


# The Role of Federated Learning in Enhancing Data Privacy in Distributed Environments in Indonesia

Ajub Ajulian ZM<sup>1</sup>, Enda Wista Sinuraya<sup>2</sup>, Bambang Winardi<sup>3</sup>  
<sup>1,2,3</sup> Departemen Teknik Elektro, Fakultas Teknik, Universitas Diponegoro

Article Info	ABSTRACT
<p><b>Article history:</b> Received Aug, 2025 Revised Aug, 2025 Accepted Aug, 2025</p> <hr/> <p><b>Keywords:</b> Compliance; Data Privacy; Distributed Environment; Federated Learning; Trust</p>	<p>This study investigates the role of federated learning (FL) in enhancing data privacy within distributed environments in Indonesia. With the increasing reliance on digital technologies, data privacy has become a critical concern, particularly in decentralized systems. A quantitative research approach was employed, involving 130 respondents from various professional backgrounds engaged with distributed data systems. Data were collected using a structured questionnaire with a five-point Likert scale (1–5) and analyzed using SPSS version 25. Descriptive, correlation, and regression analyses revealed that federated learning significantly contributes to improving confidentiality, trust, and compliance in distributed environments. The results indicate that FL not only safeguards sensitive data but also enhances stakeholder confidence and supports adherence to regulatory standards, such as Indonesia’s UU PDP. The study provides empirical evidence supporting the adoption of federated learning as a privacy-preserving technology and offers practical insights for organizations and policymakers seeking secure and compliant digital ecosystems.</p> <p><i>This is an open access article under the <a href="#">CC BY-SA</a> license.</i></p>
<p><b>Corresponding Author:</b> Name: Ajub Ajulian ZM Institution: Departemen Teknik Elektro, Fakultas Teknik, Universitas Diponegoro Email: <a href="mailto:ayub.ayulian@gmail.com">ayub.ayulian@gmail.com</a></p>	

## 1. INTRODUCTION

The rapid advancement of digital technologies has transformed the way data is generated, shared, and utilized in today’s interconnected world. In Indonesia, as in many other countries, the increasing adoption of cloud computing, Internet of Things (IoT), and artificial intelligence (AI) has led to an exponential rise in the volume of sensitive data. While this development offers significant opportunities for innovation and efficiency, it also raises serious concerns regarding data privacy and security, as conventional centralized machine learning models require data aggregation in a single server or data center, thereby creating risks of data breaches, unauthorized access, and non-

compliance with privacy regulations. Federated Learning (FL) emerges as a promising solution to these challenges by enabling decentralized model training, maintaining data privacy and security while complying with regulations, particularly in the context of cloud computing, IoT, and AI where traditional centralized models pose significant risks. FL allows data to remain on local devices, only sharing model updates rather than raw data, thus preserving user privacy and reducing the risk of data breaches [1], [2]. This decentralized approach aligns with data protection regulations such as GDPR, ensuring compliance while facilitating collaborative intelligence across distributed data sources [1], [3]. In IoT environments, FL supports collaborative learning from

distributed data, enhancing security and privacy without the need for centralized data storage [2], [4], while its integration with cloud services enables efficient and secure model exchange to address unique challenges such as resource constraints and dynamic data streams [4]. Moreover, FL's decentralized nature mitigates security vulnerabilities inherent in centralized systems, offering a robust solution for protecting sensitive IoT data [2], and techniques like homomorphic encryption and secure multi-party computation further enhance security by allowing computations on encrypted data [3].

Federated Learning (FL) has emerged as a promising paradigm to address the challenges of data privacy in rapidly expanding digital ecosystems such as Indonesia. Unlike traditional approaches, FL enables the training of machine learning models across multiple decentralized devices or servers without requiring direct data exchange, as only model parameters are shared while local datasets remain confidential. This privacy-preserving method is particularly relevant in Indonesia, where sensitive personal and organizational data are increasingly generated and regulatory frameworks on data protection are evolving to keep pace with digital growth. FL enhances privacy by keeping data on local devices, thereby eliminating the need to transfer sensitive information to central servers [5], [6], and employs techniques such as differential privacy and secure multi-party computation to mitigate risks like data reconstruction and model inversion attacks [7]. Its applications in critical sectors such as healthcare and finance allow the development of diagnostic or financial models without exposing sensitive data [8], while its decentralized nature aligns with Indonesia's increasing focus on data protection regulations [5]. Nevertheless, FL also faces challenges, including managing non-IID (non-independent and identically distributed) data and ensuring synchronization of updates across devices, but these can be addressed through the development of more robust decentralized training algorithms and aggregation strategies [8].

