edited & modified (5574)	CFA	50 items ***	10	from 49 to .82	$X^2/df=4.99$, $CFI=.97$, $TLI=.97$ $RMSEA=.027$
Model 5	Random sample 1 (1860)	CFA	50 items ***	10	from 44 to .82	$X^2/df=2.51$, $CFI=.97$, $TLI=.96$ $RMSEA=.029$
Model 6	Random sample 2 (1825)	CFA	50 items ***	10	from 49 to .83	$X^2/df=2.52$, $CFI=.97$, $TLI=.96$ $RMSEA=.029$
Model 7	Random sample 3 (1812)	CFA	50 items ***	10	from 46 to .83	$X^2/df=2.63$, $CFI=.96$, $TLI=.96$ $RMSEA=.030$

* Excluded 6 items including the option "other", ** Excluded 47 inconsistent items, *** 14 error variances paired.

Source: own elaboration

The item codes in the measurement model and the statistics were presented in Table 3. The item means ranged from 2.35 to 3.31 (SD ranged from .77 to .99), and the corrected item total correlations ranged from .24 to .69. The skewness (ranged from -1.09 to .14) and kurtosis (ranged from -1.25 to .53) statistics were at acceptable levels for the univariate normality. The 50-item Cronbach's Alpha coefficient is .96., and the coefficients of sub-dimensions are: .86 for Quality, .81 for Device, .87 for Hardware

Software, .87 for Information Systems, .88 for Management, Supporters, .83 for Externals, .86 for Data Processing, .90 for Data Protection, .88 for Internet and Social Media. Furthermore, the grand mean of digital trust was 2.935 (SD=.88), with 3.03 for Technology (SD=.87), 3.00 for People (SD=.85), and 2.74 for Process (SD=.91). All results indicated that the instrument is a valid and reliable measurement for determining the individual level of digital trust in the workplace.

Table 3. Item statistics for the digital trust instrument

Dimension	Factor	Item code	Mean	SD	CITC	CAIID	Min	Max	Sw.	Kr.
Technology	Quality	DT01_01	3.223	0.81	.458	.958	1.00	4.00	-.848	.070
	Quality	DT01_05	2.979	0.89	.412	.959	1.00	4.00	-.558	-.464
	Quality	DT01_11	3.203	0.82	.496	.958	1.00	4.00	-.787	-.133
	Quality	DT01_14	3.310	0.82	.543	.958	1.00	4.00	-1.096	.530
	Quality	DT01_15	3.206	0.85	.521	.958	1.00	4.00	-.882	.005
	Quality	DT01_17	3.281	0.83	.517	.958	1.00	4.00	-.993	.234
	Device	DT02_01	2.921	0.88	.581	.958	1.00	4.00	-.536	-.329
	Device	DT02_02	3.214	0.92	.621	.958	1.00	4.00	-1.065	.221
	Device	DT02_03	2.582	0.94	.557	.958	1.00	4.00	-.065	-.730
	Device	DT02_04	2.704	0.98	.592	.958	1.00	4.00	-.295	-.808
	Hardware Software	DT03_02	2.985	0.90	.611	.958	1.00	4.00	-.699	-.923
	Hardware Software	DT03_03	3.080	0.92	.594	.958	1.00	4.00	-.823	-.562
	Hardware Software	DT03_05	2.991	0.89	.608	.958	1.00	4.00	-.680	-.857
	Hardware Software	DT03_07	2.959	0.91	.603	.958	1.00	4.00	-.642	-.927
	Information Systems	DT04_01	3.128	0.77	.627	.958	1.00	4.00	-.625	-.065
	Information Systems	DT04_06	3.127	0.84	.565	.958	1.00	4.00	-.836	.136
	Information Systems	DT04_07	2.993	0.80	.656	.958	1.00	4.00	-.566	-.023
	Information Systems	DT04_10	3.043	0.81	.652	.958	1.00	4.00	-.663	.064
	Information Systems	DT04_11	3.023	0.81	.650	.958	1.00	4.00	-.562	-.148
	Information Systems	DT04_12	3.150	0.84	.607	.958	1.00	4.00	-.825	.064
People	Management	DT05_01	3.160	0.82	.576	.958	1.00	4.00	-.729	-.144
	Management	DT05_02	3.066	0.90	.699	.957	1.00	4.00	-.735	-.241
	Management	DT05_03	3.048	0.84	.628	.958	1.00	4.00	-.543	-.396
	Management	DT05_06	3.072	0.87	.675	.957	1.00	4.00	-.754	-.096
	Supporters	DT06_01	2.999	0.87	.673	.957	1.00	4.00	-.562	-.405
	Supporters	DT06_02	3.001	0.89	.697	.957	1.00	4.00	-.610	-.383
	Supporters	DT06_03	3.014	0.87	.677	.957	1.00	4.00	-.595	-.363
	Supporters	DT06_05	2.945	0.89	.689	.957	1.00	4.00	-.554	-.395
	Externals	DT07_01	3.024	0.79	.563	.958	1.00	4.00	-.518	-.164
	Externals	DT07_02	2.903	0.85	.660	.958	1.00	4.00	-.478	-.273
	Externals	DT07_04	2.810	0.85	.651	.958	1.00	4.00	-.391	-.315
	Externals	DT07_05	2.953	0.79	.613	.958	1.00	4.00	-.523	.044
	Externals	DT07_06	2.929	0.83	.658	.958	1.00	4.00	-.466	-.246

