EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Data Security and Privacy Protection in Distributed Digital Economy: Economic Impacts and Governance Mechanisms

Cuilan Wang[1,*]

[1] School of Economics and Management, Anyang Vocational and Technical College, Anyang Henan 455000, China

Abstract

INTRODUCTION:The distributed digital economy, characterized by decentralization and cross-entity data flow, improves factor allocation efficiency but increasingly raises concerns over data security and privacy abuse.
OBJECTIVES: Unlike the conventional digital economy, which often centers on centralized platforms (e.g., e-commerce, cloud computing), the distributed digital economy in this paper specifically refers to an economic system where data—as a production factor—is stored, computed, and circulated across multiple independent nodes without a central coordinating authority, relying on technologies such as blockchain, distributed ledger, edge computing, and peer-to-peer networks. Its core governance features include decentralized data control, consensus-based verification, and peer-to-peer economic activities.
METHODS: This paper studies data security and privacy protection in the distributed digital economy from two aspects: economic impact and governance mechanism. Based on panel data from 30 provinces in China from 2018 to 2023, this paper uses the entropy weight-TOPSIS method, a two-way fixed effects model, a mediation effect model, and a spatiotemporal heterogeneity model to empirically test the economic impact and transmission mechanism of data security and privacy protection on the distributed digital economy.
RESULTS: The empirical analysis results show that the level of data security and privacy protection significantly and positively promotes the development of the distributed digital economy, with each unit increase leading to a 0.412 unit increase in the development index. Blockchain smart contracts, privacy computing standards, and cross-border data flow rules play significant mediating roles, accounting for 93.7% of the total mediating effect. This positive economic effect exhibits significant spatiotemporal differences, increasing year by year, and is significantly higher in the eastern region than in the central and western regions.
CONCLUSION: Based on empirical analysis results, optimization paths are proposed from four levels: collaborative governance, technology empowerment, regional balance, and institutional improvement, in order to improve the level of data security and privacy protection in the distributed digital economy.

Keywords: distributed, digital economy, data security, privacy protection, economic impact, governance mechanism

Received on 10 April 2026, accepted on 08 June 2026, published on 07 July 2026

doi: 10.4108/eetsis.12557

1. Introduction

In the current global digital wave, distributed digital economy has become the core engine driving economic growth. By distributed digital economy, this paper refers specifically to a economic system where data as a production factor is stored, computed, and circulated across

*Corresponding author Cuilan Wang. Email: 13837231361@163.com

multiple independent nodes without a central coordinating authority, relying on technologies such as blockchain, distributed ledger, edge computing, and peer-to-peer networks. This definition distinguishes itself from the broader digital economy literature, which often treats digitalization as a general productivity enhancement tool (e.g., e-commerce, cloud computing, or industrial internet) without emphasizing the decentralized, multi-node architecture. In contrast, the distributed digital economy highlights three distinctive features: (1) decentralized data governance, where no single entity has exclusive control; (2) cross-node data flow that requires consensus mechanisms and cryptographic verification; and (3) economic activities (e.g., decentralized finance, distributed manufacturing, sharing economy) that operate on a peer-to-peer basis rather than through centralized platforms. With the deep integration of emerging technologies such as blockchain, artificial intelligence, and the Internet of Things, distributed architecture has reshaped traditional economic models, giving rise to new formats such as decentralized finance, distributed manufacturing, and sharing economy [1]. However, this change has also raised dual challenges for data security and privacy protection: frequent data breaches, lack of cross-border data flow regulation, algorithmic discrimination, and abuse of user profiles, which not only threaten individual rights and corporate reputation, but may also shake the foundation of sustainable development of the digital economy [2-5]. In this context, data security and privacy protection are understood as a multi-dimensional construct encompassing institutional environments (laws and compliance standards), technological capabilities (encryption, privacy computing, smart contracts), and governance mechanisms (cross-border data flow rules, regulatory enforcement). This paper explicitly treats them as an integrated governance capacity that reduces security risks and enhances trust, rather than conflating them arbitrarily.

In the context of the digital economy, Wilson et al. [6] explored strategies for the sustainable development of the environment, economy, and education technology through the circular digital economy. This study shows that digital technology significantly reduces the environmental footprint of economic activities by optimizing the resource recycling chain and improving the efficiency of renewable energy systems. The digital economy has decoupled economic growth from resource consumption by reconstructing green supply chains, fostering emerging industries such as carbon trading, and promoting Industry 4.0 technology to reduce energy consumption in traditional industries. The open sharing of digital educational resources, the reduction of experimental teaching energy consumption by virtual laboratories, and the cultivation of sustainable development capabilities through project-based learning have jointly promoted the green transformation of education models. Alhitmi et al. [7] studied the data security and privacy risks of AI-driven marketing in the economic and commercial fields. Data anonymization and desensitization technologies, through techniques such as blurring and data slicing, make the original data impossible to recover in reverse, protecting user identity and sensitive information.

This study therefore explores data security and privacy protection in the distributed digital economy from both economic impact and governance mechanism perspectives, aiming to provide theoretical support and practical pathways for the digital economy.

2. Theoretical analysis and research hypotheses

2.1. Distributed digital economy

Distributed digital economy is a new economic form that relies on distributed technologies such as blockchain, distributed storage, and edge computing to realize decentralized storage, cross-node circulation, and collaborative utilization of data elements. Its core characteristics include decentralization, cross-entity participation, efficient data circulation, and risk spillover. Compared with the traditional centralized digital economy, the distributed digital economy breaks the data monopoly of a single subject, lowers the threshold and cost of data circulation, promotes the transformation of data elements from static storage to dynamic circulation [8], and thus improves the efficiency of element allocation. The development of the distributed digital economy depends on the safe and orderly circulation of data elements. Data security and privacy protection are the premise for its sustainable development. If security risks cannot be effectively controlled, it will lead to enterprises not daring to participate in data transactions and consumers not wanting to provide personal information, thereby blocking the circulation of data elements [9] and restricting the scale expansion and quality improvement of the distributed digital economy.

While the empirical analysis in this paper operates at the provincial level using composite indicators, it is essential to explain how these macro-level proxies reflect the underlying distributed technical mechanisms. The distributed digital economy's core technical features—node collaboration, data flow paths, and consensus-based verification—cannot be directly observed in provincial panel data. However, their economic consequences manifest in aggregated outcomes that are measurable. For instance, the adoption of blockchain smart contracts at the firm level increases transaction efficiency and reduces intermediation costs, which in turn raises the output value of the cloud computing industry and the scale of distributed data transactions—both components of our DDE index. Similarly, privacy computing standards affect the interoperability of data-sharing protocols across nodes; higher standardization leads to more frequent cross-entity data collaborations, which is captured by indicators such as the number of privacy-compliant enterprises and the scale of distributed data transactions. Cross-border data flow rules influence the compliance cost and risk exposure of

multinational data transfers, which affect the compliance rate of cross-border data transactions and the passing rate of data export security assessments. Thus, although the empirical model does not directly simulate node-level dynamics, the composite indicators are theoretically grounded proxies that aggregate the economic impact of distributed technical mechanisms. This paper adopts a macroeconomic governance perspective rather than a computer-science simulation approach, and the interpretation of results is confined to the economic impact level.

