Towards an Empirical Analysis of Trustworthiness Attributes in the Context of Digitalization

Sandro Hartenstein
Berlin School Of Economics And Law
Berlin, Germany
email: sandro.hartenstein@hwr-berlin.de

Steven Schmidt
DB Station&Service AG / Berlin School Of Economics And Law
Berlin, Germany
email: s_schmidts19@stud.hwr-berlin.de

Andreas Schmietendorf
Berlin School Of Economics And Law
Berlin, Germany
email: andreas.schmietendorf@hwr-berlin.de

***Abstract*— This idea paper describes the current perception of the terms trust and trustworthiness in technical and sociological systems. Related works are examined and put into relevant context for the proposed research. The main goal is to show the missing link between those two extrema. Thus, proposed future works aim to further identify systems aspects connecting sociological and technical trustworthiness. The focus lies on socio-technical systems. Therefore, the proposed empirical research concentrates along this spectrum. The thorough examinations in the proposed study fields benefit a holistic model of trustworthiness attributes for digital systems through enrichment of empirically evaluated and compared trustworthiness attributes.**

***Keywords*-Trustworthiness; Digitalization; Information Systems; Society.**

I. INTRODUCTION

The richness of provided services in the digital world is ever evolving and rapidly growing through the establishment of digitalized aspects in everyday life, private or professional. The consumption of digital services relays on trustworthiness in a significant way [1]-[3]. Yet, the terms trust and trustworthiness are perceived differently across multiple academic and industrial disciplines, as well as the related attributes.

This idea paper aims to present a possible approach on analyzing significant factors of trustworthiness through different empirical examinations of different fields. Those *trustworthiness attributes* may vary heavily from field to field, but the general assumption is that those attributes mainly only differ in weight, relative to the observed field they are significant to.

In Section 2, different terms and viewpoints on the topic of trust and trustworthiness are described to explain the motivation for this approach. In Section 3, past and current related work is then examined, to demonstrate the variations of the current understanding and related contexts that have been evaluated. Section 4 describes what could be done to achieve a generic and general model of trustworthiness attributes and associated weights according to the area under study. The conceptional procedure to accomplish this idea is described in detail, as well as what fields are going to be involved as part of the planned project to enable this work. The fields and their individual empirical approach, thus, are presented briefly to demonstrate the general idea of the approach.

II. TERMS AND VIEWPOINTS

A definition of trust is:

"Trust by definition entails a willingness by the [trustor] to make herself vulnerable to the possibility that another will act to her detriment" [4, p. 28]

A definition of trustworthiness for software is:

"Software trustworthiness is a key enabler of IoT trustworthiness, which is the degree of confidence that a system will perform as expected. Trustworthiness is based on five characteristics—safety, security, privacy, reliability and resilience, which directly and in combination provide protection against hazards and threats related to environmental disturbances, human errors, system faults and attacks." [5, p. 6]

The digitization is depending on the well-being of the users. Entrusting data and work steps to computer systems is viewed critically by the user. Besides the advantages, there are also disadvantages. Trust is a key to the acceptance of digitised services and thus also to the increase in productivity through digitisation. This idea paper shows the dimensions of trust. These need to be addressed by the provider. There are several participants with different interests and understandings of trust and trustworthiness. The needs of the stakeholders in the context of trustworthiness of digital services are consumer, provider and third-party trustee. The consumer is striving to use a service that is as trustworthy as possible, as the effects of data misuse are becoming increasingly apparent. Digital service providers need consumer confidence in their products. They also need trustworthy supply services. The third independent authority can confirm the trustworthiness of digital services to the user, as long as it has the confidence of the users and can verify the services.

From the point of view of the service, two main elements are decisive for its reputation with consumers. User trust and the trustworthiness of the service are these two factors. In the research project that is named OPerational Trustworthiness Enabling Technologies, in short

 ISBN: 978-1-61208-760-3

OPTET, the prerequisite for trust in the context of web-based services was determined. The result is that trust can be personal, transferred and based on core trust, for example in institutions. The trustworthiness of the service is based on its attributes and on those confirmed by third parties. These correlations and their influences were summarized in Figure 1 [6]-[8].