Dimension	Factor	Item code	Mean	SD	CITC	CAIID	Min	Max	Sw.	Kr.
Process	Data Processing	DT08_02	2.581	0.99	.246	.959	1.00	4.00	-.123	-.972
	Data Processing	DT08_04	2.611	0.84	.293	.959	1.00	4.00	-.144	-1.027
	Data Processing	DT08_07	2.771	0.96	.301	.959	1.00	4.00	-.339	-.811
	Data Processing	DT08_11	2.679	0.98	.297	.959	1.00	4.00	-.229	-.924
	Data Processing	DT08_12	2.609	0.97	.266	.959	1.00	4.00	-.144	-.917
	Data Processing	DT08_15	2.611	0.88	.243	.959	1.00	4.00	-.158	-1.054
	Data Protection	DT09_01	3.110	0.84	.623	.958	1.00	4.00	-.654	-.309
	Data Protection	DT09_03	3.040	0.89	.616	.958	1.00	4.00	-.611	-.435
	Data Protection	DT09_04	3.018	0.91	.640	.958	1.00	4.00	-.609	-.489
	Data Protection	DT09_05	2.979	0.91	.634	.958	1.00	4.00	-.546	-.564
	Data Protection	DT09_06	3.021	0.90	.655	.958	1.00	4.00	-.607	-.436
	Data Protection	DT09_08	3.010	0.90	.651	.958	1.00	4.00	-.607	-.450
	Internet & Social Media	DT10_02	2.476	0.88	.508	.958	1.00	4.00	-.042	-1.116
	Internet & Social Media	DT10_03	2.391	0.87	.470	.958	1.00	4.00	.087	-1.217
	Internet & Social Media	DT10_04	2.350	0.83	.492	.958	1.00	4.00	.146	-1.252
	Internet & Social Media	DT10_05	2.734	0.99	.552	.958	1.00	4.00	-.295	-.924
	Internet & Social Media	DT10_06	2.756	0.98	.551	.958	1.00	4.00	-.304	-.914

Note: CITC = Corrected Item total correlation, CAIID = Cronbach's Alpha If Item Deleted, Sw. = Skewness, Kr. = Kurtosis, the 50-item Cronbach's Alpha Reliability is .96, and the grand mean is 2.935.

Source: own elaboration

Since our research design is cross-sectional from a single source, we have also checked whether common method variance is an issue for the confidence of our results. Although Harman's single factor test is not very strong in terms of detecting common method bias, this test was used with maximum likelihood, unrotated factor solution, and extracting one-factor options in the SPSS programme. Based on the result, the explained variance was calculated as 46.12, less than the recommended threshold value of .50, indicating that the common method variance is not a significant problem in the context of the results.

