Building VOT - Virtual Organizational Trust: Challenges and Strategies in the Digital Era

Bambang Iman Santoso, Gugup Kismono and Faturochman

September 23, 2024

BUILDING VOT - VIRTUAL ORGANIZATIONAL TRUST: CHALLENGES AND STRATEGIES IN THE DIGITAL ERA

Bambang Iman Santoso
Universitas Gadjah Mada

Gugup Kismono
Universitas Gadjah Mada

Faturochman
Universitas Gadjah Mada

ABSTRACT

This study examines virtual organizational trust (VOT), which is increasingly significant as the business landscape evolves rapidly due to advances in information technology. Trust in this context encompasses various forms of interaction through digital media within and outside the organization. The research identifies key elements of digital trust, including the security, integrity, and reliability of digital systems and data, which are vital in the era of Industry 4.0 and Society 5.0. Digital trust enables organizations and individuals to manage uncertainty and risk in the digital business environment. The article also emphasizes the importance of a positive reputation and customer ratings in building trust and fostering working relationships in the digital economy.

Keywords: Virtual Organizational Trust, Digital Trust, Digital Economy.

1. INTRODUCTION

The rapid development of information technology and the internet has forced many organizations to shift to virtual formats that provide greater flexibility and efficiency (S. Chatterjee at al., 2022). However, such transformation poses new challenges in establishing and maintaining trust between organizational members. Trust is key to increasingly complex interpersonal and organizational relationships in virtual contexts (Hacker at al., 2019). Virtual organizations tend to be limited in face-to-face interactions and rely on digital communication tools, which means trust can also have limitations. In addition, Industry 4.0 and Society 5.0, characterized by the proliferation of high-tech technologies and automation, create a greater need for digital trust, i.e. confidence in the security, integrity, and reliability of digital systems and data (Fukuyama, 2018; Lumineau at al., 2023). Although theoretical research on organizational trust has been widely conducted, the increase in the publication of such articles in the context of virtual organizations is limited. Therefore, this study aims to fill the gap by identifying the essential elements of Virtual Organizational Trust (VOT), exploring virtual organizations' challenges, and developing effective strategies to increase trust in a digital context.

2. LITERATURE REVIEW

The increasingly rapid changes in the business environment, defined as the ‘new normal’ (Lawrence, 2013), compel organizations and companies to adapt and adjust to achieve their business objectives (Bennett & Lemoine, 2014). These changes, characterized by volatility, uncertainty, complexity, and ambiguity, are collectively known as the ‘VUCA World’ (Bennis, 2007; Bennis & Nanus, 1985, 2016; Wefald & Katz, 2011). The impact of disruptive information technology advancements has led to more complex diversity, known as D-VUCAD (Woodward, 2018), posing unique challenges. Management and organizations must embrace this diversity both internally and externally. In the concept of neuroscience-based leadership (neuroleadership), leaders are required to lead their diverse teams or organizations and facilitate change inclusively (Rock & Ringleb, 2013).

A recent literature review provides a better understanding of how the Fourth Industrial Revolution affects trust within and between organizations. The article by Lumineau at al. (2023) aims to identify changes in the form, production, and target of trust in the digital era and provides insights for organizational adaptation. They argue that rather than making trust obsolete, the Fourth Industrial Revolution led to qualitative changes in trust. Therefore, micro and macro management experts must reassess what is known about organizational trust (Lumineau at al., 2023).

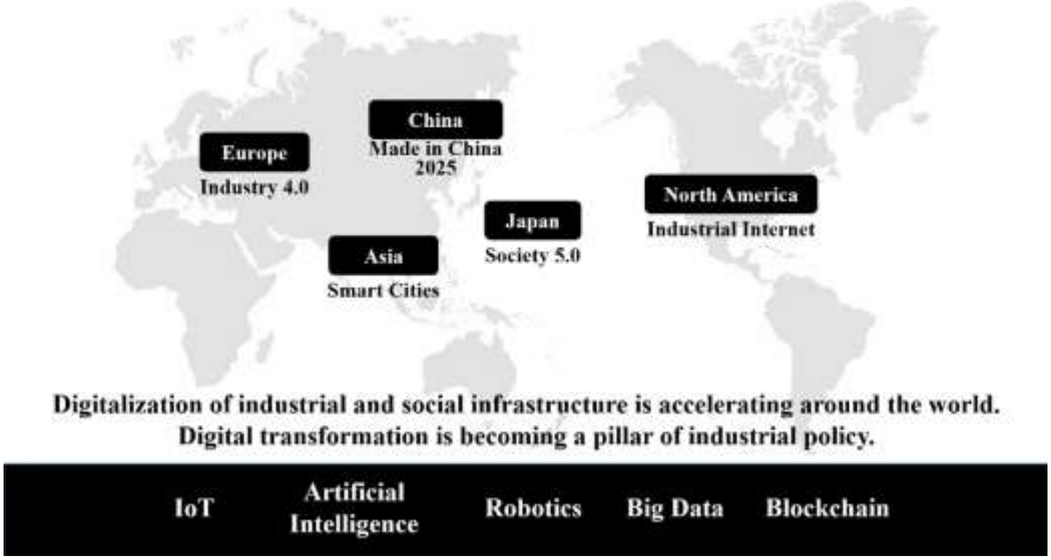
In contrast to previous studies, this study addresses the increasingly broad and complex nature of organizational trust in the context of digital and information technology advances. The focus includes all trust that arises from interactions through digital media or virtual use of information technology, whether between individuals within the same or different organizations, between individuals and groups, between individuals and organizations, between groups, between groups and organizations, and between organizations, both in the context of conventional organizations and virtual organizations. Trust in this virtual organizational context is expected to continue to grow along with advances in technology and science.

Trust and working relationships in the Gig Economy are built through positive reputations and customer ratings on digital platforms. Effective communication, responsiveness, and providing high-quality services are also key to building trust. Digital platforms that offer dispute-resolution mechanisms also play a role in maintaining trust and resolving conflicts (Flanagan, 2019). Researchers have stimulated new scientific studies to better understand trust and its implications in the digital era. They have identified three fundamental changes: a) the forms of organizational trust, b) how trust is generated, and c) who needs to be trusted (Lumineau at al., 2023).

First, trust tends to become more impersonal and systemic, with interpersonal trust increasingly replaced by trust in digital technology-based systems. Second, in terms of generating trust, production based on characteristics and institutions will become more important. Third, despite the shift towards system trust, there remains a need to trust certain individuals; these trustees are no longer interaction partners but third parties responsible for technology systems and data. Therefore, the focus on interpersonal and inter-organizational trust targets also changes (Lumineau at al., 2023). Meanwhile, the Society 5.0 concept, proposed by the Japan Business Federation, Keidanren in 2016 (Fukuyama, 2018; Hooker, 2019), is recognized as an overarching goal to anticipate global digital transformation trends. This concept is part of the Fifth Science and Technology Basic Plan adopted by the Japanese Cabinet in January 2016 (Figure 1).

Society 5.0 represents the latest evolutionary stage of societal concepts, emphasizing a return to human-centeredness, known as the ‘human-centered society’ or ‘super smart society.’ Initially, Society 1.0 referred to humans as hunter-gatherers. Society 2.0 saw humans as agrarian or farming societies. Society 3.0 was marked by industrial society, while Society 4.0 is the current information society (Fukuyama, 2018; Hooker, 2019).

Figure 1. Digital Transformation.



Source: Mayumi Fukuyama, Society 5.0: Aiming for a New Human-Centered Society, 2018.

Society 5.0 comprises many elements. Two of the most prominent are the fusion of physical and cybernetic spaces and the integration of humans with various intelligent agents to form a ‘post-humanization’ society. According to Hooker (2019), such a society relies on advanced algorithms, including optimization algorithms, to support its infrastructure. It remains to be seen whether we, as social beings, will allow algorithms to be deeply and comprehensively integrated into our lives. We will trust these algorithms, or we will come to resent them (Hooker, 2019).

Various advancements in information technology, which create the virtual world, impact trust in the 'virtual organizational trust' (VOT). Examples of these advancements, which will be discussed in the following paragraphs, include IoT (internet of things), cybersecurity, blockchain, AI (artificial intelligence), big data & data-driven platforms, messaging apps, online content & ChatGPT, wireless sensor networks, machine learning & deep learning, and others such as digital twin, quantum computing, the metaverse, AR (augmented reality), VR (virtual reality), MR (mixed reality), and XR (extended reality).

The development of digital technology changes how we work and affects trust at every level of analysis, including individual trust, team trust, intra-organizational trust, and inter-organizational trust (Faturochman, 2023). VOT requires individuals, teams, and organizations to enhance digital literacy, consisting of four main pillars: digital skills, digital safety, digital ethics, and digital culture (Ameliah at al., 2022; Kominfo, 2020). This digital literacy is based on information technology and management information systems (MIS), which comprise software, hardware, dataware (databases), netware (networks), and brainware (users). "MIS is a machine-based human system that provides information and decision support for management in planning, controlling, and operating the organization" (Leavitt & Whisler, 1958).

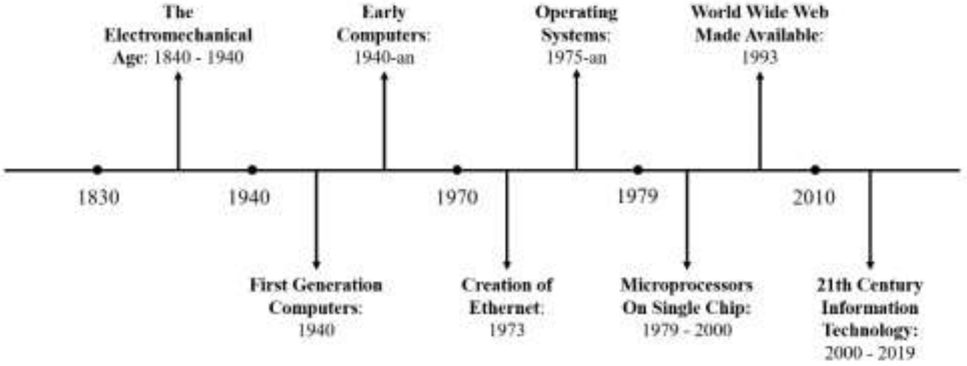
In addition to defining and understanding trust in virtual organizations (VOT), this article will also discuss some other VOT approaches and provide conclusions and future research agendas. The advancements in technology and their impacts, as well as the dynamics and cycles of trust in virtual organizations.

The rapid development of information technology has caused concern and anxiety among companies and employees. Trust in technology and the companies implementing it has been eroded by privacy violations, algorithmic bias, threats to livelihoods, and inaccurate beta testing, all of which contribute to a fertile ground for skepticism (Dobrygowski, 2023).

Dobrygowski (2023) highlights that to restore digital trust, companies need to achieve three main goals: a) ensuring security and reliability, b) enhancing accountability and oversight, and c) promoting inclusive, responsible, and ethical use. To achieve this practically, the following steps are necessary: 1) formulating a vision of digital trust, 2) planning more trustworthy actions, and 3) recruiting individuals who can help build trust (Dobrygowski, 2023).

This article also details the advancements in digital and information technology (see Figure 2) and their impact on trust in the digital world, particularly on VOT. It also discusses new technologies that require attention and their influence on VOT dynamics and cycles, as well as covers the literature on technological development. The article will conclude with future research prospects related to technological advancements and their impact on digital trust and VOT.

