

# Review of Digital Trust and its Future

Ritesh Thakur<sup>1</sup>[0009-0002-1400-2245], Ganesh Bhutkar<sup>1</sup>[0000-0002-3044-6471]

Shrikant Salve<sup>2</sup>[0000-0002-1794-3991]

<sup>1</sup> Vishwakarma Institute of Technology (VIT), Pune, India

<sup>2</sup> Indian Institute of Information Technology (IIIT), Pune, India

ritesh.thakur19@vit.edu

**Abstract.** The adoption of Information and Communication Technology (ICT) and the Internet leads to an increase in online interactions. ICT enables users from diverse backgrounds to connect and collaborate on domains like education, business and healthcare. For such domains, trust is necessary. Digital trust leads to the effective adoption of digital technology and user collaboration. This position paper consists of a literature review of 18 research papers on digital trust. The literature review focused on the needs and impact of digital trust, and trust properties. The research papers commonly defined digital trust as a binary relation. In many cases, the entities involved were unknown to each other. The review found uncertainties like these to be the originating point of digital trust. More user-oriented research on digital trust is needed. Understanding the effect of user interface design on digital trust would help system designers incorporate trust-enhancing designs and design patterns. The 'dark patterns', which cause more harm than good, and 'usable privacy and security' are identified as future directions for user-oriented research on digital trust.

**Keywords:** Digital Trust, Literature Review, Security, Sustainable Digitization, Dark Patterns, Usable Privacy.

## 1. Introduction

The world is undergoing a digital revolution, with traditional systems and processes being digitized daily. Interactions that were previously done in person are now being done using digital mediums such as e-commerce. Hermawan has highlighted how e-commerce is becoming the preferred method for shopping [4]. With the increase in e-commerce, security-related concerns have also increased. Hence, social factors like customer trust need to be translated into digital trust.

Research papers have presented definitions for digital trust, either in their context or from cited literature. Although the definitions are valid in the context of the research paper, they may not be valid in other contexts [1, 15]. Online interactions consist of entities or agents such as users, websites, digital platforms and others. The entities are categorized as trustors and trustees in digital trust interactions [8]. The trustor assesses the trustworthiness of the trustee and acts accordingly. Digital trust is most commonly defined as the 'measure of belief or confidence in the goodwill or benevo-

lence of digital entities' [2, 8, 14]. This literature review has been conducted to identify emerging trends and future directions related to digital trust. Such outcomes will help build sustainable progress of digital trust in the coming years.

## 2. Literature Review

The research work on digital trust has mainly focused on a literature review, which has been conducted using Google Scholar. This scholarly search consists of all English-language research papers. Search criteria of either 'digital trust' (the entire term) or both 'digital' and 'trust' separately being present in either the title, abstract or keywords are used. This literature review consists of 18 research papers, including 4 conference papers, 9 journal articles, 3 book chapters, a technical report and a PhD dissertation.

'Digital trust' and 'trust' have been used interchangeably in this paper. The need for digital trust and its impact varies according to context and level of interaction. For example, e-commerce platforms need digital trust to increase purchasing behavior [9], while digital information sources need trust to establish credibility. Hence, the '**Needs and Impact of Digital Trust**' section highlights the needs for digital trust and compares the domain-wise impacts of digital trust. The reviewed literature has proposed trust models, but the consensus between them has not been achieved. The comparison of the properties of digital trust has been performed to identify points of agreement and debate. Hence, the section '**Properties of Digital Trust**', compares trust properties, features and, the role of security and privacy in the models.

### 2.1. Needs and Impact of Digital Trust

In this section, the research papers related to 'Needs and Impact of Digital Trust', have been reviewed and a related summary is presented in table 1. In this table, NA stands for Not Available / Applicable.

