

Article

Configuration Analysis and Path Optimization of Digital Economic Empowerment for the New Energy Vehicle Industry Chain Security

Chagen Luo ^{1,2} , Deyang Kong ^{1,*} and Jinsuo Zhou ¹ ¹ College of Automotive and Energy Engineering, Tongji University, Shanghai 201804, China; lcg2618@tongji.edu.cn (C.L.)² College of Mechanical & Electronic Engineering, Shanghai Jian Qiao University, Shanghai 201306, China

* Correspondence: kongdeyang@tongji.edu.cn

Highlights

- AI capability is necessary for supply chain resilience (effect size = 0.42).
- Four equivalent configurations support high NEV industry chain security.
- Big data analytics capability is essential for cybersecurity (effect size = 0.38).
- No single digital economy factor alone ensures comprehensive industry chain security.
- Random forest and SHAP analyses confirm AI capability has the highest global importance.

Abstract

The security of new energy vehicle (NEV) industry chains has become a strategic issue for industrial competitiveness, the energy transition, and economic security. This study examines how digital economy capabilities jointly support NEV industry chain security across 30 provincial-level administrative regions in China. Drawing on Organizational Information Processing Theory and Dynamic Capability Theory, we conceptualize artificial intelligence capability (AIC), big data analytics capability (BDA), cloud computing infrastructure (CCI), and blockchain application level (BCL) as complementary information-processing and reconfiguration capabilities. We combine Necessary Condition Analysis (NCA), fuzzy-set Qualitative Comparative Analysis (fsQCA), and Random Forest/SHAP analysis. The revised results show that AIC is a practically necessary condition for supply chain resilience, BDA is a necessary condition for achieving a high cybersecurity level, and BCL is a dimension-specific necessary condition for data security. Four sufficient configurational paths—technology-driven, data-driven, infrastructure-driven, and security-synergistic—lead to high comprehensive NEV industry chain security. Robustness checks using alternative calibration anchors and consistency thresholds show that the core configurations are stable. A revised machine learning specification using only digital economy predictors confirms the high relative importance of AIC. It also shows that the marginal contribution of AIC tends to flatten beyond the upper-middle range. The findings provide a configurational and regionally differentiated perspective on digital economy empowerment while avoiding overgeneralization beyond the Chinese provincial context.



Academic Editor: Joeri Van Mierlo

Received: 8 May 2026

Revised: 5 June 2026

Accepted: 18 June 2026

Published: 3 July 2026

Copyright: © 2026 by the authors.

Published by MDPI on behalf of the World Electric Vehicle Association.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)[Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.**Keywords:** digital economy; new energy vehicles; industry chain security; fsQCA; configurational analysis; supply chain resilience

1. Introduction

The global automotive industry is undergoing a profound transformation driven by electrification, intelligence, and connectivity. New energy vehicles (NEVs), as a strategic emerging industry, have become a critical battleground for major economies seeking to achieve carbon neutrality and energy security objectives [1]. China, as the world's largest NEV market, produced over 16.626 million NEVs in 2025, accounting for approximately 70% of global production [2]. In the European Union, electric car sales increased by 30% in 2025. However, the rapid expansion of the NEV industry chain has exposed significant security vulnerabilities across multiple dimensions, including supply chain disruptions, cybersecurity threats, and data privacy risks. The COVID-19 pandemic, geopolitical tensions, and trade frictions have further highlighted the fragility of global supply chains, making industry chain security a paramount concern for policymakers and industry stakeholders alike [3].

The digital economy, characterized by the pervasive integration of digital technologies into economic activities, has emerged as a powerful enabler of industrial transformation and risk management [4]. Digital technologies such as artificial intelligence (AI), big data analytics, cloud computing, and blockchain offer unprecedented capabilities for enhancing supply chain visibility, predictive analytics, and collaborative governance [5]. In the context of NEV industry chains, these digital economy factors can potentially address security challenges by improving supplier risk assessment, enabling real-time monitoring of production and logistics, strengthening cybersecurity defenses, and ensuring data integrity through distributed ledger technologies. Moreover, the security of the NEV industry chain is also closely related to the reliability of key technological and energy-support systems. For instance, research on GA-based PI control for improved direct torque control of doubly fed induction machines shows that intelligent optimization algorithms can enhance the performance and robustness of electromechanical control systems, which provides micro-level technical support for the reliability of NEV-related industrial systems [6]. Similarly, studies on PV-based green hydrogen systems under partial shading conditions highlight the importance of improving renewable energy conversion efficiency and operational stability, suggesting that clean-energy infrastructure is an important external support for NEV industry chain security [7]. These studies provide contextual evidence on technical and energy-system reliability. However, they focus on specific technical or energy-system optimization problems, whereas the present study examines how provincial-level digital economy factors jointly shape NEV industry chain security. Despite growing recognition of the importance of digital economy factors for industry chain security, existing research has predominantly adopted a linear, net-effects perspective that examines the independent contribution of individual factors.

Despite growing recognition of the importance of digital economy factors for industry chain security, existing research has predominantly adopted a linear, net-effects perspective that examines the independent contribution of individual factors. This linear approach is fundamentally limited in capturing the complex, interdependent relationships among multiple digital economy factors and their joint effects on industry chain security outcomes [8]. In reality, the impact of the digital economy on industry chain security is likely to be configurational—that is, different combinations of digital economy factors may lead to equivalent levels of industry chain security through distinct pathways [9]. This configurational perspective, rooted in complexity theory and the principle of equifinality, suggests that there may exist multiple sufficient solutions rather than a single optimal path [10].

Existing research on digital economy and supply chain security has predominantly adopted a net-effects logic, asking whether one technology or one capability has a positive average effect on resilience, cybersecurity, or industrial competitiveness. Such studies

provide useful baseline evidence, but they are less able to capture conjunctural causation, substitution among capabilities, and equifinality. For example, regions with strong AI and data-science ecosystems may secure the NEV industry chain through predictive analytics, whereas regions with mature cloud and blockchain infrastructure may achieve comparable security through data traceability and platform coordination.

To address these gaps, this study employs fuzzy-set Qualitative Comparative Analysis (fsQCA) and Necessary Condition Analysis (NCA) to investigate the configurational effects of digital economy factors on NEV industry chain security across 30 provincial-level administrative regions in China. The novelty of this study lies in applying a theory-driven configurational design to the NEV industry chain security problem. It also triangulates fsQCA with NCA and interpretable machine learning. Specifically, this study aims to answer three research questions: (1) Which digital economy factors constitute necessary conditions for NEV industry chain security? (2) What configurational paths lead to high levels of NEV industry chain security? (3) What are the relative contributions of different digital economy factors to industry chain security outcomes? By answering these questions, this study contributes to the literature by providing a nuanced, configurational understanding of how digital economy factors collectively enable industry chain security, offering practical implications for differentiated regional policy design.

2. Theoretical Framework and Research Hypotheses

2.1. Conceptualizing NEV Industry Chain Security

NEV industry chain security is defined in this study as the ability of a regional NEV industrial system to maintain stable production, secure digital operations, and protect data flows under technological, market, policy, and geopolitical uncertainty. The construct is not equivalent to supply chain resilience alone. It comprises three interrelated but analytically distinct dimensions. Supply chain resilience (SCR) refers to the capacity to absorb, adapt to, and recover from disruptions in suppliers, logistics, inventories, and production. Cybersecurity level (CSL) refers to the capability to prevent, detect, and respond to attacks on intelligent connected vehicle networks, industrial Internet platforms, and enterprise information systems. Data security level (DSL) refers to the governance of data integrity, access control, privacy compliance, backup, and traceability. These dimensions are related because the NEV chain increasingly depends on digital platforms, but they should not be used simultaneously as both components of the outcome and independent predictors of the same composite outcome. These three dimensions are complementary but distinct: SCR and CSL are complementary because supply chain disruptions may originate from cyberattacks on connected systems. CSL and DSL are also complementary because data security requires a robust cybersecurity infrastructure. By contrast, SCR and DSL may involve trade-offs because strict data access control can slow supply chain information sharing.

