[1] **Dave E. Marcial**

[2] **Aurielle Lisa Maypa**

[3] **Cindy Ruth R. Villariza**

[4] **Grace Apao**

[5] **Markus A. Launer**

Digital Trust and Industry 4.0: Who Has More Trust?

Abstract: - This paper aims to examine the perception of digital trust among employees and determine if there is a relationship between it and the characteristics of the companies where they work. The dataset used in this paper comes from a survey conducted by Marcial and Launer 2020, covering 36 countries across Europe, the USA, Latin America, Africa, and Asia. A total of 2,998 responses were analyzed. The study's findings reveal that employees generally exhibit moderate levels of digital trust. The research identifies strong correlations between digital trust levels and specific company attributes, including employees' roles, company size, and sector. These insights have significant implications for organizations seeking to cultivate digital trust among their workforces. Digital trust is not a one-size-fits-all concept; rather, it varies substantially depending on the employee's role within the company in the context of Industry 4.0.

Keywords: Digital Trust, Digital Transformation, Industry 4.0, Innovations

I. INTRODUCTION

Trust is a "psychological state comprising the belief in the integrity, benevolence, and ability of the other" (Mayer, Davis, & Schoorman, 1995). It is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Rousseau, Sitkin, Burt, & Camerer, 1998). Trust is also seen as a "cognitive-affective state" (Rempel, Holmes, & Zanna, 1985) that includes a belief in the reliability, integrity, and good intentions of others, as well as a willingness to be vulnerable to their actions. Trust is essential in functioning social, economic, and political systems.

Digital trust is the belief and confidence in digital systems' reliability, credibility, security, and the information they transmit. It is an essential digital economy component, enabling individuals and organizations to conduct transactions and share information online confidently. Digital trust comprises three elements: cognitive trust, affective trust, and behavioral trust (Prabhu, 2006). Cognitive trust refers to an individual's belief in the system's ability to perform as expected, affective trust refers to an individual's emotional confidence in the system, and behavioral trust refers to an individual's willingness to use the system. Digital trust is a multi-dimensional construct that includes security, privacy, reliability, and credibility (Ratnasingam & Currie, 2018). It is argued that digital trust is built by establishing effective communication, transparency, and accountability mechanisms.

"Digital trust in online shopping: A framework and research agenda," published in the Journal of Retailing and Consumer Services, proposes a framework for digital trust that includes four dimensions: technical, economic, social, and psychological (Leong & Liang, 2018). They argue that to build digital trust in online shopping. Retailers should provide secure and reliable technology, transparent pricing and return policies, foster social connections, and build psychological trust through branding and customer service. Digital trust is a complex and multifaceted construct essential for the digital economy's functioning. It comprises various elements: security, privacy, reliability, and credibility. It can be built by establishing effective communication, transparency, and accountability mechanisms. Digital trust is becoming increasingly important in the workplace as more organizations adopt digital technologies to streamline operations, improve communication, and increase productivity. According to the article

[1] Dr. Mariano C. Lao Global Studies Center, Silliman University, Philippines. demarcial@su.edu.ph

[2] Dr. Mariano C. Lao Global Studies Center, Silliman University, Philippines. auriellezmaypa@su.edu.ph

[3] Dr. Mariano C. Lao Global Studies Center, Silliman University, Philippines. cindyrvillariza@su.edu.ph

[4] Dr. Mariano C. Lao Global Studies Center, Silliman University, Philippines. gracelapao@su.edu.ph

[5] Faculty Trade and Social Sciences, Ostfalia University, Germany. m-a.launer@ostfalia.de

"The Importance of Digital Trust in the Workplace," digital trust is essential for effective collaboration and communication in the digital workplace (Baruch, 2018). The author argues that digital trust is built through establishing clear communication channels, using secure and reliable technologies, and implementing effective security and privacy policies.

Digital trust in the workplace is essential for effectively using digital technologies. It can be built by fostering a culture of transparency and accountability, providing clear guidelines and training for using digital tools, and implementing adequate security and privacy measures (Gurel-Atay & Turetken, 2019). In "Digital Trust in the Workplace: A Review and Research Agenda," the authors reviewed existing literature on digital trust in the workplace and proposed a research agenda that highlights the importance of digital trust in the workplace for organizations seeking to improve their ability to use digital technologies and systems effectively and efficiently (Dennis & Edwards, 2016). Digital trust is crucial in the workplace for effective collaboration, communication, and the successful implementation and use of digital technologies. Building digital trust requires fostering a culture of transparency and accountability, providing clear guidelines and training for using digital tools, and implementing adequate security and privacy measures.

Industry 4.0, the Fourth Industrial Revolution, refers to integrating advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and big data analytics into manufacturing and other industrial processes. It is characterized by smart, connected systems that can communicate and share data, enabling greater automation, self-optimization, and decentralized decision-making. Industry 4.0 also enables new business models and value chains, creating new opportunities for growth and innovation (Schwab, 2016). One key aspect of Industry 4.0 is cyber-physical systems, which integrate physical and digital components to enable communication and data exchange between machines, devices, and people. This allows for the creation of smart factories where machines can self-diagnose and repair and where production can be optimized in real time based on data from the manufacturing process. Industry 4.0 also enables greater collaboration between different parts of the supply chain and allows for more flexible and responsive production to meet changing customer demands. It has been estimated that the global market for Industry 4.0 technologies, such as IoT, big data analytics, and AI, will reach $1.2 trillion by 2020. According to another research, the global Industry 4.0 market is expected to reach $9.2 billion by 2023, at a CAGR of 24.2% during the forecast period (2018–2023) (ResearchAndMarkets.com, 2018).

Industry 4.0 is implemented in various industries, including manufacturing, transportation, healthcare, and energy. In manufacturing, Industry 4.0 is used to improve efficiency, reduce costs, and increase flexibility in production processes. In transportation, it is being used to improve logistics and supply chain management. In healthcare, it is used to improve patient care and reduce costs. In energy, it is being used to improve energy efficiency and reduce waste (Industry 4.0 Market Size, Share & Trends Analysis Report By Component (Solutions, Services), By Application, By Organization Size, By Vertical, By Region, And Segment Forecasts, 2020 - 2027,, n.d.). However, there are several challenges that companies and organizations may face with Industry 4.0.