Recent studies emphasize the potential of federated learning to balance privacy with performance in collaborative data processing, yet empirical evidence on its perception and effectiveness in the Indonesian context remains limited, as most discussions are still conceptual or technical with little focus on the human and organizational dimensions of adoption. This research seeks to bridge that gap by quantitatively analyzing perceptions of federated learning's role in enhancing data privacy among Indonesian stakeholders through a structured survey designed to identify patterns and relationships between federated learning practices and perceived improvements in data privacy. The objectives of this study are threefold: first, to examine the extent to which federated learning is perceived to enhance data privacy in distributed environments; second, to identify the key dimensions of trust, confidentiality, and compliance influenced by federated learning; and third, to provide recommendations for stakeholders in adopting privacy-preserving technologies in Indonesia's digital ecosystem. Through this investigation, the study aims to deepen understanding of federated learning's role in securing distributed data and to support the development of privacy-aware technological practices in Indonesia's increasingly digital society.

## 2. LITERATURE REVIEW

### 2.1. *Federated Learning*

Federated Learning (FL) offers a promising solution for organizations in Indonesia dealing with sensitive data by enabling decentralized model training while preserving data privacy, making it particularly beneficial in sectors such as healthcare, finance, and IoT where data protection is paramount. By allowing data to remain local and only sharing model updates, FL minimizes the risk of data leakage and aligns with data protection regulations such as GDPR, which are increasingly relevant in both global and local contexts [1], [8], [9]. Beyond

privacy, FL enhances scalability and efficiency by distributing computational tasks across multiple devices, thereby reducing communication burdens and proving especially useful in IoT applications where data is generated from numerous decentralized sources [1], [9]. Nonetheless, FL implementation faces challenges, including handling non-IID data distributions, ensuring synchronization of updates, and addressing security vulnerabilities such as model inversion attacks, which necessitate robust countermeasures to maintain model efficacy and privacy [5], [9]. Furthermore, compliance with stringent data protection laws and attention to ethical considerations, such as fairness and participant accountability, are critical to ensuring the successful and responsible adoption of FL in Indonesia's digital ecosystem [1], [5].

## 2.2. Data Privacy

Ensuring data privacy in Indonesia has become increasingly critical with the rise of digital platforms, and the introduction of the Undang-Undang Perlindungan Data Pribadi (UU PDP) represents a major step in strengthening the legal framework for personal data protection by addressing the previously fragmented and sectoral nature of existing regulations. Enacted in 2022, the UU PDP provides both preventive and repressive protections, including administrative sanctions for data breaches, thereby moving towards a more unified legal framework [10]–[12]. In this context, federated learning emerges as a privacy-preserving technology that minimizes the need for raw data transfer and storage by enabling collaborative machine learning without centralizing data, thus

aligning with Indonesia's data protection goals and reducing vulnerabilities [13]. This approach is especially beneficial in sensitive sectors such as online transportation, where data misuse has previously been a concern [12]. Nevertheless, challenges remain as Indonesia's legal protections are still less comprehensive compared to neighboring countries like Singapore and Malaysia, underscoring the need for swift enactment and effective implementation of the UU PDP to provide a clear legal basis for addressing data misuse and ensuring stronger safeguards for personal data privacy [14].

## 2.3. Distributed Environment

Federated Learning (FL) is a transformative approach in distributed environments, highly relevant for Indonesia's growing digital economy, as it enables collaborative model training across decentralized nodes without sharing raw data, thus addressing privacy and security challenges. Its use in cloud computing and IoT enhances data privacy, scalability, and model performance, making FL an important innovation for Indonesian organizations. By keeping data local, FL reduces risks of centralized data collection [15], [16], though challenges such as data reconstruction and model inversion attacks remain, addressed through techniques like Differential Privacy (DP) and Secure Multi-Party Computation (SMPC) [7]. Communication links also face cyber threats, requiring strong security measures [17]. On scalability, FL supports large-scale training across many devices [18], with communication overhead reduced through gradient compression [16]. In practice, FL has been applied in healthcare and finance where privacy is critical [17], though

balancing accuracy and privacy, especially with non-IID data, remains a key challenge [16].