Figure 2. Information Technology Development Timeline


The Electromechanical Age: 1840 - 1940
Early Computers: 1940-an
Operating Systems: 1975-an
World Wide Web Made Available: 1993
1830
1940
1970
1979
2010
First Generation Computers: 1940
Creation of Ethernet: 1973
Microprocessors On Single Chip: 1979 - 2000
21th Century Information Technology: 2000 - 2019

Source: Adopted from website: https://prezi.com/blef93mja_bj/information-technology-timeline/

3. METHODOLOGY

This research uses a systematic literature review method to review, analyze, and synthesize previous researchs on organizational trust in a digital context. This process involved a comprehensive literature search, selection of studies based on established inclusion and exclusion criteria, extraction of relevant data, and analysis and synthesis of findings to provide a comprehensive and in-depth picture of Virtual Organizational Trust (VOT).

The literature search strategy involves selecting relevant topics from the past two decades and prioritizing recent years. Research articles are sourced from the Scopus database (primary) and others (secondary) using keywords such as trust, organizational trust, digital trust, and trust in virtual organizations. The selected articles are those related to organizational trust, including digital trust or organizational trust in virtual environments, excluding interpersonal trust.

The identified research articles are filtered based on keywords, recency, and journal quality, focusing on Scopus-indexed journals (Q1, Q2, Q3, and Q4). These articles are then grouped and categorized based on their relevance. Content analysis is the approach used to analyze and synthesize findings from various studies.

4. RESULTS – DEFINITION AND MEANING OF VOT

Trust in offline contexts cannot be directly applied to online contexts based on the premise that online trust relies more on interpersonal relationships than on technology (Faturochman, 2023; Friedman at al., 2000). Interpersonal relationships are not necessary to build online trust, even if the online interactions are interpersonal (Faturochman, 2023; Wade at al., 2011). Though online relationships remain interpersonal, interpersonal trust does not always require emotional involvement such as attention and care, even if these actions can be key in building trust.

According to Mayer at al. (1995), there are three criteria for being trustworthy: a) ability or competence, b) integrity, and c) benevolence, which are also indicators of a deep-level relationship (Mayer at al., 1995). Integrity and benevolence are criteria attached to media, particularly software, websites, or applications used. In addition to direct and implicit trust among users, global trust ultimately manifests in the high market value of the company (Faturochman, 2023).

Based on hypothesis testing from previous research (Yamagishi & Yamagishi, 1994) by Faturochman at al. (2023), utilizing secondary data previously collected by the Center for Indigenous and Cultural Psychology, Faculty of Psychology, Universitas Gadjah Mada for the trust project, the findings are as follows: a) global or general trust is a separate variable from 'caution,' b) the levels of general trust and caution are moderate and not significantly different, c) demographic factors do not affect either, but religious and ethnic identification play a significant role, d) general trust has a greater role in trust towards respected individuals, while caution plays a greater role in trust towards political institutions, and e) the theoretical model of their relationship with antecedents and effects fits the field conditions (Faturochman, 2023).

According to Nass at al. (1994), humans tend to anthropomorphize interactions between humans and applications and information. This means information technology is given human-like attributes, thus having some human characteristics (Nass at al., 1994). There are expectations in online trust, including choice, knowledge, experience, and familiarity. Online systems are proxies for the decisions and implementations of their designers. Trust in websites and systems is significant for users, even though there are differences in the correct concept (Cheshire, 2011; Faturochman, 2023). Like trust in offline relationships, online trust consists of general trust (global trust) and specific trust (familiar trust).

Personal factors of internet users influence their assessment of risks and uncertainties, as well as their experience using the internet over time. People will be cautious in using financial services online. Other factors include a) dynamics of online trust; b) trust in technology using software, hardware, networks, databases, big data, and end users; c) trust in the ability and validity of technology which is vulnerable to viruses and fraud; d) trust in algorithm programs; e) trust in the confidentiality of user data and trust in internet services.

Factors that hinder the development of trust include a) lack of choice leading to dependency, b) risks of trusting and not trusting, and c) when risks cannot be anticipated. Elements of virtuality include geography, communication, and culture, each playing roles as testers, developers, analysts, engineers, and project managers (Faturochman, 2023).

The definition and understanding of 'online trust' as described above are very broad. When searching on the internet, explicit definitions of 'virtual organizational trust' (VOT), 'virtual organizations trust,' or 'virtual organizations trust' are not found. To provide a clearer picture, several terminologies of online trust and VOT will be outlined, including trust in various new technological developments. Some VOT terms discussed here are limited to digital trust, cyber trust, online trust, trust in online social networks and social media (ONSs & social media trust), trust in virtual organizations, and other VOT approaches. Various developments in information or digital technology that affect VOT, as well as the stages of the VOT cycle, will also be discussed.

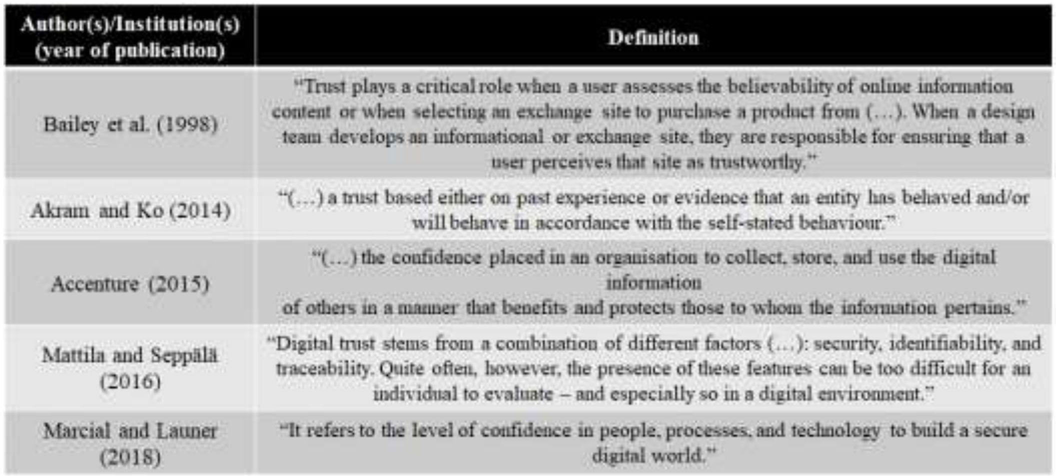
4.1. Digital Trust

Pietrzak and Takala (2021) conducted a systematic literature review and found no universally accepted definition of 'digital trust'. They defined it as “a measure of the confidence that workers, consumers, partners, and other stakeholders have in an organization's ability to protect individual data and privacy.” Their data search, using the ISI Web of Science database on April 14, 2021, included articles from 1994 to 2020 with the keyword “digital trust” (Pietrzak & Takala, 2021).

Digital trust varies across domains, involving different actors, actions, and vulnerabilities. Maintaining digital trust is crucial for a responsible organizational culture, requiring proactive evaluation of internal behaviors and knowledge ecosystems, including data transfer. Extensive empirical and theoretical research is needed to address digital trust issues (Pietrzak & Takala, 2021).

Akram and Ko (2015) highlight that digital trust evolves differently across fields, referring to confidence built through technology use in digital environments. This trust is placed in organizations or individuals managing digital resources. With the rapid growth of the internet, offline trust has become impractical, prompting the evolution of digital trust, which varies across domains. In the semantic web, digital trust involves confidence in information through reputation, context, and content mechanisms. In secure computing, it ensures technology's trustworthiness in distributed environments (Akram & Ko, 2015).

Table 1. Definition of Digital Trust.



Author(s)/Institution(s) (year of publication)	Definition
Bailey et al. (1998)	"Trust plays a critical role when a user assesses the believability of online information content or when selecting an exchange site to purchase a product from (…). When a design team develops an informational or exchange site, they are responsible for ensuring that a user perceives that site as trustworthy."
Akram and Ko (2014)	"(…) a trust based either on past experience or evidence that an entity has behaved and/or will behave in accordance with the self-stated behaviour."
Accenture (2015)	"(…) the confidence placed in an organisation to collect, store, and use the digital information of others in a manner that benefits and protects those to whom the information pertains."
Mattila and Seppälä (2016)	"Digital trust stems from a combination of different factors (…): security, identifiability, and traceability. Quite often, however, the presence of these features can be too difficult for an individual to evaluate – and especially so in a digital environment."
Marcial and Launer (2018)	"It refers to the level of confidence in people, processes, and technology to build a secure digital world."

Source: Pietrzak & Takala, 2021.

Levine (2019) states that trust and cooperation are fundamental in digital commerce, viewing digital business communities as morally relevant per the integrative social contract theory (ISCT). Digital trust, a social efficiency hyper norm in ISCT, emphasizes its importance in promoting cooperation, fairness, and economic well-being in digital business. It involves accepting vulnerability in risky digital environments, rooted in high intra-communal trust and spontaneous sociability (Levine, 2019).

Chatterjee at al. (2023) highlight digital trust in Industry 4.0 and 5.0 as crucial, involving confidence in the security, integrity, and reliability of digital systems. This trust is essential for successful digitalization, impacting political, economic, and social aspects of digital transformation (Chatterjee at al., 2023)

Bapna at al. (2017) measured digital trust using a Facebook application and an investment game, testing tie strength through interaction levels, shared friends, and being tagged in photos. Results showed that conventional trust measures like connectivity might not predict digital trust effectively, varying with the number of a user's Facebook friends (Bapna at al., 2017).

Alpcan at al. (2011) tested digital trust at the game theory level, highlighting its complexity for organizations. Digital trust is challenging due to unpredictable consumer interactions (Alpcan at al., 2011; Kluiters at al., 2023). Culnan and Armstrong (1998) found specific measures enhance digital trust, but trust marks' effectiveness is reduced by a lack of awareness (Rüdiger & Rodríguez, 2013).

Digital trust scores have little impact on changing consumer behavior, indicating a need for deeper exploration (Kluiters at al., 2023). The evolution of digital trust requires diverse approaches and interpretations across fields. Initially based on real-world trust, digital trust has evolved with internet growth, making previous offline trust impractical (Akram & Ko, 2015).

4.2. Cyber Trust

The rise in online trust illustrates society's tendency to trust and rely on online platforms for many of their needs. Previously, building trust in cyberspace was challenging due to high levels of anonymity, which posed significant obstacles. Trust in the digital economy is a major concern for consumers, leading to hesitancy in online shopping due to worries about privacy, IT security, and performance risks (Rüdiger & Rodríguez, 2013). Despite reports that companies in the sharing economy and e-commerce platforms are often ineffective in protecting privacy and frequently face hacking attacks, cyber trust mechanisms have evolved significantly. According to Etzioni (2019), trust in strangers continues to grow even as distrust in institutions rises (Etzioni, 2019).

Cyber trust is increasingly vital for various organizations across different industries, especially in healthcare, where protecting patient data is crucial due to the growing threat of ransomware attacks. Vukotich (2023) proposes a new approach called 'zero-trust' in response to evolving cyber risks. This approach emphasizes the need for organizations to enhance cybersecurity and consider new strategies like 'zero-trust,' as current methods may be vulnerable to ongoing cyberattacks, necessitating regular system audits (Vukotich, 2023). Cybersecurity, as a developing discipline, faces challenges in accommodating human nature and potential errors. To gain a more holistic understanding of cybersecurity, Renaud and Dupuis (2023) conducted research combining religious literature and interviews with religious leaders. Their findings, evaluated by cybersecurity experts, highlight the importance of understanding human nature, using narratives, building communities, and acknowledging human needs in cybersecurity (Renaud & Dupuis, 2023).

In another study, Renaud and Searle developed a multi-level conceptual trust model addressing resilience and risk at individual, team, and organizational levels to combat cyberattacks affecting emotional, cognitive, and social processes. This model distinguishes between different types of threats and their relational consequences, examining the dynamics of trust and distrust within organizations and employees in the context of cyberattacks, and considering potential financial and reputational losses (Searle & Renaud, 2023).