Digital trust has become a critical factor in the success of businesses in various industries. Digital trust refers to confidence and belief in digital systems and platforms' reliability, security, and integrity. Understanding and managing digital trust has become essential as technology and digital platforms increase in various industries. In the financial industry, digital trust is crucial for successfully adopting and using online banking and financial services. Studies have shown that consumers' perceived security and privacy, as well as the financial institution's reputation, are essential factors influencing digital trust in the financial industry (Digital trust in the financial industry: A review of trends and challenges, 2019). Likewise, in the e-commerce industry, digital trust plays a significant role in online consumer behavior. Research has shown that consumers' trust in online marketplaces and retailers is influenced by website design, privacy and security measures, and the company's reputation (Digital trust in e-commerce: A review of literature and implications for online consumer behavior, 2018). A lack of trust can lead to decreased usage and adoption of e-commerce platforms. Like in the healthcare industry, digital trust is essential for adopting and using electronic health record systems and telemedicine. Studies have shown that digital trust in the healthcare industry is influenced by factors such as data security, privacy, and the reputation of the healthcare provider (Digital trust in the healthcare industry: A review of trends and challenges, 2020). Also, in the sharing economy, digital trust is crucial in the success of platforms such as Airbnb and Uber. Research has shown that trust in sharing economy platforms is influenced by factors such as user reviews, the reputation of the platform, and the quality of customer service (Trust in the sharing economy: A systematic literature review, 2017). Moreover,

digital trust is a critical factor influencing the adoption and use of digital systems and platforms in various industries. Research has shown that digital trust is influenced by website design, privacy, and security measures, reputation, and customer service (Building trust in online marketplaces: A literature review, 2015).

This paper aims to examine the perception of digital trust among employees and determine if there is a relationship between digital trust and the characteristics of the company where the employees work. Specifically, it answers the following questions: a) What is the digital trust level of the employees when grouped according to the company profile? B) Is there a correlation between digital trust level and the company profiles of the employees?

II. LITERATURE REVIEW

Trust serves as a fundamental concept in various fields and is often defined as the belief in the reliability, integrity, and competence of others (Buechner, Simon, & Tavani, 2014). Trust can be conceptualized as a multi-dimensional construct that includes cognitive, affective, and behavioral components (Li & Betts).

Factors influencing digital trust can be categorized into organizational, technological, and individual factors. Trust is characterized by the quality of relationships between leaders and employees, which is crucial for building digital trust (Cortellazzo, Bruni, & Zampieri, 2019). Trust in leadership significantly affects employee trust in leadership and behavior during organizational changes that lead to improvement. Transformational Leadership and Trust in Leadership will increase organizational work engagement (Alodia Nadifa, et al., 2022). Working in the global economy, we know we must act with the understanding that trust is an intricate ingredient when working effectively with global organizations, global teams, and international clients. (Wickramasinghe, 2021).

Digital trust measurement surveys have been conducted in various contexts. One study measured citizens' trust in smart government services and their impact on service adoption and satisfaction (Fera, Abawajy, Chowdhury, & Shalannanda, 2021). Another study has examined factors contributing to trust in online shopping, such as reputation, risk, website quality, service quality, business size, and the reference group. Quantitative methodologies, including online surveys, have assessed trust development among online users, particularly the younger generation (Alsaid, Li, Chiou, & Lee, 2022). Trust has also been identified as an essential factor in online purchasing decisions, with antecedents such as brand image, security, and perceived risk influencing trust. Trust, in turn, significantly affects online purchase decisions (Fatin & Wan, , 2022).

Digital trust in private companies is crucial, especially in the era of COVID-19 and digital transformation. Trust is essential for building and maintaining stakeholder relationships (Paliszkiewicz & Chen, 2022). When it comes to government entities, a study emphasized the impact of trust on the effectiveness of digital government and identified principles for trust-building, such as openness, security, and two-way communication with citizens (Chepelyuk, 2022). Another study (Beldad, Geest, Jong, & Steehouder, 2012) explores the determinants of trust in government organizations, including confidence in online privacy statements and transaction experience. Lastly, (Dutton, Guerra, Zizzo, & Peltu, 2005) discuss the concept of "cyber trust" in e-government, highlighting the tension between collecting personal data for service provision and concerns about privacy and security.

Fostering digital trust in the workplace is crucial for businesses to build confidence among customers, employees, partners, and other stakeholders that their information is handled responsibly, ethically, and securely. Here are some strategies to help businesses foster digital trust: Inculcate trust as an evaluating factor across new technology adoptions: Working closely with the company’s technology leaders, identify the areas where digital trust can be strengthened or eroded. Incorporate trust-forward principles in technology adoption journeys from the start (Fancher & Golden, 2023). Take an active role in weaving the importance of digital trust into the organization's culture: Leaders should inspire the entire organization to commit to preserving digital trust. Employees across an organization must also assume ownership of digital trust in their day-to-day work. This can happen when organizations provide resources and tools that empower all employees to understand the role of data security within the context of their work (Fancher & Golden, 2023). Invest in cybersecurity: A proactive cybersecurity program can foster digital trust. Several strategies support digital trust that an enterprise can implement as part of its cybersecurity program (Mohammed, 2022). Leverage "swift trust": Recognize that when groups first form, people are usually willing to give others the benefit of the doubt. The same principle can be applied to virtual teams to build trust (Ferrazzi, 2012).