#### **2.4. Federated Learning and Data Privacy in Indonesia**

Federated Learning (FL) is a promising approach to balancing data utility and privacy by enabling decentralized model training without sharing raw data, thereby enhancing privacy by keeping sensitive information on local devices and reducing the risk of data breaches [6]. Privacy-preserving techniques such as Differential Privacy (DP) and Secure Multi-Party Computation (SMPC) further mitigate risks like data reconstruction and model inversion attacks [7], though challenges remain in verifying server-side DP guarantees and managing diverse device types [19]. Despite its potential, the adoption of FL in Indonesia faces significant barriers due to technical complexity, high computational costs, and the need for advanced techniques like homomorphic encryption [6], [20]. Regulatory frameworks such as GDPR highlight the importance of strong legal support, yet Indonesia still requires robust regulations to facilitate FL implementation [7]. Moreover, a limited understanding of how organizations and individuals perceive FL's role in enhancing data privacy, coupled with the lack of empirical studies in Indonesia, underscores the need to explore stakeholder perceptions and socio-cultural factors influencing adoption beyond purely technical considerations [6], [19].

#### **2.5. Previous Empirical Studies**

Prior empirical studies in other countries indicate that federated learning (FL) positively influences perceptions of security and trust in digital systems, with research in healthcare and finance

showing that FL improves compliance with data protection standards while supporting efficient analytics. Quantitative surveys have demonstrated significant relationships between FL implementation and variables such as confidentiality, transparency, and organizational trust. In healthcare, FL enables privacy-preserving data sharing and secure AI model training across distributed datasets, reducing risks of breaches and ensuring compliance with regulations like HIPAA and GDPR [21], [22], while in finance, it addresses privacy challenges by enabling model training at the data source, thereby maintaining confidentiality and enhancing trust [23]. However, few studies have been conducted in Southeast Asia, particularly in Indonesia, where the regulatory landscape is still evolving with the enactment of Law No. 27 of 2022 on Personal Data Protection, which strengthens consumer trust but also imposes compliance costs and technical requirements [24]. Given Indonesia's unique digital ecosystem and regulatory framework, tailored FL solutions are needed, especially since prior evidence suggests that clarity of privacy policies strongly correlates with trust and user behavior in the country [25]. Thus, implementing FL in Indonesia holds potential to enhance data protection, build organizational trust, ensure regulatory compliance, and foster innovation and competitiveness in the digital economy.

#### **2.6. Research Gap and Hypotheses Development**

Although federated learning has been studied extensively from a technical perspective, limited research has examined its impact on perceptions of data privacy in Indonesia's distributed environments. This study addresses

that gap by empirically analyzing how stakeholders perceive federated learning as a tool for enhancing data privacy. Based on the literature, the following hypotheses are proposed:

- H1: Federated learning has a positive effect on perceived data confidentiality in distributed environments.
- H2: Federated learning has a positive effect on trust in digital systems.
- H3: Federated learning has a positive effect on perceived compliance with data protection standards.

### 3. RESEARCH METHODS

#### 3.1. Research Design

This study employs a quantitative research design to investigate the role of federated learning in enhancing data privacy within distributed environments in Indonesia. The quantitative approach was chosen because it allows the systematic collection and statistical analysis of data to identify relationships between variables. A survey method using a structured questionnaire was applied to capture respondents' perceptions of federated learning and its impact on data privacy dimensions, namely confidentiality, trust, and compliance with data protection standards.

#### 3.2. Population and Sample

The population of this study consists of professionals and stakeholders in Indonesia who are actively involved in digital ecosystems, such as those working in information technology, data management, and digital business sectors. A purposive sampling technique was applied to select respondents who have sufficient knowledge or experience in distributed systems and data privacy practices. A total of 130 respondents

participated in this study, which is considered an adequate sample size for statistical analysis using SPSS version 25.

#### 3.3. Data Collection Method

Primary data were collected through a structured online questionnaire distributed to respondents, consisting of two sections: the first covered demographic information such as gender, age, occupation, and level of experience with digital and distributed systems, while the second measured research variables related to perceptions of federated learning's role in enhancing data privacy, specifically focusing on confidentiality, trust, and compliance. All items were assessed using a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree, designed to capture the intensity of respondents' perceptions.

