

Article

Internet Governance in the Context of Global Digital Contracts: Integrating SAR Data Processing and AI Techniques for Standards, Rules, and Practical Paths

Xiaoying Fu ¹, Wenyi Zhang ² and Zhi Li ^{3,*} 

¹ Xiangshan Film and Television Academy, Ningbo University of Finance & Economics, Ningbo 315175, China; fuxiaoying@nbufe.edu.cn

² School of Information Management, Nanjing University, Nanjing 210023, China; 602024140037@smail.nju.edu.cn

³ School of Media and Law, NingboTech University, Ningbo 315000, China

* Correspondence: lizhi@nbt.edu.cn

Abstract

With the increasing frequency of digital economic activities on a global scale, internet governance has become a pressing issue. Traditional multilateral approaches to formulating internet governance rules have struggled to address critical challenges such as privacy leakage and low global internet defense capabilities. To tackle these issues, this study integrates SAR data processing and interpretation using AI techniques with the development of governance rules through international agreements and multi-stakeholder mechanisms. This approach aims to strengthen privacy protection and enhance the overall effectiveness of internet governance. This study incorporates differential privacy protection laws and cert-free cryptography algorithms, combined with SAR data analysis powered by AI techniques, to address privacy protection and security challenges in internet governance. SAR data provides a unique layer of spatial and environmental context, which, when analyzed using advanced AI models, offers valuable insights into network patterns and potential vulnerabilities. By applying these techniques, internet governance can more effectively monitor and secure global data flows, ensuring a more robust defense against cyber threats. Experimental results demonstrate that the proposed approach significantly outperforms traditional methods. When processing 20 GB of data, the encryption time was reduced by approximately 1.2 times compared to other methods. Furthermore, satisfaction with the newly developed internet governance rules increased by 13.3%. By integrating SAR data processing and AI, the model enhances the precision and scalability of governance mechanisms, enabling real-time responses to privacy and security concerns. In the context of the Global Digital Compact, this research effectively improves the standards, rules, and practical pathways for internet governance. It not only enhances the security and privacy of global data networks but also promotes economic development, social progress, and national security. The integration of SAR data analysis and AI techniques provides a powerful toolset for addressing the complexities of internet governance in a digitally connected world.

Keywords: global digital contract; internet governance standards; internet governance rules; SAR data processing; AI techniques



Academic Editor: Aneta Poniszewska-Maranda

Received: 8 June 2025

Revised: 13 August 2025

Accepted: 15 August 2025

Published: 16 August 2025

Citation: Fu, X.; Zhang, W.; Li, Z. Internet Governance in the Context of Global Digital Contracts: Integrating SAR Data Processing and AI Techniques for Standards, Rules, and Practical Paths. *Information* **2025**, *16*, 697. <https://doi.org/10.3390/info16080697>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the increasing frequency of digital economic activities around the world, internet governance has become a pressing issue. Traditional multilateral rulemaking methods are unable to cope with key challenges such as privacy breaches and weak global network defense capabilities [1]. This study aims to solve the privacy protection and security problems in internet governance by integrating SAR data processing and AI technology, combining international agreements and multi-stakeholder mechanism governance rule-making in the context of global digital contracts, building a more accurate and scalable governance mechanism, and optimizing the standards, rules, and practice paths of internet governance [2].

Recent advancements in digital technology are catalyzing the emergence of new business models within virtual environments, particularly within the context of metaverses. This shift is giving rise to a new economy where traditional, physical-world business models are adapted, new virtual-world models are developed, and hybrid approaches that blend both are explored. The integration of these evolving business models with internet governance is crucial. It ensures that as businesses expand into virtual spaces, they do so within a framework that promotes transparency, security, and accountability, aligning with broader regulatory standards and contributing to the sustainable growth of digital ecosystems [3].

Digital twins are sophisticated digital models of assets that play a crucial role across the Industry 4.0 value chain. As industrial processes become increasingly digitized, the use of digital twins is expected to become more prevalent. Integrating digital twins with internet governance will enhance the oversight and efficiency of these technological advancements, ensuring they align with broader regulatory and operational frameworks. This integration will likely lead to more robust, transparent, and accountable digital ecosystems in various industrial sectors [4,5].