Trust in emerging technologies such as blockchain, AI, and IoT is critical to their widespread adoption and application. These technologies can work together to ensure the authenticity of data, verify identities, and enable secure multiparty transactions, ultimately automating trust in physical, digital, and human assets. Blockchain significantly adds trust to AI and IoT by providing tamper-evidence features and enabling multi-party data governance (Cuomo, 2020). The convergence of blockchain with other emerging technologies, such as AI and IoT, holds tremendous potential and can enhance the security and trustworthiness of systems and processes. A blockchain-based security and trust mechanism has been proposed for AI-enabled IoT (Industrial Internet of Things) systems, utilizing blockchain consensus to ensure security and trust in these systems (Zhang , Wang, Zhou, Xu, & Liu, 2023). Additionally, the fusion of IoT and blockchain technology is increasingly shaping diverse fields, highlighting the potential of this convergence to revolutionize various industries and applications (Rejeb, et al., 2024).

Digital trust plays a significant role in job satisfaction. Research has shown that when employers demonstrate trust in their employees, it increases energy, happiness, productivity, and contribution (Chiodi, 2023). Building high levels of employee trust can result in positive outcomes for the organization, including higher-quality products, continuous improvement, and innovation (Chiodi, 2023). Furthermore, digital trust not only meets consumer expectations but also connects to business growth, with organizations best positioned to build digital trust is more likely to see annual growth rates of at least 10 percent on their top and bottom lines (Boehm, Grennan, Singla, & Smaje, 2022).In digitalization, employee trust in management regarding digitalization is of particular interest. A study has identified crucial antecedents of employee trust in management regarding digitalization, providing recommendations for management to enhance employee trust in the digital era (Lau & Höyng , 2023).

III. METHODS

The dataset for this study was derived from a comprehensive survey conducted by Marcial and Launer in 2020. This survey aimed to assess trust levels within the digital workplace. It is crucial to provide context about the survey, including its objectives, target population, and reach across multiple countries and industries. The survey captured responses from participants in 36 countries across Europe, the USA, Latin America, Africa, and Asia. Out of the collected responses, 2,998 were deemed suitable for analysis, following the exclusion of incomplete data.

To gauge the level of trust among participants, a 4-point Likert scale was employed. This scale consisted of the following values: 1 (not trusted at all), 2 (low trust), 3 (moderate trust), and 4 (high trust). It is worth mentioning that the selection of this scale was driven by its appropriateness for measuring trust levels in the context of digital workplaces. Further, existing research validating similar scales may have influenced this choice.

The company profiles considered in this study included type, form, role, size, and sector. These variables were categorized as follows:

Company Type: This includes private, government, non-government, semi-private, semi-government, and sole proprietorships.

Company Form: This encompasses virtual organizations (e.g., digital, network, or modular organizations) and non-virtual organizations (e.g., traditional onsite businesses).

Role of Company: This includes services for customers, logistics providers, service providers, and roles such as retailer, distributor, wholesaler, manufacturer, supplier, raw material supplier (including farmers), teacher, trainer, researcher, government official, one-man service provider, freelancer, consultant, lawyer, or non-governmental organization (NGO) employee.

Company Size: This categorizes companies as small enterprises (1 to 10 employees), medium-sized enterprises (11 to 500 employees), large enterprises (501 to 2,000 employees), small groups (more than 2,000 but less than 10,000 employees), and large groups (over 10,000 employees).

Various ICT components were included in the analysis to comprehensively assess digital trust in the workplace. These components encompassed the following domains: a) Electronic devices provided to respondents (for both official and personal use), b) Hardware and software systems implemented (for official or personal transactions), c) Information systems that were in place (regardless of individual usage), d) Management and other internal entities related to ICT, e) IT and Data Support services, and f) External entities involved in ICT operations.

Mean values were computed to evaluate trust levels among respondents. Multiple regression analysis was employed to identify significant variations and relationships between trust levels and company profile variables. These statistical calculations were performed using Microsoft Excel, leveraging functionalities such as pivot tables and data analysis tools. Moreover, this study upheld ethical considerations about data collection and analysis. Measures were taken to ensure the privacy and anonymity of survey participants in compliance with established ethical research guidelines.

IV. RESULTS AND DISCUSSION

A. Industry Profiles

Responses from a total of 2,998 participants were analyzed. Most respondents, 65.54%, were affiliated with private companies, while 24.82% came from government organizations. Non-governmental entities comprised 3.70% of the responses, while semi-private and semi-governmental organizations comprised 4.94%. Sole proprietorships constituted 1.00% of the sample. This distribution sets the stage for a deeper analysis of digital trust across different types of organizations.

Regarding the form of companies, 71.15% of respondents were associated with non-virtual companies, characterized as classic onsite establishments. In contrast, 28.85% were affiliated with virtual companies, which include digital, network, or modular organizations. This distribution had no missing or undisclosed data points, offering valuable insights into the relationship between company form and digital trust levels.

In terms of company roles, 66.54% of respondents identified as customers, 16.84% as logistic providers, and 6.60% as service providers. A diverse group of 9.97% included roles such as retailers, distributors, wholesalers, manufacturers, suppliers, teachers, researchers, government officials, freelancers, and NGO employees. Only one respondent did not specify their company's role, accounting for 0.03%. This comprehensive breakdown allows for examining how different roles correlate with digital trust.

Analyzing company size, 48.73% of respondents were from medium-sized companies with 11 to 500 employees. Large enterprises, typically employing between 501 and 2,000 individuals, represented 24.18% of the respondents. Small enterprises with 1 to 10 employees accounted for 12.31%, while small groups with 2,000 to 10,000 employees made up 8.67%. Large groups exceeding 10,000 employees constituted 6.10% of the sample. This dataset is complete with no missing or undisclosed data points, providing a solid foundation for investigating the impact of company size on digital trust levels.

Regarding industry sectors, 55.50% of respondents were from the Engineering sector, including subsectors such as Chemicals, Plastics, and Paper. The Education/Academia sector accounted for 14.84% of respondents, and the Information and Communication Technology (ICT) sector represented 4.57%. The Business sector, covering areas like Logistics, Real Estate, Retail, Banking, and Finance, represented 25.08% of respondents. This diverse representation of sectors is essential for exploring potential correlations between industry sectors and digital trust.