4.3. Online Trust

Online trust is a key focus in understanding cyber trust and trust in virtual organizations. Bhattacherjee (2002) developed a scale for trust with three dimensions: ability, benevolence, and integrity. Using surveys of online retail and banking users, he created a 7-item trust scale showing reliability and validity. Trust significantly predicts users' willingness to transact online, reducing friction, limiting opportunistic behavior, and encouraging future transactions.

Bhattacharjee identified trust dimensions like integrity, competence, consistency, and promise fulfillment. High path coefficients were noted between trust and the three main dimensions. Simple measurement scales were emphasized to avoid respondent fatigue. Increased internet use during the pandemic raised concerns about privacy, security, and vendor reliability. Clear disclosures, personalization techniques, and digital certificates are vital for building trust (Bhattacherjee, 2002; Koehn, 2003)

Cheshire (2011) highlighted the importance of trust, trustworthiness, cooperation, and assurance in online interactions. Trust involves belief in expected actions, trustworthiness includes data security and transparency, cooperation is mutually beneficial collaboration, and assurance involves confidence-building actions like security certifications. Over-reliance on security structures instead of interpersonal trust poses risks (Cheshire, 2011).

Hurwitz (2013) discussed "trust lost" (diminished trust) and "losing trust" (gradual erosion). Challenges in intermediary responsibility due to a lack of transparency were noted. Legal rules for internet technology development are crucial, despite transparency challenges. Adapting intermediary responsibility frameworks to changing internet capabilities is key (Hurwitz, 2013).

Martin (2023) commented on Etzioni's (2019) "Cyber Trust" article, emphasizing the role of online market makers and system design in fostering trust. Ethical decisions in design and development can strengthen or undermine trust. Hussein at al. (2020) highlighted the importance of interface design elements like simplicity, familiarity, transparency, and trust indicators in building online trust (Hussein at al., 2020; Martin, 2023).

4.4. OSNs & Social Media Trust

Trust in social media and online social networks (OSNs) is vital for virtual organizations. Trust development in OSNs includes four phases: data collection, feature extraction, trust computation, and trust utilization (Faturochman, 2023; Jethava & Pratap, 2022).

Pierson (2021) studied messaging apps like WhatsApp and Facebook Messenger, highlighting their role in social communication and the concerns about data privacy and corporate influence. He introduced 'infrastructure inversion' to describe these dynamics and the need to empower users (Pierson, 2021).

Sabatini and Sarracino (2019) found that participation in social networking sites (SNS) like Facebook and Twitter negatively affects trust in strangers, neighbors, and institutions. Their study, based on interviews with over 24,000 households, showed significant trust reduction linked to SNS use (Sabatini & Sarracino, 2019).

Su (2014) examined virtual communities in OSNs, identifying opportunities for businesses to interact with customers. The study categorized OSNs into homogeneous OSNs, heterogeneous OSNs, and social internetworking scenarios (SISs), each with unique trust-related issues like interoperability and data privacy (Su, 2014).

Aggarwal at al. (2016) validated Mayer's trust model for social media within organizations, finding that the norm of reciprocity is crucial for social media trust, more so than trust propensity. Their study, involving 200 professionals and students in India, emphasized that social media trust hinges on users' belief in the reliability and authenticity of information and interactions on the platform. The research has implications for developing trustworthy social media platforms and improving organizational trust dynamics (Aggarwal at al., 2016).

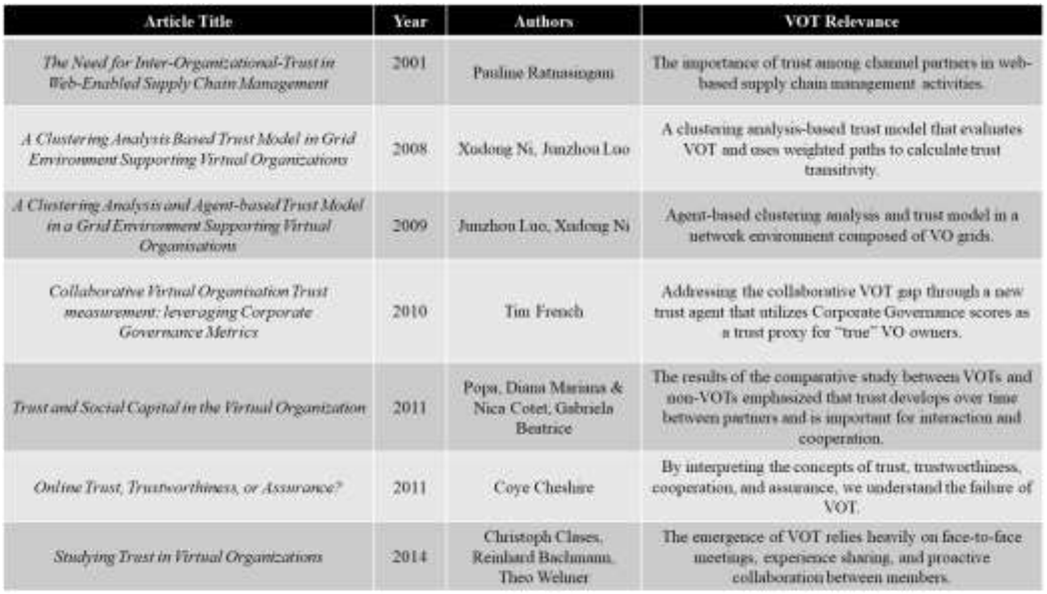
4.5. VOT – Virtual Organizational Trust

Trust in B2B (business-to-business) relationships has been a key aspect of supply chain management (SCM) for decades, predating e-commerce's growth in B2C (business-to-consumer) and C2C (consumer-to-consumer) contexts. However, Virtual Organizational Trust (VOT) still lacks a clear definition. Pauline Ratnasingam's 2001 study emphasized trust as crucial for maintaining channel partner relationships in web-based SCM, highlighting the need for better communication and trust-building among partners to thrive in e-commerce.

In B2B relationships, trust is shaped by the complexity of e-commerce applications and the nature of partner relationships. It operates on two levels: technological trust, related to web application operations, and channel partner trust (CPT), which focuses on cooperation and business commitment. CPT is built on reliability, dependability, and responsiveness, involving sub-trusts in partner competence, predictability, and benevolence. These elements offer economic, relational, and strategic benefits, suggesting that VOT reflects organizational confidence in partner reliability and performance in web-based SCM (Ratnasingam, 2001).

Crossman and Kelley (2004) noted that VOT forms through firm commitments and is essential for long-term partnerships. Trust may be harder to establish in culturally diverse virtual organizations due to the lack of prior working relationships. However, repeated interpersonal exchanges, even in virtual settings, can build trust. A trusting atmosphere fosters tolerance and sustains alliances, making trust development vital for long-term cooperation in virtual environments (Crossman & Lee-Kelley, 2004).

Table 2. Overview of the Discussion 'Trust in Virtual Organizations'
(VOT - Virtual Organizational Trust)



Article Title	Year	Authors	VOT Relevance
The Need for Inter-Organizational-Trust in Web-Enabled Supply Chain Management	2001	Pauline Ratnasingam	The importance of trust among channel partners in web-based supply chain management activities.
A Clustering Analysis Based Trust Model in Grid Environment Supporting Virtual Organizations	2008	Xudong Ni, Junzhou Luo	A clustering analysis-based trust model that evaluates VOT and uses weighted paths to calculate trust transitivity.
A Clustering Analysis and Agent-based Trust Model in a Grid Environment Supporting Virtual Organisations	2009	Junzhou Luo, Xudong Ni	Agent-based clustering analysis and trust model in a network environment composed of VO grids.
Collaborative Virtual Organisation Trust measurement: leveraging Corporate Governance Metrics	2010	Tim French	Addressing the collaborative VOT gap through a new trust agent that utilizes Corporate Governance scores as a trust proxy for "true" VO owners.
Trust and Social Capital in the Virtual Organization	2011	Popa, Diana Mariana & Nica Cotet, Gabriela Beatrice	The results of the comparative study between VOTs and non-VOTs emphasized that trust develops over time between partners and is important for interaction and cooperation.
Online Trust, Trustworthiness, or Assurance?	2011	Coye Cheshire	By interpreting the concepts of trust, trustworthiness, cooperation, and assurance, we understand the failure of VOT.
Studying Trust in Virtual Organizations	2014	Christoph Clases, Reinhard Bachmann, Theo Wehner	The emergence of VOT relies heavily on face-to-face meetings, experience sharing, and proactive collaboration between members.

Ni and Luo (2008, 2009) explored VOT in grid computing environments, focusing on trust formation and evaluation among entities. This involves secure access to grid services in dynamic environments, enabling resource sharing and cooperation among unknown entities without a central authority, relying on recommendations from existing service providers. VOT has also been applied in distributed, peer-to-peer (P2P), and grid systems, addressing trust relationships and network-specific challenges (Luo & Ni, 2008, 2009).

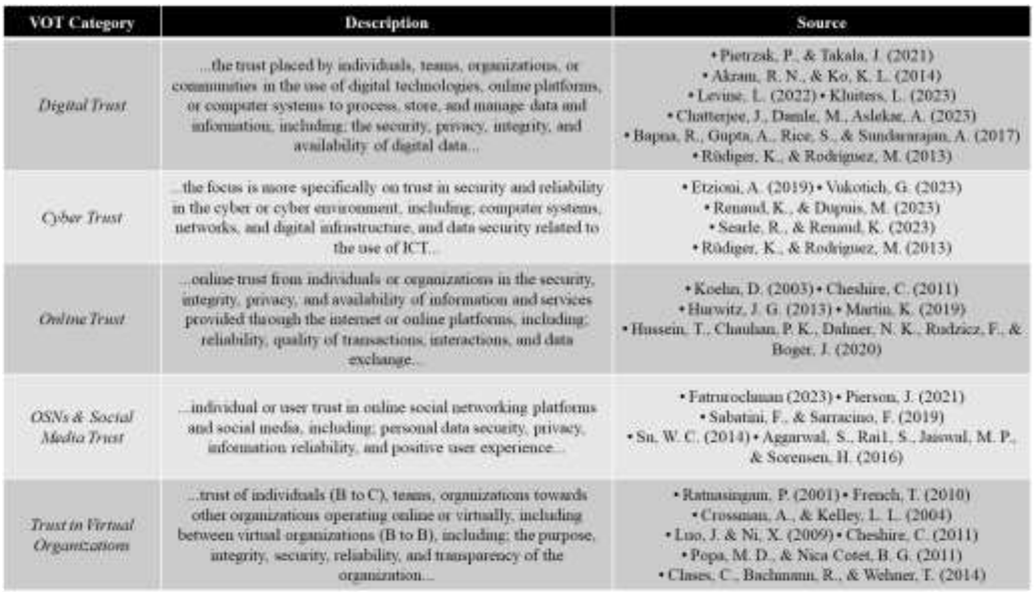
French (2010) examined VOT as the trust level among electronic partners in virtual collaboration, focusing on trust formation and validation in secure electronic transactions. Using corporate governance metrics, the study emphasized trust's importance throughout the virtual partnership lifecycle and addressed broader trust dimensions like reputation management, risk reduction, and service reliability (French, 2010).

Popa and Cotet (2011) compared virtual and non-virtual organizations, suggesting VOT is the confidence individuals have in their peers' abilities, intentions, and reliability without physical interaction. VOT is essential for cooperation and knowledge exchange in virtual settings, where communication is primarily virtual. Cheshire (2011) clarified key concepts like trust and cooperation in online environments, contributing to understanding VOT failures and online trust (Cheshire, 2011).