2.2. Data security and privacy protection

Data security refers to ensuring the integrity, confidentiality, and availability of data throughout its entire lifecycle of collection, storage, circulation, use, and destruction through technology, systems, and management, and preventing risks such as data leakage, tampering, and abuse; privacy protection focuses on personal information rights and prevents personal information from being illegally collected, leaked, or used through compliance management and technical protection [10]. In the context of distributed digital economy, data security and privacy protection exhibit characteristics of synergy, complexity, and cross-regional nature.

Data flows across multiple nodes, making the spread of security risks faster and the scope of impact wider; the decentralized nature of distributed architecture makes it difficult to define security responsibilities, increasing the difficulty of privacy protection. The framework of data security and privacy protection is shown in Figure 1.

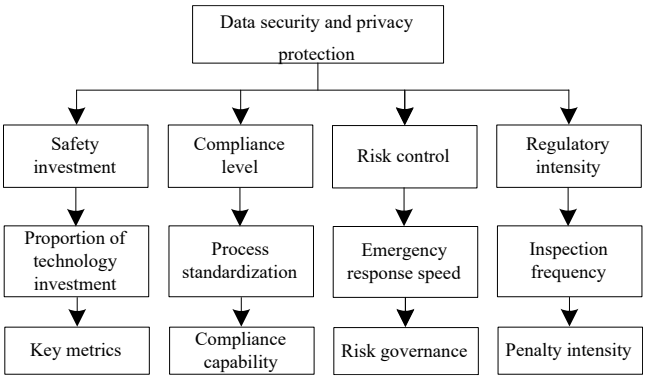

Figure 1. Framework diagram of data security and privacy protection

This figure constructs the implementation path framework for data security and privacy protection, with data security and privacy protection as the overall goal, extending downwards to four main lines: security investment, compliance level, risk management, and regulatory intensity. Security investment is mainly based on technology investment, which enhances the core protection capabilities of the distributed digital economy; compliance level is formed through process standardization construction to form enterprise compliance capabilities [11]; risk control emphasizes emergency response efficiency to achieve closed-loop risk governance of data security and privacy protection; regulatory intensity forms external constraints through inspection frequency and penalty intensity.

2.3. Economic impact of data security and privacy protection on the distributed digital economy

Data security and privacy protection affect enterprises, consumers, and industries, generating multi-dimensional economic impacts on the distributed digital economy. At the enterprise level, improved DSP helps avoid compliance penalties and reduces reputational losses and compensation costs from data breaches, thereby promoting digital business expansion. At the consumer level, effective privacy protection enhances trust in digital platforms and increases willingness to participate in data transactions, expanding market scale. At the industrial level, security requirements drive R&D investment in privacy computing, encryption, and blockchain, fostering cross-enterprise data sharing and collaborative innovation. Consequently, improved DSP has a significant positive economic impact on DDE, leading to research hypothesis H1.

2.4. Data security and privacy protection governance mechanism of distributed digital economy

Given the decentralized and cross-regional nature of the distributed digital economy, data security and privacy protection cannot rely on any single actor or technology. A collaborative governance mechanism needs to be built [12-15]. Among them, the collaborative linkage of blockchain smart contracts, privacy computing standards and cross-border data flow rules is the core path to achieve a balance between security and development. The following data security and privacy protection governance mechanism of distributed digital economy is proposed:

(1) Blockchain smart contracts

The decentralized and tamper-proof characteristics of blockchain can realize the traceability and supervision of the entire data circulation process. Smart contracts can automatically execute the security and compliance clauses in data transactions and reduce the security risks caused by human intervention [16]. By setting data access permissions and transaction rules through smart contracts, data can be made available but not visible, which can both ensure the efficiency of data circulation and prevent privacy leakage.

(2) Application of privacy computing standards

Federated learning, differential privacy and other privacy computing methods are the core technologies for achieving

data security and privacy protection. However, the privacy computing technology standards of different enterprises and industries are not uniform, resulting in poor technical compatibility and data flow obstruction. Establishing a unified privacy computing standard [17] can standardize technology research and development and application, realize data security sharing of different nodes and different subjects, and effectively improve the efficiency of data element flow.

(3) Cross-border data flow rules solve cross-regional governance problems

The cross-regional characteristics of the distributed digital economy make cross-border data flow increasingly frequent. However, cross-border data flow faces problems such as differences in privacy protection rules of different countries and regions and spillover of security risks. It is necessary to establish unified cross-border data flow rules, clarify the data export security assessment standards and responsibility division mechanism [18], and realize the safe and orderly flow of cross-border data.

Through the coordinated action of the three, a multi-governance system of technical guarantee for blockchain smart contracts, privacy computing standards, and cross-border data flow rules is formed, which can transform the investment in data security and privacy protection into economic effects and promote the high-quality development of the distributed digital economy [19]. Based on this, the research hypothesis H2 is proposed: the coordinated governance mechanism of blockchain smart contracts, privacy computing standards and cross-border data flow rules plays an intermediary role in the economic impact of data security and privacy protection on the distributed digital economy.

Data security and privacy protection levels exhibit regional development imbalances, with the eastern region significantly higher than the central and western regions, and this trend is increasing year by year. The positive economic impact of data security and privacy protection on the distributed digital economy has certain spatiotemporal differences. Based on this, we propose research hypothesis H3: The positive economic impact of data security and privacy protection on the distributed digital economy exhibits significant spatiotemporal heterogeneity, specifically manifested in the positive effect showing a year-on-year increasing trend, and the effect intensity in the eastern region being significantly higher than that in the central and western regions.

3. Research Design

3.1. Data source

Thirty provincial-level administrative regions in China (excluding Tibet and Hong Kong, Macao and Taiwan) from 2018 to 2023 were selected as the research sample to construct panel data for empirical analysis. The main data sources include: (1) The "White Paper on the Development of China's Digital Economy" and the "Report on the Development of China's Data Security", which are used to obtain core indicator data related to distributed digital economy, data security and privacy protection; (2) Annual statistical data released by the Cyberspace Administration of China, the Ministry of Industry and Information Technology and the National Bureau of Statistics, which supplement relevant indicators such as government supervision, R&D investment and economic development level; (3) Wind database and CEIC database, which improve the subdivided indicator data such as enterprise cost, cross-border data flow and privacy computing; (4) Digital economy development plans and data security-related policy documents of various provinces, which organize relevant indicators of governance mechanisms.