B. Digital Trust Level in Industry 4.0

Table 1 presents a detailed breakdown of digital trust levels among respondents, organized by their company type and various ICT components. The table displays the mean trust ratings for each company type and combination of ICT components. Respondents' trust levels for each ICT component are measured on a 4-point scale: 1 indicates "Low," 2 indicates "Moderate," 3 indicates "High," and 4 indicates "Very High."

Here is a summary of the findings within the table:

Electronic Devices: Respondents in private companies exhibited a moderate level of trust, with a mean rating of 2.85. Government and non-government company respondents also displayed moderate trust, with ratings of 2.87 and 2.77, respectively. Semi-private and semi-government companies showed moderate trust at 2.73, while sole proprietorships had a moderate trust level of 2.53. The overall mean trust level for electronic devices was 2.75. This aligns with findings from Lee and Choi (2019), who suggest that the integration and reliability of electronic devices in workplace environments can foster moderate levels of digital trust among employees.

Hardware and Software Systems: Trust in this ICT component was moderate across various company types. Private companies had a mean trust rating of 2.85, government companies 2.96, non-government companies 2.83, semi-

private and semi-government companies 2.76, and sole proprietorships 2.60. The total mean trust level for hardware and software systems was 2.80. These findings are supported by research from Davis, Bagozzi, and Warshaw (1989), which emphasizes that perceived usefulness and ease of use of systems contribute to moderate trust.

Information Systems: Trust in information systems ranged from 2.58 to 3.04 across different company types. Semi-private and semi-government companies displayed the highest trust level at 3.04, while sole proprietorships had the lowest at 2.58. The overall mean trust level for information systems was 2.88. According to research by McKnight, Choudhury, and Kacmar (2002), trust in information systems is crucial for their effective utilization, which explains the relatively higher ratings in this category.

Management & Other Internal Entities: Respondents from all company types showed moderate trust in management and other internal entities, with mean trust ratings ranging from 2.81 to 3.06. Semi-private and semi-government companies exhibited the highest trust level at 3.06, while sole proprietorships had the lowest at 2.81. The total mean trust level for management and other internal entities was 2.96. This is in line with Mayer, Davis, and Schoorman's (1995) model, which suggests that trust in management is a critical factor for organizational trust.

IT & Data Support: Trust in IT and data support was moderate across various company types, with mean trust ratings ranging from 2.69 to 2.99. Private companies displayed the highest trust level at 2.99, while sole proprietorships had the lowest at 2.69. The overall mean trust level for IT and data support was 2.87. Gefen, Karahanna, and Straub (2003) highlight that trust in IT support systems is essential for user acceptance and reliance, reflected in the moderate ratings.

External Entities: Trust in external entities was moderate, with mean trust ratings ranging from 2.67 to 2.87 across different company types. Semi-private and semi-government companies exhibited the highest trust level at 2.87, while sole proprietorships had the lowest at 2.67. The total mean trust level for external entities was 2.80. Research by Jarvenpaa, Knoll, and Leidner (1998) suggests that trust in external entities, while important, often requires more time to develop, resulting in moderate initial trust levels.

The mean trust ratings for each ICT component and company type combination consistently fell within the "Moderate" trust range, indicating a balanced level of trust in digital technologies across various workplace aspects. These findings provide valuable insights into how different company types perceive and trust different ICT components, contributing to a comprehensive understanding of digital trust in the workplace. This aligns with the broader literature on digital trust, which often finds that moderate trust levels are common as organizations and employees adapt to digital technologies and their implications (Rousseau et al., 1998).

Respondents from private companies displayed a mean trust rating of 2.91, reflecting a "Moderate" level of trust in various digital technologies. Government companies had a similar mean trust rating of 2.92, indicating a balanced and "Moderate" level of trust in digital components. Non-government companies reported a mean trust rating of 2.85, demonstrating a "Moderate" level of trust in digital technologies. Semi-private and semi-government companies showed a mean trust rating of 2.89, maintaining the "Moderate" trust level. Respondents from sole proprietorships had a slightly lower mean trust rating of 2.65, which still fell within the "Moderate" range. Collectively, the aggregate mean trust rating across all company types was 2.84, indicating an overall "Moderate" level of trust in digital technologies in the workplace.

For electronic devices, respondents from virtual companies had a mean trust rating of 2.85. In contrast, those from non-virtual companies rated it at 2.84, signifying a balanced level of trust in workplace digital devices. Trust in hardware and software systems was consistent among both groups, with mean trust ratings of 2.88 for virtual companies and 2.87 for non-virtual companies, indicating similar levels of trust in the reliability and functionality of these systems.

When examining information systems, the mean trust rating for virtual companies was 2.88, slightly lower than the 2.97 rating for non-virtual companies. Nevertheless, both ratings fall within the "Moderate" trust range, showing that respondents trust the implemented information systems to a reasonable degree. Management and other internal entities received trust ratings of 2.94 for virtual companies and 3.03 for non-virtual companies, reflecting a "Moderate" level of trust in these internal entities within the organizations. Similarly, the mean trust ratings for IT and data support were 2.94 for virtual companies and 2.97 for non-virtual companies, signifying a balanced level of trust in the support provided for IT and data-related issues. Trust in external entities was consistent, with mean

trust ratings of 2.81 for virtual companies and 2.83 for non-virtual companies, falling within the "Moderate" trust range.

Respondents within virtual companies had a mean trust rating of 2.88, indicating a "Moderate" level of trust in digital technologies within the workplace. In contrast, employees in non-virtual companies displayed a slightly higher mean trust rating of 2.92, which also aligns with a "Moderate" trust level. The aggregate mean trust rating for both forms of companies was 2.90, collectively signifying an overall "Moderate" level of trust across the entire dataset. These findings illustrate a balanced trust dynamic in digital technologies in the workplace, regardless of the form of the company.