#### 3.4. Research Variables and Indicators

The study examines one independent variable, Federated Learning (FL), and three dependent variables, namely Confidentiality (CF), Trust (TR), and Compliance (CP), with indicators developed from prior studies and adapted to the Indonesian context. For FL, the indicators include efficiency of collaborative learning, reduced reliance on centralized data, and the ability to secure local datasets; CF is measured through the protection of sensitive data, minimized exposure, and secure data handling; TR is assessed by stakeholder confidence, system reliability, and reduced risk of breaches; while CP focuses on alignment with data protection regulations, adherence to privacy standards, and organizational responsibility.

#### 3.5. Data Analysis Technique

The data collected were processed and analyzed using SPSS

version 25 through several stages, beginning with descriptive statistics to summarize respondent demographics and provide an overview of variable distributions. Reliability testing using Cronbach's Alpha was conducted to assess the internal consistency of the measurement instruments, followed by validity testing through KMO and Bartlett's Test and factor loadings to ensure the accuracy of indicators in representing the variables. Correlation analysis was then applied to identify the relationships between federated learning and the dependent variables, while regression analysis was performed to test the hypotheses and measure the extent to which federated learning influences confidentiality, trust, and compliance in distributed environments.

## 4. RESULTS AND DISCUSSION

### 4.1. Descriptive Findings

A total of 130 respondents participated in this study,

representing professionals engaged in digital and distributed environments in Indonesia. The demographic profile shows that 60% were male (78 respondents) and 40% female (52 respondents), with the majority aged 25–34 years (50%), followed by 35–44 years (35%) and 22–24 years (15%). In terms of work experience, 55% had 3–5 years of experience in digital systems, 30% had more than 5 years, and 15% had less than 3 years. Their professional backgrounds included IT specialists (40%), data analysts (25%), digital business managers (20%), and other roles such as network administrators and system developers (15%). The survey also assessed perceptions of federated learning and its impact on three dimensions of data privacy—confidentiality, trust, and compliance—using a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree), with descriptive statistics indicating generally positive perceptions among respondents.

Table 1. Descriptive Statistics

Variable	Minimum	Maximum	Mean	Standard Deviation
Federated Learning (FL)	3	5	4.12	0.48
Confidentiality (CF)	3	5	4.05	0.52
Trust (TR)	3	5	3.98	0.55
Compliance (CP)	3	5	4.00	0.50

Source: Results processing data (2025)

The interpretation of results shows that Federated Learning (FL) received a mean score of 4.12, indicating that respondents generally perceive it as effective in supporting collaborative data processing while maintaining privacy. Confidentiality (CF) scored a mean of 4.05, reflecting agreement that FL helps protect sensitive data and reduces exposure risks. Trust (TR) achieved a mean of 3.98, suggesting a positive perception of trust in systems implementing FL, though slightly lower compared to

confidentiality and compliance. Meanwhile, Compliance (CP) recorded a mean of 4.00, indicating that respondents view FL as well-aligned with regulatory and organizational privacy requirements.

### 4.2. Reliability and Validity Analysis

#### a. Reliability Analysis

Reliability refers to the consistency of the measurement instruments in capturing the intended constructs. Cronbach's Alpha was used to assess internal consistency reliability. A

threshold of 0.7 is generally considered acceptable

(Nunnally, 1978). The results are presented in Table 2:

Table 2. Reliability Analysis

Variable	No. of Items	Cronbach's Alpha	Reliability Status
Federated Learning (FL)	5	0.878	Reliable
Confidentiality (CF)	4	0.861	Reliable
Trust (TR)	4	0.845	Reliable
Compliance (CP)	4	0.852	Reliable

Source: Results processing data (2025)

All variables showed Cronbach's Alpha values above 0.7, confirming high internal consistency and indicating that the questionnaire items reliably measure the intended constructs. Federated Learning (FL), measured with five items, achieved a Cronbach's Alpha of 0.878, reflecting strong reliability in capturing respondents' perceptions of collaborative model training and data privacy. Confidentiality (CF), assessed with four items, obtained a value of 0.861, showing consistency in measuring the extent to which FL protects sensitive data and reduces risks of exposure. Trust (TR), also measured with four items, recorded a Cronbach's Alpha of 0.845, indicating reliable measurement of stakeholder confidence, system reliability, and reduced risks of breaches. Compliance (CP), with four items, scored 0.852, affirming that the indicators consistently represent alignment with regulatory and organizational privacy standards. Overall, the reliability status of all variables is confirmed as "Reliable,"

demonstrating that the instruments used in this study are robust and dependable for further analysis.