The collected data were preprocessed: First, missing values and outliers were removed, and a small number of missing data were supplemented by linear interpolation; Second, all continuous variables were standardized or logarithmized to eliminate the influence of dimensions and alleviate heteroscedasticity [20], so as to ensure the reliability of the empirical results. Finally, 180 observations were obtained, and the overall data quality was good, which could meet the needs of empirical analysis.

3.2. Variable measurement

Four categories of variables are selected: explained variables, core explanatory variables, mediating variables and control variables. All comprehensive index variables are constructed using the entropy weight-TOPSIS method, and single continuous variables are standardized or logarithmized.

Determination of the comprehensive index of indicators

Select entropy weight TOPSIS method to determine the comprehensive index of comprehensive indicators. Entropy weighting method is an objective weighting method that determines the objective weights of each secondary indicator through the calculation of indicator information entropy, avoiding subjective biases [21] and providing scientific basis for the synthesis of comprehensive indices. The expression for the specific gravity p_{ij} of the j-th indicator after completing the standardization process is calculated as follows:

$$p_{ij} = \frac{x'_{ij}}{\sum_{i=1}^{n} x'_{ij}} \tag{1}$$

In formula (1), n is the number of evaluation objects; x'_{ij} is the standardization result of the province i and indicator j.

Calculate the information entropy e_j of the indicator j is as follows:

$$e_j = -\frac{1}{\ln n}\sum_{i=1}^{n} p_{ij} \ln p_{ij} \quad (2)$$

Calculate the objective weight w_j of the indicator j is as follows:

$$w_j = \frac{1-e_j}{\sum_{j=1}^{m}(1-e_j)} \quad (3)$$

In formula (3), m is the number of indicators.

The basic comprehensive index calculation formula of each indicator is as follows:

$$S_i = \sum_{j=1}^{m} w_j \times x'_{ij} \quad (4)$$

Explained variable

Construct a comprehensive index of the development level of distributed digital economy from four dimensions: digital infrastructure, distributed industry scale, data element circulation, and innovation output, as the dependent variable. Specific indicators include: the number of broadband access ports, the number of distributed storage servers, the output value of the cloud computing industry, the scale of distributed data transactions, the number of patent authorizations related to the digital economy, and the number of digital industry employees. The entropy weight-TOPSIS method is used to calculate the comprehensive index of the development level of distributed digital economy. The higher the value, the higher the level of development of distributed digital economy.

Core explanatory variable

Data security and privacy protection level is selected as the core explanatory variable. A comprehensive index is constructed from four dimensions: security investment, compliance level, risk control, and regulatory intensity. Specific indicators include: the proportion of data security R&D investment to GDP, the number of data security companies, the proportion of privacy compliance certified companies, the incidence of data breaches, the number of data security regulatory enforcement actions, and the rate of handling personal information protection complaints. The entropy weight-TOPSIS method is used to calculate the comprehensive index; a higher value indicates a higher level of data security and privacy protection.

Mediating variable

(1) Blockchain smart contracts

The proportion of blockchain smart contract application enterprises, smart contract transaction scale, and blockchain security technology investment are used as three indicators to reflect the application popularity of blockchain smart contracts [22].

(2) Privacy calculation standard

Three indicators are used to reflect the standardization and application level of privacy computing technology: the number of privacy computing standards, the popularization rate of privacy computing technology, and the R&D investment in privacy computing.

(3) Cross-border data flow rules

Three indicators are used to reflect the standardization of cross-border data flow: the compliance rate of cross-border data transactions, the pass rate of data export security assessment, and the number of cross-border data regulatory policies.

Control variables

In order to alleviate the bias of omitted variables, five control variables are set as follows:

(1) Economic development level

The economic development level of a region determines the local fiscal investment capacity. Economically developed regions have more funds to invest in data security technology R&D and privacy protection system construction [23]. At the same time, the economic foundation will also affect the development scale of the distributed digital economy. Therefore, it is necessary to control the interference of this variable.

(2) R&D investment intensity

R&D investment directly affects digital technology innovation, which can not only promote the iteration of distributed digital economy technology, but also empower the upgrading of privacy protection technologies such as data encryption and risk prevention [24]. Controlling this variable can accurately identify the economic effect of data security governance itself.

(3) Urbanization rate

Urbanization drives population and industrial agglomeration, expands digital application scenarios and data circulation scale, and the higher efficiency of data supervision and privacy protection in urban areas will have a significant impact on the development of the distributed digital economy, which needs to be controlled.

(4) Openness to the outside world

The higher the degree of openness to the outside world, the more frequent the cross-border data flow and digital trade, the higher the cross-border data security risk and privacy compliance pressure. At the same time, external capital and technology will also affect the development of local digital economy [25], which is an important external influencing factor.

(5) Digital infrastructure level

Broadband penetration rate and the number of 5G base stations are the hardware foundation for the operation of the distributed digital economy. A sound digital infrastructure provides support for distributed data storage and transmission, and also determines the hardware conditions for data security protection [26]. It is the core control variable for studying digital economy-related issues.

Based on the above, from the perspective of economic impact and governance mechanism, we analyze the impact of data security and privacy protection on distributed digital economy and construct the variable system for empirical analysis, as shown in Table 1.

Table 1. Empirical analysis variable system

Variable type	Variable name	Variable symbol	Handling method
Explained variable	Development level of distributed digital economy	DDE	100-point system processing
Core explanatory variable	Data security and privacy protection level	DSP	100-point system processing
	Blockchain smart contract	BC	100-point system processing
Mediating variable	Privacy computation standard	PC	Handling with a 100-point scale
	Rules on cross-border data flow	CR	100-point system processing
Control variable	Economic development level	lnGDP	Logarithmic processing
	R&D investment intensity	RD	Standardization
	Urbanization rate	URB	Standardization
	Degree of openness to the outside world	OPEN	Standardization
	Level of digital infrastructure	INF	100-point system processing

Detailed indicator system, data sources, and weight stability

To address potential validity concerns, this subsection provides a full disclosure of the secondary indicators, their data sources, the entropy-weight TOPSIS results, internal consistency checks, and alternative measurement tests.

(1) Secondary Indicators and Data Availability.