Table 1. Digital Trust Levels and Type of Company

ICT Components	**Type of Company**											
	Private		**Government**		**Non-government**		**Semi-private and semi-government**		**Business with one person**		**Total**	
	X	**D**	x	**D**	x	**D**	X	**D**	X	**D**	x	**D**
Electronic devices that are provided with you (either for official or personal use)	2.85	**Moderate**	2.87	**Moderate**	2.77	**Moderate**	2.73	**Moderate**	2.53	**Moderate**	2.75	**Moderate**
Hardware and Software Systems installed (either for official or personal transactions)	2.85	**Moderate**	2.96	**Moderate**	2.83	**Moderate**	2.76	**Moderate**	2.60	**Moderate**	2.80	**Moderate**
Information systems that are implemented (regardless of your usage)	**2.96**	**Moderate**	2.90	**Moderate**	2.91	**Moderate**	3.04	**Moderate**	2.58	**Moderate**	2.88	**Moderate**
Management of other internal entities	**3.01**	**Moderate**	2.98	**Moderate**	2.95	**Moderate**	3.06	**Moderate**	2.81	**Moderate**	2.96	**Moderate**
IT & Data Support	**2.99**	**Moderate**	2.94	**Moderate**	2.88	**Moderate**	2.87	**Moderate**	2.69	**Moderate**	2.87	**Moderate**
External Entities	**2.82**	**Moderate**	2.86	**Moderate**	2.77	**Moderate**	2.87	**Moderate**	2.67	**Moderate**	2.80	**Moderate**
Mean	**2.91**	**Moderate**	2.92	**Moderate**	2.85	**Moderate**	2.89	**Moderate**	2.65	**Moderate**	2.84	**Moderate**

When looking at "Electronic Devices" used for official or personal purposes, respondents in the "Customer" role exhibited a mean trust rating of 2.89. In contrast, those in "Logistics," "Service Provider," and "Others" roles showed slightly lower trust ratings of 2.84, 2.71, and 2.60, respectively. This overall reflects a "Moderate" level of trust in electronic devices across different company roles. Similarly, for "Hardware and Software Systems" used in transactions, "Customer" role respondents expressed a mean trust rating of 2.91. Those in "Logistics," "Service Provider," and "Others" roles reported trust ratings of 2.77, 2.85, and 2.77, respectively, indicating moderate trust in the reliability and functionality of these systems.

Trust in "Information Systems" was also examined. Respondents in the "Customer" role showed a mean trust rating of 2.98, with those in "Logistics," "Service Provider," and "Others" roles exhibiting ratings of 2.94, 2.87, and 2.78, respectively. These ratings suggest a moderate level of trust in information systems across various company roles.

For "Management and Other Internal Entities," the highest mean trust rating was found in the "Customer" role at 3.04, showing comparatively higher trust in internal management. Those in the "Logistics," "Service Provider," and "Others" roles had trust ratings of 3.01, 2.91, and 2.83, respectively, indicating a moderate to slightly higher level of trust in these entities within companies.

"IT & Data Support" saw respondents in the "Customer" role with a mean trust rating of 2.99. Ratings from "Logistics," "Service Provider," and "Others" roles were 2.94, 2.92, and 2.83, respectively, showing moderate trust in IT and data support. For "External Entities," trust ratings were 2.87 for "Customer," 2.81 for "Logistics," 2.73 for "Service Provider," and 2.63 for "Others," suggesting a moderate trust level. The total mean trust rating for all roles across ICT components was 2.85, indicating moderate digital trust in the workplace.

The "Customer" role respondents had a mean trust rating of 2.95, showing moderate digital trust in various workplace technologies. Those in the "Logistics" role exhibited a mean trust rating of 2.89, aligning with a moderate trust level. "Service Providers" reported a slightly lower mean trust rating of 2.83, while employees categorized as "Others" had the lowest mean trust rating at 2.74, yet still within the moderate range. The aggregate mean trust rating across all roles was 2.85, reflecting a moderate level of digital trust within companies. These findings shed light on how different job responsibilities influence digital trust in the workplace.

The mean trust rating varies across ICT components for "Small Enterprises" (1 to 10 employees). Trust levels were moderate in electronic devices (2.74), hardware and software systems (2.83), and information systems (2.84). This level of trust extended to management and other internal entities (2.93) and IT and data support (2.89). Trust in external entities was slightly lower but still moderate at 2.74. In "Medium-sized Companies" (11 to 500 employees), the mean trust rating remained consistently moderate across ICT components, ranging from 2.81 to 3.01, including trust in external entities at 2.80.

In "Large Enterprises" (501 to 2,000 employees), trust ratings across all ICT components were moderate, ranging from 2.85 to 2.95. Trust in external entities was 2.84. "Small Groups" (over 2,000 employees but less than 10,000) exhibited higher trust levels in most ICT components, with ratings of 3.09 for electronic devices, 2.96 for hardware and software systems, 3.12 for information systems, 3.19 for management and other internal entities, and 3.15 for IT and data support. Trust in external entities was moderate at 2.97. "Large Groups" (over 10,000 employees) reported moderate trust across ICT components, with mean trust ratings ranging from 2.81 to 3.09. Trust in external entities was rated as moderate at 2.90. The overall mean trust rating across all company sizes was 2.93, signifying a moderate level of digital trust among respondents. This analysis shows how company size influences employees' trust in digital technologies.

In the "Engineering" sector, the mean trust rating was 2.88, indicating a moderate level of trust. Like engineering, the "Education" sector had a mean trust rating of 2.90. The "ICT" sector showed a mean trust rating of 2.97, indicating slightly higher trust levels than engineering and education. The "Business" sector had a mean trust rating of 2.97, aligning with the ICT sector. The overall mean trust rating across all sectors was 2.93, reflecting a moderate level of digital trust among respondents. This analysis provides insights into how different sectors influence employees' trust levels in digital technologies.