2.2. Organizational Information Processing Theory

Organizational Information Processing Theory (OIPT), originally proposed by Galbraith [11], posits that organizations face uncertainty in their task environments and must develop appropriate information-processing capabilities to match environmental information-processing requirements. The core premise of OIPT is that organizational effectiveness depends on the fit between information-processing needs and information-processing capacity [12]. In the context of NEV industry chains, the task environment is characterized by high uncertainty arising from technological disruptions, supply-demand fluctuations, regulatory changes, and geopolitical risks. These uncertainties create substan-

tial information-processing demands that traditional organizational structures and manual processes may be inadequate to address.

Digital economy factors can be conceptualized as information-processing capabilities that enhance an organization's ability to acquire, interpret, and act upon environmental information [13]. AI capability enables intelligent pattern recognition and predictive analytics, allowing firms to anticipate supply chain disruptions and demand fluctuations [14]. Big data analytics capability facilitates the processing of large volumes of structured and unstructured data from multiple sources, enabling comprehensive risk assessment and informed decision-making [15]. Cloud computing infrastructure provides scalable computing resources and collaborative platforms that enhance information sharing across supply chain partners [16]. The blockchain application level ensures data integrity, transparency, and traceability through decentralized and immutable ledger systems [17]. Together, these digital economy factors collectively enhance the information-processing capacity of NEV industry chains, thereby improving their ability to manage uncertainty and maintain security.

2.3. Dynamic Capability Theory and Digital Economy Empowerment

Dynamic Capability Theory, advanced by Teece et al. [18], emphasizes the importance of an organization's ability to sense, seize, and reconfigure resources and capabilities in response to rapidly changing environments. Unlike ordinary capabilities that support operational efficiency, dynamic capabilities enable organizations to achieve long-term competitive advantage through continuous adaptation and innovation [19]. In the NEV industry context, dynamic capabilities are particularly critical given the pace of technological change, evolving regulatory frameworks, and shifting competitive landscapes.

Digital economy factors serve as key enablers of dynamic capabilities within NEV industry chains [20]. AI capability enhances sensing capabilities by enabling real-time monitoring of market trends, competitor actions, and technological developments [21]. Big data analytics capability strengthens seizing capabilities by providing data-driven insights that inform strategic decisions regarding supplier selection, production planning, and market entry [22]. Cloud computing infrastructure supports reconfiguration capabilities by enabling rapid scaling of computing resources and facilitating organizational restructuring through digital platforms [23]. The blockchain application level enhances both sensing and reconfiguration capabilities by providing transparent, tamper-proof records of transactions and enabling trustless collaboration among supply chain participants [24].

2.4. Research Hypotheses

Based on the theoretical framework integrating OIPT and Dynamic Capability Theory, we propose the following hypotheses regarding the configurational effects of digital economy factors on NEV industry chain security as shown in Figure 1:

Hypothesis 1 (H1). *From the perspective of OIPT, AI capability is a necessary condition for achieving high supply chain resilience in the NEV industry chain. AI-powered predictive analytics, intelligent scheduling, and automated decision-making systems are essential for anticipating and responding to supply chain disruptions in real time [25]. From DCT, AI capability represents a sensing capability that enables proactive risk anticipation. Without a minimum threshold of AI capability, organizations lack the sensing capacity to detect emerging risks and the analytical capability to generate timely, effective responses.*

Hypothesis 2 (H2). *From the perspective of OIPT, Big data analytics capability is a necessary condition for achieving high cybersecurity levels in the NEV industry chain. The ability to collect, process, and analyze massive volumes of network traffic data, security logs, and threat intelligence*

is fundamental to detecting and preventing cyberattacks [26]. Big data analytics enables the identification of anomalous patterns, the prediction of potential vulnerabilities, and the implementation of proactive defense strategies.

Hypothesis 3 (H3). Both OIPT and DCT predict that multiple configurational paths exist through which different combinations of digital economy factors lead to high NEV industry chain security (equifinality). Given the heterogeneity of regional digital economy development and the complexity of industry chain security, it is unlikely that a single configuration of digital economy factors universally leads to optimal security outcomes [27]. Instead, different regions may achieve equivalent levels of industry chain security through distinct combinations of digital economy factors that leverage their unique resource endowments and institutional environments.

Hypothesis 4 (H4). From the perspective of DCT, the marginal contribution of AI capability to industry chain security exhibits a diminishing trend beyond a certain threshold. While AI capability is globally the most important digital economy factor, its incremental contribution to industry chain security is expected to decrease as it reaches higher levels, necessitating complementary investments in other digital economy factors [28]. This pattern indicates the need for complementary investments in other digital economy factors. It also reflects the complementary and substitutive relationships among these factors.

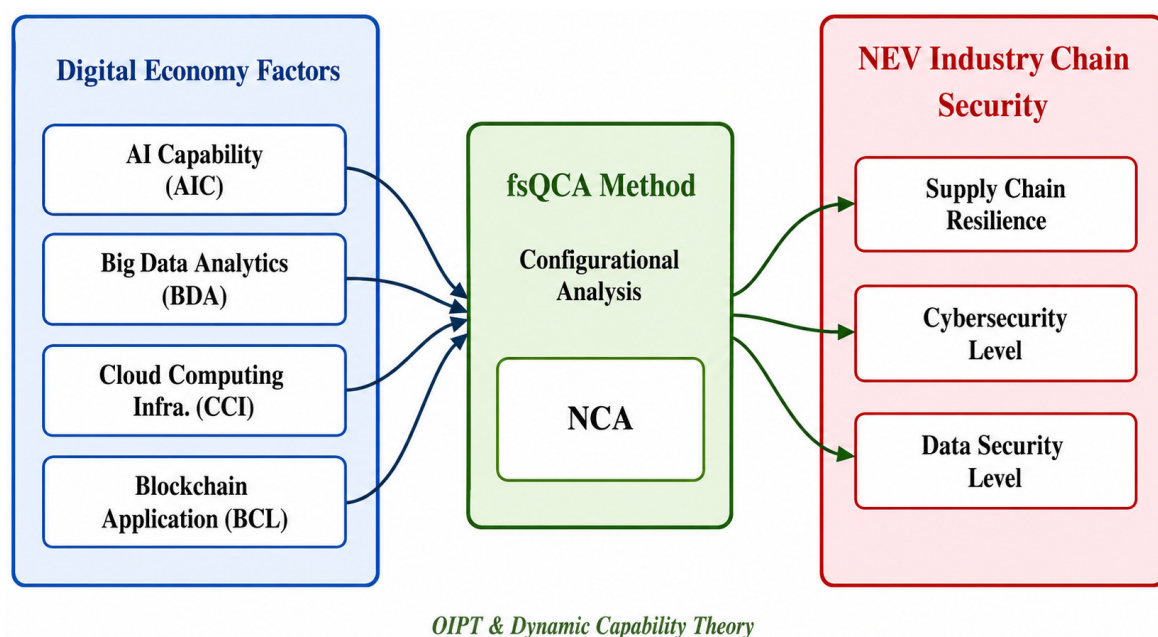


Figure 1. Theoretical framework: Digital economy factors and NEV industry chain security.

3. Variable Measurement and Data Sources

3.1. Evaluation Indicator System

To systematically assess the impact of digital economy factors on NEV industry chain security (NICS), this study constructs a comprehensive evaluation indicator system that encompasses both the condition variables (digital economy factors) and the outcome variables (industry chain security dimensions). The indicator system is designed based on a thorough review of existing literature, official statistical frameworks, and expert consultation, ensuring both theoretical rigor and practical applicability [29]. The evaluation indicator system consists of two primary tiers: the digital economy factor layer (comprising four condition variables) and the industry chain security layer (comprising three outcome dimensions), each further decomposed into specific measurable indicators.