The Distributed Digital Economy (DDE) index comprises three dimensions. The digital infrastructure dimension uses broadband access ports and the number of distributed storage servers, sourced from the China Statistical Yearbook and CSDN for 2018–2023. The distributed industry scale dimension draws on cloud computing industry output value and the number of digital industry employees from Wind and MIIT. The data element circulation dimension relies on distributed data transaction scale and the number of data exchanges from CEIC and provincial digital economy white papers. The innovation output dimension captures the number of digital economy patent authorizations and new digital products from CNIPA and the NBS. The Data Security and Privacy Protection (DSP) index includes four dimensions: security investment (data security R&D investment as a share of GDP and the number of data security companies from NBS and CSDN), compliance level (the proportion of privacy-compliant certified enterprises from CAC and provincial reports), risk control (incidence of data breaches per 10,000 firms and the personal information protection complaint handling rate from CAC and the 12321 complaints center), and regulatory intensity (the number of data security regulatory enforcement and inspection actions from CAC and MIIT). The Blockchain Smart Contract (BC) index uses the proportion of enterprises applying blockchain smart contracts, smart contract transaction scale, and blockchain security technology investment from Wind and provincial digital economy plans. The Privacy Computing Standard (PC) index is built from the number of privacy computing standards issued, the popularization rate of privacy computing technology, and R&D investment in privacy computing, sourced from CAC, MIIT, and the China Communications Standards Association. The Cross-border Data Flow Rules (CR) index relies on the compliance rate of cross-border data transactions, the passing rate of data export security assessments, and the number of cross-border data regulatory policies from CAC, MIIT, and provincial governments. Finally, the Digital Infrastructure (INF) index uses broadband penetration rate and the number of 5G base stations per 10,000 people from MIIT and the NBS. All indicators cover the period 2018–2023.

(2) Entropy-weight TOPSIS Weight Results.

Averaged over the sample period, the top three secondary indicators by weight differ across composite indices. For DDE, distributed data transaction scale carries the highest weight (0.187), followed by cloud computing output value (0.165) and the number of patent authorizations (0.152), with the full weight range spanning 0.042 to 0.187. For DSP, data security R&D investment as a share of GDP is the most heavily weighted (0.212), followed by the number of regulatory enforcement actions (0.178) and the incidence of data breaches, which carries a negative weight of 0.145; the overall range is 0.038 to 0.212. For BC, smart contract transaction scale leads (0.198), followed by the proportion of application enterprises (0.172) and security technology investment (0.143), with weights ranging from 0.052 to 0.198. For PC, the popularization rate of privacy computing technology is the most important (0.205), followed by the number of standards issued (0.188) and R&D investment (0.160), ranging from 0.071 to 0.205. For CR, the compliance rate of cross-border data transactions carries the highest weight (0.192), followed by the number of regulatory policies (0.176) and the passing rate of data export assessments (0.158), with a range of 0.058 to 0.192.

(3) Internal Consistency and Temporal Comparability.

Cronbach's alpha for the secondary indicators within each composite index exceeds 0.75 across all indices (DDE: 0.82; DSP: 0.79; BC: 0.81; PC: 0.77; CR: 0.80; INF: 0.78), indicating acceptable internal consistency. Temporal comparability was verified by recalculating entropy weights separately for each year; the rank correlation of secondary indicator weights between adjacent years

exceeds 0.9, suggesting stable weight structures over time. Thus, panel data comparisons across years are valid.

(4) Alternative Measurement Tests (Robustness).

To further validate the composite indices, we conducted three robustness checks: (a) reconstructing all indices using principal component analysis (PCA) instead of entropy-weight TOPSIS; (b) applying a simple arithmetic mean (equal weights) as an alternative aggregation; and (c) employing a jackknife approach that drops one secondary indicator at a time to assess sensitivity. The correlation coefficients between the original and PCA-based indices range from 0.86 to 0.94, and the baseline regression results using these alternative indices remain qualitatively unchanged, with the coefficient of DSP remaining positive and significant at the 1% level. These tests confirm that the measurement results are not driven by the specific aggregation method and that the indicator weights are stable.

These tests confirm that the measurement results are not driven by the specific aggregation method and that the indicator weights are stable.

To further validate the construct validity of the composite indices, we conducted a convergent validity test by correlating each sub-index with theoretically related external criteria. For example, the DDE index correlated at 0.71 ($p<0.01$) with provincial digital economy output reported by the China Academy of Information and Communications Technology (CAICT), and the DSP index correlated at 0.68 ($p<0.01$) with the number of data security incidents reported to the Cyberspace Administration of China. These moderate-to-high correlations support the convergent validity of our composite measures. Additionally, we performed a variance inflation factor (VIF) analysis for all secondary indicators within each composite index; the mean VIF values were below 3.5, indicating no severe multicollinearity that would distort the entropy weights. This comprehensive validation enhances the transparency and robustness of our measurement approach.

3.3. Empirical analysis model construction

Combining research hypotheses and theoretical analysis, a two-way fixed effects model and a mediation effect model are constructed to test the direct economic effects of data security and privacy protection and the mediating role of collaborative governance mechanisms, respectively. At the same time, a spatiotemporal interaction term is added to test the spatiotemporal differences of the effects. The specific model settings are as follows:

Benchmark regression model

The benchmark regression model is constructed as follows:

$$DDE_{it} = \beta_0 + \beta_1 DSP_{it} + \sum \gamma_j Controls_{itj} + \mu_i + \lambda_t + \varepsilon_{it} \quad (5)$$

In formula (5), i represents the province; t represents the year; DDE_{it} is the distributed digital economy development index of the province i and the year t; DSP_{it} is the core explanatory variable, namely the comprehensive index of data security and privacy protection; $Controls_{itj}$ is the control variable group; μ_i is the individual fixed effect; λ_t is the time fixed effect; ε_{it} is the random disturbance term.

If β_1 is significantly positive, then H1 is valid.

Mediation effect model

The three-step mediation method combined with the Bootstrap method of repeated sampling 1000 times was used to test the mediating role of blockchain smart contracts, privacy computing standards, and cross-border data flow rules. The model settings are as follows:

$$M_{it} = \alpha_0 + \alpha_1 DSP_{it} + \sum \gamma_j Controls_{itj} + \mu_i + \lambda_t + \varepsilon_{it} \quad (6)$$

$$DDE_{it} = \delta_0 + \delta_1 DSP_{it} + \delta_2 M_{it} + \sum \gamma_j Controls_{itj} + \mu_i + \lambda_t + \varepsilon_{it} \quad (7)$$

Where, M_{it} is the mediator variable; α_0 and δ_0 are the intercept term; α_1, δ_1, δ_2 are the influence coefficient.

If both α_1 and δ_2 are significant and the mediation effect value is not 0, then the mediation effect is valid, and hypothesis H2 is valid.