The structure of the known Social-, Technological-, Economic-, Environmental-, Political-, Legal- and Ethical-environment analyses, in short STEEPLE, was used to classify the trust building measures as a view from outside [9, pp. 80-84]. From the authors' point of view, the environment analysis for a digital service is essential for its trustworthiness and the trust of its consumers. For this reason, the influencing factors can be classified with STEEPLE.

This idea paper focuses on the social, economic and technical factors that influence trust in digital services. Based on the analysis of trust and trustworthiness, the following influencing factors can be assigned. The social factors are distinguishable by personal, referral and derived trust. Personal trust is characterised by emotions, e.g., browser certifications status colour (red – danger, green – ok) or knowledge, e.g., knowledge about the two-factor authentication procedure. Referral trust is based on a third party who is trusted. Derived trust is often shaped by experience with institutions and their status. The technological factors are the trustworthiness attributes of the services. These should be measured objectively during development and operation or confirmed by third parties. The economic factors are characterised by the expectation of profit. The provider aims to offer trusted digital services. He can achieve this by optimising all factors, but there must be a minimum level of each factor. For example, a service may be technically perfect, i.e., fully trusted, but the provider has a bad reputation, so the derived trust is low and the service is not fully trusted. One factor influencing the consumer is the absence of risk or low risk. If the stakes are low, the service will be trusted more because the potential loss is manageable. However, many users are not aware of the value of the user data. A risk assessment is therefore useful for all stakeholders.

III. RELATED WORK

The research on trust goes back a long way; basics were already interesting in the 50s. More recent research has commercial reasons [10]. For trust in software and its use, this section introduces the most important concepts briefly.

The social drivers for trust are honesty, integrity and reliability of the interaction partners. It is the nature of trust to address these interpersonal relationships. That's also the basis for stability in social institutions and markets. It is undisputed that trust is the fundament of the interactions of the daily life.

Simmel sees the generation of trust on the expected result [11]. If it is good, trust is created. If it is bad, trust is destroyed. Trček highlights the emotional aspects and the behaviour of the participants as important influencing factors [12]. The change in perceived competence appeared to occur largely for citizens with high trust and little knowledge and a shift in perceived benevolence could mainly be noted among citizens with low knowledge and low trust. [13]