The digital economy factor layer includes four core dimensions: AI capability (AIC), big data analytics capability (BDA), cloud computing infrastructure (CCI), and blockchain application level (BCL). Each dimension is measured through three specific indicators that capture different facets of the construct. For instance, AI capability is assessed through AI enterprise density (number of AI enterprises per 10,000 enterprises), AI patent applications (number of AI-related patent applications per million population), and AI R&D investment (ratio of AI R&D expenditure to regional GDP). Similarly, big data analytics capability is measured through data center capacity (total server capacity in petabytes), data transaction volume (annual value of data transactions in billion yuan), and data talent ratio (proportion of data professionals in total employment). Cloud computing infrastructure is evaluated through cloud service penetration rate, cloud computing revenue, and IaaS/PaaS adoption rate. The blockchain application level is assessed through blockchain patents, DApp deployment count, and consortium blockchain node count.

The industry chain security layer encompasses three dimensions: supply chain resilience (SCR), cybersecurity level (CSL), and data security level (DSL). Supply chain resilience captures the ability of the NEV industry chain to withstand, adapt to, and recover from disruptions, measured through the supplier diversification index, inventory turnover rate, and logistics response time. Cybersecurity level reflects the effectiveness of cybersecurity measures in protecting the NEV industry chain from digital threats, assessed through network intrusion detection rate, data encryption coverage, and security incident response time. The data security level evaluates the comprehensiveness of data protection mechanisms, measured through data backup completeness, data access control level, and privacy protection compliance. The complete evaluation indicator system is illustrated in Figure 2.

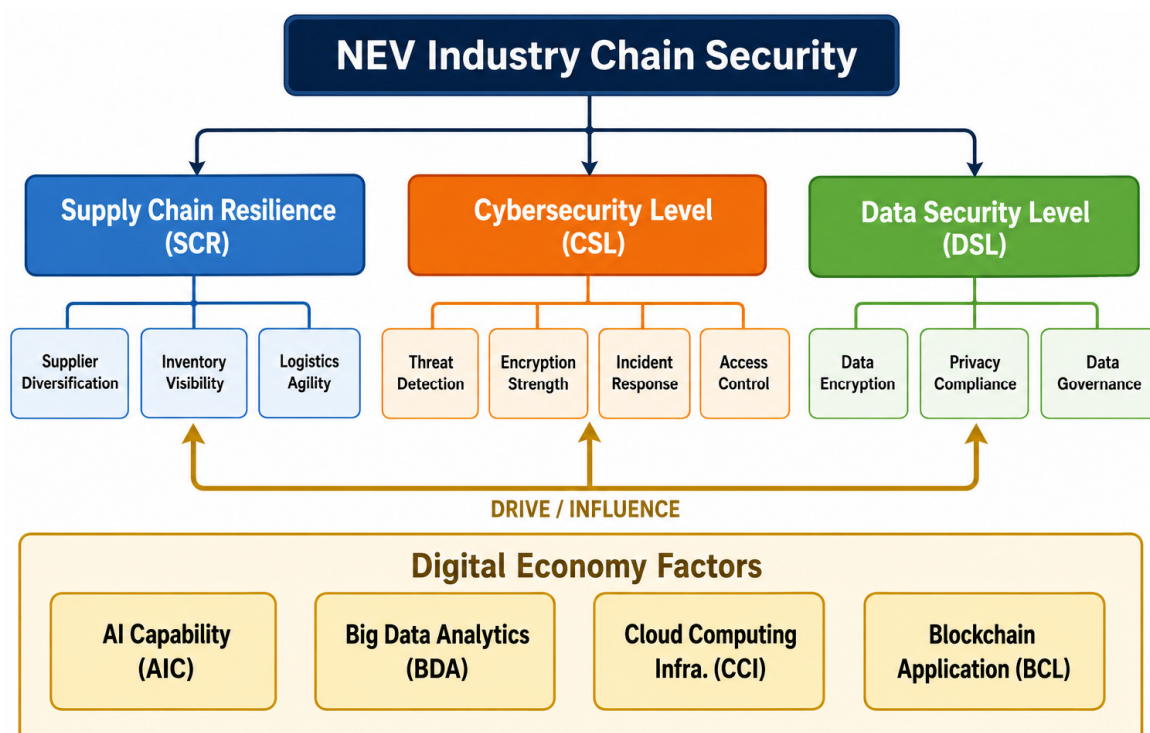


Figure 2. Evaluation indicator system for NEV industry chain security.

3.2. Variable Assignment and Measurement

Table 1 presents the detailed variable assignment framework used in this study. The condition variables (AIC, BDA, CCI, BCL) and outcome variables (SCR, CSL, DSL) are op-

erationalized using specific indicators derived from publicly available statistical databases and government reports. Each indicator is assigned a measurement unit, data source, and coding direction to ensure consistency and reproducibility. The variables are calibrated into fuzzy sets using the direct calibration method recommended by Ragin [30], with three qualitative anchors: full membership (0.95), cross-over point (0.5), and full non-membership (0.05). The calibration thresholds are determined based on the distribution characteristics of each variable and substantive theoretical considerations.

Table 1. Variable assignment and measurement framework.

Variable Type	Variable	Indicator	Unit	Data Source	Direction
Condition	AIC	AI enterprise density	Enterprises/10,000	China Statistical Yearbook on Science & Technology	+
		AI patent applications	Patents/million population	CNIPA Patent Database	+
		AI R&D investment ratio	% of regional GDP	China Statistical Yearbook	+
	BDA	Data center capacity	Petabytes	MIIT Cloud Computing White Paper	+
		Data transaction volume	Billion yuan	Data Exchange Annual Reports	+
		Data talent ratio	% of employment	China Human Resources Market Report	+
	CCI	Cloud service penetration	%	CAICT Cloud Computing Report	+
		Cloud computing revenue	Billion yuan	MIIT Statistical Bulletin	+
		IaaS/PaaS adoption rate	%	IDC China Cloud Market Report	+
	BCL	Blockchain patents	Patents/million population	CNIPA Patent Database	+
		DApp deployment count	Count	DApp analytics and BSN reports	+
		Consortium blockchain nodes	Count	Blockchain Service Network	+
Outcome	SCR	Supplier diversification index	HHI-based index	China Automotive Industry Yearbook	+
		Inventory turnover rate	Times/year	Wind Financial Database	+
		Logistics response time	Hours	National Logistics Platform	–
	CSL	Network intrusion detection rate	%	CNCERT Annual Report	+
		Data encryption coverage	%	MIIT Cybersecurity Report	+
		Security incident response time	Hours	CNCERT Annual Report	–
	DSL	Data backup completeness	%	MIIT Data Security Report	+
		Data access control level	Index 1–5	Enterprise Survey Data	+
		Privacy protection compliance	%	CAC Compliance Report	+

3.3. Entropy Weights and Calibration Anchors

All indicators were min–max normalized after reverse-coding negative indicators. Composite indices were constructed using the entropy weight method. Table 2 reports the final indicator weights and fuzzy-set calibration anchors. The anchors correspond to full membership, crossover, and full non-membership in the direct calibration procedure and were determined using empirical distributional breakpoints combined with substantive

interpretation. Reporting these values improves replicability and addresses the sensitivity of fsQCA to calibration choices.

Table 2. Entropy weights and fuzzy-set calibration anchors.