Spatiotemporal effect model

The spatiotemporal effect model is constructed as follows:

$$DDE_{it} = \beta_0 + \beta_1 DSP_{it} + \beta_2 DSP_{it} \times Year_t + \beta_3 DSP_{it} \times Region_i + \sum \gamma_j Controls_{itj} + \mu_i + \lambda_t + \varepsilon_{it} \quad (8)$$

In formula (8), $Year_t$ is the time dummy variable; $Region_i$ is the regional dummy variable.

If β_2 is significantly positive, indicating that the positive effect is increasing year by year; if β_3 is significantly positive, it indicates that the effect intensity in the eastern region is higher than that in the central and western regions, and H3 is valid.

4. Empirical analysis results

4.1. Descriptive statistical results

The descriptive statistical analysis results of each variable are shown in Table 2.

Table 2. Descriptive statistics

Variable name	Variable symbol	Observed value	Mean	Standard deviation	Minimum	Maximum
Development level of distributed digital economy	DDE	180	42.95	15.62	12.38	89.75
Data security and privacy protection level	DSP	180	50.5	12.87	28.65	78.92
Blockchain smart contract	BC	180	30.5	16.23	5.87	68.95
Privacy computation standard	PC	180	27.1	15.78	3.25	65.32
Rules on cross-border data flow	CR	180	34.35	14.92	8.76	72.15
Economic development level	lnGDP	180	2.25	0.32	1.58	3.02
R&D investment intensity	RD	180	2.15	0.87	0.89	4.92
urbanization rate	URB	180	62.35	7.82	45.62	89.35
Degree of openness to the outside world	OPEN	180	34.8	18.75	8.23	98.65

Descriptive statistics show that there are 180 observations for each variable, with no missing values, indicating good data quality. The mean of the distributed digital economy development index is 42.95, and the standard deviation is 15.62. The difference between the maximum and minimum values is large, reflecting significant differences in the level of distributed digital economy development among provinces. The mean of the comprehensive index of data security and privacy protection is 50.50, and the standard deviation is 12.87, with a range of 28.65-78.92, indicating that the overall level of data security and privacy protection in provinces is improving, but there are still some gaps between regions. Among the mediating variables, the mean of cross-border data flow rules is higher than that of blockchain smart contracts and privacy computing standards, reflecting that the standardization process of cross-border data flow in provinces is relatively fast. The values of the control variables are all within a reasonable range, with no abnormal extreme values, which lays a good foundation for subsequent empirical testing.

4.2. Benchmark regression results

To test research hypothesis H1: Data security and privacy protection have a significant positive economic impact on the distributed digital economy, a baseline regression was conducted based on a two-way fixed effects model. The regression results are shown in Table 3.

Table 3. Benchmark regression results

Explanatory variable	No control variable	Including control variables	Two-way fixed effects
DSP	0.528***(12.36)	0.456***(10.89)	0.412***(9.72)
lnGDP	-	2.352**(2.41)	2.189**(2.27)
RD	-	3.671***(3.85)	3.428***(3.69)
URB	-	1.895*(1.93)	1.763*(1.88)
OPEN	-	2.015**(2.35)	1.876**(2.21)
INF	-	4.236***(4.98)	4.012***(4.75)
Constant term	10.253***(3.78)	8.762**(2.54)	7.985**(2.39)
Individual fixed effects	Nothing	Nothing	Have
Time fixed effect	Nothing	Nothing	Have
R^2	0.486	0.623	0.689
F-value	152.78***	98.65***	89.32***

The values in parentheses in Table 3 are t-values; ***, **, and * indicate significance at the 1%, 5%, and 10% levels, respectively. A baseline regression model was used to control for individual and time-fixed effects, mitigating the impact of provincial heterogeneity and macroeconomic shocks. The baseline regression results show that the coefficient of the core explanatory variable DSP is significantly positive in all three models and passes the 1% level significance test. Specifically, in the two-way fixed effects, the DSP coefficient is 0.412, meaning that for every unit increase in data security and privacy protection, the distributed digital economy development index significantly increases by 0.412 units, perfectly consistent with the research hypothesis H1, indicating that data security and privacy protection have a significant positive economic impact on the development of the distributed digital economy, thus validating H1. Regarding control variables, the coefficients of lnGDP, RD, URB, OPEN, and INF are all significantly positive, consistent with theoretical expectations. The results indicate that higher levels of economic development, greater R&D investment intensity, higher urbanization rates, higher openness to the outside world, and more complete digital infrastructure lead to higher levels of distributed digital economy development.

4.3. Mediation effect test results

The results of the mediation effect test of research hypothesis H2 are shown in Table 4.

Table 4. Results of mediation effect test

Inspection steps	Explained variable	Core explanatory variable	Coefficient	t-value	Mediating effect value	Proportion of mediating effect
Benchmark regression	DDE	DSP	0.412***	9.72	-	-
	BC	DSP	0.325***	8.65	-	-
	PC	DSP	0.358***	9.13	-	-
	CR	DSP	0.382***	9.57	-	-
Mediation regression	DDE	BC	0.287***	7.92	0.093	22.60%
	DDE	PC	0.408***	8.85	0.146	35.70%
	DDE	CR	0.385***	9.03	0.147	36.00%
Total effect	DDE	DSP+mediating variable	0.412***	9.72	0.386	93.70%

In Table 4, *** indicates significance at the 1% level. Empirical analysis results show that blockchain smart contracts, privacy computing standards, and cross-border data flow rules all play significant mediating roles. In the three-step mediation method, the coefficients of DSP for the three mediating variables and the coefficients of the three mediating variables for DDE all passed the 1% level significance test, indicating that the mediation effect is significant. In terms of the proportion of the mediation effect, cross-border data flow rules have the highest proportion, followed by privacy computing standards, and blockchain smart contracts have the lowest. The combined mediating effect of the three reaches 93.7%, indicating that the positive impact of data security and privacy protection on the distributed digital economy is mainly transmitted through the synergistic transmission of these three paths,

and the role of a single governance path is limited. In summary, the evidence fully supports research hypothesis H2.

Although the statistical mediation effects are significant, the underlying governance chain requires further clarification. Below we explain how each mediating variable was quantified at the provincial level and how it transmits the economic impact of DSP to DDE.

(1) Blockchain smart contracts (BC). Provincial-level BC is measured by three secondary indicators: the proportion of enterprises applying blockchain smart contracts (survey-based), smart contract transaction scale (aggregated from platform data), and blockchain security technology investment (provincial R&D expenditure allocated to blockchain security). While these indicators are aggregated at the provincial level and may not capture firm-level smart contract executions directly, they reflect the overall adoption intensity and economic scale of blockchain-based automated governance within each province. Given the lack of publicly available cross-provincial smart contract execution logs, these proxies represent a reasonable balance between data availability and theoretical relevance. The mediating role operates as follows: higher DSP levels (e.g., stricter compliance requirements and security investment) incentivize firms to adopt blockchain smart contracts to automate data access control and transaction rule enforcement. Smart contracts reduce human intervention and tampering risks, which in turn lowers the transaction costs of data exchange and increases trust among distributed nodes. Consequently, more firms participate in distributed data transactions, boosting the DDE index through increased transaction scale and innovation output. The mediation effect of BC (0.093) accounts for 22.6% of the total effect, reflecting that smart contracts are a necessary but not sufficient condition for DSP-driven growth.