#### b. Validity Analysis

Validity testing was conducted to ensure that the measurement items accurately represent the intended constructs using the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy and Bartlett's Test of Sphericity. The KMO value of 0.812, which is greater than the threshold of 0.6, indicates that the sample is adequate for factor analysis, while Bartlett's Test of Sphericity ( $\chi^2 = 356.41$ ,  $p < 0.001$ ) confirms that the correlation matrix is not an identity matrix, making factor analysis appropriate. Furthermore, convergent validity was assessed using factor loadings obtained from principal component analysis, with values greater than 0.6 demonstrating that each indicator is valid in representing the respective construct (Hair et al., 2010). Table 3 provides a detailed summary of the factor loadings.

Table 3. Validity Analysis

Variable	Indicator	Factor Loading	Validity Status
FL	FL1	0.725	Valid
FL	FL2	0.752	Valid
FL	FL3	0.786	Valid
FL	FL4	0.741	Valid
FL	FL5	0.763	Valid

CF	CF1	0.716	Valid
CF	CF2	0.733	Valid
CF	CF3	0.709	Valid
CF	CF4	0.722	Valid
TR	TR1	0.694	Valid
TR	TR2	0.707	Valid
TR	TR3	0.714	Valid
TR	TR4	0.688	Valid
CP	CP1	0.724	Valid
CP	CP2	0.741	Valid
CP	CP3	0.733	Valid
CP	CP4	0.717	Valid

Source: Results processing data (2025)

All indicators have factor loadings above 0.6, confirming convergent validity and demonstrating that the questionnaire items accurately measure the intended constructs of federated learning, confidentiality, trust, and compliance. Specifically, the Federated Learning (FL) variable with five indicators (FL1–FL5) recorded factor loadings ranging from 0.725 to 0.786, showing consistency in capturing perceptions of decentralized model training and data privacy. The Confidentiality (CF) variable, with four indicators (CF1–CF4), produced factor loadings between 0.709 and 0.733, reflecting strong validity in measuring sensitive data protection and secure handling. Trust (TR) was also well-represented, with four indicators (TR1–TR4) yielding factor loadings from 0.688 to 0.714, confirming reliable

measurement of stakeholder confidence, system reliability, and reduced risk of breaches. Likewise, the Compliance (CP) variable demonstrated robust construct validity, with four indicators (CP1–CP4) producing factor loadings between 0.717 and 0.741, affirming their accuracy in representing adherence to data protection regulations and organizational responsibility. Overall, the results confirm that all measurement items are valid and suitable for further analysis in this study.

#### 4.3. Correlation Analysis

Correlation analysis was conducted to examine the relationships between the independent variable, Federated Learning (FL), and the dependent variables: Confidentiality (CF), Trust (TR), and Compliance (CP). Pearson correlation coefficients were calculated to determine the strength and direction of the associations.

Table 4. Pearson Correlation Results

Variable Pair	Pearson Correlation (r)	Significance (p-value)	Interpretation
FL ↔ CF	0.652	< 0.001	Strong positive correlation
FL ↔ TR	0.601	< 0.001	Moderate positive correlation
FL ↔ CP	0.625	< 0.001	Moderate to strong positive correlation

Source: Results processing data (2025)



#### 4.4. Correlation Analysis

The interpretation of results shows that federated learning has a significant positive association with all three dimensions of data privacy. The correlation coefficient between Federated Learning and Confidentiality (FL ↔ CF) is 0.652, indicating a strong positive relationship, meaning that higher perceptions of federated learning implementation are linked to stronger perceptions of data confidentiality in distributed environments. The correlation between Federated Learning and Trust (FL ↔ TR) is 0.601, reflecting a moderate positive relationship and suggesting that federated learning enhances stakeholders' trust in digital systems. Meanwhile, the correlation between Federated Learning and Compliance (FL ↔ CP) is 0.625, signifying a moderate to strong positive relationship, which implies that federated learning

improves perceptions of adherence to data protection regulations and organizational standards. All these correlation results were statistically significant at  $p < 0.01$ , confirming that federated learning is positively associated with confidentiality, trust, and compliance.

#### 4.5. Regression Analysis and Hypotheses Testing

Multiple linear regression analysis was conducted to examine the effect of Federated Learning (FL) on the dependent variables—Confidentiality (CF), Trust (TR), and Compliance (CP)—with the aim of testing the hypotheses formulated in the literature review. This analysis provides insight into the extent to which the independent variable predicts changes in the dependent variables, thereby clarifying the influence of FL on perceptions of data privacy in distributed environments. The results of the regression analysis are summarized in Table 5.