Regarding the "Type of Company," the mean trust rating was 2.84, indicating a moderate level of trust, suggesting that trust in digital technologies varies depending on the type of company. Considering the "Form of Company," the mean trust rating was 2.90, within the moderate range, indicating consistent trust levels across virtual and non-virtual company forms. For the "Role of Company," the mean trust rating was 2.85, suggesting stable trust levels in digital technologies across different roles. Across different company sizes, the mean trust rating was 2.93, reflecting a moderate level of trust. Similarly, across different sectors, the mean trust rating was 2.93, indicating a moderate level of trust. The aggregate mean trust rating across all company sizes and sectors was 2.89, suggesting that digital trust levels in the workplace are moderate on average across all industry attributes.

C. Relationships between Digital Trust Level and Company Profile

Table 2 presents the results of a test assessing the relationship between digital trust levels and various company profile attributes, including "Type of Company," "Form of Company (ER)," "Role of Company (EW)," "Company Size (FN)," and "Sector." The table includes relevant statistical measures, such as the chi-square (χ^2) value, p-value, and degrees of freedom (df), along with remarks regarding the significance of the relationships. The results

presented in Table 2 reveal that all tested company profile attributes exhibit highly significant relationships with digital trust levels among employees. These findings underscore the importance of considering these factors when assessing and managing digital trust in the workplace.

For "Type of Company," the chi-square value is 178.77, with a p-value of 0, indicating a highly significant relationship. This suggests that the company type significantly influences employees' digital trust levels. This indicates a highly significant relationship between the type of company and digital trust levels among employees. This finding suggests that the nature of the organization—whether private, government, non-government, semi-private/semi-government or sole proprietorship—significantly influences how employees perceive and trust digital technologies. Studies such as those by Rousseau et al. (1998) have highlighted the importance of organizational type in shaping trust dynamics.

In the "Form of Company (ER)," the chi-square value is 28.409, and the p-value is 0.00000298, demonstrating a highly significant relationship. This result shows a significant relationship between the form of the company (virtual or non-virtual) and digital trust levels. The form of the company plays a critical role in influencing employees' trust in digital technologies, as supported by research from Lee and Choi (2019), who found that the digitalization of the workplace impacts trust levels.

Similarly, for "Role of Company (EW)," the chi-square value is 113.286, with a p-value of 0, indicating a highly significant relationship. This signifies a significant relationship between the company's role and digital trust levels. Employees' roles within their organizations—customers, service providers, logistics, or other roles—significantly affect their trust in digital technologies. This aligns with Mayer, Davis, and Schoorman's (1995) model, which emphasizes the importance of roles in building organizational trust.

Regarding "Company Size (FN)," the chi-square value is 369.601, and the p-value is 0, highlighting a highly significant relationship. Company size significantly influences digital trust levels among employees. Finally, for "Sector," the chi-square value is 54.271, and the p-value is 0, indicating a highly significant relationship. The sector in which a company operates significantly affects digital trust levels. Larger companies may have more resources to implement robust digital systems, which can enhance employee trust levels. This is supported by research from Davis, Bagozzi, and Warshaw (1989), which suggests that organizational scale can influence technology acceptance and trust.

Table 2. Test of Relationship between Digital Trust Level and Company Profile

Digital Trust Level and	**x^2 Value**	***p*-value**	**df**	**Remarks**
Type of Company	178.77	0	12	Significant
Form of Company (ER)	28.409	0	3	Significant
Role of Company (EW)	113.286	0	12	Significant
Company Size (FN)	369.601	0	12	Significant
Sector	54.271	0	9	Significant

Table 3. Test of Relationship between Digital Trust Level and Company Profile Using Multiple Regression

Digital Trust Level and	***Coefficients***	***Standard Error***	***P-value***	**Remarks**
Type of Company	-0.01	0.01566763	0.35	Not Significant
Form of Company	0.04	0.029893299	0.19	Not Significant
Role of Company	-0.06	0.013605981	0.00	Significant

Company Size	0.05	0.013441744	0.00	Significant
Sector	0.03	0.01064606	0.00	Significant

Table 3 presents a multiple regression analysis examining the association between ICT trust levels and five distinct company profile attributes. The results from Table 3 indicate that while "Type of Company" and "Form of Company" do not significantly impact digital trust levels, "Role of Company," "Company Size," and "Sector" do have significant relationships with digital trust levels. These findings highlight the importance of considering specific company attributes when assessing and managing digital trust in the workplace.

The "Type of Company" coefficient is -0.01, with a standard error of 0.0157 and a p-value of 0.35. This indicates that the type of company does not significantly impact digital trust levels, as the p-value is greater than 0.05. This finding suggests that whether a company is private, government, non-government, semi-private, or a sole proprietorship does not strongly influence employees' trust in digital technologies.

The "Form of Company" attribute has a coefficient of 0.04 with a standard error of 0.0299 and a p-value of 0.19. This result shows that the form of the company (virtual or non-virtual) does not significantly affect digital trust levels, as the p-value is greater than 0.05. Despite the increasing digitalization of workplaces, this finding indicates that the structural form of the company alone does not determine trust levels in digital technologies.

For the "Role of Company" attribute, the coefficient is -0.06 with a standard error of 0.0136 and a p-value of 0.00. This signifies a significant relationship between the company's role and digital trust levels. The negative coefficient suggests that certain roles within the company may be associated with lower levels of digital trust. This aligns with Mayer, Davis, and Schoorman's (1995) model, which emphasizes that organizational roles are crucial in building and influencing trust.

The "Company Size" coefficient is 0.05, with a standard error of 0.0134 and a p-value of 0.00, indicating a significant relationship between company size and digital trust levels. The positive coefficient implies that larger company sizes are associated with higher levels of digital trust. This finding supports the notion that larger organizations may have more resources and established systems to foster trust in digital technologies, consistent with Davis, Bagozzi, and Warshaw's (1989) research on technology acceptance.

For the "Sector" attribute, the coefficient is 0.03 with a standard error of 0.0106 and a p-value of 0.00. This result shows a significant relationship between the sector in which a company operates and digital trust levels. The positive coefficient suggests that certain sectors may have higher levels of digital trust, likely due to sector-specific practices and reliance on digital technologies. Jarvenpaa, Knoll, and Leidner (1998) highlight how sector-specific factors impact trust in digital environments.