In virtual work, trust replaces traditional mechanisms to ensure cooperation, especially when no permanent contact or institutional arrangements exist. VOT involves personal and professional aspects, social relationships, and competence, playing a crucial role in collaboration and achieving organizational goals (Popa & Cotet, 2011).

Clases at al. (2014) analyzed VOT's subjective meaning, identifying constructs like 'feeling safe,' 'reliability,' and 'active networks.' The study emphasized proactive collaboration and personal bonds in building VOT, with communication and feedback being key (Clases at al., 2003). Details and definitions of each category and their relevance to virtual organizational trust are summarized in Table 3 for easier reference.

Table 3. Different Categories of Trust in Virtual Organizations
(VOT - Virtual Organizational Trust)



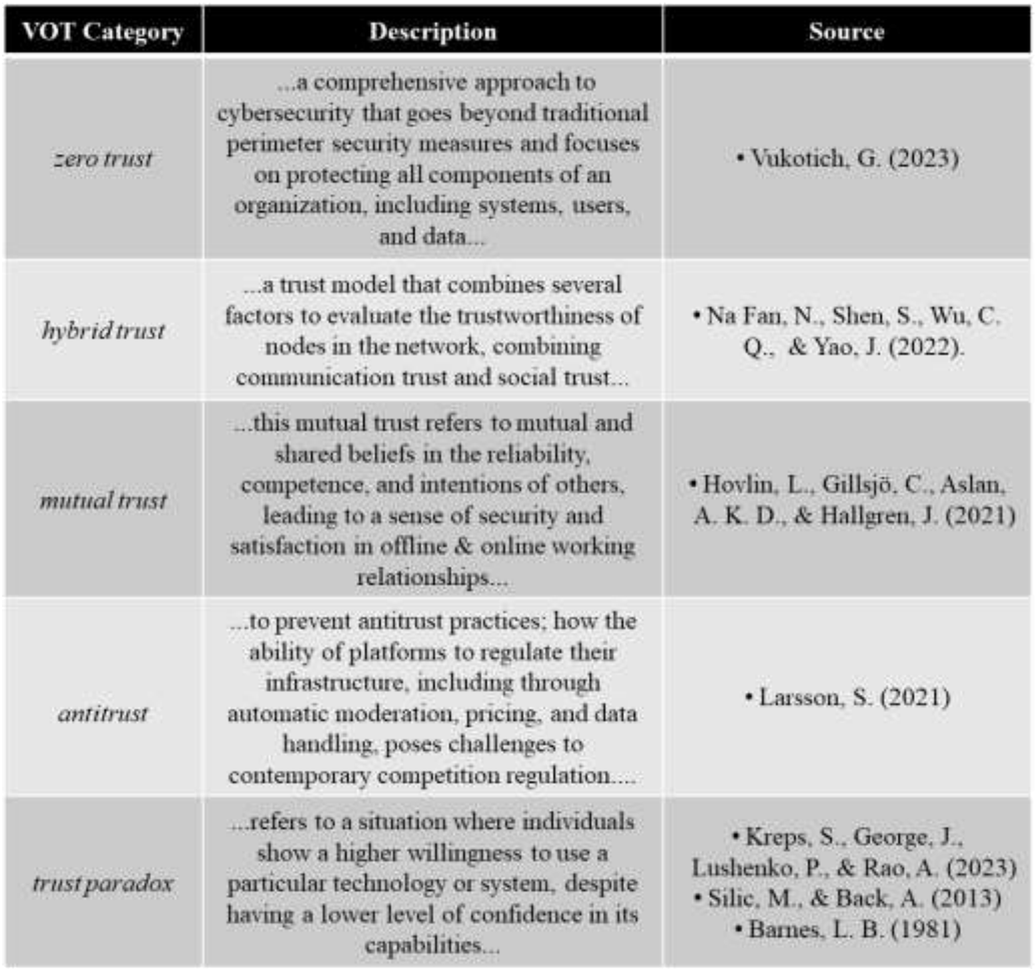
VOT Category	Description	Source
Digital Trust	...the trust placed by individuals, teams, organizations, or communities in the use of digital technologies, online platforms, or computer systems to process, store, and manage data and information, including: the security, privacy, integrity, and availability of digital data...	• Pietrzak, P., & Takala, J. (2021) • Akram, R. N., & Ko, K. L. (2014) • Levine, L. (2022) • Kluiters, L. (2023) • Chatterjee, J., Damle, M., Aslekar, A. (2023) • Bapna, R., Gupta, A., Rice, S., & Sundararajan, A. (2017) • Rüdiger, K., & Rodriguez, M. (2013)
Cyber Trust	...the focus is more specifically on trust in security and reliability in the cyber or cyber environment, including: computer systems, networks, and digital infrastructure, and data security related to the use of ICT...	• Etzioni, A. (2019) • Vukotich, G. (2023) • Renaud, K., & Dupuis, M. (2023) • Searle, R., & Renaud, K. (2023) • Rüdiger, K., & Rodriguez, M. (2013)
Online Trust	...online trust from individuals or organizations in the security, integrity, privacy, and availability of information and services provided through the internet or online platforms, including: reliability, quality of transactions, interactions, and data exchange...	• Koehn, D. (2003) • Cheshire, C. (2011) • Hurwitz, J. G. (2013) • Martin, K. (2019) • Hussein, T., Chauhan, P. K., Dalmer, N. K., Rudzicz, F., & Boger, J. (2020)
OSNs & Social Media Trust	...individual or user trust in online social networking platforms and social media, including: personal data security, privacy, information reliability, and positive user experience...	• Fatrurochman (2023) • Pierson, J. (2021) • Sabatini, F., & Sarracino, F. (2019) • Su, W. C. (2014) • Aggarwal, S., Rai1, S., Jaiswal, M. P., & Sorensen, H. (2016)
Trust in Virtual Organizations	...trust of individuals (B to C), teams, organizations towards other organizations operating online or virtually, including between virtual organizations (B to B), including: the purpose, integrity, security, reliability, and transparency of the organization...	• Ratnasingam, P. (2001) • French, T. (2010) • Crossman, A., & Kelley, L. L. (2004) • Luo, J. & Ni, X. (2009) • Cheshire, C. (2011) • Popa, M. D., & Nica Cotet, B. G. (2011) • Clases, C., Bachmann, R., & Wehner, T. (2014)

Emerging VOT-related concepts include zero trust, mutual trust, and the trust paradox. The zero trust approach is a cybersecurity strategy assuming no user or system is trustworthy by default, focusing on protecting all organizational components (Vukotich, 2023). Mutual trust involves reciprocal confidence in others' reliability and competence, impacting collaboration, job satisfaction, and service quality, requiring time investment and routine interactions (Hovlin at al., 2021).

4.6. Other VOT Approaches

The hybrid trust model combines communication and social trust to evaluate node reliability in vehicular social networks, significantly improving accuracy and communication efficiency (Fan at al., 2022).

Table 4. Other 'trust' terms in VOT.



VOT Category	Description	Source
zero trust	...a comprehensive approach to cybersecurity that goes beyond traditional perimeter security measures and focuses on protecting all components of an organization, including systems, users, and data...	• Vukotich, G. (2023)
hybrid trust	...a trust model that combines several factors to evaluate the trustworthiness of nodes in the network, combining communication trust and social trust...	• Na Fan, N., Shen, S., Wu, C. Q., & Yao, J. (2022).
mutual trust	...this mutual trust refers to mutual and shared beliefs in the reliability, competence, and intentions of others, leading to a sense of security and satisfaction in offline & online working relationships...	• Hovlin, L., Gillsjö, C., Aslan, A. K. D., & Hallgren, J. (2021)
antitrust	...to prevent antitrust practices; how the ability of platforms to regulate their infrastructure, including through automatic moderation, pricing, and data handling, poses challenges to contemporary competition regulation....	• Larsson, S. (2021)
trust paradox	...refers to a situation where individuals show a higher willingness to use a particular technology or system, despite having a lower level of confidence in its capabilities...	• Kreps, S., George, J., Lushenko, P., & Rao, A. (2023) • Silic, M., & Back, A. (2013) • Barnes, L. B. (1981)

In digital business competition, "putting trust into antitrust" emphasizes trust in data protection, privacy, and security within competition regulation. Larsson (2021) discusses how this concept addresses challenges in market definition, data valuation, dominance abuse, and transparency in digital platforms. Balancing data-sharing regulations with privacy and consumer protection is key to ensuring fairness, consumer welfare, and innovation in the data-driven economy (Larsson, 2021).

The trust paradox describes situations where individuals support technologies despite low trust in them. Kreps at al. (2023) highlight this paradox in areas like AI, armed drones, and driverless cars, where support remains high despite trust concerns. Contributing factors include FOMO, optimism about future advancements, and perceived benefits outweighing risks. Understanding this paradox is crucial for integrating AI technologies, as public trust is essential for success (Kreps at al., 2023).

Silic and Back (2013) explore the trust paradox in open-source dual-use security software (OSSS), where professionals trust the software despite its potential misuse by hackers. This paradox highlights the conflicting risks and benefits of OSSS, emphasizing the trust placed in its developers and functionality (Silic & Back, 2013).

Previously, the trust paradox in organizations was defined as balancing trust and distrust, with both extremes potentially harming organizational dynamics. Barnes (1981) noted that fragile trust could lead to widespread distrust, while excessive trust might negatively impact the organization (Barnes, 1981). About this trust paradox, James (2002) further emphasizes understanding how trust is developed and incentivized in economic contexts, exploring when agents are willing to trust (James, 2002). Thus, the explanation of various trust-related terms in VOT is summarized in Tables 2, 3, and 4.