4. Discussion and Conclusions

Based on individual expectations, perceptions, and beliefs, digital trust refers to the interactions between individuals and their digital environment. Even though it is an uncertain, complex, and ambiguous concept, digital trust is becoming a key phenomenon in our digitalised workplace and life. Since today's digital workplace is the key to individual and organisational cooperation and success, the main purpose of this research is to explore the concept of digital trust and related factors in the workplace, departing from the employees' point of view of trust. For the initial concept, a new digital trust model suggested by Marcial and Launer

(2019) has been explained within the framework of Technology, People, and Processes factors. This model emphasises employees' perceived trust in these three factors in terms of meeting their digital expectations in the workplace toward a secure digital environment. Covering key mechanisms of digital trust in the workplace, this model uncovers three basic factors which are the core mechanisms in constructing and sustaining trust beliefs.

The study has also tested and confirmed a digital trust instrument with its three basic factors, including 10 subdimensions in total, namely Quality, Device, Hardware/Software, and Information Systems subdimensions for the Technology factor; Management, Supporters, and Externals subdimensions for the People factor; and Data Processing, Data Protection, and Internet & Social media subdimensions for the Processes factor. The explanatory and confirmatory factor analyses have been conducted to test the newly developed instrument on a worldwide diversified sample. After selecting three random sub-samples from the total sample, the confirmatory factor analyses have been re-conducted to increase the generalisability. In addition, the item statistics and correlations indicate acceptable values in terms of the normality and consistency of the instrument. Lastly, the Cronbach's Alpha coefficients of all of the subdimensions have been calculated and confirmed the reliability of the instrument. All these results have confirmed that this instrument is reliable and valid for measuring the core factors and subdimensions of the proposed model. Thus, this research has primarily presented pieces of evidence that digital trust is a generalisable multidimensional construct among employees working in different industries and cultures.

4.1. Implications

The findings of this study have several theoretical implications. The main contribution is building and testing a new three-dimen-

sional model of digital trust in the workplace. Focusing on employees' trust perceptions of technologies, people, and processes in the workplace, this study presents three factors which are fundamental to answering the question of "what influences employees' digital trust in the workplace?" Furthermore, by testing these fundamental factors on a diversified sample, this study proposes a valid and reliable instrument for measuring digital trust in the workplace in different environments.

This research can be helpful for managers in creating an awareness of the factors that influence the level of digital trust in the workplace. It addresses different segments of the organisation and can help protect business and enable profitable digital growth, thanks to the consideration of factors that influence the development of digital trust. Managers should have this knowledge to appropriately manage people and propose appropriate training and access to knowledge. The proposed Digital Trust model also offers the flexibility to respond to the specific needs of the organisation.

4.2. Limitations and future directions of research

There are also certain limitations inherent in the research. The number of items in the original scale may influence participants' responses, since it takes 30 to 45 minutes to finish the questionnaire. The selected response type may limit the scope of interpretation, since it leaves participants with a forced response. Although the research has an advantage in generalising the results with a culturally and industrially diversified group of employees, the unequal number of these groups may influence the general findings.

In general, the study is based on a quantitative approach. Future studies may benefit from using a mixed method, combining quantitative and qualitative research to explore the topic. Secondly, a snowball sample was used to collect data for the study.

Although snowball sampling is an accepted standard process in research design, a random sample may have produced improved generalisability of the findings. In future research, it would be worth taking this into consideration. Third, in this study, we used the self-reporting method, which is widely used in collecting data in this field. In selecting the measures for this study, we made every effort to include a uniform view in the wording for the items of each construct to improve the validity of self-reported data. However, self-reported data can have potential sources of bias, such as subjects' selective memory or even exaggeration, that may influence the generalisability of the results. In future studies, this should be improved.