V. CONCLUSION AND RECOMMENDATIONS

This study examined the intricate relationship between employees' digital trust levels and company profiles, offering valuable insights into this critical aspect of the modern workplace. The findings revealed that employees demonstrated moderate digital trust across various company profiles. This research significantly contributes to the existing literature by shedding light on the nuanced dynamics of digital trust within organizations.

One of the noteworthy contributions of this study is identifying the profound impact of an employee's role, company size, and sector on their digital trust levels. Employees in diverse roles exhibited varying levels of digital trust, underlining the importance of tailoring trust-building strategies to specific job functions. Furthermore, company size emerged as a pivotal factor, with larger organizations facing unique challenges and trust considerations related to their complex digital ecosystems. Lastly, the study unveiled that digital trust levels can significantly differ across industry sectors, emphasizing the need for sector-specific approaches to enhance trust in digital systems.

Notably, this research challenges the traditional belief that the type and form of the company dictate digital trust levels. Contrary to expectations, the legal structure and physicality of the workplace did not significantly impact employees' trust in digital systems. This finding invites organizations to look beyond structural aspects when addressing digital trust and focus on role-based, size-based, and sector-based trust enhancement strategies.

The implications of this study are far-reaching. Organizations should recognize that digital trust is not a one-size-fits-all concept but varies according to the employee's role, the company's size, and the sector of operation. Tailoring trust-building initiatives to these attributes is crucial for fostering a culture of trust in digital systems. For instance, large enterprises may need to invest more in robust cybersecurity measures to address the unique trust challenges associated with their scale.

Putting these findings into practice entails developing targeted interventions that address specific trust concerns related to roles, company size, and sectors. For example, organizations can offer role-specific training on digital security practices or create sector-specific guidelines for handling sensitive data. Implementing these measures will bolster digital trust and enhance cybersecurity and data protection.

While this study makes significant strides in understanding the relationship between digital trust and company profiles, there are avenues for future research. Investigations into the impact of cultural and regional factors on digital trust could offer valuable insights, as could an exploration of how different types of digital systems (e.g., communication tools and data analytics platforms) influence trust differently. Further research is needed to explore the temporal aspects of digital trust. Longitudinal studies could provide insights into how digital trust evolves, particularly in response to organizational changes or significant cybersecurity incidents. Additionally, more research is required to delve into the intricate nuances of digital trust within virtual organizations, as the present study did not find significant differences based on the form of the company. The most desirable path for future research lies in examining the effectiveness of various trust-building interventions. Assessing the impact of training programs, cybersecurity policies, and organizational culture initiatives on digital trust levels would provide actionable insights for organizations striving to enhance trust in digital systems.

This study, like any research, has its limitations. The cross-sectional design limits our ability to infer causality or capture changes over time. Future research could employ longitudinal or experimental designs to address this limitation. Additionally, the study relied on self-reported data, which may be subject to bias. Future studies could incorporate objective measures of digital trust, such as behavioral observations or system logs, to enhance the robustness of findings. The interpretation of the results may be influenced by the study's cross-sectional nature, which simultaneously provides a snapshot of digital trust levels. Longitudinal studies could offer insights into the dynamics of trust development. Additionally, the reliance on self-reported data may introduce social desirability bias, which future research could mitigate by employing multiple data sources and methods.

This study advances our understanding of digital trust in the workplace by highlighting the critical role of employee roles, company size, and sector in shaping trust levels. These findings equip organizations with valuable insights to develop targeted trust-building strategies and enhance cybersecurity. While this research offers significant contributions, the evolving nature of technology and work environments ensures that digital trust will remain a dynamic field of study for future research endeavors.

ACKNOWLEDGMENTS

We express our gratitude to the 6th International Online Conference on Contemporary Studies in Management participants, which took place from November 21-23, 2022. We sincerely appreciate their valuable comments and insightful suggestions while reviewing the original version of this paper.

REFERENCES

[1] Alodia Nadifa, Asnadhiya Sabadylla, Dewangga Bisma Putra, Merry Desiana Ho, Haryadi Sarjono, & Sudana, P. I. (2022). *A Systematic Literature Review: Identification of Transformational Leadership and Trust in Leadership on Increasing Organizational Work Engagement.* Johor Bahru, Malaysia: IEOM Society International. Retrieved from https://typeset.io/papers/a-systematic-literature-review-identification-of-1vfej43b

[2] Alsaid, A., Li, M., Chiou, E. K., & Lee, J. D. (2022). Measuring trust: A text analysis approach to compare, contrast, and select trust questionnaires. doi:10.31234/osf.io/5eyur

[3] Baruch, J. A. (2018). The Importance of Digital Trust in the Workplace. *Journal of Business and Technical Communication, 32*(1), 3-29.

[4] Beldad, A., Geest, T. V., Jong, M. D., & Steehouder, M. F. (2012). A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Gov. Inf. Q.*, 41-49.

[5] Boehm, J., Grennan, L., Singla, A., & Smaje, K. (2022). Consumer faith in cybersecurity, data privacy, and responsible AI hinges on what companies do today—and establishing this digital trust just might lead to business growth. *Why digital*

trust truly matters. Retrieved from https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

[6] Buechner, J., Simon, J., & Tavani, H. T. (2014). Re-Thinking Trust and Trustworthiness inDigital Environments. *In Autonomous Technologies: Philosophical Issues, PracticalSolutions, Human Nature: Proceedings of the Tenth International Conference on Computer EthicsPhilosophical Enquiry: CEPE 2013.* . Menomonie.

[7] Building trust in online marketplaces: A literature review. (2015). *Journal of Management Information Systems, 31*(4), 13-48.