5. DISCUSSION – NEW TECHNOLOGY ADVANCEMENTS AND THEIR IMPACT

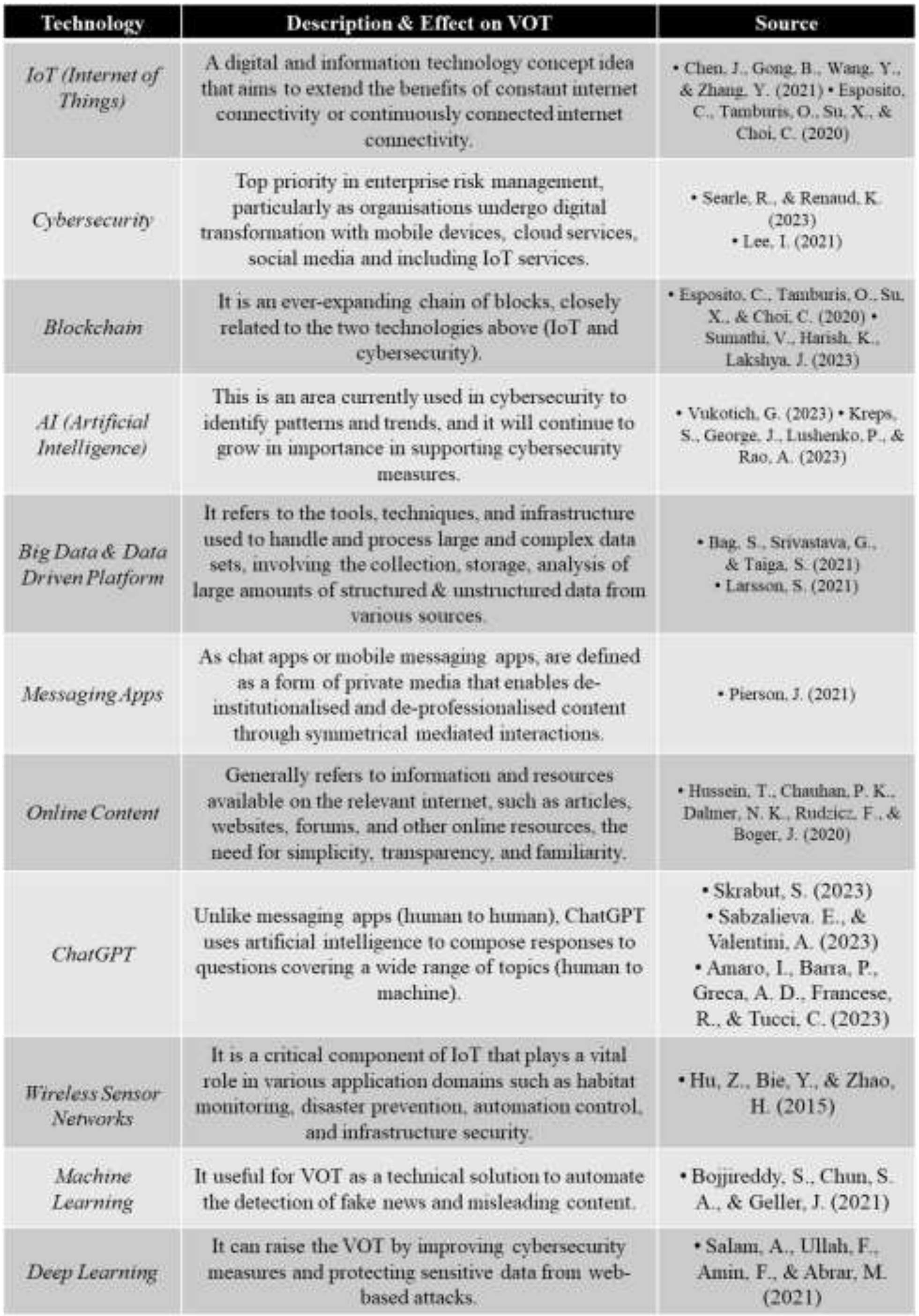
Advancements in science and technology have reshaped work dynamics, influencing trust at individual, team, organizational, and inter-organizational levels. Trust in the virtual realm, particularly VOT (Virtual Organizational Trust), is now intertwined with public and global trust (Faturochman, 2023). Technological progress introduces new challenges for trust, especially in information and digital technologies, making discussions about VOT increasingly relevant. These advancements affect interpersonal trust, leadership, organizational development, and overall performance

Emerging technologies such as IoT, cybersecurity, blockchain, AI, big data, messaging apps, and online content (Table 5), along with digital twins, quantum computing, metaverse, AR, VR, MR, and XR (Table 6), will increasingly influence digital trust and VOT.

5.1. IoT – Internet of Things

The concept of IoT aims to expand the benefits of constant internet connectivity and advances in IoT technology impact VOT (Virtual Organizational Trust). Chen at al. (2021) proposed a multidimensional attribute trust model to enhance the security of interactions between IoT nodes by using satisfaction records to identify abnormal data and reduce its influence on trust evaluation.

Table 5. Different Types of Technology and Their Effects on VOT.



Technology	Description & Effect on VOT	Source
IoT (Internet of Things)	A digital and information technology concept idea that aims to extend the benefits of constant internet connectivity or continuously connected internet connectivity.	• Chen, J., Gong, B., Wang, Y., & Zhang, Y. (2021) • Esposito, C., Tamburis, O., Su, X., & Choi, C. (2020)
Cybersecurity	Top priority in enterprise risk management, particularly as organisations undergo digital transformation with mobile devices, cloud services, social media and including IoT services.	• Searle, R., & Renaud, K. (2023) • Lee, I. (2021)
Blockchain	It is an ever-expanding chain of blocks, closely related to the two technologies above (IoT and cybersecurity).	• Esposito, C., Tamburis, O., Su, X., & Choi, C. (2020) • Sumathi, V., Harish, K., Lakshya, J. (2023)
AI (Artificial Intelligence)	This is an area currently used in cybersecurity to identify patterns and trends, and it will continue to grow in importance in supporting cybersecurity measures.	• Vukotich, G. (2023) • Kreps, S., George, J., Lushenko, P., & Rao, A. (2023)
Big Data & Data Driven Platform	It refers to the tools, techniques, and infrastructure used to handle and process large and complex data sets, involving the collection, storage, analysis of large amounts of structured & unstructured data from various sources.	• Bag, S., Srivastava, G., & Taiga, S. (2021) • Larsson, S. (2021)
Messaging Apps	As chat apps or mobile messaging apps, are defined as a form of private media that enables de-institutionalised and de-professionalised content through symmetrical mediated interactions.	• Pierson, J. (2021)
Online Content	Generally refers to information and resources available on the relevant internet, such as articles, websites, forums, and other online resources, the need for simplicity, transparency, and familiarity.	• Hussein, T., Chauhan, P. K., Dalmer, N. K., Rudzicz, F., & Boger, J. (2020)
ChatGPT	Unlike messaging apps (human to human), ChatGPT uses artificial intelligence to compose responses to questions covering a wide range of topics (human to machine).	• Skrabut, S. (2023) • Sabzalieva, E., & Valentini, A. (2023) • Amaro, I., Barra, P., Greca, A. D., Francese, R., & Tucci, C. (2023)
Wireless Sensor Networks	It is a critical component of IoT that plays a vital role in various application domains such as habitat monitoring, disaster prevention, automation control, and infrastructure security.	• Hu, Z., Bie, Y., & Zhao, H. (2015)
Machine Learning	It useful for VOT as a technical solution to automate the detection of fake news and misleading content.	• Bojjireddy, S., Chun, S. A., & Geller, J. (2021)
Deep Learning	It can raise the VOT by improving cybersecurity measures and protecting sensitive data from web-based attacks.	• Salam, A., Ullah, F., Amin, F., & Abrar, M. (2021)

By building trusted groups based on this model, network overhead is minimized, improving group consensus and enhancing trust and security within IoT networks (Chen at al., 2021).

However, IoT technology faces challenges in establishing security policies and access control with decentralized VOT management. Traditional static access control models struggle with moving objects and multi-tenant infrastructure. Esposito at al. (2020) proposed a solution using game theory and Dempster-Shafer theory for decentralized, robust VOT, tolerant of malicious nodes. Empirical research supported this approach with blockchain-based trust management for IoT. The study recommended using SSL/TLS for secure communication and restricting nodes that can update trust levels, though noting limitations against compromised nodes sending false scores. SSL/TLS is a cryptographic protocol ensuring secure communication and protecting sensitive information online (Esposito at al., 2020).

5.2. Cybersecurity

In the context of Virtual Organizational Trust (VOT), cybersecurity is vital in managing corporate risk, particularly during digital transformations involving mobile devices, cloud services, social media, and IoT. Cyberattacks can undermine VOT by creating vulnerabilities and eroding trust among employees and stakeholders. The emotional, cognitive, and social impacts of such attacks can lead to widespread distrust. Limited cybersecurity resources and insufficient leadership further weaken organizational resilience against future attacks. The severity and intensity of these attacks amplify their negative effects on trust (Searle & Renaud, 2023).

Lee (2021) proposed a cybersecurity risk management framework with a critical risk assessment layer, focusing on data protection and privacy amid evolving regulations and rising cyber threats. Organizational factors, including positive attitudes towards cybersecurity policies and leadership support, are crucial in shaping cyber defense strategies. The framework also emphasizes leveraging machine learning and AI to enhance cybersecurity, with a focus on developing and operationalizing systems based on performance goals. This includes assessing cyber technologies and considering both internal and external factors that influence cybersecurity outcomes (Lee, 2021).

5.3. Blockchain

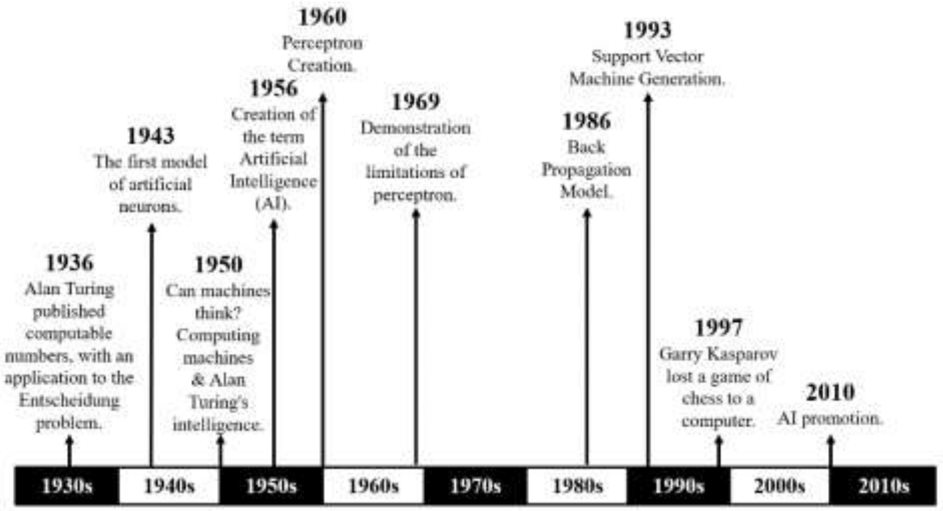
Blockchain technology secures communication and ensures system integrity using cryptographic techniques, particularly in IoT trust management. Its decentralized approach is effective for establishing security policies and access control in IoT environments, where nodes validate security claims through cryptographic methods. However, compromised nodes can still deceive the system by sending false scores, a challenge that conventional cryptographic techniques may not fully address (Esposito at al., 2020).

Blockchain is also viewed as a solution to enhance trust in financial services like crowdfunding and stock markets. On the Ethereum platform, blockchain offers transparency and security, making it ideal for developing decentralized crowdfunding applications (dApps). Ethereum’s smart contracts eliminate intermediaries, creating a more efficient, trustworthy, and automated system that ensures transparency and security in crowdfunding (Sumathi at al., 2023).

5.4. AI – Artificial Intelligence

Artificial intelligence (AI) will not replace humans; rather, as Prof. Karim Lakhani from Harvard Business School stated on August 4, 2023, "AI will not replace humans — but humans with AI will replace humans without AI." AI is increasingly used across various fields, particularly in cybersecurity, to identify threats and reduce response times. AI's rapid growth (Figure 3), including machine learning and natural language processing, is crucial for providing insights and automating security responses. AI-enabled technologies, such as driverless cars and social media content moderation, enhance efficiency and safety in their respective areas. AI has the potential to support VOT by mimicking human cognitive abilities and decision-making processes (Kreps at al., 2023; Vukotich, 2023).

Figure 3. Timeline of Artificial Intelligence (AI) Development


1960
Perceptron Creation.
1993
Support Vector Machine Generation.
1956
Creation of the term Artificial Intelligence (AI).
1969
Demonstration of the limitations of perceptron.
1943
The first model of artificial neurons.
1986
Back Propagation Model.
1936
Alan Turing published computable numbers, with an application to the Entscheidung problem.
1950
Can machines think? Computing machines & Alan Turing's intelligence.
1997
Garry Kasparov lost a game of chess to a computer.
2010
AI promotion.
1930s
1940s
1950s
1960s
1970s
1980s
1990s
2000s
2010s

Source: Adopted from Fernandez at al. (2020).

5.5. Big Data & Data-Driven Platforms

Big data technology encompasses tools and techniques for managing and processing large, complex datasets, both structured and unstructured. It involves collecting, storing, and analyzing data to uncover patterns, correlations, and insights, enhancing organizational productivity, decision-making, and sustainability. Trust in organizations is strengthened through ethical training and audits, which are essential for maintaining a positive ethical culture (Bag at al., 2021).