The vital observations from entries in Table 1 are provided as follows:

- **Almost all the papers reviewed (13 out of 15 papers) have mentioned uncertainty as a necessary condition for digital trust.** When uncertain, users compare their confidence in the involved entities to the possible risks.
- **The majority of research papers (12 out of 15 papers) highlighted how users are unknown to each other and can't verify their identities / authenticity.**
  - Business and economics are the most common domains in the reviewed literature (5 out of 15 papers).
  - **Out of 15, 5 papers mentioned ubiquitous or pervasive computing as a key reason for need of digital trust.**
  - Other studies (3 out of 15 papers) cited the chaotic and complex nature of the Internet as a key reason for need of digital trust.

**Table 1.** Summary of the Needs and Impact of Digital Trust

Research Paper	Domain	Interaction with Unknown Entities	Trust arises from Uncertainty	Reason for Need of Digital Trust	Impact of Digital Trust
Pietrzak & Takala, 2021	NA	Yes	Yes	Chaotic nature of Internet	Purchase intent
Kozuch, 2021	NA	Yes	Yes	Chaotic nature of Internet	Effective communication
Hermawan, 2020	Business	Yes	Yes	Customer protection	Brand image, customer loyalty
Yan et al., 2011	NA	Yes	Yes	NA	NA
Joinson et al., 2010	NA	NA	Yes	Ubiquitous computing	Self-disclosure
Kelton et al., 2008	Information Science	Yes	Yes	Ubiquitous computing	Credibility of information
Glazer et al., 2014	Medicine	NA	Yes	Telehealth	Embedded healthcare
Zhghenti & Chkareuli, 2021	Business	Yes	Yes	Sharing economy	Economic transaction
Mazzella et al., 2016	Business	Yes	NA	Sharing economy	P2P sharing
Möhlmann & Geissinger, 2018	Economy	Yes	Yes	Ubiquitous computing	P2P sharing
Dwyer, 2011	NA	NA	Yes	Ubiquitous computing	NA
Ting et al., 2021	NA	Yes	Yes	Chaotic nature of Internet	Credibility of agent
Yan & Holtmanns, 2007	NA	Yes	Yes	Ubiquitous computing	NA
McKnight & Chervany, 2002	Business	Yes	Yes	E-commerce	Purchase intent, self-disclosure
Gkinko & Elbanna, 2023	Management	Yes	NA	Digital Transformation	Effective communication

## 2.2. Properties of Digital Trust

The research papers related to ‘Properties of Digital Trust’, have been reviewed in this section and a related summary is presented in table 2.

**Table 2.** Properties of Digital Trust

Research Paper	Entities / Stakeholders	Subjective Nature	Depends on Past History	Security Improves Trust	Privacy Paradox	Trust in Developed Nations vs Developing Nations
Akram & Ko, 2014	TPM chip, inquisitor	No	Yes	Yes	NA	NA
Pietrzak & Takala, 2021	Trustor, trustee	Yes	Yes	Yes	NA	NA
Kozuch, 2021	Trustor, trustee	NA	Yes	Yes	NA	NA
Hermawan, 2020	Customer, vendor, intermediary	NA	Yes	Yes	NA	More
Yan et al., 2011	NA	Yes	Yes	Yes	Yes	NA
Sas & Khairuddin, 2015	Trustor, trustee	Yes	Yes	Yes	NA	NA
Kelton et al., 2008	Trustor, Information (as trustee)	Yes	Yes	NA	NA	NA
Glazer et al., 2014	Trustor, digital service (as trustee)	Yes	Yes	NA	Yes	NA
Zhghenti & Chkareuli, 2021	NA	Yes	Yes	Yes	NA	NA
Möhlmann & Geissinger, 2018	Two peers, digital platform	Yes	Yes	NA	NA	NA
Dwyer, N., 2011	Trustor, trustee	Yes	Yes	NA	Yes	NA
Ting et al., 2021	Trustor, trustee	Yes	Yes	Yes	NA	NA
Yan & Holtmanns, 2007	Trustor, trustee	Yes	Yes	Yes	NA	NA
McKnight & Chervany, 2002	Trustor, trustee	Yes	Yes	Yes	NA	NA
Bartolini & Casassa Mont, 2000	Customer, vendor	Yes	Yes	NA	NA	NA

The key observations from entries in Table 2 are provided as follows:

- **Trust as an interaction, is mentioned as a binary relation in 11 papers and as a tertiary relation in 2 out of 15 papers.**

- The high variability in uncertain scenarios causes trust to be highly contextual or subjective (12 out of 15 papers).