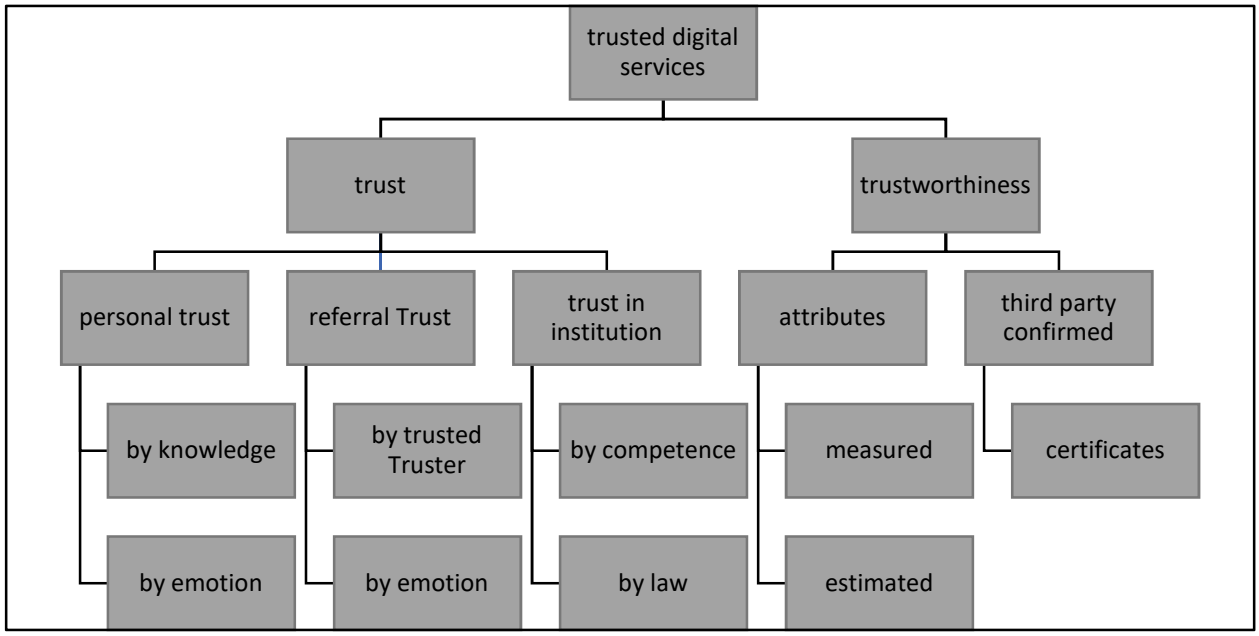

Figure 1. Trust and trustworthiness for digital services [own representation based on [6]-[8][14]]

In the commercial context, Patrick and his team have determined that cognitive and emotional dimensions of trust are strong, independent and interconnected in building trusting relationships with firms [10]. Grimmelikhuijsen and Meijer examined the relations with public institutions and found that they are considered more trustworthy than private companies [15]. In 2001, McKnight brought together the various aspects and their dependencies on trust in one design. This is illustrated in Figure 2. Basically, he distinguishes in trust in the institution through psychology and sociology, which influences the personal trust.

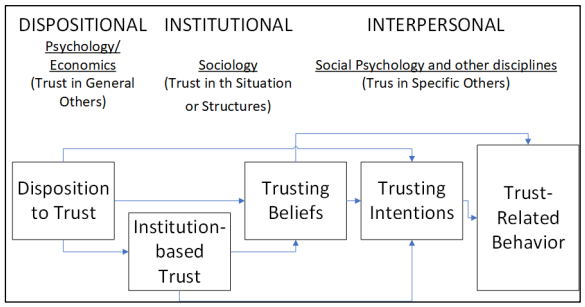

Figure 2. Interdisciplinary model of trust constructs [recreated from 16, p. 33].

Robbins shows a modern trust-risk-act-model, called relational trust in the year 2016 [17, p. 985]. It is illustrated in Figure 3 and visualizes the connections between trust, risk assessment and the relation to activities. The factors influencing trust are the characteristics of the actors and the relationships between the actors and external parties.

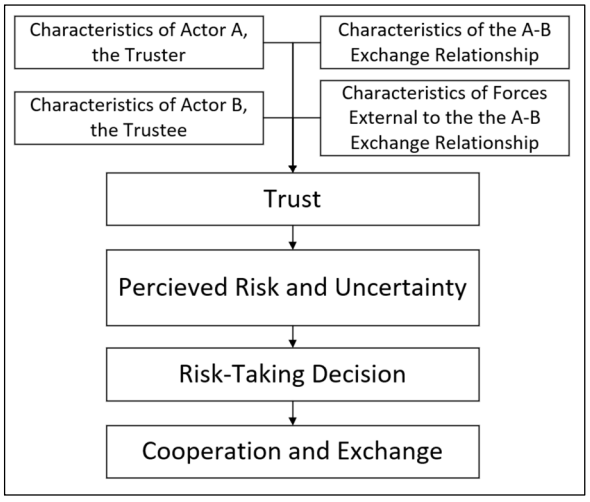

Figure 3. Structural-cognitive model of trust [recreated from 17, p. 982].