Lastly, the literature review and findings of this research inspired the authors to ask the following questions for future study: How does digital trust depend on the characteristics of individuals and organisational culture? How can we build and rebuild digital trust? Did digital trust increase during the COVID-19 pandemic? Research related to digital trust in different countries is in its infancy; therefore, it requires further attention for building theory and practice in the future.

Funding

The research was funded by the European Union and the State of Lower Saxony in the framework of the EFRE research project "Digital Trust and Teamwork" (ZW6-85007939). A follow-up project was conducted which was entitled "Digital Trust @ the Workplace" financed by Ostfalia University of Applied Sciences, Faculty of Trade and Social Sciences (H).

Acknowledgments

We acknowledge all participating professors and researchers of the personal network of Prof. Markus Launer (Head). Co-Head of

the study of digital trust in the workplace was Prof. Dave Marcial (Philippines) from Silliman University in Dumaguete. He was also visiting professor to Ostfalia University of Applied Sciences in 2019/2020. For the translation and distribution of the questionnaire, we thank (in alphabetical order by country): Argentina: Prof. Liliana Bianchi (University of Buenos Aires), Buenos Aires, and Prof. Sebastian Torres (Universidad Nacional de Quilmes), Quilmes; Brasil: Prof. Valter de Assis Moreno Jr (Rio de Janeiro State University), Rio de Janeiro; Chile: Prof. Eduardo Kohler and Prof. Erich Spencer (University de Chile), Santiago de Chile; China: Prof. Bo Aquila Michael Yang (Beijing Open University), Peking, and Prof. Wenming Yang (Shenzhen Polytechnic University); Estonia: Prof. Harald Kitzmann (Tallinn University of Applied Sciences), Tallinn; Ghana: Dr. Kobby Mensah (University of Ghana Business School), Accra; India: Prof. Himadri Roy Chaudhuri (Xavier School of Management), Jamshedpur; Japan: Prof. Yasushi Kuno (University of Electro-Communication), Tokyo, and Ph.D. cand. Natsuko Uchida (Ferris University), Yokohama; Kenya: Dr. George Katete (University of Nairobi), Nairobi; Korea: Prof. Kim Gun-do (Semyung University), Semyung, and Prof. Joeffrey Maddatu Calimag (University of Ulsan), Ulsan; Paraguay: Ph.D. cand. Simon Zalimben (Prof. at the Universidad Católica Nuestra Señora de la Asunción) and Ph.D. cand. Thorben Stemme (Prof. at the Americana University), Asunción; Philippines: Prof. Eric Capistrano (University of the Philippines), Manila, and Prof. Joane Serrano (University of the Philippines Open University), Los Banos, and Prof. Virgilio Manzano (Pangasinan State University), Pangasinan; Poland: Dr. Anna Jasiulewicz (Warsaw University of Life Sciences), Warsaw, and Dr. Kamila Malewska (Poznań University of Economics and Business), Poznań; Romania: Dr. Sebastian Vaida (Babeş-

Bolyai University), Cluj-Napoca; Russia: Prof. Viktoria Yatsenko (Bauman Moscow State Technical University), Moscow; Slovakia: Dr. Eva Ballová Mikušková (Slovak Academy of Sciences), Bratislava; Switzerland: Christian Weber (ZHAW), Zürich; Taiwan: Prof. Victor Chen (National Cheng Kung University), Tainan; Thailand: Prof. Chanita Rukspollmuang and Prof. Jaratdao Suwan (Siam University), Bangkok; USA: Prof. Emre Yetgin (Rider University), Lawrenceville, NJ; Vietnam: Prof. Thennie Mariano (Philippines E-Learning Society), Ho Chi Minh City. From Ostfalia University, we acknowledge our colleagues from the research project pertaining to digital trust and teamwork, Stephanie Borsych and Dirk Schneider, as well as Ph.D. Frithiof Svenson, Dierk Ohler, Michael Ferwagner, Lukas Alvermann, and Johanna Meyer.