Larsson (2021) highlights that data-driven platforms are pivotal in the digital economy, significantly influencing competition regulation and governance in building VOT. These platforms use algorithms and data analysis to generate insights, make decisions, and offer personalized experiences. However, their control over infrastructure, such as automated moderation and pricing, poses challenges for competition authorities and can lead to anti-competitive effects. Transparency and public trust are crucial in the governance of these platforms. (Larsson, 2021).

5.6. Messaging Apps, Online Content & ChatGPT

Messaging apps, essential for mobile communication and information exchange, play a key role in Virtual Organizational Trust (VOT). Despite their importance, a trust paradox exists: users rely on these platforms daily but feel powerless regarding data privacy. Popular apps like WhatsApp and Messenger, owned by Facebook, highlight the need for data transparency to build long-term trust (Pierson, 2021).

Hussein at al. (2020) emphasize that "online content," such as articles and websites, must be easily accessible and trustworthy, with interface design focusing on simplicity and transparency to support VOT (Hussein at al., 2020).

Skrabut (2023) highlights that since its launch in November 2022, ChatGPT has significantly impacted various sectors, including higher education, print media, and the Internet. Unlike messaging apps, ChatGPT uses AI to generate responses on diverse topics, facilitating human-AI interactions. It can be explained that it is an OpenAI-developed language model, a variant of GPT, trained on extensive conversational text data. ChatGPT performs tasks like language translation, question answering, and text generation (Skrabut, 2023).

In higher education, Sabzalieva and Valentini (2023) describe ChatGPT as a generative AI system that creates realistic images and art from text. They emphasize its role in enabling natural human-computer interactions, making it a powerful tool in educational contexts (Sabzalieva & Valentini, 2023).

Amaro at al. (2023) examines the role of trust in ChatGPT, comparing trust levels among participants exposed to true and false information. The Wilcoxon signed-rank test revealed significant differences in trust levels, with a p-value of 0.0077, suggesting that the type of information received can influence trust (Amaro at al., 2023).

5.7. Wireless Sensor Networks

Hu at al. (2015) state that wireless sensor networks (WSNs) are essential to IoT, with applications in habitat monitoring, disaster prevention, automation, and infrastructure security. WSNs use nodes with sensors to collect data, relying on ad hoc routing due to their limited communication range and computing power. Traditional network protocols are unsuitable for WSNs, requiring specialized routing protocols and algorithms for efficient data transmission and security. Implementing cryptography, authentication, and VOT management is crucial to enhancing security and protecting network performance (Hu at al., 2015).

5.8. Machine Learning & Deep Learning

Machine learning can enhance VOT by automating the detection of fake news. Bojjireddy at al. (2021) developed a web application that allows users to select machine-learning models and datasets for fake news detection. They tested six models—support vector machine, multilayer perceptron, random forest, decision tree, gradient boosting, and multinomial naive Bayes—on combined datasets, providing real-time news classification and sentiment analysis (Bojjireddy at al., 2021).

Salam at al. (2023) highlight that deep learning, including CNNs, RNNs, and transformer models, can improve VOT by enhancing cybersecurity and protecting against web-based attacks. These technologies help create secure virtual environments and build stakeholder confidence (Salam at al., 2023).

5.9. The Influence of Other Technologies

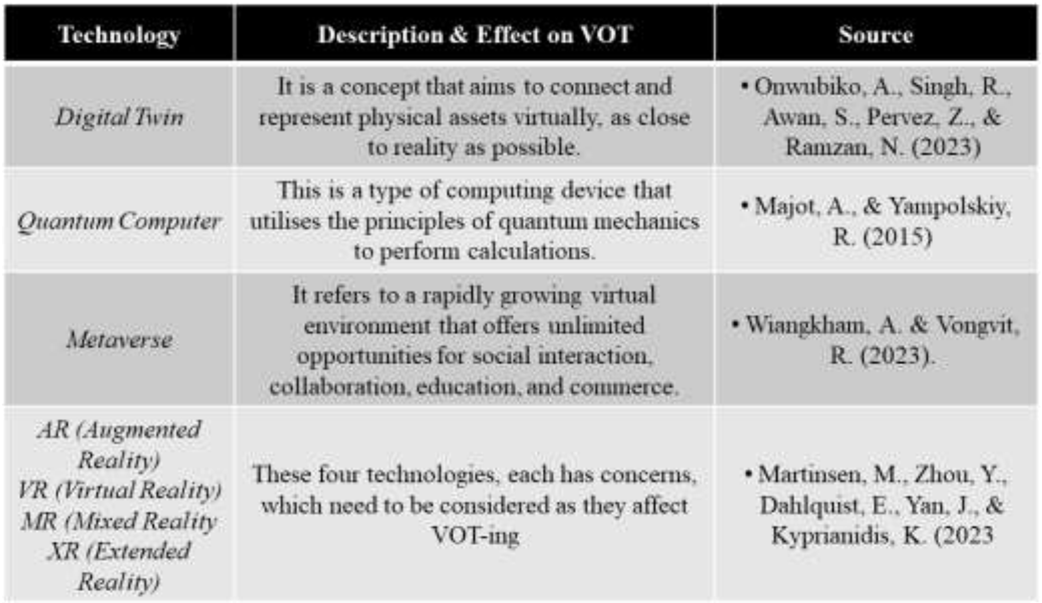
This session explores emerging technologies like digital twins, quantum computers, the metaverse, and AR/VR/MR/XR (Table 6). Digital twins replicate physical assets virtually, using data across their lifecycles. Blockchain, especially Ethereum, can address trust and security issues, enhancing VOT with reliable, cost-effective systems and secure data transactions (Onwubiko at al., 2023).

Quantum computers, leveraging quantum mechanics, offer faster processing than classical computers. While promising in fields like cryptography, they pose risks if misused, necessitating restrictions on reputable institutions and governments (Majot & Yampolskiy, 2014).

The metaverse, a virtual space powered by VR and AR, enables global collaboration, education, and commerce. Its success in VOT hinges on reliability, privacy, and asset protection (Wiangkham & Vongvit, 2023).

Martinsen at al. (2023) highlight that AR, VR, MR, and XR technologies enhance VOT by improving service experiences, training, productivity, and cost savings across various sectors, including gaming, healthcare, and engineering (Martinsen at al., 2023).

Table 6. Other Technologies and Their Influence on VOT.



Technology	Description & Effect on VOT	Source
Digital Twin	It is a concept that aims to connect and represent physical assets virtually, as close to reality as possible.	• Onwubiko, A., Singh, R., Awan, S., Pervez, Z., & Ramzan, N. (2023)
Quantum Computer	This is a type of computing device that utilises the principles of quantum mechanics to perform calculations.	• Majot, A., & Yampolskiy, R. (2015)
Metaverse	It refers to a rapidly growing virtual environment that offers unlimited opportunities for social interaction, collaboration, education, and commerce.	• Wiangkham, A. & Vongvit, R. (2023).
AR (Augmented Reality) *VR (Virtual Reality)* *MR (Mixed Reality* *XR (Extended Reality)*	These four technologies, each has concerns, which need to be considered as they affect VOT-ing	• Martinsen, M., Zhou, Y., Dahlquist, E., Yan, J., & Kyprianidis, K. (2023

Each technology poses concerns for VOT. AR raises privacy issues due to real-world data capture, potentially compromising security. VR can cause motion sickness or discomfort, limiting its adoption. MR may blur the line between virtual and real worlds, leading to confusion or disorientation, affecting physical and mental health. XR, combining AR, VR, and MR, may inherit challenges from all three (Martinsen at al., 2023).

6. IMPLICATION – DYNAMICS AND CYCLE OF VOT STAGES

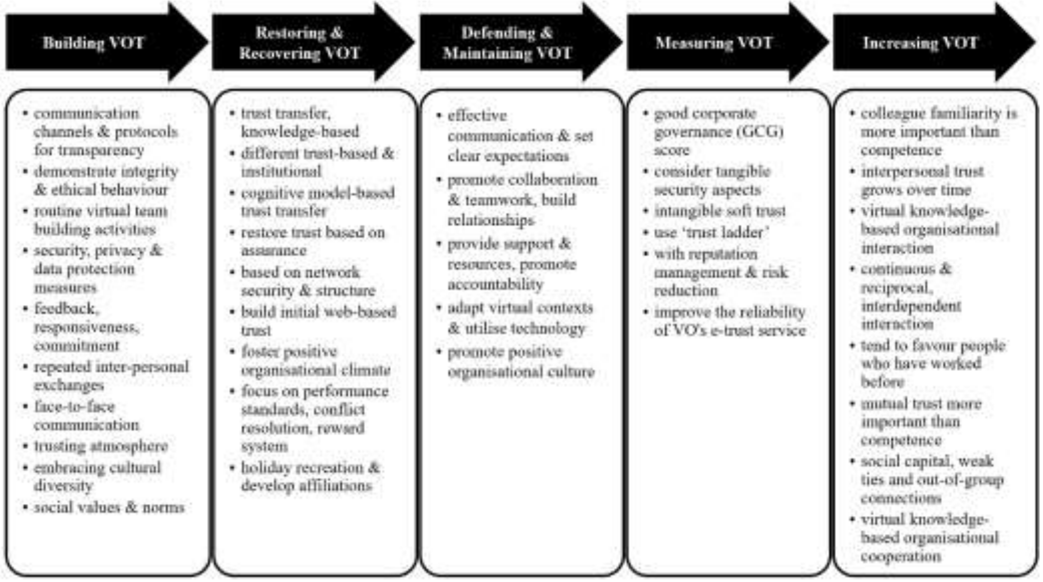
As technology rapidly advances, trust dynamics in VOT evolve. Trust dynamics involve changes in trust levels in a virtual organization. This discussion covers the stages of the trust cycle—building, restoring, maintaining, measuring, and enhancing trust (Figure 4)—with examples of how trust is developed, maintained, and transferred amid technological changes in online relationships (Giest, 2019).

6.1. Building VOT

Bhattacherjee (2022) outlines key steps for building trust in VOT: establish clear communication for transparency, demonstrate integrity to foster collaboration, create opportunities for personal connections through team activities, implement strong security measures to protect data and encourage feedback to show responsiveness and commitment (Bhattacherjee, 2002).

Building VOT also involves developing personal relationships within networks, with intermediaries extending trust between individuals (Giest, 2019). A sustainable VOT process requires strong commitment, repeated interpersonal exchanges, a mutual trust atmosphere, acceptance of cultural diversity, and addressing the limitations of computer-mediated communication (Crossman & Lee-Kelley, 2004).

Figure 4. Dynamics and Cycle of VOT Stages.



Building VOT

- communication channels & protocols for transparency
- demonstrate integrity & ethical behaviour
- routine virtual team building activities
- security, privacy & data protection measures
- feedback, responsiveness, commitment
- repeated inter-personal exchanges
- face-to-face communication
- trusting atmosphere
- embracing cultural diversity
- social values & norms

Restoring & Recovering VOT

- trust transfer, knowledge-based
- different trust-based & institutional
- cognitive model-based trust transfer
- restore trust based on assurance
- based on network security & structure
- build initial web-based trust
- foster positive organisational climate
- focus on performance standards, conflict resolution, reward system
- holiday recreation & develop affiliations

Defending & Maintaining VOT

- effective communication & set clear expectations
- promote collaboration & teamwork, build relationships
- provide support & resources, promote accountability
- adapt virtual contexts & utilise technology
- promote positive organisational culture

Measuring VOT

- good corporate governance (GCG) score
- consider tangible security aspects
- intangible soft trust
- use 'trust ladder'
- with reputation management & risk reduction
- improve the reliability of VO's e-trust service

Increasing VOT

- colleague familiarity is more important than competence
- interpersonal trust grows over time
- virtual knowledge-based organisational interaction
- continuous & reciprocal, interdependent interaction
- tend to favour people who have worked before
- mutual trust more important than competence
- social capital, weak ties and out-of-group connections
- virtual knowledge-based organisational cooperation

6.2. Restoring and Recovering VOT

Stewart (2003) argues that trust transfer is crucial in restoring VOT and can occur through various methods, including knowledge-based, domain-based, institution-based, and cognitive trust transfer. Trust can be transferred from trusted websites or associations to virtual organizations, shaping consumers' initial trust. Restoring trust may also involve assurances, safety nets, or similar structures. Developing and testing cognitive models of trust transfer can help establish trust in online organizations (Stewart, 2003).