The technical drivers for trust are characterized by the trustworthy properties of the service. By evaluating 72 scientific articles on trustworthiness and corresponding quality categories, the attributes were determined within the OPTET project (EU FP7-project from 2012 till 2015). These are shown in Figure 4. [18, p. 24][19, p. 236]

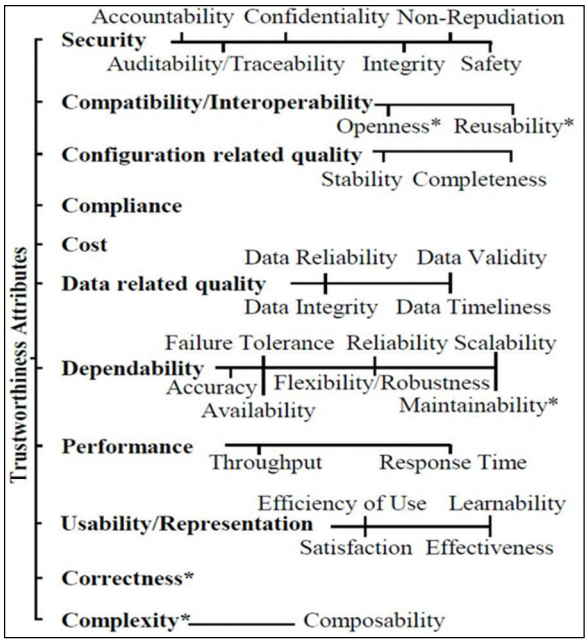

Figure 4. Trustworthiness attributes [19, p. 236].

The attributes have context-specific influence on the trustworthiness. The domain and the type of the Social-Technical- System, in short STS, are relevant. The attributes are measurable and can map the influence with a weighting. The top three attributes of the study of 72 relevant papers by Mohammadi et. al are Security, Dependability and Usability. In almost 2/3 of the literature, security is mentioned as the most important attribute. Reliability is mentioned in almost half of them. 1/4 of the papers mention usability as an important attribute for trustworthiness. All attributes and their relevance are shown in Figure 5. [18, p. 25]

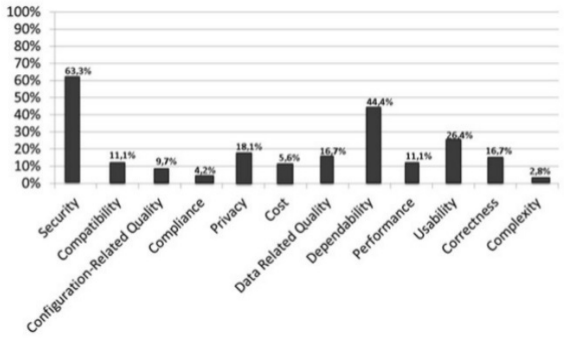

Figure 5. Classified trustworthiness attributes [18, p. 24].

IV. Conclusion and Future Work

The description of related works shows that the focused dimensions range from very technological to very sociological but fail to respect both extremes equally. Trust is related to many more fields than solely sociology or technology. Different legal or political institutions might perceive trustworthiness different than individuals and therefore evaluate the same systems attributes dissimilar with varying implications on the systems evaluation and consumption of its services.

Considering classical environmental approaches such as the STEEPLE analysis would enable a system that models trustworthiness and related attributes to take different aspects of the systems whole environment into account. The systems attributes in relation to different environments is important especially for the socio technical view, as the connection of these two fields is the main motivation for the intended research project in the context of digitalization and its impacts. The width of all fields enables a greater richness for the model itself in terms of representativeness and – if examined – empirical argumentation.

This thought leads to the proposed idea regarding the planned feature works related to trustworthiness and trustworthiness enabling attributes to achieve a generalized set of empirical evaluated and weighed attributes examined in different fields of the project to model trustworthiness. The architecture shall be designed to be extended through further research in different fields across the socio technical spectrum through the views of the STEEPLE dimensions. The first fields and respective systems which will be observed, are as follows:

S1 - Simulation of a trustworthy scrum process

The observation concentrates on the impacts of different trustworthiness enabling attributes along a simulated software engineering process. The aim is to examine weights of different attributes to achieve a high trustworthiness score.