Table 5. Hypothesis Testing

Dependent Variable	$\beta$ (Standardized Coefficient)	t-value	p-value	Hypothesis Result
Confidentiality (CF)	0.651	8.722	<0.001	Supported
Trust (TR)	0.602	7.956	<0.001	Supported
Compliance (CP)	0.623	8.213	<0.001	Supported

Source: Results processing data (2025)

The interpretation of regression results shows that Federated Learning (FL) has a significant positive effect on all three dependent variables—Confidentiality (CF), Trust (TR), and Compliance (CP)—with all hypotheses supported. For confidentiality, the standardized coefficient ( $\beta = 0.651$ ,  $t = 8.72$ ,  $p < 0.001$ ) indicates a strong positive and significant effect, confirming that implementing FL enhances the protection of sensitive data by reducing exposure and limiting data transfer in distributed environments. In terms of trust, the coefficient ( $\beta =$

$0.602$ ,  $t = 7.95$ ,  $p < 0.001$ ) reflects a moderate yet significant effect, suggesting that the privacy-preserving features of FL strengthen stakeholders' confidence in digital systems by ensuring reliability and minimizing risks of breaches. For compliance, the coefficient ( $\beta = 0.623$ ,  $t = 8.21$ ,  $p < 0.001$ ) demonstrates a strong positive effect, indicating that FL supports adherence to data protection regulations and organizational standards, thereby aligning technical practices with legal and ethical requirements. Overall, these results highlight that FL significantly contributes to

enhancing data confidentiality, building trust, and ensuring compliance within Indonesia's digital ecosystem.

#### 4.6. Discussion

##### a. Federated Learning and Confidentiality

The regression and correlation results indicate a strong positive effect of Federated Learning (FL) on confidentiality, as respondents perceived that FL reduces the need for centralized data storage and minimizes the risk of unauthorized access, aligning with prior studies highlighting its ability to preserve privacy while enabling collaborative model training. In practice, organizations in Indonesia can adopt FL to protect sensitive customer and operational data, particularly in finance, healthcare, and e-commerce, where breaches could have serious consequences. FL ensures privacy preservation by keeping raw data localized on client devices and sharing only model updates, significantly reducing breach risks [5], while techniques such as encryption and differential privacy further safeguard sensitive information during training [22]. In finance, FL supports applications like credit card fraud detection by enabling collaborative model training without exposing sensitive financial data [26], in healthcare, it allows AI models to be trained on patient data without transfer, thereby maintaining confidentiality while improving outcomes [22], [27], and in e-commerce, it enhances personalized recommendations and fraud detection while preserving customer trust [22]. Despite

these benefits, challenges such as communication overhead and data heterogeneity remain, though solutions like model compression and robust aggregation techniques are being developed [27], [28]. Moreover, ensuring compliance with regulatory frameworks is critical, and FL's privacy-preserving nature aligns closely with stringent data protection laws [5], [27].

##### b. Federated Learning and Trust

The study found a significant positive relationship between Federated Learning (FL) and trust, as stakeholders expressed greater confidence in digital systems that implement FL, indicating that privacy-preserving mechanisms strengthen reliability and credibility. This is particularly relevant in Indonesia's evolving digital ecosystem, where concerns about data misuse and cyber threats are growing. By processing data locally and minimizing exposure, FL aligns with Indonesia's Personal Data Protection Law No. 27 of 2022, safeguarding personal data and enhancing consumer trust [24], [29]. Reducing the need to transfer sensitive data also mitigates risks of breaches, a key issue in public services and fintech sectors [24]. Trust is a critical factor in adopting digital services such as digital banking, where perceived security strongly influences user acceptance, and implementing FL enhances this perception, fostering loyalty and broader platform use [30]. Furthermore, FL supports Indonesia's digital transformation policies, which emphasize cybersecurity and privacy protections, by offering a

secure framework for data processing that underpins sustainable growth and resilience against cyber threats [31].

**c. Federated Learning and Compliance**

FL was shown to have a significant positive effect on compliance with data protection standards. Respondents indicated that FL aligns with regulatory requirements, such as Indonesia's Undang-Undang Perlindungan Data Pribadi (UU PDP), and supports organizational adherence to privacy policies. This demonstrates that FL is not only a technical innovation but also a governance tool, helping organizations meet legal obligations and ethical standards in handling distributed data.