References

- Alcazar, V. (2017), U.S.A.F. Data you can trust: Blockchain technology, *Air & Space Power Journal*, 31(2), 91-101. <https://doi.org/10.4236/ti.2021.123008>
- Alsmairat, A.K.M. (2021). Transformative supply chain drivers during Covid-19: A customer perspective, *Polish Journal of Management Studies*, 24(2), 9-23. <https://doi.org/10.17512/pjms.2021.24.2.01>
- Amin, F., Ahmad, A., Choi, G. S. (2019), Towards trust and friendliness approaches in the social internet of things, *Applied Sciences*, 9(1), 166. <https://doi.org/10.3390/app9010166>
- Bennett, E. E., Bierema, L. L. (2010), The ecology of virtual human resource development, *Advances in Developing Human Resources*, 12(6), 632-647. <https://doi.org/10.1177/1523422310394789>
- Bos, N., Olson, J., Gergle, D., Olson, G., Wright, Z. (2002), Effects of four computer-mediated communications channels on trust development, *ACM Conference on Human Factors and Computing Systems*, CHI Letters, 4, 135-140. <https://doi.org/10.1145/503376.503401>
- Breuer, C., Hertel, G. (2017), Vertrauen per Mausklick: Wie Vertrauen in virtuellen Teams entstehen kann, *Personal quarterly, Wissenschaftsjournal für die Praxis*, 69, 10-16.
- Cao, X., Guo, X., Vogel, D., Zhang, X. (2016), Exploring the influence of social media on employee work performance, *Internet Research*, 26(2), 529-545. <https://doi.org/10.1108/IntR-11-2014-0299>
- Castelfranchi, C., Falcone, R. (1998), Principles of trust for MAS: Cognitive anatomy, social importance, and quantification, 3rd International Conference on Multi-Agent Systems (ICMAS'98), Paris: IEEE Computer Society. <https://doi.org/10.1109/ICMAS.1998.699034>
- Cecere, G., Rochelandet, F. (2013), Privacy intrusiveness and web audiences: Empirical evidence, *Telecommunications Policy*, 37(10), 1004-1014. <https://doi.org/10.1016/j.telpol.2013.09.003>
- Chakravorti, B., Bhalla, A., Chaturvedi, R. S. (2021), How Digital Trust Varies Around the World, *Harvard Business Review*, retrieved from: <https://hbr.org/2021/02/how-digital-trust-varies-around-the-world> (accessed 17 January 2022).
- Charalambous, G., Fletcher, S., Webb, P. (2016), The development of a scale to evaluate trust in industrial human-robot collaboration, *International Journal of Social Robotics*, 8(2), 193-209. <https://doi.org/10.1007/s12369-015-0333-8>
- Corritore, C. L., Kracher, B., Wiedenbeck, S. (2003), On-line trust: concepts, evolving themes, a model, *International Journal of Human-Computer Studies*, 58, 737-758. [https://doi.org/10.1016/S1071-5819\(03\)00041-7](https://doi.org/10.1016/S1071-5819(03)00041-7)
- Dwyer, N. (2011), Traces of digital trust: An interactive design perspective, PhD thesis, School of Communication and the Arts, Faculty of Arts, Education and Human Development, Victoria University, Canada.
- Ebrahim, N.A., Ahmed, S., Taha, Z. (2009), Virtual Teams: A Literature Review, *Australian Journal of Basic and Applied Sciences*, 3(3), 2653-2669