Birdie and Jain (2016) suggest key steps for restoring and rebuilding VOT. First, create a positive organizational climate by focusing on performance, conflict resolution, rewards, and identity, as these factors boost trust among virtual workers. To build affiliation, organize recreational activities, such as special holidays or club memberships for virtual workers and their families (Birdie & Jain, 2016).

Another critical step is to encourage face-to-face contact. Physical interactions can be key to developing VOT, so promoting in-person meetings can enhance trust among members of a virtual organization. Birdie and Jain (2016) also highlight the need for further research to draw concrete conclusions and implications for organizational behavior in virtual work contexts. Research comparing face-to-face professional workers, cross-cultural and longitudinal studies, increasing sample sizes, involving more sectors, and adding demographic variables can provide deeper and more comprehensive insights. Encouraging face-to-face interactions is also crucial for developing VOT, as in-person meetings can strengthen trust within virtual organizations. They emphasize the need for further research, including cross-cultural studies, larger sample sizes, and more diverse sectors, to gain deeper insights into organizational behavior in virtual contexts (Birdie & Jain, 2016).

6.3. Defending and Maintaining VOT

Maintaining VOT requires ongoing efforts to strengthen trust in remote teams. Gustafsson at al. (2021) suggest strategies such as effective communication, clear expectations, teamwork, relationship building, providing support, promoting accountability, adapting to the virtual environment, and fostering a positive organizational culture. VOT is sustained through clear expectations, transparency, collaboration, support, and adaptability, requiring cooperation and effective organization to navigate disruptions or changes (Gustafsson at al., 2021).

6.4. Measuring VOT

French (2010) suggests that VOT can be measured using objective metrics and trust concepts, with Corporate Governance (CG) scores serving as a proxy for trust in virtual organizations. CG scores, provided by trusted third parties, offer an objective measure of e-service trustworthiness at runtime and indicate consumer trust levels in the virtual organization. The Trust Ladder is also proposed to simplify and manage trust throughout the e-trust lifecycle in VOs. VOT considers both tangible security and intangible trust factors, like reputation management and reliability. However, the limitations of CG scores highlight the need for further research in VOT measurement (French, 2010).

6.5. Increasing VOT

Popa and Cotet (2011) conducted a comparative case study using online surveys among members of virtual and non-virtual organizations in Europe. Their findings emphasize that a) familiarity with colleagues is more critical than competence, b) interpersonal trust, which develops over time, is fundamental to interactions in virtual knowledge-based organizations, c) ongoing interaction and mutual dependence foster virtual organizations, d) individuals in virtual organizations prefer working with those they trust rather than just those who are competent, e) social capital, including weak ties, contributes to VOT, and f) cooperation in virtual knowledge-based organizations relies heavily on trust.

Overall, familiarity, interpersonal trust, ongoing interaction, mutual dependence, prior relationships, social capital, and trust are key to building VOT (Popa & Cotet, 2011).

Vukotich (2023) suggests several measures enhance VOT: 1) implementing strong cybersecurity measures, including AI to detect threats, and improve security and trust; 2) adopting a ‘zero trust’ approach, which verifies every user and device, prevents unauthorized access and builds VOT; 3) educating users on cybersecurity best practices helps prevent malware and unauthorized access, increasing trust; 4) using two-factor or multi-factor authentication, such as 2-step verification, further strengthens security and VOT (Vukotich, 2023).

7. CONCLUSIONS

Advancements in science and technology, especially in information and digital technology, continuously shape and redefine trust among individuals, teams, and organizations. This rapid evolution necessitates ongoing adaptation within organizations to navigate volatile, uncertain, complex, and ambiguous environments.

Virtual Organizational Trust (VOT) is intrinsically linked to public trust, as both are general and global (Faturochman, 2023). Trust dynamics within and between virtual organizations have become increasingly complex due to technological progress, influencing interpersonal trust, leadership trust, organizational development, and overall performance. Future research will explore VOT's impact on collaboration, knowledge sharing, and performance (Gefen at al., 2008). This includes addressing challenges and strategies for building and maintaining VOT, considering factors like geographical dispersion, cultural differences, and technology-mediated communication.

Additionally, the research will examine the role of trust in virtual markets and online platforms, investigating how it affects consumer behavior, online transactions, and e-commerce success (Gefen at al., 2008). Chatterjee at al. (2023) highlight future research opportunities to study the impact of fraud on digital trust in Industry 4.0 and Society 5.0, exploring techniques to mitigate fraud risks in virtual organizations (Chatterjee at al., 2023; Fukuyama, 2018).

Scientific progress, particularly in cognitive neuroscience, offers significant potential for understanding online trust (Gefen at al., 2008; Mhatre & Mehta, 2022). Future research could explore the neural mechanisms underlying VOT, including brain processes related to trust, such as prefrontal cortex activation and oxytocin release. Integrating neuroscience with organizational psychology can provide deeper insights into the cognitive and emotional processes underlying

VOT, guiding the development of effective trust-building interventions in virtual teams (Mhatre & Mehta, 2022; Zak, 2018).

Research on digital transformation technologies, including AI and security measures, is crucial for enhancing VOT (Lumineau at al., 2023). Practical steps include implementing robust cybersecurity measures, adopting 'zero trust' approaches, and educating users on best practices for cybersecurity to prevent fraud and enhance trust among stakeholders (Chatterjee at al., 2023; Fukuyama, 2018). Furthermore, fostering face-to-face interactions and team-building activities can enhance interpersonal trust and organizational culture within virtual environments.

Future research should concentrate on cross-cultural and longitudinal studies, the impact of digital transformation technologies, neural correlates of trust, fraud risk mitigation, and the effects of Industry 4.0 and Society 5.0 on virtual organizational dynamics and worker well-being. The limitations of this study include reliance on survey data, geographical constraints, the rapid evolution of technology, and the complexity of measuring trust.

REFERENCES

Aggarwal, S., Rai, S., Jaiswal, M. P., & Sorensen, H. (2016). *Norm of Reciprocity – Antecedent of Trustworthiness*. *2*, 411–418. https://doi.org/10.1007/978-3-319-45234-0

Akram, R. N., & Ko, R. K. L. (2015). Digital trust - Trusted computing and beyond: A position paper. *Proceedings - 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, 884–892. https://doi.org/10.1109/TrustCom.2014.116

Alpcan, T., Levi, A., & Savas, E. (2011). *Digital Trust Games : An Experimental Study*. 182–183.

Amaro, I., Barra, P., Greca, A. Della, Francese, R., & Tucci, C. (2023). Believe in Artificial Intelligence? A User Study on the ChatGPT&#x2019;s Fake Information Impact. *IEEE Transactions on Computational Social Systems*, 1–10. https://doi.org/10.1109/TCSS.2023.3291539

Ameliah, R., Negara, R. A., Minarto, B., Manurung, T. M., & Akba, M. (2022). Status Literasi Digital di Indonesia 2022. *Kominfo*, *November*, 205–207. https://www.c2es.org/content/renewable-energy/

Bag, S., Srivastava, G., Gupta, S., & Taiga, S. (2021). Diffusion of Big Data Analytics Innovation in Managing Natural Resources in the African Mining Industry. *Journal of Global Information Management*, *30*(6), 1–21. https://doi.org/10.4018/JGIM.297074

Bapna, R., Gupta, A., Rice, S., & Sundararajan, A. (2017). Trust and The Strength of Ties in Online Social Networks: An Exploratory Field Experiment. *MIS Quarterly*, *41*(1), 115–130. https://www.jstor.org/stable/10.2307/26629639%0AJSTOR

Barnes, L. B. (1981). Managing the paradox of organizational trust. *Harvard Business Review*, *March*, 107–116.

Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. *Business Horizons*, *57*(3), 311–317. https://doi.org/10.1016/j.bushor.2014.01.001

Bennis, W. (2007). The challenges of leadership in the modern world: Introduction to the special Issue. *American Psychologist*, *62*(1), 2–5. https://doi.org/10.1037/0003-066X.62.1.2

Bennis, W., & Nanus, B. (1985). *Leaders : the strategies for taking charge* (I. Archive (ed.); second). Harper & Row.

Bennis, W., & Nanus, B. (2016). *Leaders: STRATEGIES FOR TAKING CHARGE SECOND EDITION*. *4*(1), 1–23.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems*, *19*(1), 211–241. https://doi.org/10.1080/07421222.2002.11045715

Birdie, A. K., & Jain, M. (2016). Perceived Organizational Climate & Interpersonal Trust among Virtual Workers. *Indian Journal of Industrial Relations*, *51*(4), 609–619.

Bojjireddy, S., Chun, S. A., & Geller, J. (2021). Machine Learning Approach to Detect Fake News, Misinformation in COVID-19 Pandemic. *ACM International Conference Proceeding Series*, 575–578. https://doi.org/10.1145/3463677.3463762

Chatterjee, J., Damle, M., & Aslekar, A. (2023). *Digital Trust in Industry 4.0 & 5.0: Impact of Frauds*. *vi*, 922–928. https://doi.org/10.1109/iciccs56967.2023.10142925

Chatterjee, S., Chaudhuri, R., & Vrontis, D. (2022). Does remote work flexibility enhance organization performance? Moderating role of organization policy and top management support. *Journal of Business Research*, *139*(October 2021), 1501–1512. https://doi.org/10.1016/j.jbusres.2021.10.069

Chen, J., Gong, B., Wang, Y., & Zhang, Y. (2021). Construction of Internet of things trusted group based on multidimensional attribute trust model. *International Journal of Distributed Sensor Networks*, *17*(1). https://doi.org/10.1177/1550147721989888

Cheshire, C. (2011). Online Trust, Trustworthiness, or Assurance? *Academy of Management Review*, *8*(4), 539–546.

Crossman, A., & Lee-Kelley, L. (2004). Trust, commitment and team working: The paradox of virtual organizations. *Global Networks*, *4*(4), 375–390. https://doi.org/10.1111/j.1471-0374.2004.00099.x

Dobrygowski, D. (2023). *Companies Need to Prove They Can Be Trusted with Technology*. Harvard Business Review. https://hbr.org/2023/07/companies-need-to-prove-they-can-be-trusted-with-technology

Esposito, C., Tamburis, O., Su, X., & Choi, C. (2020). Robust Decentralised Trust Management for the Internet of Things by Using Game Theory. *Information Processing and Management*, *57*(6), 102308. https://doi.org/10.1016/j.ipm.2020.102308

Etzioni, A. (2019). Cyber Trust Author (s): Amitai Etzioni. *Journal of Business Ethics*, *156*(1), 1–13. https://doi.org/10.1007/sl0551-017-3627-y

Fan, N., Shen, S., Wu, C. Q., & Yao, J. (2022). A hybrid trust model based on communication and social trust for vehicular social networks. *International Journal of Distributed Sensor Networks*, *18*(5). https://doi.org/10.1177/15501329221097588

Faturochman. (2023). *Kepercayaan Interpersonal* (A. I. A. (ed.); 1st ed., Vol. 1). Pustaka Pelajar.