S2 – Trustworthy public WiFi

The empirical assessment in this field emphases trustworthiness attributes in public WiFis through questionnaires and compared interviews between user groups of different services with different suspected trustworthiness levels.

S3 – Trustworthy AI-Webservices

This research area is concerned with determining and evaluating the trustworthiness of web services that use artificial intelligence.

S4 – Trustworthy web presence of mediators

Similar to the previous field, a variety of web presences of self-established mediators is examined to gain a collection of empirical validated trustworthiness attributes in this field, to enrich the overall proposed model with weights unique to this field.

Figure 6 shows the planned research goal in a schematic diagram. Each empirically determined trustworthiness attribute (Ai) per examined system (Sj) should be weighted. In addition, these attributes are categorized according to the STEEPLE dimensions and thus enable the formation of clusters. This is helpful to create the general model. Each further investigation of similar or different systems will contribute to the overall set, but also add information on different weights, unique per examined field.

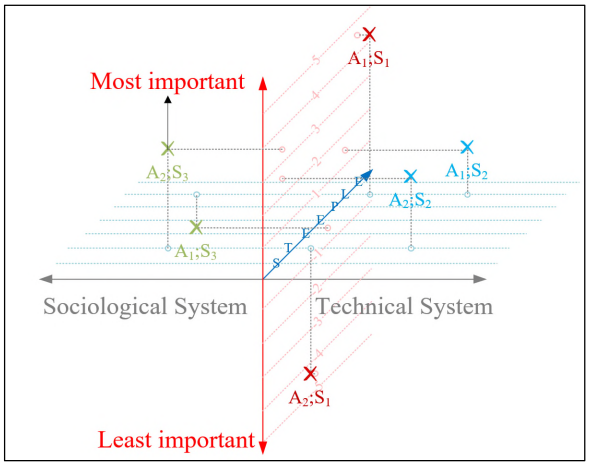

Figure 6. Visualization of the proposed approach

The empirical research and contribution of insights to the proposed system shall be established at the Berlin School of Economics and Law as a research project abbreviated as EUMoVe – Empirische Untersuchung der Modelierung von Vertrauenswürdigkeit (Empirical Examination Of Modeling Trustworthiness). The main objective of the planned research project is to achieve the said model, enriched with a static set of attributes empirically weighted per domain and thus applicable to most of the socio-technical spectrum of systems.

Without sufficient confidence in appropriate solutions, problems of acceptance or even difficult to resolve conflicts arise. Accordingly, the question arises as to what a systemic approach to improving customer-related trust in the discourse of digital solutions can look like.

We see here a combination of organizational, sociological and technological approaches to solving problems, whereby potential conflicts of involved parties are monitored immanently (if necessary, also algorithmically) by a mediatory approach and solved if necessary. The aim is to establish intelligent conflict resolution strategies as an integral part of digital products and services. On this basis, customer-centered trust can be ensured through transparency, control options, conflict resolution strategies and considered liability issues.

References

[1] S. Utz, P. Kerkhof, and J. van den Bos, “Consumers rule: How consumer reviews influence perceived trustworthiness of online stores,” *Electronic Commerce*

Research and Applications, vol. 11, no. 1, pp. 49–58, 2012, doi: 10.1016/j.elerap.2011.07.010.

[2] European Commission, *Trustworthy AI.* [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/trustworthy-ai-brochure [retrieved: 10, 2020].

[3] World Economic Forum, *Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society: Insight Report.* [Online]. Available: http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf [retrieved: 10, 2020].

[4] C. A. Hill and E. A. O'Hara O'Connor, "A Cognitive Theory of Trust," *SSRN Journal*, 2005, doi: 10.2139/ssrn.869423.

[5] M. Buchheit, F. Hirsch, S. Rix, M. Hermeling, and B. Martin, *Software Trustworthiness Best Practices.* [Online]. Available: https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf [retrieved: 10, 2020].