- Ejdys, J. (2018), Building technology trust in ICT application at a university, *International Journal of Emerging Markets*, 13(5), 980-999. DOI: 10.1108/IJoEM-07-2017-0234
- Ettlie, J. E., Tucci, C., Gianiodis, P. T. (2017), Trust, integrated information technology and new product success, *European Journal of Innovation Management*, 20(3), 406-427. <https://doi.org/10.1108/EJIM-12-2015-0128>
- Ferrario, A., Loi, M., Viganò, E. (2021), Trust does not need to be human: It is possible to trust medical AI, *Journal of Medical Ethics*, 47(6), 437-438. <http://dx.doi.org/10.1136/medethics-2020-106922>
- Gibb J.R., (1978), *Trust, a New View of Personal and Organizational Development*, Los Angeles: Guild of Tutors Press.
- Gulati, S., Sousa, S., Lamas, D. (2019), Design, development and evaluation of a human-computer trust scale, *Behaviour & Information Technology*, 38(10), 1004-1015. <https://doi.org/10.1080/0144929X.2019.1656779>
- Hart, P., Saunders, C. (1997), Power and trust: Critical factors in the adoption and use of electronic data interchange, *Organizational Science*, 8(1), 2-42, <https://doi.org/10.1287/orsc.8.1.23>
- Hooper, D., Coughlan, J., Mullen, M. (2008), Structural Equation Modelling: Guidelines for Determining Model Fit, *Journal of Business Research Methods*, 6(1), 53-60. <https://doi.org/10.21427/D7CF7R>
- Hu, L., Bentler, P.M. (1999), Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, *Structural Equation Modeling*, 6, 1-55, <https://doi.org/10.1080/10705519909540118>
- Intalar, N., Chumnumporn, K., Jeenanunta, Ch., Tunpan, A. (2021), Towards Industry 4.0: digital transformation of traditional safety shoes manufacturer in Thailand with a development of production tracking system, *Engineering Management in Production and Services*, 13(4), 79-94. doi: 10.2478/emj-2021-0033
- Jarvenpaa, S. L., Shaw, T. R., Staples, D. S. (2004), Toward Contextualized Theories of Trust: The Role of Trust in Global Virtual Teams, *Information Systems Research*, 15(3), 250-267. <https://doi.org/10.1287/isre.1040.0028>
- Karri, R., Rajendran, J., Rosenfeld, K., Tehranipoor, M. (2010), Trustworthy Hardware: Identifying and Classifying Hardware Trojans, *Computer*, 43(10), 39-46. <https://doi.org/10.1109/MC.2010.299>
- Kirs, P., Bagchi, K. (2012), The impact of trust and changes in trust: A national comparison of individual adoptions of information and communication technologies and related phenomenon, *International Journal of Information Management*, 32(5), 431-441. <https://doi.org/10.1016/j.ijinfomgt.2012.02.003>
- Lankton, N. K., McKnight, D. H., Tripp, J. (2015), Technology, humanness, and trust: Rethinking trust in technology, *Journal of the Association for Information Systems*, 16(10), 880-918. <https://doi.org/10.17705/1jais.00411>
- Launer, M. (2014), Definitionen für Handels- und Logistikdienstleister: Definitionen für handelsnahe und -spezifische sowie logistiknahe und -spezifische Dienstleistungen, Amazon Online.
- Launer, M., Borsych, S., Alvermann, L. (2019), *Digitales Vertrauen und Teamwork (DigVertr)*, part 2: Digitales Vertrauen Business to Business in Supply Chains, Working Paper No. 8, Ostfalia University, Germany.
- Mackenzie, M. L. (2010), Manager communication and workplace trust: Understanding manager and employee perceptions in the e-world, *International Journal of Information Management*, 30(6), 529-541. <https://doi.org/10.1016/j.ijinfomgt.2010.04.001>
- Marcial, D., Launer, M. (2019), Towards the Measurement of Digital Trust in the Workplace: A Proposed Framework, *International Journal of Scientific Engineering and Science*, 3(12), 1-7. <https://doi.org/10.5281/zenodo.3595295>
- Marcial, D., Launer, M. (2021), Test-retest Reliability and Internal Consistency of the Survey Questionnaire on Digital Trust in the Workplace, *Solid State Technology*, 64(2), 4369-4381.