With the continuous development of the economy, the status of the internet has become increasingly important, but it has also triggered various network security risks. Therefore, how to improve the level of internet governance and establish reasonable governance standards and rules has become the focus of many scholars' research, and some research results have been achieved. Wang (2018) explored the role of the public in the debate on internet governance and linked public theory and technological research to internet governance, believing that they are of great help to stakeholders in internet governance [6]. White (2019) believed that the internet, as a facilitator of the peace-building process, had great potential and might become a tool for oppression or a channel for the dissemination of false information [7]. Therefore, studying internet governance is of great significance for international peace and stability. Tjahja et al. (2022) examined how individual participants identify themselves within the framework of the Internet Governance Forum and how they understand the internet governance ecosystem, based on the list of participants in the Public Internet Governance Forum, opening up a new path for further research on the legitimacy of multiple stakeholders [8]. Flonk (2020) analyzed the conflicts between norms and institutions in internet governance, helping to address the low level of institutionalization in dispute resolution in this emerging field [9]. For the development of internet governance rules, Malcic (2018) established a digital identity management system by utilizing a digital address allocation agency [10]. The system itself was the infrastructure of the global identity industry and used infrastructure configuration to connect global internet governance with the digital identity terminology data base. Guan (2019), considering the characteristics of the internet, conducted an experiment on the internet governance model with multiple stakeholders as the core, using internet startups as carriers [11]. He also posed challenges to the subject qualifications, operational rules, and other aspects of traditional sovereignty

models. In summary, many scholars have conducted various studies on the rules and standards of internet governance using different methods. However, these studies have shortcomings in areas such as privacy breaches and security. As a new type of contractual tool, global digital contracts have significant advantages in privacy protection and security, which can solve the problems existing in the aforementioned research.

As a new type of contract, digital contracts store and transmit contract content in electronic form, providing convenient, efficient, and secure signing and execution methods for all parties. Therefore, it has significant advantages in privacy protection and security and is also a current research hotspot. Zhang (2018) utilized the technical characteristics of digital financial assets to study the illegal behavior of digital currency and used digital contracts to study legislation in this area, improving the rationality of utilization and also improving the security of currency [12]. Jiang (2023) believed that global digital economy regulation has been continuously improved in practice [13]. Therefore, he used digital contracts to set basic rules to reflect national or regional characteristics, so as to strengthen industry compliance and fairness, improve data governance, and jointly formulate international rules. Wylde (2023) aimed to advance the United Nations' goal of "an open, free, and secure digital future for all" by reviewing the requirements of the Global Digital Compact in order to better address potential risks of the future internet [14], such as national isolation, sovereignty, and internet fragmentation, and enhance privacy protection efforts. Saravistha et al. (2022) discussed the issue of optimizing consumer protection in the context of new forms of contracts [15], where standard digital contracts and new cross-border market mechanisms coexisted in the business world to better protect consumer privacy. Ong (2021) conducted a comparative analysis and interpretation of the enforceability of digital contracts in contract law between New Zealand and Indonesia, using normative legal research to ensure the enforceability of digital contracts and improve legal security [16]. In summary, digital contracts have absolute advantages in terms of privacy protection and network security. Applying them to internet governance can effectively solve the current problem of low security in internet governance.

This study studies the standards, rules, and practice paths of internet governance, with the aim of exploring and analyzing how to effectively conduct internet governance under the framework of the global digital contract, including the formulation of appropriate standards, rules, and practice paths. Its goal is to create a transparent, fair, and stable network environment to support global social progress and the development of the digital economy. The main ways to achieve this goal include formulating laws, regulations, and standards for internet governance and using these laws and regulations to protect the security and privacy of users. Through international cooperation and multilateral consultation, differentiated privacy protection measures are adopted to maintain the privacy of members. It aims to promote the construction of a stable, fair, and transparent internet ecosystem and provide practical guidance and support for global internet governance.

To this end, this paper proposes the following hypotheses:

H1. *The governance model that integrates SAR data processing and AI technology will have significantly better encryption efficiency when processing data than traditional governance methods and can effectively improve the technical feasibility of internet governance.*

H2. *The user satisfaction of Internet governance rules formulated based on the multi-stakeholder mechanism (MSM) will be higher than that of rules formulated based on traditional methods such as multilateralism and international agreements and can better balance the interests of all parties.*

H3. *The internet governance standards constructed using the OSI model are superior to other governance standards in terms of rationality and applicability and can better meet the requirements for the uniformity and security of network protocols in the context of global digital contracts.*

2. Formulation of Standards and Rules for Internet Governance

2.1. Formulation of Internet Governance Standards

Internet governance is a standard for managing and using the internet formulated by multiple parties based on actual situations, aimed at regulating and promoting the development of the internet and forming consensus, legal regulations, technical norms, etc. [17,18]. The purpose of internet governance is to enable the development of the internet to benefit various countries and fields and to benefit the world. With the help of Abood Amany et al. (2021) and Wang et al. (2018), the hierarchy of Transmission Control Protocol/Internet Protocol (TCP/IP) for internet transmission is studied, and internet governance standards are created based on different functions at different levels [19,20]. The summary is shown in Table 1.