**d. Implications for Practice and Policy**

The study highlights several practical and policy implications. First, organizations should consider integrating FL into their digital systems to safeguard sensitive data, especially in distributed networks. Second, policymakers can promote FL adoption through guidelines and incentives, emphasizing privacy-enhancing technologies as part of national digital transformation strategies. Third, ongoing training and awareness programs are essential to ensure that stakeholders understand FL's benefits and limitations, fostering effective implementation and maximizing trust and compliance.

**e. Theoretical Implications**

The results contribute to the literature on privacy-preserving machine learning

and distributed computing by providing quantitative evidence from an Indonesian context. While previous research focused largely on technical and global perspectives, this study demonstrates that FL has tangible effects on organizational perceptions of confidentiality, trust, and compliance. This enhances the understanding of human and organizational factors in adopting FL, offering a holistic view of its role beyond algorithmic efficiency.

**f. Limitations and Future Research**

Although the study provides important insights, some limitations should be noted. The sample size (130 respondents) may limit generalizability, and the study focused primarily on perception rather than actual FL implementation outcomes. Future research could explore longitudinal effects of FL adoption, sector-specific applications, or integrate mixed-method approaches to combine perception data with performance metrics.

## 5. CONCLUSION

This study demonstrates that federated learning (FL) plays a significant role in enhancing data privacy in distributed environments in Indonesia, with quantitative analysis confirming its positive effects on confidentiality by protecting sensitive data, on trust by increasing stakeholders' confidence in digital systems, and on compliance by aligning with regulatory and organizational standards. These results indicate that FL is not only a technical innovation but also a strategic tool for organizations seeking to secure distributed data while maintaining legal and ethical obligations. The study carries practical

implications for organizations and policymakers by underscoring the importance of adopting privacy-preserving technologies and raising awareness of their benefits, while also contributing theoretically to the understanding of FL's impact on human and organizational perceptions of data privacy.

Future research is encouraged to investigate sector-specific applications, long-term outcomes of implementation, and mixed-method approaches that combine quantitative and qualitative analyses to further deepen insights into the role of federated learning in Indonesia's evolving digital ecosystem.