- Marsh, H.W., Hocevar, D. (1985), Application of confirmatory factor analysis to the study of self-concept: First- and higher order factor models and their invariance across groups, *Psychological Bulletin*, 97(3), 562–582. <https://doi.org/10.1037/0033-2909.97.3.562>
- Mcknight, D.H., Carter, M., Thatcher, J.B., Clay, P.F. (2011), Trust in a specific technology: An investigation of its components and measures, *ACM Transactions on Management Information Systems*, 2(2), 20–44. <https://doi.org/10.1145/1985347.1985353>
- Mishra, P. Bhunia, S., Tehranipoor, M. (Eds.) (2017), *Hardware IP security and trust*, Cham: Springer.
- Moldabekova, A., Zhidebekkyzy, A., Akhmetkaliyeva, S., Baimukhanbetova, E. (2020), Advanced technologies in improving the management of logistics services: Bibliometric network analysis, *Polish Journal of Management Studies*, 21(1), 211–223. <https://doi.org/10.17512/pjms.2020.21.1.16>
- Mubarak, M.F., Petraite, M. (2020), Industry 4.0 technologies, digital trust and technological orientation: What matters in open innovation? *Technological Forecasting & Social Change*, 161. <https://doi.org/10.1016/j.techfore.2020.120332>
- Nikodemaska-Wołowik, A.M., Bednarz, J., Wach, D., Little, J.P., Kubik, M.A. (2020), Building aware and unaware consumers' trust towards family business: Evidence from Poland, *Entrepreneurial Business and Economics Review*, 8(3), 135–154. <https://doi.org/10.15678/EBER.2020.080308>
- O'Brien, J.A., Marakas, G.M. (2011), *Management Information Systems*, New York, NY: McGraw-Hill/Irwin.
- Paliszkievicz, J. (2010), Organizational trust – a critical review of the empirical research, *Proceedings of 2010 International Conference on Technology Innovation and Industrial Management*, 16–18 June 2010 Pattaya, Thailand.
- Peters, L., Karren, R. (2009), An examination of the roles of trust and functional diversity on virtual team performance ratings, *Group and Organization Management*, 34(4), 479–504. <https://doi.org/10.1177/1059601107312170>
- Pietrzak, P., Takala, J. (2021), Digital trust – a systematic literature review, *Forum Scientiae Oeconomia*, 9(3), 59–71. https://doi.org/10.23762/FSO_VOL9_NO3_4
- Pinkham, J. (2019), Data Protection. What's the Best Way to Build Digital Trust? Show Your Customers You Care About Their Data Privacy, *Security Intelligence*, retrieved from: <https://securityintelligence.com/posts/whats-the-best-way-to-build-digital-trust-show-your-customers-you-care-about-their-data-privacy/> (accessed 20 November 2021).
- PWC (nd), *Cybersecurity and Privacy, Together we're building a secure digital society*, retrieved from: <https://www.pwc.com/gx/en/issues/cybersecurity.html> (accessed 4 April 2021).
- Rakowska, W. (2021), Trust and other factors impacting the platform choice in sharing economy: A case from Poland, *International Entrepreneurship Review*, 7(3), 23–35. <https://doi.org/10.15678/IER.2021.0703.02>
- Reed, D., Jain, Y. (2015), DMA email tracking report 2014, *Journal of Direct Data Digit Marketing Practice*, 16, 184–192. <https://doi.org/10.1057/dddmp.2015.2>
- Rita, P., Oliveira, T., Farisa, A. (2019), The impact of e-service quality and customer satisfaction on customer behavior in online shopping, *Heliyon* 5(10). <https://doi.org/10.1016/j.heliyon.2019.e02690>
- Rotter, J. B., (1967), A New scale for the measurement of interpersonal trust, *Journal of Personality*, 35, 651–665. <https://doi.org/10.1111/j.1467-6494.1967.tb01454.x>
- Rousseau, D. M., Sitkin, S. B., Burt, R. S. Camerer, C. (1998), Not so different after all: A cross-discipline view of trust, *Academy of Management Review*, 23(3), 393–404. <https://doi.org/10.5465/amr.1998.926617>
- Sako, M., Prices, (1992), *Quality and Trust, Inter-firm Relations in Britain & Japan*, Cambridge: Cambridge University Press.
- Sindwani, R. (2020), Predictor of customer trust: Role of technology, *SCMS Journal of Indian Management*, 17(4), 77–88.