- Another factor affecting trust is the experience or history between the entities / stakeholders (14 out of 15 papers).

- Out of the 15, 10 papers mentioned security as a contributor to trust.

- **The ‘privacy paradox’ concept mentioned in 3 papers explains how increasing privacy concerns does not change users’ behavior.**

- Developed countries such as Sweden and Switzerland are ranked higher in the ‘Digital Trust Index’ [4].

### 3. Future Areas of Digital Trust Research

There are 17 Sustainable Development Goals defined by the United Nations (UN). Digital trust is related to UN goals such as ‘Decent Work and Economic Growth’ and ‘Sustainable Cities and Communities’ [19]. Information and Communication Technology (ICT) opens new opportunities for businesses, more employment opportunities and subsequently economic growth.

Most businesses design digital platforms according to their benefits. Such designs may not be beneficial for users. For example, online social networking websites prioritize continued usage, which can negatively impact users. But, digital trust is also a necessity for retaining users. Therefore, research on the effect of user interface design on digital trust is desirable. These user interfaces convey a lack of system security or privacy if designed inappropriately. User-oriented research related to dark patterns and, usable privacy and security can be future directions for digital trust research.

#### 3.1. Dark Patterns

Sometimes design patterns do not sufficiently reflect the ethical considerations emphasized by Human-Computer Interaction (HCI) research [20]. This leads to creation of dark patterns that cause more harm than good to users. They are used to deceive users into doing certain actions or disclosing information unethically [21]. Dark patterns are possible sources of ambiguity and make navigation more difficult, especially for differently-abled users. Future HCI research studies should target the impact of dark patterns on digital trust.

#### 3.2. Usable Privacy and Security

Usable Privacy and Security refers to secure and privacy-supporting tools that can even be used by naive users [22]. The lock pattern available on Android is inspired by usable privacy and security research [23]. Almost all websites post privacy policies, but users tend to ignore them as they are lengthy and difficult to understand. Usable privacy policies, which summarize the privacy policy using natural language processing, are currently being researched [24].