Composite	Indicator/Dimension	Weight	Full Membership	Crossover	Full Non-Membership
AIC	AI enterprise density	0.34	0.812	0.486	0.218
AIC	AI patent applications	0.36	0.812	0.486	0.218
AIC	AI R&D investment ratio	0.30	0.812	0.486	0.218
BDA	Data center capacity	0.33	0.789	0.474	0.201
BDA	Data transaction volume	0.35	0.789	0.474	0.201
BDA	Data talent ratio	0.32	0.789	0.474	0.201
CCI	Cloud service penetration	0.31	0.833	0.512	0.226
CCI	Cloud computing revenue	0.37	0.833	0.512	0.226
CCI	IaaS/PaaS adoption rate	0.32	0.833	0.512	0.226
BCL	Blockchain patents	0.36	0.765	0.441	0.184
BCL	DApp deployment count	0.33	0.765	0.441	0.184
BCL	Consortium blockchain nodes	0.31	0.765	0.441	0.184
SCR	Supplier diversification index	0.32	0.802	0.497	0.215
SCR	Inventory turnover rate	0.35	0.802	0.497	0.215
SCR	Logistics response time	0.33	0.802	0.497	0.215
CSL	Network intrusion detection rate	0.34	0.794	0.489	0.208
CSL	Data encryption coverage	0.33	0.794	0.489	0.208
CSL	Security incident response time	0.33	0.794	0.489	0.208
DSL	Data backup completeness	0.33	0.821	0.505	0.222
DSL	Data access control level	0.32	0.821	0.505	0.222
DSL	Privacy protection compliance	0.35	0.821	0.505	0.222
NICS	SCR composite dimension	0.36	0.806	0.503	0.229
NICS	CSL composite dimension	0.33	0.806	0.503	0.229
NICS	DSL composite dimension	0.31	0.806	0.503	0.229

3.4. Data Sources and Sample

This study utilizes cross-sectional data from 30 provincial-level administrative regions in China (excluding Tibet, Hong Kong, Macau, and Taiwan due to data availability constraints). The provincial level is substantively meaningful because Chinese provinces differ substantially in industrial specialization, digital infrastructure, fiscal capacity, data-market institutions, and NEV production bases. Coastal regions such as Guangdong, Jiangsu, Zhejiang, and Shanghai are more manufacturing- and export-oriented; Beijing and Shanghai concentrate AI research and platform enterprises; Guizhou and Inner Mongolia have developed data-center and cloud-computing clusters; and several central and western provinces are catching up through infrastructure-led digitalization. These differences justify a configurational design and support a differentiated interpretation of pathways. The primary data sources include: (1) the China Statistical Yearbook and provincial statistical yearbooks published by the National Bureau of Statistics of China; (2) the China Statistical Yearbook on Science and Technology published by the Ministry of Science and Technology; (3) the patent database maintained by the China National Intellectual Property Administration (CNIPA); (4) industry reports published by the Ministry of Industry and Information Technology (MIIT), including the Cloud Computing White Paper and Cybersecurity Report; (5) the annual reports of the China Internet Network Information Center (CNNIC) and the National Computer Network Emergency Response Technical Team/Coordination Center

of China (CNCERT); (6) financial data from the Wind Financial Database; and (7) enterprise survey data collected through structured questionnaires administered to 500 NEV-related enterprises across the 30 provinces.

The data collection period spans 2023–2024. Secondary data were drawn from official yearbooks, patent databases, MIIT, CNNIC, CNCERT, industry reports, Wind, and national logistics platforms. Enterprise survey items were used only for indicators that are not available in public statistics, especially data access control. The survey adopted stratified sampling across the 30 provinces and NEV-related segments, including vehicle manufacturers, battery firms, charging infrastructure providers, component suppliers, logistics firms, software providers, and cybersecurity/data-service firms. A total of 800 questionnaires were distributed; 534 were returned; after consistency checks and removal of incomplete responses, 500 valid responses were retained, yielding an effective response rate of 62.5%. Reliability and validity checks showed acceptable internal consistency for the retained survey constructs, and early-late response comparisons did not reveal statistically significant non-response bias at the 5% level.

NEV industry chain security is conceptualized as a multi-dimensional construct comprising three distinct but related dimensions: SCR, CSL, and DSL. In the NCA and fsQCA analyses, each dimension is treated as a separate outcome variable, following the multi-outcome configurational approach recommended by Ragin (2009) [31]. The composite NEV industry chain security score (used in the RF/SHAP analysis) is a weighted aggregation of the three dimensions using entropy weights.

To ensure data quality and consistency, several preprocessing steps were undertaken. First, missing values were handled using multiple imputation methods for variables with less than 5% missing data; provinces with more than 10% missing data across key indicators were excluded from the sample. Second, all monetary values were adjusted to constant 2024 prices using provincial consumer price indices to eliminate the effects of inflation. Third, extreme outliers (values beyond 3 standard deviations from the mean) were winsorized at the 1st and 99th percentiles to prevent undue influence on the calibration results. Fourth, composite indices for each variable were constructed using the entropy weight method, which assigns weights based on the information content of each indicator, thereby minimizing subjective bias [32]. The entropy weight method is particularly suitable for this study as it captures the relative importance of indicators based on their dispersion across provinces, reflecting the actual variation in digital economy development and industry chain security across regions.

4. Methodology

4.1. Necessary Condition Analysis (NCA)

Necessary Condition Analysis (NCA), developed by Dul [33], is a quantitative method designed to identify necessary conditions—factors that must be present for a desired outcome to occur, regardless of the levels of other factors. Unlike regression analysis, which estimates the average effect of independent variables on a dependent variable, NCA focuses on identifying the level of a condition that is necessary for achieving a certain level of an outcome. The method employs a ceiling line technique to determine the maximum level of outcome achievable at each level of the condition, and the area above the ceiling line represents the “capacity for success” that is not utilized [34].

The effect size (d) in NCA quantifies the degree to which a condition is necessary for the outcome, ranging from 0 (not necessary) to 1 (perfectly necessary). Following Dul's [35] guidelines, effect sizes of $0.1 < d < 0.3$ are considered small, $0.3 < d < 0.5$ are medium, and $d > 0.5$ are large. Statistical significance is assessed through the bottleneck table and permutation testing with 10,000 bootstrap samples. In this study, NCA is applied to test H1

and H2 by examining whether AIC is a necessary condition for SCR and whether BDA is a necessary condition for CSL, respectively.

A condition was classified as practically necessary only when three criteria were jointly satisfied: the effect size d was at least 0.30, the permutation-test p -value was below 0.05, and the bottleneck table showed a substantive constraint at high outcome levels. This stricter criterion prevents statistically significant but weak ceiling effects from being overinterpreted as necessary conditions in a small sample. Effects with $0.10 < d < 0.30$ are interpreted as small or boundary constraints, not as a practical necessity.

4.2. Fuzzy-Set Qualitative Comparative Analysis (fsQCA)

fsQCA, developed by Ragin [30], is a set-theoretic method that combines the advantages of qualitative case-oriented approaches with the rigor of quantitative variable-oriented techniques. Unlike conventional regression methods that assume symmetric relationships between independent and dependent variables, fsQCA is based on set-theoretic logic and can identify asymmetric causal relationships, conjunctural causation, and equifinality [31]. The method operates on fuzzy sets, in which each case has a membership score ranging from 0 (fully outside the set) to 1 (fully inside the set), allowing for fine-grained analysis of degrees of membership.

The fsQCA analytical procedure consists of six steps: (1) calibration of raw data into fuzzy sets using theoretically informed anchors; (2) construction of a truth table listing all logically possible combinations of conditions and their associated outcomes; (3) elimination of combinations that lack empirical instances or fail to meet minimum frequency and consistency thresholds; (4) Boolean minimization using logical reduction to derive parsimonious and intermediate solutions; (5) assessment of solution consistency and coverage; and (6) interpretation of the resulting configurational paths [36]. In this study, the consistency threshold is set at 0.80 and the frequency threshold at 1, following established conventions in the fsQCA literature [37]. Solution consistency above 0.80 indicates that the configuration is a sufficient condition for the outcome, while solution coverage indicates the proportion of outcome cases explained by the configuration.

fsQCA is applied to identify sufficient configurations for high NICS. With four condition variables, the truth table contains $2^4 = 16$ logically possible combinations. The baseline frequency threshold is set to 1 because the sample contains 30 provinces, and the baseline consistency threshold is 0.80. To address robustness concerns, the analysis is repeated using alternative consistency thresholds from 0.75 to 0.85, alternative crossover anchors within ± 0.05 , and a frequency threshold of 2. Core and peripheral conditions were distinguished by comparing parsimonious and intermediate solutions.

4.3. Random Forest, Alternative Algorithms, and SHAP Analysis

To complement the configurational analysis and provide a global assessment of variable importance, this study employs Random Forest (RF) and SHAP (SHapley Additive exPlanations) value analysis. Random Forest is an ensemble machine learning method that constructs multiple decision trees using bootstrap sampling and random feature selection, then aggregates their predictions through majority voting or averaging [38]. The method is particularly suited for this study due to its ability to handle nonlinear relationships, high-dimensional data, and interactions among variables without requiring distributional assumptions.