Table 1. Functional tasks and behaviors of internet governance.

Functional Area	Task	Main Behavior Subject
Key internet resources	Central supervision of domain names and addresses	Number internet name and word address allocation agency, the internet number administration
	Technology and design of IP addresses	Internet engineering task force
	Domain name allocation	Internet registration authority
	Automatic digital distribution system	Internet numbering authority and regional internet registration
	IP address allocation	Regional internet registration, local internet registration, internet numbering authority
Setting up internet standards	Protocol number distribution	Internet numbering authority
	Core internet standard design	Internet engineering task force
	Core web page standard design	Internet alliance
Access and connection coordination	Multi-layer network interconnection	Internet exchange center and network operator
	Network management	Private network operator
	Access management	National government
Network security governance	Network infrastructure security	Operator
	Encryption standard design	Standard-setting agency
	Network security management	National governments and multilateral protocols
	Software security vulnerability repair	Software company
	Software patch management	End user
	Routing and address security	Operator and registrar
	Website security certification	Certification body
Information transmission	Commercial trading institutions	E-commerce agency
	Content review	Search engines and social media
	Private policy	Social networks and service providers
	Manage privacy and speech	Law and constitution

As shown in Table 1, the functions and tasks of network governance are divided into five aspects, mainly including key internet resources, internet standard setting, access and connection coordination, network security governance, and information transmission.

These five aspects are subdivided, and then the behavioral objects of these subdivided subjects are introduced.

Internet governance requires the development of a series of technical standards to ensure the security, stability, and interoperability of the internet in order to ensure the relevance and interoperability of digital contracts. The global digital contract proposes requirements to support network security to prevent network attacks and data leakage. Internet governance standards should include the best practices and technical standards for cybersecurity to help protect the cybersecurity of online users and various international organizations. Among them, network protocol is a special communication standard designed by humans to improve communication, helping global digital contracts better manage the internet. Due to special needs, based on the research on network protocol standards [21–23], the details of internet protocols were identified and extracted. Network protocols often use specific formats, and identifying these fixed features can help analysts identify formats and protocol types, analyze protocol types and formats, and differentiate content. The schematic diagram of the internet protocol architecture is shown in Figure 1.

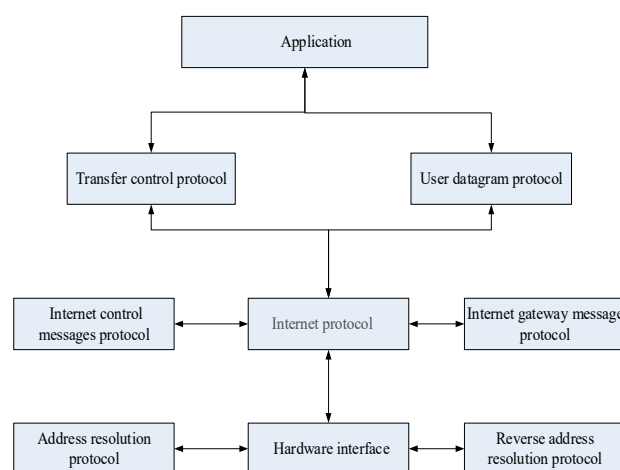


Figure 1. Schematic diagram of internet protocol architecture.

As shown in Figure 1, the composition of protocols on the internet is often tree-shaped. Any high-level application layer protocol relies on the existence of lower-layer protocols, and in front of each application layer message, there are several lower-layer protocol frame headers. Therefore, the prerequisite for parsing high-level protocols is to first parse low-level protocols. Different data frames of the same protocol often have similar structures. Therefore, they can be compared and processed by searching for similarities between them.

In order to facilitate better communication between different parts of the network on the internet, an open communication model is studied using the standards proposed by ISO, which is known as the OSI model (Open System Interconnection model). It is used to study the most important standard in internet governance standards, namely, network protocols. The OSI model can divide the communication process of the internet architecture into seven layers from bottom to top, with interfaces used to communicate between each layer, maximizing the utilization of internet network protocols and helping to better govern the internet in the future. Figure 2 shows the ISO/OSI of the network protocols corresponding to each layer in the OSI model.