## References

1. Akram, R.N., Ko, R.K.L.: Digital Trust - Trusted Computing and Beyond: A Position Paper. 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. (2014). <https://doi.org/10.1109/trustcom.2014.116>.
2. Pietrzak, P., Takala, J.: Digital trust – a systematic literature review. *Forum Scientiae Oeconomica*. 9, (2021). [https://doi.org/10.23762/FSO\\_VOL9\\_NO3\\_4](https://doi.org/10.23762/FSO_VOL9_NO3_4).
3. Koźuch, B.: The Dimensions of Trust in the Digital Era. In: Paliszkievicz, J. and Chen, K. (eds.) *Trust, Organizations and the Digital Economy*. pp. 15–26 (2021).
4. Hermawan, D.: The Importance of Digital Trust in E-Commerce: Between Brand Image and Customer Loyalty. *International Journal of Applied Research in Management and Economics*. 2, 18–30 (2020). <https://doi.org/10.33422/ijarme.v2i3.268>.
5. Yan, Z., Kantola, R., Zhang, P.: A Research Model for Human-Computer Trust Interaction. 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. (2011). <https://doi.org/10.1109/trustcom.2011.37>.
6. Sas, C., Khairuddin, I.E.: Exploring Trust in Bitcoin Technology. *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15)*. (2015). <https://doi.org/10.1145/2838739.2838821>.
7. Joinson, A.N., Reips, U.-D., Buchanan, T., Schofield, C.B.P.: Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction*. 25, 1–24 (2010). <https://doi.org/10.1080/07370020903586662>.
8. Kelton, K., Fleischmann, K.R., Wallace, W.A.: Trust in digital information. *Journal of the American Society for Information Science and Technology*. 59, 363–374 (2008). <https://doi.org/10.1002/asi.20722>.
9. Glazer, E., Mieczkowski, A., King, J., Fehnert, B.: Digital Trust: An Analysis of Trust in the Adoption of Digital Support Services. *Ethnographic Praxis in Industry Conference Proceedings*. 2014, 213–226 (2014). <https://doi.org/10.1111/1559-8918.01028>.
10. Zhghenti, T., Chkareuli, V.: Enhancing online business sector: digital trust formation process. *Marketing and Management of Innovations*. 5, 87–93 (2021). <https://doi.org/10.21272/mmi.2021.2-07>.
11. Mazzella, F., Sundararajan, A., D’Espous, V.B., Möhlmann, M.: How Digital Trust Powers the Sharing Economy: The Digitization of Trust. *IESE Insight*. 24–31 (2016). <https://doi.org/10.15581/002.art-2887>.
12. Möhlmann, M., Geissinger, A.: Trust in the Sharing Economy: Platform-Mediated Peer Trust. In: Davidson, N.M., Finck, M., and Infranca, J.J. (eds.) *Cambridge Handbook of the Law of the Sharing Economy*. pp. 27–37. Cambridge University Press (2018). <https://doi.org/10.1017/9781108255882>.
13. Dwyer, N.: *Traces of digital trust : An interactive design perspective*. PhD thesis, Victoria University (2011). <https://vuir.vu.edu.au/17663/>
14. Ting, H.L.J., Kang, X., Li, T., Wang, H., Chu, C.-K.: On the Trust and Trust Modeling for the Future Fully-Connected Digital World: A Comprehensive Study. *IEEE Access*. 9, 106743–106783 (2021). <https://doi.org/10.1109/access.2021.3100767>.
15. Yan, Z., Holtmanns, S.: Trust Modeling and Management: From Social Trust to Digital Trust. In: Subramanian, R. (ed.) *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*. pp. 290–323 (2008). <https://doi.org/10.4018/978-1-59904-804-8.ch013>.
16. McKnight, D.H., Chervany, N.L.: What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*. 6, 35–59 (2001). <https://doi.org/10.1080/10864415.2001.11044235>.

17. Bartolini, Casassa Mont, M.: Digital Credentials and Authorization to Enhance Trust in Negotiation within E-Services Marketplaces. (2000).
18. Gkinko, L., Elbanna, A.: Designing trust: The formation of employees' trust in conversational AI in the digital workplace. *Journal of Business Research*. 158, 113707 (2023). <https://doi.org/10.1016/j.jbusres.2023.113707>.
19. THE 17 GOALS | Sustainable Development, <https://sdgs.un.org/goals>, last accessed 2023/04/27.
20. Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L.: The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. (2018). <https://doi.org/10.1145/3173574.3174108>.
21. Lacey, C., Caudwell, C.: Cuteness as a 'Dark Pattern' in Home Robots. 2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI). (2019). <https://doi.org/10.1109/hri.2019.8673274>.
22. De Luca, A., von Zezschwitz, E.: Usable privacy and security. *it - Information Technology*. 58, 215–216 (2016). <https://doi.org/10.1515/itit-2016-0034>.
23. Mathis, F., Vaniea, K., Khamis, M.: Prototyping Usable Privacy and Security Systems: Insights from Experts. *International Journal of Human-Computer Interaction*. 38, 468–490 (2021). <https://doi.org/10.1080/10447318.2021.1949134>.
24. Liu, F., Ramanath, R., Sadeh, N., Smith, N.A.: A Step Towards Usable Privacy Policy: Automatic Alignment of Privacy Statements. *Proceedings of the International Conference on Computational Linguistics*. (2014).