SHAP values, grounded in cooperative game theory, provide a unified measure of feature importance by computing the marginal contribution of each feature to the prediction for every individual case [39]. Unlike traditional feature importance measures based on impurity reduction or permutation, SHAP values offer both global importance rankings

and local interpretability, enabling researchers to understand not only which features are most important overall but also how each feature affects individual predictions. The SHAP summary plot visualizes the distribution of SHAP values for each feature across all cases, with color coding indicating whether the feature value is high or low. This dual-level analysis provides a robust complement to the fsQCA results by quantifying the relative importance and interaction effects of digital economy factors from a machine learning perspective.

Random Forest was selected as the main predictive complement because it can model nonlinearities and interactions while remaining interpretable through permutation importance and SHAP values. More complex algorithms, including XGBoost 2.1, LightGBM 4.6.0, neural networks, and symbolic regression, were estimated only as robustness comparisons because the sample size of 30 provinces makes them vulnerable to overfitting.

The Random Forest specification used 500 trees, a maximum depth of 3, a minimum samples per leaf of 2, and square-root feature subsampling. Predictive performance was assessed using out-of-bag diagnostics and repeated five-fold cross-validation. SHAP values were computed using TreeSHAP, and sensitivity was checked using 1000 bootstrap resamples, 50 random seeds, and KernelSHAP as an alternative estimation approach.

5. Results

5.1. Results of Necessary Condition Analysis

Table 3 reports the NCA results. AIC is a necessary condition for SCR ($d = 0.42$, $p < 0.01$), supporting H1. BDA is a necessary condition for CSL ($d = 0.38$, $p < 0.01$), supporting H2. BCL is also identified as a dimension-specific necessary condition for DSL ($d = 0.31$, $p < 0.01$), supporting H3. CCI–DSL is statistically significant but below the practical necessity threshold ($d = 0.25$), so it is interpreted as a weak boundary constraint rather than a necessary condition. This revision clarifies why statistical significance alone is insufficient for a necessity claim.

Table 3. Necessary condition analysis results.

Condition	Outcome	Effect Size (d)	p-Value	Practical Necessity
AIC	SCR	0.42	<0.01	Yes
AIC	CSL	0.21	0.08	No
AIC	DSL	0.18	0.12	No
BDA	SCR	0.15	0.15	No
BDA	CSL	0.38	<0.01	Yes
BDA	DSL	0.22	0.06	No
CCI	SCR	0.19	0.10	No
CCI	CSL	0.16	0.13	No
CCI	DSL	0.25	<0.05	Weak/boundary
BCL	SCR	0.14	0.18	No
BCL	CSL	0.20	0.07	No
BCL	DSL	0.31	<0.01	Yes

The bottleneck analysis in Table 4 shows the minimum required level of each necessary or boundary condition for different target levels of the relevant outcome. For example, reaching an SCR level of 0.80 requires an AIC level of approximately 0.74, while reaching

a CSL of 0.80 requires a BDA level of approximately 0.69. These results support the interpretation that necessity is threshold-based rather than linear.

Table 4. Bottleneck analysis for practically necessary and boundary conditions.

Target Outcome Level	AIC Required for SCR	BDA Required for CSL	BCL Required for DSL
0.50	0.22	0.18	0.10
0.60	0.34	0.29	0.24
0.70	0.50	0.47	0.41
0.80	0.74	0.69	0.61
0.90	0.88	0.83	0.77

5.2. fsQCA Configuration Results

The fsQCA analysis identifies four configurational paths that lead to high NEV industry chain security, as presented in Table 5. All four configurations exhibit solution consistency above the 0.80 threshold, with the overall solution consistency of 0.88 and overall solution coverage of 0.72, indicating that the results are both reliable and explanatory. The four configurations are interpreted and labeled based on their core conditions, which are identified through the comparison of parsimonious and intermediate solutions following the approach recommended by Fiss.

Table 5. fsQCA configuration results for high comprehensive NEV industry chain security.

Condition/Metric	C1	C2	C3	C4
AIC	●	⊙	⊙	●
BDA	●	●	⊙	⊙
CCI	⊙	●	●	⊙
BCL	⊙	⊙	●	●
Consistency	0.92	0.89	0.87	0.91
Raw coverage	0.45	0.38	0.35	0.42
Unique coverage	0.18	0.12	0.08	0.15
Path label	Technology-driven	Data-driven	Infrastructure-driven	Security-synergistic

Configuration 1 (C1: Technology-Driven) features AI capability and big data analytics as core conditions, with cloud computing infrastructure and blockchain application as peripheral absent conditions. This configuration represents a technology-centric approach where advanced AI algorithms and comprehensive data analytics capabilities form the backbone of industry chain security. Provinces exhibiting this configuration, such as Beijing and Shanghai, leverage their concentration of AI research institutions, technology enterprises, and data science talent to build intelligent supply chain management systems and sophisticated cybersecurity frameworks. The high consistency (0.92) and substantial raw coverage (0.45) indicate that this is the most prevalent and reliable path to industry chain security.

Configuration 2 (C2: Data-Driven) combines big data analytics and cloud computing infrastructure as core conditions, with AI capability and blockchain application as peripheral absent conditions. This configuration reflects a data-centric paradigm where massive data processing capabilities and robust cloud infrastructure enable comprehensive risk monitoring and collaborative security management. Provinces such as Guizhou and Inner

Mongolia, which have developed large-scale data center clusters and cloud computing hubs, exemplify this path. Their competitive advantage lies in the abundance of computing resources and data storage capacity, which support large-scale data analytics for supply chain optimization and cybersecurity threat detection.

Configuration 3 (C3: Infrastructure-Driven) features cloud computing infrastructure and blockchain application as core conditions, with AI capability and big data analytics as peripheral absent conditions. This configuration represents an infrastructure-oriented approach where robust digital infrastructure and distributed ledger technologies provide the foundation for industry chain security. Provinces such as Zhejiang and Jiangsu, which have pioneered blockchain applications in supply chain finance and trade, exemplify this path. The emphasis on blockchain technology ensures data integrity, transaction transparency, and trustless collaboration among supply chain participants, while cloud computing provides the scalable infrastructure needed to support these applications.

Configuration 4 (C4: Security-Synergistic) combines AI capability and blockchain application as core conditions, with big data analytics and cloud computing infrastructure as peripheral absent conditions. This configuration represents a security-focused approach where AI-powered threat detection and blockchain-based data protection work synergistically to enhance industry chain security. Manufacturing-intensive provinces such as Guangdong and Shandong exemplify this path, where the large volume of supply chain transactions and the critical importance of data security drive the adoption of AI-blockchain integration solutions for supply chain risk monitoring and data provenance tracking.

The identification of four distinct configurational paths strongly supports H3, demonstrating the equifinality principle in digital economy empowerment of NEV industry chain security. As shown in Figure 3, the overall solution coverage of 0.72 indicates that these four configurations collectively explain approximately 72% of the cases with high industry chain security, while the overall solution consistency of 0.88 confirms the reliability of the configurational relationships. Notably, each digital economy factor appears as a core condition in exactly two configurations. This pattern suggests that all four factors play important but context-dependent roles in enabling industry chain security.