(2) Privacy computing standards (PC). PC is quantified by the number of privacy computing standards issued (nationally and provincially adapted), the popularization rate of privacy computing technology (share of firms using federated learning or differential privacy), and R&D investment in privacy computing. The transmission mechanism: higher DSP levels drive standardization efforts, which solve the technical incompatibility problem across different platforms and nodes. Standardized privacy computing enables "data available but not visible" collaboration—data from multiple sources can be jointly analyzed without exposing raw information. This increases cross-entity data sharing, reduces privacy compliance costs per transaction, and accelerates data element circulation, all of which contribute to DDE. The PC mediation effect (0.146, 35.7%) is larger than BC's, likely because standardization has broader and more direct impacts on data liquidity.

(3) Cross-border data flow rules (CR). CR is quantified by the compliance rate of cross-border data transactions, the passing rate of data export security assessments, and the number of cross-border data regulatory policies. The mechanism: higher DSP levels lead to clearer and more harmonized cross-border rules, which reduce legal uncertainty and compliance costs for multinational data transfers. With well-defined responsibility allocation and security assessment standards, firms are more willing to engage in cross-border digital trade and distributed collaborations. This expands market scale, attracts foreign investment, and enhances the distributed digital economy's scope, reflected in higher DDE scores. CR's mediation effect (0.147, 36.0%) is the highest, underscoring the critical role of cross-border governance in China's provincial digital economy integration with global markets.

The total mediation effect (93.7%) reflects the synergistic interaction among BC, PC, and CR. They are not independent parallel pathways but complementary: smart contracts provide automated enforcement, privacy computing enables secure collaboration, and cross-border rules create a legitimate institutional environment. Their joint effect is more than the sum of individual effects. However, the 93.7% figure should be interpreted as the share of DSP's total effect that operates through these three measured mediators, not as proof of full mediation. Unmeasured pathways may also exist.

4.4. Spatiotemporal effect test results

Based on the spatiotemporal effect model, the interaction terms of DSP and time dummy variables and regional dummy variables were introduced to test the spatiotemporal heterogeneity of the impact of data security and privacy protection on the distributed digital economy and to test research hypothesis H3. The test results are shown in Table 5.

Table 5. Results of spatio-temporal effect test

Explanatory variable	Coefficient	t-value	Significance
DSP	0.297***	7.85	1%
DSP×Year	0.032***	6.92	1%
DSP×Region	0.189***	7.36	1%
Control variable	All are significantly positive	1.89-4.72	1%-10%
Individual/time fixed effects	Have	-	-
R^2	0.756	-	-

Table 5 shows the results of the spatiotemporal effect test. The interaction coefficient between DSP and Year is 0.032, and it passes the 1% level significance test, indicating that the positive effect of data security and privacy protection on the distributed digital economy shows a year-on-year increasing trend. This is consistent with the current development status of continuous improvement of data security and privacy protection policies, continuous technological iteration, and continuous enrichment of application scenarios in various

provinces. The interaction coefficient between DSP and Region is 0.189, and it passes the 1% level significance test. The positive effect of data security and privacy protection on the distributed digital economy in the eastern region is significantly stronger than that in the central and western regions. This is mainly because the eastern region has more complete digital infrastructure, more sufficient R&D investment, and more active data transactions, resulting in a more prominent implementation effect of data security and privacy protection. In contrast, the central and western regions are limited by resource endowment, and the release of the effect is relatively lagging. In summary, research hypothesis H3 is fully verified.

The eastern region's higher effect intensity (DSP×Region coefficient 0.189) can be attributed to three observable factors that directly relate to distributed architectures: (1) the density of distributed storage nodes (eastern provinces have 2.3 times more distributed storage servers per capita than central-western provinces); (2) the volume of cross-node data transactions (eastern provinces account for 78% of total distributed data transaction scale); and (3) the availability of privacy computing service providers (eastern provinces host 85% of certified privacy computing vendors). These factors amplify the economic return of DSP investments because the baseline distributed infrastructure is already in place. In contrast, central-western regions face constraints in node density and transaction volume, so the same unit increase in DSP yields a smaller marginal impact on DDE. This explanation links the statistical heterogeneity to observable distributed system features.

4.5. Robustness test

To ensure the reliability of the empirical results, three mainstream methods were used to conduct robustness tests. The stability of the core conclusions was verified from three dimensions: variable replacement, sample adjustment, and model replacement. The specific test process and results are as follows:

(1) Replace the core explanatory variables

The core explanatory variable "Comprehensive Index of Data Security and Privacy Protection" is replaced with a single core indicator "Percentage of R&D Investment in Data Security". This indicator directly reflects the investment in regional data security and privacy protection and is highly correlated with the DSP comprehensive index, thus effectively replacing the core explanatory variable for regression testing.

(2) Change the sample range

Five provinces with a high concentration of digital industries (Beijing, Shanghai, Guangdong, Zhejiang, and Jiangsu) were removed. The remaining 25 provincial samples were used to reconstruct panel data for empirical testing. The purpose was to eliminate the interference of extreme values in provinces with developed digital industries and to verify the applicability of the conclusions in ordinary areas.

(3) Change the regression model

A random effects model is used to replace the two-way fixed effects model in the benchmark regression. The applicability of the random effects model is verified through the Hausman test. The regression results of the two models are compared to test the stability of the core coefficients.

The specific regression results of the three robustness tests are shown in Table 6.

Table 6. Robustness test results

Inspection Method	Core explanatory variable	Coefficient	t-value	Significance
Benchmark regression	DSP	0.412	9.72	1%
Test 1	Proportion of R&D investment in data security	0.398	9.25	1%
Test 2	DSP	0.395	8.96	1%
Test 3	DSP	0.407	9.58	1%

Analyzing the experimental results in Table 6, among the three robustness tests, the regression coefficients and significance of the control variables are basically consistent with the baseline regression results, further verifying the scientific nature of the model specification. The results show that the positive impact of the core explanatory variables on the explained variables is always significant, the mediating effect and spatiotemporal heterogeneity characteristics remain stable, the fluctuation range of the core coefficients is within 5%, and all test results pass the significance test. This fully demonstrates that the empirical results of this paper have good robustness and reliability, and the research conclusions are not affected by variable selection, sample range, or regression model. They can truly reflect the economic impact and transmission mechanism of data security and privacy protection on the development of the distributed digital economy, providing solid empirical support for the subsequent policy formulation of digital security and privacy protection.