[6] S. van der Graaf, W. Vanobberghen, M. Kanakakis, and C. Kalogiros, "Usable Trust: Grasping Trust Dynamics for Online Security as a Service," vol. 9190, pp. 271–283, 2015, doi: 10.1007/978-3-319-20376-8_25.

[7] A. Chakravarthy *et al.,* "OPTET D2.4 Socio-economic evaluation of trust and trustworthiness," OPTET. Accessed: Oct. 16 2020. [Online]. Available: https://www.researchgate.net/publication/317488309_OPTET_D24_Socio-economic_evaluation_of_trust_and_trustworthiness.

[8] S. Wiegand *et al.,* "D2.5 – Consolidated report on the socio-economic basis for trust and trustworthiness," OPTET, 2015. Accessed: Oct. 16 2020. [Online]. Available: https://www.researchgate.net/publication/317488377_OPTET_D25_-_Consolidated_report_on_the_socio-economic_basis_for_trust_and_trustworthiness.

[9] G. Johnson, K. Scholes, and R. Whittington, *Strategic Management [orig.: Strategisches Management]: An Introduction; Analysis, Decision and Implementation [orig.: Eine Einführung; Analyse, Entscheidung und Umsetzung],* 9th ed. München: Pearson Studium, 2011, ISBN: 9783868940565.

[10] A. Patrick, S. Marsh, and P. Briggs, "Designing Systems That People Will Trust," *Security and Usability*, NRC 47438, pp. 75–99, 2005. [Online]. Available: https://www.researchgate.net/profile/Pamela_Briggs/publication/44081283_Designing_Systems_That_People_Will_Trust/links/00b7d5344d8b27f675000000.pdf.

[11] G. Simmel, *The sociology of Georg Simmel: Selected writings*. New York: Free Pr, 1964, ISBN: 9780029289204.

[12] D. Trček, "A Brief Overview of Trust and Reputation over Various Domains," in *SpringerBriefs in Information Systems, Trust and Reputation Management Systems: An e-Business Perspective*, D. Trček, Ed., Cham: Springer International Publishing, 2018, pp. 5–19.

[13] T. Nguyen, "Trust and Sincerity in Art," *Ergo*, 2020. [Online]. Available: https://www.researchgate.net/publication/343239976_Trust_and_Sincerity_in_Art.

[14] N. Gol Mohammadi *et al.,* "An Analysis of Software Quality Attributes and Their Contribution to Trustworthiness," *Proceedings of the 3rd International Conference on Cloud Computing and Services, Science*, pp. 542–552, 2013.

[15] S. G. Grimmelikhuijsen and A. J. Meijer, "Effects of Transparency on the Perceived Trustworthiness of a Government Organization: Evidence from an Online Experiment," *JOPART*, vol. 24, no. 1, pp. 137–157, 2014, doi: 10.1093/jopart/mus048.

[16] D. H. McKnight and N. L. Chervany, "Trust and Distrust Definitions: One Bite at a Time," in *Lecture Notes in Computer Science*, vol. 2246, *Trust in Cyber-societies: Integrating the Human and Artificial Perspectives*, R. Falcone, M. Singh, and Y.-H. Tan, Eds., Berlin, Heidelberg: Springer, 2001, pp. 27–54.

[17] B. G. Robbins, "What is Trust? A Multidisciplinary Review, Critique, and Synthesis," *Sociology Compass*, vol. 10, no. 10, pp. 972–986, 2016, doi: 10.1111/soc4.12391.

[18] N. G. Mohammadi *et al.,* "Trustworthiness Attributes and Metrics for Engineering Trusted Internet-Based Software Systems," in *Communications in Computer and Information Science, Cloud Computing and Services Science*, M. Helfert, F. Desprez, D. Ferguson, and F. Leymann, Eds., Cham: Springer International Publishing, 2014, pp. 19–35.

[19] S. Paulus, N. G. Mohammadi, and T. Weyer, "Trustworthy Software Development," in *Lecture Notes in Computer Science, Communications and Multimedia Security*, D. Hutchison et al., Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 233–247.

 ISBN: 978-1-61208-760-3