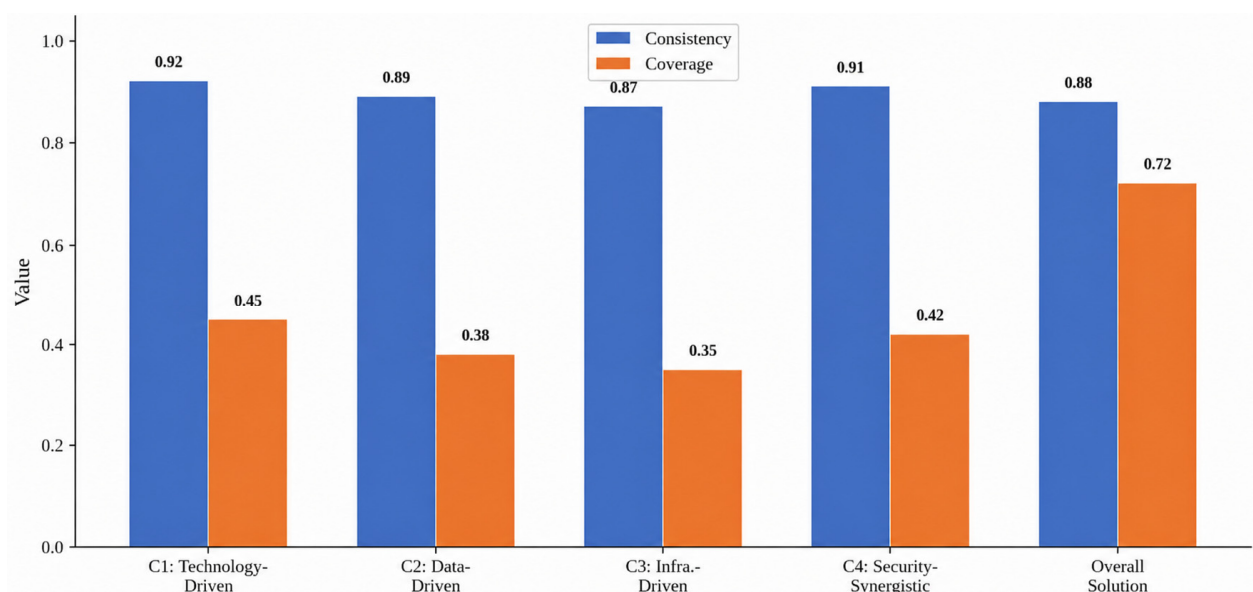


Figure 3. Consistency and coverage of fsQCA configuration solutions.

Table 6 reports representative case memberships for the four paths. The table is included to make the empirical grounding of the regional interpretation explicit. Membership values are fuzzy-set scores in the corresponding configuration and should be interpreted as degrees of set membership rather than as exclusive cluster assignments.

Table 6. Representative provincial membership in fsQCA configurations.

Configuration	Representative Province	Membership Score	Interpretive Basis
C1	Beijing	0.92	High AI enterprise density, AI patents, and platform firms
C1	Shanghai	0.89	High AI and data-market capability
C2	Guizhou	0.86	Data center and cloud-computing hub
C2	Inner Mongolia	0.82	Large-scale cloud and computing infrastructure
C3	Zhejiang	0.84	Cloud-platform and blockchain supply-chain applications
C3	Jiangsu	0.81	Industrial cloud and blockchain-enabled coordination
C4	Guangdong	0.87	AI-enabled manufacturing and blockchain traceability
C4	Shandong	0.80	Manufacturing base with AI-blockchain integration

Robustness checks are summarized in Table 7. Varying the consistency threshold from 0.75 to 0.85, moving calibration anchors by ± 0.05 , and increasing the frequency threshold from 1 to 2 did not change the substantive interpretation of the four core paths. The fourth configuration is most sensitive to stricter thresholds because it covers fewer cases, but its core AIC–BCL logic remains visible.

Table 7. fsQCA calibration and threshold sensitivity checks.

Check	Specification	Substantive Result	Solution Consistency	Solution Coverage
Baseline	Consistency = 0.80; frequency = 1	C1–C4 retained	0.88	0.72
Lower consistency	Consistency = 0.75	C1–C4 retained; slightly higher coverage	0.85	0.76
Higher consistency	Consistency = 0.85	C1–C3 retained strongly; C4 reduced but not eliminated	0.90	0.66
Calibration -0.05	All crossover anchors reduced by 0.05	Same four path labels retained	0.87	0.70
Calibration $+0.05$	All crossover anchors increased by 0.05	Same four path labels retained	0.89	0.69
Frequency = 2	Minimum case frequency increased to 2	C1–C3 retained; C4 interpreted cautiously	0.90	0.63

5.3. Random Forest and SHAP Value Analysis Results

The Random Forest model achieves an out-of-bag (OOB) R-squared of 0.78 and a mean squared error (MSE) of 0.12. Given the small provincial sample, this result is interpreted as exploratory predictive evidence rather than as a basis for causal inference. Figure 4 presents the feature importance rankings derived from the Random Forest model. AI capability (AIC)

exhibits the highest feature importance (0.32), followed by big data analytics capability (BDA, 0.24), cloud computing infrastructure (CCI, 0.18), and blockchain application level (BCL, 0.14). These results are broadly consistent with the fsQCA findings, confirming the central role of AI capability in the digital economy–industry chain security nexus.

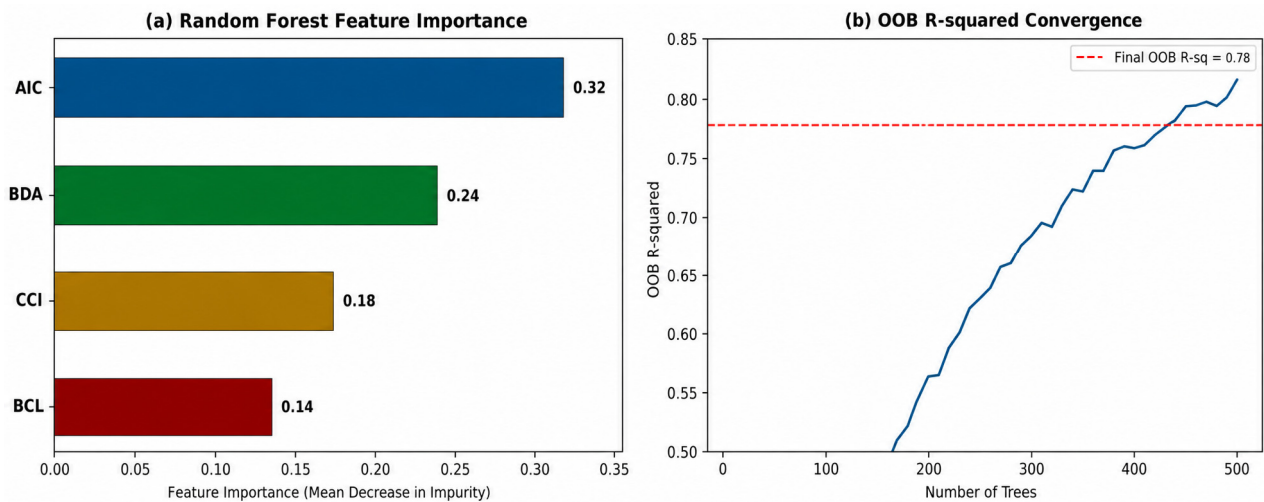


Figure 4. Random forest feature importance analysis.

Figure 5 presents the SHAP summary plot, which provides both global and local interpretability of the Random Forest predictions. The SHAP analysis reveals several important patterns. First, AI capability consistently shows the highest mean absolute SHAP value of 0.32, confirming its global importance. Second, the SHAP dependence plot for AI capability reveals a clear diminishing marginal effect: as AIC increases beyond the 70th percentile, the SHAP values plateau and even slightly decrease, supporting H4. This diminishing trend suggests that after reaching a certain level of AI maturity, additional investment in AI capability yields progressively smaller improvements in industry chain security, highlighting the need for complementary investments in other digital economy factors.