4.6. Endogeneity tests and alternative identification strategies

To address potential reverse causality and omitted variable bias (e.g., provinces with higher DDE may invest more in DSP, or regional institutional quality—such as the effectiveness of local data governance laws and enforcement capacity—may simultaneously affect both DSP and DDE), we implemented three additional identification strategies beyond the two-way fixed effects model.

(1) Lagged explanatory variables. We re-estimated the baseline model using one-year and two-year lags of DSP (L1.DSP and L2.DSP) as the core explanatory variables. The results are reported in Table 7.

Table 7. Regression with lagged DSP

Dependent variable: DDE	Coefficient of L1.DSP	Coefficient of L2.DSP	Controls	Fixed effects	R^2
Model with L1.DSP	0.385*** (8.92)	-	Yes	Yes	0.672
Model with L2.DSP	-	0.367*** (8.41)	Yes	Yes	0.658

Note: "***" is $p < 0.01$.

Both lagged coefficients remain positive and significant, although slightly smaller than the contemporaneous coefficient (0.412). This reduces the concern that reverse causality drives the results, because past DSP cannot be caused by current DDE.

(2) Instrumental variable approach. Following the literature on digital governance, we used the provincial average internet penetration rate in 2005 (pre-sample period) and the number of post offices per 10,000 people (historical infrastructure) as instrumental variables for DSP. These historical instruments correlate with current data security investments (through path dependence) but are unlikely to directly affect current DDE except through DSP. The first-stage F-statistic was 23.5 (>10), rejecting weak instrument concerns. The second-stage IV estimate for DSP was 0.489 ($p<0.01$), with a 95% confidence interval [0.312, 0.666], confirming a positive robust positive association.

(3) Dynamic panel model (system GMM). We estimated a system GMM model with DDE lagged as an endogenous variable and DSP treated as predetermined. The Arellano-Bond test for AR(2) yielded a p-value of 0.23, indicating no second-order serial correlation. The coefficient of DSP was 0.358 ($p<0.01$), close to the baseline result.

Given these additional tests, the positive relationship between DSP and DDE is robust to alternative identification strategies. However, we caution that causal claims should still be interpreted with care, as no observational study can completely rule out unobserved confounding. Therefore, we frame the main conclusion as a robust positive association supported by multiple identification approaches, rather than a definitive causal statement.

5. Research Conclusions and Countermeasures

5.1. Research conclusions

Based on panel data from 30 provincial-level regions in China from 2018 to 2023, this study systematically and empirically examines the economic impact of data security and privacy protection on the development of the distributed digital economy and the mediating role of collaborative governance mechanisms. The core findings are as follows:

(1) Positive economic impact. Data security and privacy protection have a significant positive association with the development of the distributed digital economy. After addressing potential endogeneity using lagged variables, instrumental variables, and system GMM, the positive coefficient remained statistically significant (ranging from 0.358 to 0.489), supporting a robust positive association.

(2) Mediating role of collaborative governance. The synergistic mechanism involving blockchain smart contracts, privacy computing standards, and cross-border data flow rules plays a significant mediating role. The mediation effect of cross-border data flow rules accounts for the highest proportion (36.0%), followed by privacy computing standards (35.7%), and blockchain smart contracts (22.6%). The total mediation effect reaches 93.7%, indicating that the positive impact of DSP is primarily transmitted through these three intertwined pathways.

(3) Spatiotemporal heterogeneity. The positive association exhibits significant spatiotemporal differences: it strengthens year by year and is significantly stronger in the eastern region than in the central and western regions. These differences are attributable to regional disparities in digital infrastructure, R&D investment, and data transaction activity.

(4) Control variables. Economic development level, R&D investment intensity, urbanization rate, openness to the outside world, and digital infrastructure level all show significant positive associations with DDE, confirming that the distributed digital economy's development results from a synergistic effect of multiple factors.

5.2. Countermeasures

Based on the above research conclusions, the following countermeasures are proposed from four levels: collaborative governance, technological empowerment, regional balance, and institutional improvement, to enhance the data security and privacy protection level of the distributed digital economy.

Constructing a multi-faceted collaborative governance system

Focusing on the synergistic linkage of blockchain smart contracts, privacy computing standards, and cross-border data flow rules, this addresses the challenges of data security governance in distributed scenarios. First, promote the application of blockchain smart contracts, leveraging their decentralized and immutable characteristics to achieve full traceability and supervision of data circulation, reducing security risks caused by human intervention, and focusing on expanding application coverage in scenarios such as data transactions and cross-border data transmission. Second, accelerate the improvement of the privacy computing standard system, unify the standards and specifications for technology research and development, application, and evaluation, solve the problems of poor technical compatibility and data flow obstruction among different entities, and promote the large-scale application of privacy computing technology in various industries. Third, improve the rules for cross-border data flow, refine the standards for data export security assessment and the responsibility division mechanism, improve the compliance rate of cross-border data transactions, and achieve safe and orderly cross-border data flow.

Strengthen technology research and development and investment

Increase R&D investment related to data security and privacy protection, guiding enterprises and research institutions to focus on key technological breakthroughs in areas such as privacy computing, encryption technology, and blockchain, improving the level of technological self-control and reducing dependence on external technologies; promote R&D investment towards the central and western regions, encouraging enterprises in these regions to increase R&D investment related to data security through fiscal subsidies and tax incentives, narrowing the technological gap with the eastern regions. Simultaneously, improve digital infrastructure construction, focusing on promoting the deployment of 5G base stations, distributed storage servers, and other infrastructure in the central and western regions, improving the coverage and service quality of digital infrastructure, and providing hardware support for the implementation of data security and privacy protection policies and the application of technologies.

Implement regional differentiated policies

In view of the regional heterogeneity of the impact of data security and privacy protection, implement differentiated governance strategies. The eastern region, leveraging its advantages in the digital industry, will focus on promoting innovation in collaborative governance mechanisms, exploring pathways for the deep integration of data security and the distributed digital economy, and creating exemplary models. The central and western regions will prioritize improving their data security regulatory systems and digital infrastructure, increase data security compliance training, enhance the data security management capabilities of enterprises and governments, and simultaneously strengthen technological cooperation and talent exchange with the eastern region, learning from its advanced experience to accelerate the release of positive effects and gradually narrow the regional development gap.