Flanagan, F. (2019). Theorising the gig economy and home-based service work. *Journal of Industrial Relations*, *61*(1), 57–78. https://doi.org/10.1177/0022185618800518

French, T. (2010). Collaborative virtual organisation trust measurement: Leveraging Corporate Governance metrics. *2010 International Conference on Information Society, i-Society 2010*, 490–497. https://doi.org/10.1109/i-society16502.2010.6018763

Friedman, B., Kahn, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34–40. https://doi.org/10.1145/355112.355120

Fukuyama, M. (2018). Society 5.0: Aiming for a New Human-centered Society. *Japan SPOTLIGHT*, *August*, 8–13.

Gefen, D., Benbasat, I., & Pavlou, P. A. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems*, *24*(4), 275–286. https://doi.org/10.2753/MIS0742-1222240411

Giest, S. (2019). Trust Dynamics in Innovation Networks: The Chicago Life Science Cluster. *Administration and Society*, *51*(2), 325–343. https://doi.org/10.1177/0095399717701522

Gustafsson, S., Gillespie, N., Searle, R., Hailey, V. H., & Dietz, G. (2021). Preserving Organizational Trust During Disruption. *Organization Studies*, *42*(9), 1409–1433. https://doi.org/10.1177/0170840620912705

Hacker, J., Johnson, M., Saunders, C., & Thayer, A. L. (2019). Trust in virtual teams: A multidisciplinary review and integration. *Australasian Journal of Information Systems*, *23*(January), 1–36. https://doi.org/10.3127/ajis.v23i0.1757

Hooker, J. N. (2019). Trusting Algorithms in Society 5.0. *Springer Optimization and Its Applications*, *152*, 13–16. https://doi.org/10.1007/978-3-030-28565-4_3

Hovlin, L., Gillsjö, C., Aslan, A. K. D., & Hallgren, J. (2021). Mutual trust is a prerequisite for nurses' sense of safety and work satisfaction – Mobile Integrated Care Model: A qualitative interview study. *Nordic Journal of Nursing Research*, 205715852110621. https://doi.org/10.1177/20571585211062166

Hu, Z., Bie, Y., & Zhao, H. (2015). Trusted tree-based trust management scheme for secure routing in wireless sensor networks. *International Journal of Distributed Sensor Networks*, *2015*. https://doi.org/10.1155/2015/385849

Hurwitz, J. (2013). *Author (s): Justin (Gus) Hurwitz Source : University of Pennsylvania Law Review , May 2013 , Vol . 161 , No . 6 (May 2013), Published by : The University of*

Pennsylvania Law Review Stable URL : https://www.jstor.org/stable/23527813. *161*(6), 1579–1622.

Hussein, T., Chauhan, P. K., Dalmer, N. K., Rudzicz, F., & Boger, J. (2020). Exploring interface design to support caregivers' needs and feelings of trust in online content. *Journal of Rehabilitation and Assistive Technologies Engineering*, *7*, 205566832096848. https://doi.org/10.1177/2055668320968482

James, H. S. (2002). The trust paradox: A survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior and Organization*, *47*(3), 291–307. https://doi.org/10.1016/S0167-2681(01)00214-1

Jethava, G., & Pratap, U. (2022). A novel trust prediction approach for online social networks based on multifaceted feature similarity. *Cluster Computing*, *25*(6), 3829–3843. https://doi.org/10.1007/s10586-022-03617-z

Kluiters, L., Srivastava, M., & Tyll, L. (2023). The impact of digital trust on firm value and governance: an empirical investigation of US firms. *Society and Business Review*, *18*(1), 71–103. https://doi.org/10.1108/SBR-07-2021-0119

Koehn, D. (2003). The Nature of and Conditions for Online Trust Author(s): *Journal of Business Ethics*, *43*(1/2), 3–19. https://www.jstor.org/stable/25074972

Kominfo. (2020). *Program LiterasiDigital Nasional: "Indonesia Makin CakapDigital."* https://literasidigital.id/profil

Kreps, S., George, J., Lushenko, P., & Rao, A. (2023). Exploring the artificial intelligence "Trust paradox": Evidence from a survey experiment in the United States. *PloS One*, *18*(7), e0288109. https://doi.org/10.1371/journal.pone.0288109

Larsson, S. (2021). Putting trust into antitrust? Competition policy and data-driven platforms. *European Journal of Communication*, *36*(4), 391–403. https://doi.org/10.1177/02673231211028358

Lawrence, K. (2013). Developing Leaders in a VUCA Environment. *UNC Executive Development*, 1–15.

Leavitt, H. J., & Whisler, T. L. (1958). by Management in the 1980 ' s. *Harvard Business Review*, *36*(6), 41–48.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Levine, L. (2019). Digital trust and cooperation with an integrative digital social contract. *Business and the Ethical Implications of Technology*, *160*(2), 87–101. https://doi.org/10.1007/s10551-019-04201-z

Lumineau, F., Schilke, O., & Wang, W. (2023). Organizational Trust in the Age of the Fourth Industrial Revolution: Shifts in the Form, Production, and Targets of Trust. *Journal of Management Inquiry*, *32*(1), 21–34. https://doi.org/10.1177/10564926221127852

Luo, J., & Ni, X. (2009). A clustering analysis and agent-based trust model in a grid environment supporting virtual organisations. *International Journal of Web and Grid Services*, *5*(1), 3–16. https://doi.org/10.1504/IJWGS.2009.023865

Majot, A., & Yampolskiy, R. (2014). Global catastrophic risk and security implications of quantum computers. *Futures*, *72*, 17–26. https://doi.org/10.1016/j.futures.2015.02.006

Martin, K. (2023). *Trust and the Online Market Maker : A Comment on Etzioni ' s Cyber Trust Author (s): Kirsten Martin Published by : Springer Stable URL : https://www.jstor.org/stable/45106472 Trust and the Online Market Maker : A Comment on Etzioni ' s Cyber Trust*. *156*(1), 21–24.

Martinsen, M., Zhou, Y., Dahlquist, E., Yan, J., & Kyprianidis, K. (2023). Positive climate effects when AR customer support simultaneous trains AI experts for the smart industries of the future. *Applied Energy*, *339*(April 2022), 120988. https://doi.org/10.1016/j.apenergy.2023.120988

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.1002/9781444316704.ch30

Mhatre, S. G., & Mehta, N. K. (2022). A review of workplace spirituality: identifying present development and future research agenda. *Management Research Review*, *46*(9), 1185–1206. https://doi.org/10.1108/MRR-11-2021-0800

Nass, C., Steuer, J., & Tauber, E. R. (1994). Computer are social actors. *Conference on Human Factors in Computing Systems - Proceedings*, *January*, 72–78. https://doi.org/10.1145/259963.260288

Ni, X., & Luo, J. (2008). A clustering analysis based trust model in grid environment supporting virtual organizations. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 100–105. https://doi.org/10.1109/WAINA.2008.162

Onwubiko, A., Singh, R., Awan, S., Pervez, Z., & Ramzan, N. (2023). Enabling Trust and Security in Digital Twin Management: A Blockchain-Based Approach with Ethereum and IPFS. *Sensors (Basel, Switzerland)*, *23*(14). https://doi.org/10.3390/s23146641

Pierson, J. (2021). Digital platforms as entangled infrastructures: Addressing public values and trust in messaging apps. *European Journal of Communication*, *36*(4), 349–361. https://doi.org/10.1177/02673231211028374

Pietrzak, P., & Takala, J. (2021). Digital trust – a systematic literature review. *Forum Scientiae Oeconomia*, *9*(3), 59–71. https://doi.org/DOI: 10.23762/FSO_VOL9_NO3_4

Popa, D. M., & Cotet, G. B. N. (2011). Trust and social capital in the virtual organization. *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, *22*(1), 289–290. https://doi.org/10.2507/22nd.daaam.proceedings.143

Ratnasingam, P. (2001). *The Need forInter-Organizational-Trust in Web-E " nabled Supply Chain Management*. 55–65.

Renaud, K., & Dupuis, M. (2023). Cybersecurity Insights Gleaned from World Religions. *Computers & Security*, *132*, 103326. https://doi.org/10.1016/j.cose.2023.103326

Rock, D. D., & Ringleb, D. A. H. (2013). *Handbook of NeuroLeadership*.

Rüdiger, K., & Rodríguez, M. J. G. (2013). Do we need innovative trust intermediaries in the digital economy? *Global Business Perspectives*, *1*(4), 329–340. https://doi.org/10.1007/s40196-013-0021-8

Sabatini, F., & Sarracino, F. (2019). Online Social Networks and Trust. *Social Indicators Research*, *142*(1), 229–260. https://doi.org/10.1007/s11205-018-1887-2

Sabzalieva, E., & Valentini, A. (2023). ChatGPT and Artificial Intelligence in higher education: Quick start guide. *Unesco*, 1–15. http://en.unesco.org/open-access/terms-use-ccbysa-en

Salam, A., Ullah, F., Amin, F., & Abrar, M. (2023). Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach. *Technologies*, *11*(4), 1–19. https://doi.org/10.3390/technologies11040107

Searle, R., & Renaud, K. (2023). Trust and Vulnerability in the Cybersecurity Context. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2023-Janua*, 5228–5240.

Silic, M., & Back, A. (2013). Information security and open source dual use security software: Trust paradox. *IFIP Advances in Information and Communication Technology*, *404*, 194–206. https://doi.org/10.1007/978-3-642-38928-3_14

Skrabut, S. (2023). *80 Ways to Use ChatGPT in the Classroom*.

Stewart, K. J. (2003). Trust transfer on the World Wide Web. *Organization Science*, *14*(1), 5–17. https://doi.org/10.1287/orsc.14.1.5.12810

Su, W. C. (2014). Integrating and mining virtual communities across multiple Online Social Networks: Concepts, approaches and challenges. *2014 4th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2014*, 199–204. https://doi.org/10.1109/DICTAP.2014.6821682

Sumathi, V., Harish, K. S., Lakshya, J., & Ahmed, H. (2023). Crowd-Funding Using Blockchain. *2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation, ICAECA 2023*, 1–5. https://doi.org/10.1109/ICAECA56562.2023.10200116

Vukotich, G. (2023). Healthcare and Cybersecurity: Taking a Zero Trust Approach. *Health Services Insights*, *16*. https://doi.org/10.1177/11786329231187826

Wade, C. E., Cameron, B. A., Morgan, K., & Williams, K. C. (2011). Are interpersonal relationships necessary for developing trust in online group projects? *Distance Education*, *32*(3), 383–396. http://dx.doi.org/10.1016/j.jaci.2012.05.050

Wefald, A. J., & Katz, J. P. (2011). Leaders: The Strategies for Taking Charge. *Academy of Management Perspectives*, *21*(3), 105–106. https://doi.org/10.5465/amp.2007.26421248

Wiangkham, A., & Vongvit, R. (2023). Exploring the Drivers for the Adoption of Metaverse Technology in Engineering Education using PLS-SEM and ANFIS. *Education and Information Technologies*, *0123456789*. https://doi.org/10.1007/s10639-023-12127-3

Woodward, I. C. (2018). *Develop insight in a D-VUCAD world*.

Yamagishi, T., & Yamagishi, M. (1994). *Trust and Commitment in the United States and Japan 1*. *18*(2).

Zak, P. J. (2018). The neuroscience of high-trust organizations. *Consulting Psychology Journal*, *70*(1), 45–58. https://doi.org/10.1037/cpb0000076