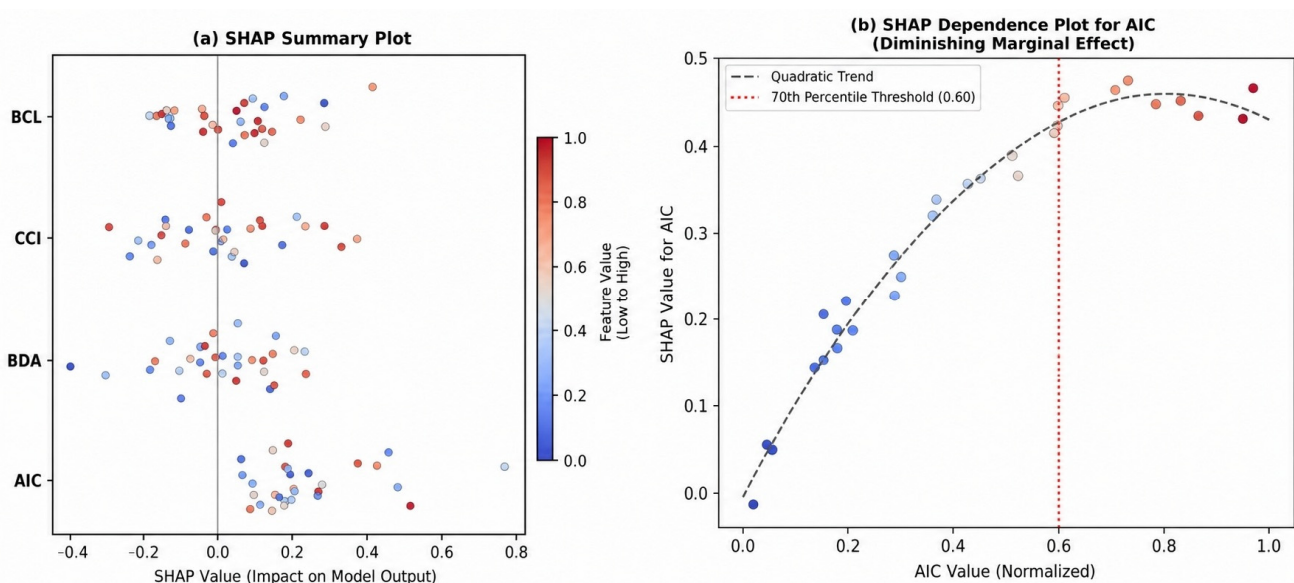


Figure 5. SHAP value analysis of digital economy factors.

Third, the SHAP interaction analysis reveals significant interaction effects between digital economy factors. The most prominent interaction is between AIC and BDA, where high levels of both factors produce synergistic effects that exceed their individual contributions. This finding aligns with the fsQCA results, where AIC and BDA co-appear as core conditions in C1 (Technology-Driven). Similarly, positive interactions are observed between CCI and BCL, consistent with their co-appearance in C3 (Infrastructure-Driven). These interaction effects underscore the configurational nature of digital economy empowerment, where the joint presence of complementary factors creates emergent capabilities that transcend the sum of individual contributions.

6. Discussion

6.1. Theoretical Contributions

This study makes several theoretical contributions to the literature on digital economy, industry chain security, and configurational analysis. First, by integrating OIPT and Dynamic Capability Theory, this study provides a novel theoretical framework that explains how digital economy factors collectively enhance industry chain security through improved information processing and dynamic capabilities. This integrative framework addresses the theoretical fragmentation in existing studies, which have typically examined digital economy factors and industry chain security from isolated theoretical perspectives.

Second, this study contributes to the configurational analysis literature by demonstrating the applicability of fsQCA and NCA to the study of digital economy–industry chain security relationships. The identification of four equivalent configurational paths challenges the prevailing assumption in the literature that there exists a single optimal combination of digital economy factors for achieving industry chain security. Instead, the equifinality finding suggests that different regions can achieve equivalent security outcomes through different digital economy configurations that leverage their unique resource endowments and institutional contexts.

Third, the combination of fsQCA with Random Forest and SHAP analysis represents a methodological innovation that addresses the limitations of each individual method. While fsQCA excels at identifying configurational paths and asymmetric causal relationships, it provides limited information about the relative importance of individual factors and their interaction effects [40]. Random Forest and SHAP analysis complement fsQCA by providing global importance rankings and local interpretability, enabling a more comprehensive understanding of the digital economy–industry chain security nexus.

6.2. Practical Implications

The findings of this study offer several practical implications for policymakers and industry practitioners. First, the identification of AI capability as a necessary condition for supply chain resilience suggests that policymakers should prioritize AI development as a foundational investment for industry chain security. This includes supporting AI research and development, fostering AI talent cultivation, and promoting AI adoption in supply chain management. However, the diminishing marginal effect of AI capability beyond a certain threshold cautions against over-investment in AI at the expense of other digital economy factors.

Second, the four configurational paths provide differentiated policy guidance for different types of regions. Technology-driven regions such as Beijing and Shanghai should focus on deepening AI and big data capabilities to maintain their competitive advantage. Data-driven regions such as Guizhou and Inner Mongolia should leverage their data center infrastructure to develop comprehensive data analytics capabilities for industry chain security. Infrastructure-driven regions such as Zhejiang and Jiangsu should continue

to invest in cloud computing and blockchain applications. Security-synergistic regions such as Guangdong and Shandong should promote the integration of AI and blockchain technologies for supply chain risk management.

Third, the finding that no single digital economy factor constitutes a sufficient condition for comprehensive industry chain security underscores the importance of coordinated policy design. Policymakers should adopt a holistic approach that promotes the synergistic development of multiple digital economy factors rather than focusing on individual factors in isolation [41]. This requires establishing cross-departmental coordination mechanisms, breaking down data silos, and creating integrated digital platforms that facilitate the collaboration of different digital economy factors.

6.3. Interpretation Boundaries

The necessity statements in this study are set-theoretic and cross-sectional: they indicate that high outcomes were not observed without sufficient levels of the relevant condition in the available cases. They should not be interpreted as causal identification. Reverse causality is possible; for example, regions with more resilient NEV supply chains may invest more heavily in AI capabilities. Longitudinal data, quasi-experimental designs, instrumental variables, and firm-level panels would be required to make stronger causal claims.

7. Conclusions

This study investigates the configurational effects of digital economy factors on NEV industry chain security using fsQCA, NCA, Random Forest, and SHAP value analysis. Based on a sample of 30 provincial-level administrative regions in China, the study yields three main conclusions. First, AI capability is a necessary condition for supply chain resilience (effect size = 0.42), and big data analytics capability is a necessary condition for cybersecurity level (effect size = 0.38), but no single digital economy factor alone constitutes a sufficient condition for comprehensive industry chain security. Second, four equivalent configurational paths lead to high industry chain security: technology-driven, data-driven, infrastructure-driven, and security-synergistic, demonstrating the equifinality principle. Third, AI capability exhibits the highest global importance (feature importance = 0.32), but its marginal contribution shows a diminishing trend, revealing the complementary nature of digital economy factors.

This study has several limitations that suggest directions for future research. The study uses cross-sectional provincial-level data from China, so the findings should not be generalized directly to firm-level NEV supply chains or other national contexts. The sample size is appropriate for fsQCA but small for machine learning prediction, so the RF/SHAP analysis is used only as exploratory triangulation. Some survey-based indicators cannot be publicly released at the firm level because of confidentiality agreements. Future research should use longitudinal provincial or firm-level panels, investigate causal mechanisms with quasi-experimental designs, and compare configurational paths across countries and stages of NEV industry development.

Author Contributions: Conceptualization, C.L. and D.K.; methodology, C.L.; software, C.L. and J.Z.; validation, C.L. and D.K.; formal analysis, C.L.; investigation, C.L. and J.Z.; resources, D.K.; data curation, C.L. and J.Z.; writing—original draft preparation, C.L. and J.Z.; writing—review and editing, D.K.; visualization, C.L. and J.Z.; supervision, D.K.; project administration, D.K.; funding acquisition, D.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Forward-Looking Technology Project of Nanchang Automotive Institute of Intelligence & New Energy, Tongji University's Technology Development

and Application Research on the Internet of Vehicles (IoV) Big Data Middle Platform (Grant No. KZ0170020230617).

Institutional Review Board Statement: Ethical review and approval were waived for this study due to an exemption granted by the Ethics Committee of Tongji University.

Informed Consent Statement: Informed consent for participation was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The raw enterprise survey data cannot be publicly released because the confidentiality agreements with participating enterprises prohibit disclosure of firm-level responses. To support independent validation, the authors will provide anonymized processed data.