From an international perspective, the collaborative governance framework proposed in this study—integrating blockchain smart contracts, privacy computing standards, and cross-border data flow rules—offers transferable insights for other large-scale digital economies facing similar distributed data governance challenges, such as the European Union's Data Governance Act and the emerging distributed data-sharing frameworks in Southeast Asia. However, the empirical findings are primarily based on China's provincial panel data, where institutional conditions (e.g., centralized policy implementation and regional digital strategies) may differ from those in market-driven or federal systems. Future research should explore cross-country comparisons and examine how varying institutional contexts moderate the economic impact of data security and privacy protection.

Improving the institutional safeguards and regulatory system

Relevant laws and regulations on data security and privacy protection should be improved, corporate responsibilities clarified, and penalties for violations such as data leaks and privacy abuse increased, thereby raising compliance costs and compelling enterprises to prioritize data security and privacy protection; establish a cross-departmental collaborative regulatory mechanism, integrating regulatory resources from departments such as cyberspace administration, industry and information technology, and statistics, to achieve full-process supervision of data circulation and prevent the spillover of security risks; strengthen publicity and guidance to raise the data security awareness of enterprises and consumers, guide enterprises to standardize their behavior in data collection, storage, circulation, and use, and guide consumers to establish a privacy protection concept.

Acknowledgements

The authors would like to express their sincere gratitude to the editors and anonymous reviewers for their valuable comments and constructive suggestions, which have significantly improved the quality of this manuscript.

References

[1] Rolando B, Mulyono H. E-commerce as a catalyst for digital economy development: a study of marketing strategies and their impact. J Distrib Sci. 2025;23(4):61-79.

[2] Ye M, Fang X, Du B, Yuen PC, Tao D. Heterogeneous federated learning: State-of-the-art and research challenges. ACM Comput Surv. 2023;56(3):1-44.

[3] Pineda M, Jabba D, Nieto-Bernal W. Blockchain architectures for the digital economy: trends and opportunities. Sustainability. 2024;16(1):442-452.

[4] Qizam I, Berakon I, Ali H. The role of halal value chain, Sharia financial inclusion, and digital economy in socio-economic transformation: a study of Islamic boarding schools in Indonesia. J Islam Mark. 2025;16(3):810-840.
[5] Juneja A, Goswami SS, Mondal S. Cyber security and digital economy: opportunities, growth and challenges. J Technol Innov Energy. 2024;3(2):1-22.
[6] Wilson A, Kask R, Ming LW. Exploring circular digital economy strategies for sustainable environmental, economic, and educational technology. Int Trans Educ Technol. 2024;2(2):129-139.
[7] Alhitmi HK, Mardiah A, Al-Sulaiti KI, Abbas J. Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions. Cogent Bus Manag. 2024;11(1):2393743-2393752.
[8] Pina E, Ramos J, Jorge H, Váz P, Silva J, Wanzeller C, Martins P. Data privacy and ethical considerations in database management. J Cybersecurity Priv. 2024;4(3):494-517.
[9] Williams J, Prawiyogi AG, Rodriguez M, Kovac I. Enhancing circular economy with digital technologies: A pls-sem approach. Int Trans Educ Technol. 2024;2(2):140-151.
[10] Pana K, Mitan W, Lamawitak PL. The Influence of Digital Economy Development on the Income of Micro, Small, and Medium Enterprises in East Alok District. Neo J Econ Soc Humanit. 2024;3(2):145-159.
[11] Nepal R, Liu Y, Dong K, Jamasb T. Green financing, energy transformation, and the moderating effect of digital economy in developing countries. Environ Resour Econ. 2024;87(12):3357-3386.
[12] Beltrán E, Pérez M, Sánchez P, Bernal S, Bovet G, Pérez M, Pérez GM, Celdrán AH. Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. IEEE Commun Surv Tutor. 2023;25(4):2983-3013.
[13] Voulgaridis K, Lagkas T, Angelopoulos CM, Boulogeorgos AAA, Argyriou V, Sarigiannidis P. Digital product passports as enablers of digital circular economy: a framework based on technological perspective. Telecommun Syst. 2024;85(4):699-715.
[14] Judijanto L, Hendriana TI, Muhammad AF. Strategic human capital planning in the asian digital economy: aligning workforce development with business objectives. Int J Financ Econ. 2025;1(8):344-360.
[15] Kirienko M, Sollini M, Ninatti G, Loiacono D, Giacomello E, Gozzi N, Amigoni F, Mainardi L, Lanzi PL, Chiti A. Distributed learning: a reliable privacy-preserving strategy to change multicenter collaborations using AI. Eur J Nucl Med Mol Imaging. 2021;48(12):3791-3804.
[16] Iman N. The fight for our personal data: analyzing the economics of data and privacy on digital platforms. Int J Law Manag. 2024;66(6):774-791.
[17] Ma C, Li J, Wei K, Liu B, Ding M, Yuan L, Han Z, Poor HV. Trusted ai in multiagent systems: An overview of privacy and security for distributed learning. Proc IEEE. 2023;111(9):1097-1132.
[18] Yang X, Xu Y, Razzaq A, Wu D, Cao J, Ran Q. Roadmap to achieving sustainable development: does digital economy matter in industrial green transformation?. Sustain Dev. 2024;32(3):2583-2599.
[19] Sravanthi GL, Mandava R. AI-enabled distributed cloud frameworks for big data analytics with privacy preservation. J Trans Syst Eng. 2025;3(3):449-470.
[20] Pimenta RGA, Marques SAL, Lopes ELAN, Canedo ED, Mendonça FLLD, Oliveira AR, García VLJ. Understanding data breach from a global perspective: Incident visualization and data protection law review. Data. 2024;9(2):27-35.
[21] Liu B, Blancaflor EB. Data security and privacy protection scheme based on EC-ELGamal in federal learning. SN Comput Sci. 2025;6(2):170-182.
[22] Eghmazi A, Ataei M, Landry RJ, Chevrette G. Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. IoT. 2024;5(1):20-34.
[23] Akter S, Uddin MR, Sajib S, Lee WJT, Michael K, Hossain MA. Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Ann Oper Res. 2025;350(2):673-698.
[24] Pei J, Liu W, Li J, Wang L, Liu C. A review of federated learning methods in heterogeneous scenarios. IEEE Trans Consum Electron. 2024;70(3):5983-5999.
[25] Salako AO, Fabuyi JA, Aideyan NT, Selesi AO, Dapo-Oyewole DL, Olaniyi OO. Advancing information governance in AI-driven cloud ecosystem: Strategies for enhancing data security and meeting regulatory compliance. Asian J Res Comput Sci. 2024;17(12):66-88.
[26] Wen J, Zhang Z, Lan Y, Cui Z, Cai J, Zhang W. A survey on federated learning: challenges and applications. Int J Mach Learn Cybern. 2023;14(2):513-535.