## REFERENCE

- [1] K. Lazaros, D. E. Koumadorakis, A. G. Vrahatis, and S. Kotsiantis, "Federated learning: Navigating the landscape of collaborative intelligence," *Electronics*, vol. 13, no. 23, p. 4744, 2024.
- [2] S. A. Moeed, R. Karnati, G. Ashmitha, G. B. Mohammad, and S. N. Mohanty, "A Novel Enhanced Approach for Security and Privacy Preserving in IoT Devices with Federal Learning Technique," *SN Comput. Sci.*, vol. 5, no. 6, p. 750, 2024.
- [3] T. K. Vashishth, V. Sharma, K. K. Sharma, B. Kumar, S. Chaudhary, and M. Gupta, "Privacy-Preserving Machine Learning Techniques for IoT Data in Cloud Environments," in *Emerging Technologies for Securing the Cloud and IoT*, IGI Global Scientific Publishing, 2024, pp. 144–173.
- [4] J. G. Gonçalves *et al.*, "Decentralized Machine Learning Framework for the Internet of Things: Enhancing Security, Privacy, and Efficiency in Cloud-Integrated Environments," *Electronics*, vol. 13, no. 21, p. 4185, 2024.
- [5] M. Aggarwal, V. Khullar, and N. Goyal, "A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training," *Appl. Data Sci. Smart Syst.*, pp. 570–575, 2024.
- [6] A. Joshi, "Federated Learning: Enhancing Data Privacy and Security in Machine Learning through Decentralized Training Paradigms," *J. Artif. Intell. Cloud Comput.*, vol. 1, 2022.
- [7] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 619–640, 2021.
- [8] A. S. Alardawi, A. Odeh, A. Aboshgifa, and N. Belhaj, "Challenges and Opportunities in Federated Learning," 2024.
- [9] S. Adsure and M. Devare, "A Research Review on Challenges of Federated Machine Learning," in *2024 8th International Conference on Computing, Communication, Control and Automation (IC3UBEA)*, 2024, pp. 1–7.
- [10] S. Dewi, "Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia," *J. Jure*, vol. 15, no. 2, p. 165, 2015.
- [11] J. E. Widodo, A. Suganda, and T. A. Darodjat, "DATA PRIVACY AND CONSTITUTIONAL RIGHTS IN INDONESIA: DATA PRIVACY AND CONSTITUTIONAL RIGHTS IN INDONESIA," *PENA LAW Int. J. Law*, vol. 2, no. 2, 2024.
- [12] S. S. Soewarno and D. D. Heniarti, "Perlindungan Hukum terhadap Data Pribadi Pengguna Jasa Transportasi Online di Indonesia Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," 2022.
- [13] D. R. Kale, T. S. Mane, A. Buchade, P. B. Patel, L. K. Wadhwa, and R. G. Pawar, "Federated Learning for Privacy-Preserving Data Mining," in *2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA)*, 2024, pp. 1–6.
- [14] S. W. Attidhira and Y. S. Permana, "Review of Personal Data Protection Legal Regulations in Indonesia," *Awang Long Law Rev.*, vol. 5, no. 1, pp. 280–294, 2022.
- [15] W. Qiu, D. Shi, Q. Li, Y. Zheng, and X. Shen, "Application of Federated Learning in Distributed Environments: Experiments and Evaluation," in *2023 5th International Academic Exchange Conference on Science and Technology Innovation (IAECST)*, 2023, pp. 58–62.
- [16] N. N. Kodakandla, "Federated learning in cloud environments: Enhancing data privacy and AI model training across distributed systems," *Int. J. Sci. Res. Arch.*, vol. 5, no. 2, pp. 347–356, 2022.
- [17] C. Chen *et al.*, "Trustworthy federated learning: privacy, security, and beyond," *Knowl. Inf. Syst.*, vol. 67, no. 3, pp. 2321–2356, 2025.
- [18] A. S. Rao, "Unifying Intelligence: Federated Learning in Cloud Environments for Decentralized Machine Learning".
- [19] M. Bharathi and T. A. S. Srinivas, "Federated Learning Unveiled: From Practical Insights to Bold Predictions".
- [20] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informatics*, vol. 16, no. 10, pp. 6532–6542, 2019.
- [21] S. Pal, K. Jha, and D. Sharma, "Blockchain-Enhanced AI Diagnostics in Healthcare," in *2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN)*, 2024, pp. 258–263.
- [22] S. Patil and N. Umashankar, "Federated Learning for Privacy-Preserving AI: Revolutionizing Data Sharing Across Industries".
- [23] Y. Shi, H. Song, and J. Xu, "Responsible and effective federated learning in financial services: A comprehensive survey," in *2023 62nd IEEE Conference on Decision and Control (CDC)*, 2023, pp. 4229–4236.
- [24] Z. S. Zuwanda, L. Judijanto, H. Khuan, and A. Triyanto, "Normative Study of Law No. 27 of 2022 on the Protection of Personal Data and Its Impact on the Fintech Industry in Indonesia," *West Sci. Law Hum. Rights*, vol. 2, no. 04, pp. 421–428, 2024.
- [25] I. Fathni, B. Basri, S. Zulaika, and R. S. Dewi, "Pengaruh Kebijakan Privasi, dan Tingkat Kepercayaan Pada Platform

- Digital terhadap Perilaku Pengguna dalam Melindungi Privasi Online di Indonesia," *Sanskara Huk. Dan HAM*, vol. 2, no. 02, pp. 118–126, 2023.
- [26] T. El Hallal and Y. El Mourabit, "Federated Learning for Credit Card Fraud Detection: Key Fundamentals and Emerging Trends," in *2024 International Conference on Circuit, Systems and Communication (ICCSC)*, 2024, pp. 1–6.
- [27] E. Nowell and S. Gallus, "Advancing Privacy-Preserving AI: A Survey on Federated Learning and Its Applications," 2025.
- [28] J. Fan, H. Lian, and W. Liu, "Privacy-preserving AI analytics in cloud computing: A federated learning approach for cross-organizational data collaboration," *Spectr. Res.*, vol. 4, no. 2, 2024.
- [29] R. A. Prastyanti and R. Sharma, "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India," *J. Hum. Rights, Cult. Leg. Syst.*, vol. 4, no. 2, pp. 354–390, 2024.
- [30] K. Kantika, F. Kurniasari, and M. Mulyono, "The factors affecting digital bank services adoption using trust as mediating variable," *J. Bus. Manag. Rev.*, vol. 3, no. 10, pp. 690–704, 2022.
- [31] M. Hafel, "Digital transformation in politics and governance in Indonesia: Opportunities and challenges in the era of technological disruption," *Society*, vol. 11, no. 2, pp. 742–757, 2023.