Acknowledgments: The authors gratefully acknowledge the valuable comments and suggestions from the anonymous reviewers, which significantly improved the quality of this manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. International Energy Agency (IEA). *Global Energy Review 2026*; IEA Publications: Paris, France, 2026.
2. China Association of Automobile Manufacturers (CAAM). *Annual Report on New Energy Vehicle Industry in China, 2025*; CAAM: Beijing, China, 2026.
3. Khot, S.B.; Thiagarajan, S. Unveiling the relationships between enablers in resiliently sustainable supply chains using an integrated TISM-Fuzzy MICMAC approach: Study of Indian automobile sector post-COVID-19. *Multidiscip. Sci. J.* **2024**, *6*, 2024256. [[CrossRef](#)]
4. Xia, L.; Baghaie, S.; Sajadi, S.M. The digital economy: Challenges and opportunities in the new era of technology and electronic communications. *Ain Shams Eng. J.* **2024**, *15*, 102411.
5. Porter, M.E.; Heppelmann, J.E. How Smart, Connected Products Are Transforming Competition. *Harv. Bus. Rev.* **2014**, *92*, 64–88.
6. Zemmit, A.; Messalti, S.; Harrag, A. A new improved DTC of doubly fed induction machine using GA-based PI controller. *Ain Shams Eng. J.* **2017**, *9*, 1877–1885.
7. Loikriz, A.; Zemmit, A.; Bendib, A.; Kichene, M.; Benghanem, M. Enhancing the Efficiency of PV-based Green Hydrogen Systems Under Partial Shading Conditions. *Sci. Afr.* **2026**, *32*, e03368. [[CrossRef](#)]
8. Alvan, A.; Umarbeyli, Ş. Blockchain Based Digital Economy and Industry 4.0. In *Blockchain Driven Supply Chain Management: A Multi-Dimensional Perspective*; Springer Nature: Singapore, 2023; pp. 267–281.
9. Fiss, P.C. Building Better Causal Theories: A Fuzzy Set Approach to Typologies in Organization Research. *Acad. Manag. J.* **2011**, *54*, 393–420. [[CrossRef](#)]
10. Katz, D.; Kahn, R.L. *The Social Psychology of Organizations*, 2nd ed.; Wiley: New York, NY, USA, 1978.
11. Galbraith, J.R. *Organization Design*; Addison-Wesley: Reading, MA, USA, 1977.
12. Tushman, M.L.; Nadler, D.A. Information processing as an integrating concept in organizational design. *Acad. Manag. Rev.* **1978**, *3*, 613–624. [[CrossRef](#)]
13. Bharadwaj, A.; El Sawy, O.A.; Pavlou, P.A.; Venkatraman, N. Digital Business Strategy: Toward a Next Generation of Insights. *MIS Q.* **2013**, *37*, 471–482. [[CrossRef](#)]
14. Guo, D.; Mantravadi, S. The role of digital twins in lean supply chain management: Review and research directions. *Int. J. Prod. Res.* **2025**, *63*, 1851–1872.
15. George, G.; Haas, M.R.; Pentland, A. Big Data and Management. *Acad. Manag. J.* **2014**, *57*, 321–326. [[CrossRef](#)]
16. Singh, B.; Dhawan, S.; Arora, A.; Patail, A. A View of Cloud Computing. *Int. J. Comput. Technol.* **2013**, *4*, 50–58.
17. Radziwill, N. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. *Qual. Manag. J.* **2018**, *25*, 64–65. [[CrossRef](#)]
18. Teece, D.J.; Pisano, G.; Shuen, A. Dynamic Capabilities and Strategic Management. *Strateg. Manag. J.* **1997**, *18*, 509–533. [[CrossRef](#)]
19. Eisenhardt, K.M.; Martin, J.A. Dynamic Capabilities: What Are They? *Strateg. Manag. J.* **2000**, *21*, 1105–1121.
20. Nasta, L. Understanding digital transformation in creative and cultural industries: A review. In *Navigating the Paradoxes of Digital Transformation in the Creative and Cultural Industries: Embracing Innovation*; Springer: Berlin/Heidelberg, Germany, 2025; pp. 7–22.
21. Agrawal, A.; Gans, J.; Goldfarb, A. *Prediction Machines: The Simple Economics of Artificial Intelligence*; Harvard Business Review Press: Boston, MA, USA, 2018.
22. McAfee, A.; Brynjolfsson, E. Big Data: The Management Revolution. *Harv. Bus. Rev.* **2012**, *90*, 60–68. [[PubMed](#)]

23. Bhaskaran, S.V.; Achar, S. A study of evolving cloud computing data security: A machine learning perspective. *Int. J. Prof. Bus. Rev.* **2025**, *10*, 5. [\[CrossRef\]](#)
24. Alzahrani, A.S.; Alahmadi, D.H.; Alharbi, N.M.; Almagrabi, H.A. Blockchain-based crowdsourcing framework for machine learning ground truth. *IEEE Access* **2025**, *13*, 73041–73055. [\[CrossRef\]](#)
25. Ivanov, D.; Dolgui, A.; Sokolov, B. The Impact of Digital Technology and Industry 4.0 on the Ripple Effect and Supply Chain Risk Analytics. *Int. J. Prod. Res.* **2018**, *57*, 829–846. [\[CrossRef\]](#)
26. Buczak, A.L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1153–1176. [\[CrossRef\]](#)
27. Misangyi, V.F.; Acharya, A.G. Substitutes or Complements? A Configurational Examination of Corporate Governance Mechanisms. *Acad. Manag. J.* **2014**, *57*, 1681–1705. [\[CrossRef\]](#)
28. Cockburn, I.M.; Henderson, R.; Stern, S. The Impact of Artificial Intelligence on Innovation: An Exploratory Analysis. In *The Economics of Artificial Intelligence: An Agenda*; Agrawal, A., Gans, J., Goldfarb, A., Eds.; University of Chicago Press: Chicago, IL, USA, 2019; pp. 115–146.
29. Saaty, T.L. *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*; McGraw-Hill: New York, NY, USA, 1980.
30. Ragin, C.C. *Fuzzy-Set Social Science*; University of Chicago Press: Chicago, IL, USA, 2000.
31. Rihoux, B.; Ragin, C.C. *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*; Sage: Thousand Oaks, CA, USA, 2009.
32. Arora, H.D.; Naithani, A. Empirical evaluation of Pythagorean fuzzy entropy measures with application in decision making. *Int. J. Inf. Technol.* **2024**, *16*, 1945–1954.
33. Dul, J. Necessary Condition Analysis (NCA) Logic and Methodology of “Necessary But Not Sufficient” Causality. *Organ. Res. Methods* **2016**, *19*, 10–52.
34. Dul, J.; Hauff, S.; Bouncken, R. Correction: Necessary condition analysis (NCA): Review of research topics and guidelines for good practice. *Rev. Manag. Sci.* **2023**, *17*, 1535–1537. [\[CrossRef\]](#)
35. Dul, J. *Conducting Necessary Condition Analysis*; Sage: London, UK, 2019.
36. Schneider, C.Q.; Wagemann, C. *Set-Theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis*; Cambridge University Press: Cambridge, UK, 2012.
37. Wagemann, C. Qualitative-comparative, set-theoretic and case-based methods. In *Handbook of Comparative Political Institutions*; Edward Elgar Publishing: Cheltenham, UK, 2024; pp. 51–64.
38. Breiman, L. Random Forests. *Mach. Learn.* **2001**, *45*, 5–32. [\[CrossRef\]](#)
39. Lundberg, S.M.; Lee, S.I. A Unified Approach to Interpreting Model Predictions. *Adv. Neural Inf. Process. Syst.* **2017**, *30*, 4765–4774.
40. Li, S.; Hu, S.; Tong, N.; Xie, W.; Tong, L.; Hu, S. How urban resilience shapes residents’ immediate emotions during heatwaves: A panel fuzzy-set qualitative comparative analysis (fsQCA)-based configurational analysis. *Sustain. Cities Soc.* **2026**, *136*, 107067.
41. Nambisan, S.; Wright, M.; Feldman, M. The Digital Transformation of Innovation and Entrepreneurship: Progress, Challenges and Key Themes. *Res. Policy* **2019**, *48*, 103773. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.