- Stair, R. Reynolds, G. (2021), Principles of Information Systems (Chapter 4), Hardware and Software systems, Cengage Learning Systems, 100-170.
- Staples, W.G. (2014), Everyday Surveillance: Vigilance and Visibility in Postmodern Life, Littlefield: Rowman.
- Taddeo, M. (2010), Modelling Trust in Artificial Agents, A First Step Toward the Analysis of e-Trust, Minds & Machines, 20, 243–257. <https://doi.org/10.1007/s11023-010-9201-3>
- Tehraniipoor, M., Wang, C. (2011), Introduction to hardware security and trust, Cham: Springer.
- Valenzuela, S., Park, N., Kee, K. F. (2009), Is There Social Capital in a Social Network Site?: Facebook Use and College Students' Life Satisfaction, Trust, and Participation, Journal of Computer Mediated Communication, 14, 875-901. <https://doi.org/10.1111/j.1083-6101.2009.01474.x>
- Voigt, P., von dem Bussche, A. (2017), The EU General Data Protection Regulation (GDPR). A Practical Guide, Cham: Springer.
- Wang, C. R., Jeong, M. (2018), What makes you choose Airbnb again? An examination of users' perceptions toward the website and their stay, International Journal of Hospital Management, 74, 162-170. <https://doi.org/10.1016/j.ijhm.2018.04.006>
- Wilson, J., Straus, S., Mc Evily, B. (2006), All in due time: The development of trust in computer-mediated and face-to-face teams, Organizational Behavior and Human Decision Processes, 99(1), 16-33. <https://doi.org/10.1016/j.obhdp.2005.08.001>

Markus Launer received his Ph.D. in Economics from the Tallinn University of Technology, Estonia, in the European Doctoral Programme. He earned his master's degree from the University of Mannheim, Germany. He is a professor of business administration and service management at Ostfalia University of Applied Sciences (Suderburg Campus), Germany. Markus researches in the fields of digitalisation and social sciences as well as sustainability and supply chains. Financed by the European Union and the state of Lower Saxony, Germany, he has undertaken research in two EU projects on digital trust and intuition in the workplace. In a follow-up study with 30 researchers, he conducted global research in 13 languages and 30 countries. He is the author of several publications including journal articles, book chapters, and proceedings. He organises an international Service Management Congress on an annual basis. ORCID no. 0000-0001-9384-0807.

Fatih Çetin is a professor of Management in the Department of Business Administration at Niğde Ömer Halisdemir University in Turkey. His research focuses on the field of positive organisational behaviour and knowledge management studies. He has authored over 100 publications including journal articles, book chapters, and proceedings. His recent research has appeared in the *Journal of Computer Information Systems*, *The Journal of General Psychology*, *Eurasian Business Review*, *Management Research Review*, and the 79th Annual Meeting of the Academy of Management. ORCID no. 0000-0002-2487-9553.

Joanna Paliszkievicz is a full professor at the Warsaw University of Life Sciences (WULS—SGGW), where she is the director of the Management Institute. She is also an adjunct professor at the University of Vaasa in Finland. She is renowned in Poland and abroad for her expertise in management issues: knowledge management and trust management. She has published over 220 papers/manuscripts and is the author/co-author/editor of 14 books. She has been a part of numerous scholarship endeavours in the United States, Ireland, Slovakia, Taiwan, the United Kingdom, and Hungary. She has actively participated in presenting research

results at various international conferences. Currently, she serves as the deputy editor-in-chief of the *Management and Production Engineering Review*. She is an associate editor for the *Journal of Computer Information Systems*, *Expert Systems with Applications* and *Intelligent Systems with Applications*. She is the vice-president of the Polish Association for Production Engineering. She also serves as chair of the International Cooperation in the European Business Club. She serves as the vice-president of the International Association for Computer Information Systems in the United States. She is a board member of the Intellectual Capital Accreditation Association, and is actively involved in participating in the scientific committees of many international conferences. She was named the 2013 Computer Educator of the Year by IACIS. ORCID no. 0000-0002-6250-0583.