[8] Chepelyuk, S. G. (2022). he Phenomenon of "Digital Trust" in the Context of Digital Government in Russia. *RUDN Journal of Political Science.* doi:10.22363/2313-1438-2022-24-3-447-459

[9] Chiodi, M. (2023). The Intersection of Trust and Employee Productivity. *ISACA*. Retrieved from https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-4/the-intersection-of-trust-and-employee-productivity

[10] Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). The Role of Leadership in a Digitalized World: A Review. *Front Psychol*.

[11] Cuomo, J. (2020). How blockchain adds trust to AI and IoT. *IBM*. Retrieved from https://www.ibm.com/blog/how-blockchain-adds-trust-to-ai-and-iot/

[12] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982-1003.

[13] Dennis, R., & Edwards, K. R. (2016). Digital Trust in the Workplace: A Review and Research Agenda. *Information Systems Research, 27*(2), 389-410.

[14] Digital trust in e-commerce: A review of literature and implications for online consumer behavior. (2018). *Journal of Business Research, 85*, 263-276.

[15] Digital trust in the financial industry: A review of trends and challenges. (2019). *IEEE Transactions on Industrial Informatics, 15*(6), 3894-3912.

[16] Digital trust in the healthcare industry: A review of trends and challenges. (2020). *IEEE Journal of Biomedical and Health Informatics, 24*(6), 2224-2234.

[17] Dutton, W. H., Guerra, G. A., Zizzo, D. J., & Peltu, M. (2005). The cyber trust tension in E-government: Balancing identity, privacy, security. *Inf. Polity*, 13-23.

[18] Fancher, D., & Golden, D. (2023). 5 actions C-suite leaders can take to protect digital trust in their organization. *Deloitte Insights*. Retrieved from https://www.deloitte.com/global/en/issues/trust/five-actions-c-suite-leaders-can-take-to-protect-digital-trust-in-their-organization.html

[19] Fatin, F. K., & Wan, , F. Z. (2022). Online trust development in online shopping. *Journal of Information System and Technology Management*. doi:10.35631/JISTM.518003

[20] Fera, T. H., Abawajy, J. H., Chowdhury, M. U., & Shalannanda, W. (2021). Citizens' Trust Measurement in Smart Government Services. *IEEE Access*. doi: doi: 10.1109/ACCESS.2021.3124206

[21] Ferrazzi, K. (2012). How to Build Trust in a Virtual Workplace. *Harvard Business Review Home*.

[22] Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90.

[23] Gurel-Atay, E., & Turetken, O. (2019). Digital Trust in the Workplace: A Conceptual Framework. *Journal of Business Research, 96*, 79-91.

[24] *Industry 4.0 Market Size, Share & Trends Analysis Report By Component (Solutions, Services), By Application, By Organization Size, By Vertical, By Region, And Segment Forecasts, 2020 - 2027,*. (n.d.). Retrieved from Grand View Research: https://www.grandviewresearch.com/industry-analysis/industry-40-market

[25] Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. (1998). Is anybody out there? Antecedents of trust in global virtual teams. *Journal of Management Information Systems*, 14(4), 29-64.

[26] Lau, A., & Höyng , M. (2023). Digitalization?A Matter of Trust: A Double-Mediation Model Investigating Employee Trust in Management Regarding Digitalization. *Review of Managerial Science*, 2165-2183.

[27] Lee, S., & Choi, J. (2019). Understanding the relationship between trust in the Internet and social media services and the acceptance of digital service innovation. *Telematics and Informatics*, 38, 80-93.

[28] Leong, M. H., & Liang, T. P. (2018). Digital trust in online shopping: a framework and research agenda. *Journal of Retailing and Consumer Services, 42*, 1-13.

[29] Li, F., & Betts, S. C. (n.d.). Trust: What It Is And What It Is Not. *International Business & Economics Research Journal, 2*(7).

[30] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

[31] McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334-359.

[32] Mohammed, R. (2022). [Cybersecurity] is an enabler of digital trust and a key success factor of the digital transformation journey. *Cybersecurity Strategies to Enable Digital Trust*.

[33] Paliszkiewicz, J., & Chen, K. (2022). *Building Digital Trust in Business* (1st ed.). doi:10.4324/9781003266525-2

[34] Prabhu, J. (2006). Digital Trust: A Conceptual Framework. *Journal of Management Information Systems, 22*(4), 191-234.

[35] Ratnasingam, P., & Currie, W. L. (2018). Building Digital Trust: A Conceptual Framework. *Journal of Business Research, 72*, 1-14.

[36] Rejeb, A., Karim Rejeb , K., Appolloni, A., Jagtap, S., Iranmanesh , M., Alghamdi, S., . . . Kayikci, Y. (2024). Unleashing the power of Internet of Things and Blockchain: A comprehensive analysis and future directions. *Internet of Things and Cyber-Physical Systems*, 1-18. Retrieved from https://www.sciencedirect.com/science/article/pii/S2667345223000366

[37] Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Psychological Bulletin, 97*(2), 311-327.

[38] ResearchAndMarkets.com. (2018). *Industry 4.0 Market By Component, Application, Organization Size, Vertical, And Region - Global Forecast to 2023*. Retrieved from ResearchAndMarkets.com: https://www.researchandmarkets.com/research/w5zq3x/industry_40_market

[39] Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trsut. *Academy of Management Review, 23*(3), 393-404.

[40] Schwab, K. (2016). The Fourth Industrial Revolution. *World Economic Forum*.

[41] Trust in the sharing economy: A systematic literature review. (2017). *Journal of Business Research, 70*, 287-298.

[42] Wickramasinghe, A. S. (2021). Trust and Organizational Leadership. In A. S. Wickramasinghe, *Handbook of Research on Multidisciplinary Perspectives on Managerial and Leadership Psychology* (p. 22). USA: IGI Global . doi:10.4018/978-1-7998-3811-1.ch025

[43] Zhang , F., Wang, H., Zhou, L., Xu, D., & Liu, L. (2023). A blockchain-based security and trust mechanism for AI-enabled IIoT systems. *Future Generation Computer Systems*, 78-85. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0167739X23000882