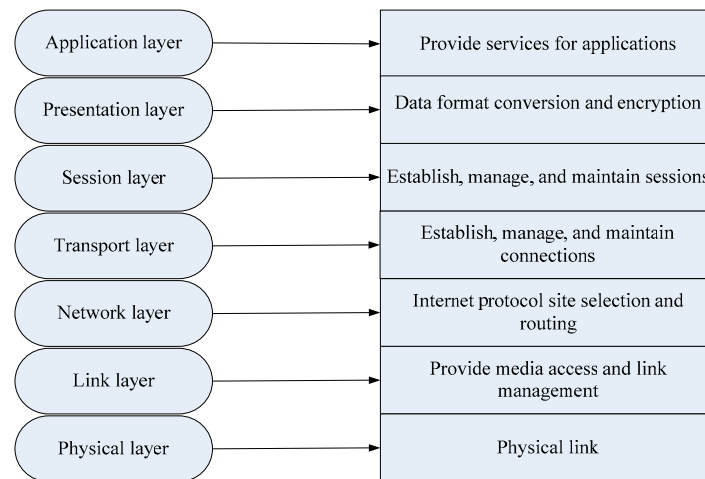


Figure 2. ISO/OSI of network protocols corresponding to each layer in the OSI model.

As shown in Figure 2, the main steps for designing and creating network protocol models based on different levels are as follows. Firstly, with the emergence of demand for internet governance business and the growth of data processing volume, the complexity of management and operation is also increasing exponentially. Adopting a layered system makes it easier for operation and maintenance personnel to maintain and develop the internet in the future. Next, operations are standardized to enable different products to communicate according to the same communication standard. Unknown processes built in unknown environments can also follow the same hierarchical process, but the process structure of each layer may differ from the hierarchical standards of governance on the internet. Data frames are the foundation of communication between link layers, and all content above the link layer in a network is ultimately encapsulated in frames layer by layer.

SAR data has unique spatial and environmental contextual characteristics. By capturing geospatial information, network infrastructure distribution, and environmental interference factors, it can provide a correlation perspective between the physical layer and the network layer for internet governance. SAR data can reflect the geographical distribution density of global network nodes, the environmental risks of submarine cable routes, or the correspondence between the physical location of cross-border data centers and the scope of sovereign jurisdiction. After being processed by AI technology, this information can be converted into an assessment basis for the vulnerability of network topology, the physical path risks of cross-border data flow, and the security of infrastructure, thereby providing data support for the formulation of targeted governance rules. This connection extends internet governance from a purely digital level to a “physical–digital” fusion dimension, enhancing the spatial accuracy and risk predictability of governance.

2.2. Transformer Architecture in SAR Data-Driven Applications

The Transformer architecture can effectively process the spatial characteristics and temporal dynamic changes in the network infrastructure in SAR images by virtue of its self-attention mechanism’s ability to capture long-distance dependencies, providing technical support for network security governance. In the SAR image feature extraction and infrastructure identification process, an improved Vision Transformer (ViT) model is used to segment SAR images into fixed-size image patches based on the scattering characteristics of facilities such as base stations and data centers. The spatial location information is retained through linear embedding and position encoding, and the multi-head self-attention mechanism is used to calculate the association between patches and

extract key features such as the geometric shape and scattering intensity of the facilities. The feature extraction process can be expressed as

$$Embedding_i = Linear(Patch_i) + Positional\ Encoding(i) \quad (1)$$

$$Feature_i = MultiHeadAttention(Embedding_i, Embedding_j) \quad (2)$$

Among them, $Positional\ Encoding(i)$ ensures that the model captures the spatial position relationship of image blocks, and $MultiHeadAttention$ strengthens the focus on features such as facility edges and signal coverage, thereby achieving accurate positioning and classification of network infrastructure.

In terms of time series analysis and load pressure prediction, we combined historical SAR data and network traffic data to build a time series Transformer model. This model captures the dependencies in the time dimension through the self-attention mechanism, and the prediction formula is

$$Load_t = Transformer(Feature_{t-1}, Feature_{t-2}, \dots, Feature_{t-n}) \quad (3)$$

Among them, $Feature_{t-k}$ is the fusion vector of SAR features and network traffic features at the $t - k$ th moment. By setting the load threshold θ , when $Load_t > \theta$, the load overload warning is triggered, providing a basis for resource scheduling and improving the foresight of network governance.

2.3. Formulation of Internet Governance Rules

Internet governance should establish a comprehensive and inclusive set of rules to manage all aspects of the internet. The content involved in global internet governance is very rich. For these contents, some have already existed before the emergence of the internet, and others have occurred after the emergence of the internet. Therefore, it is necessary to conduct research on internet governance rules in the context of global digital contracts based on this characteristic. Firstly, it is necessary to divide the problems, and then collect, combine, and derive governance rule elements based on the impact of existing problems. The main rules of global internet governance include six aspects, as shown in Figure 3. Among them, key resource management, network, and security are special rights of the internet. Intellectual property protection is an extension of existing internet rights. With the development of the internet, specialized internet rules are gradually being established, and the extension of existing rules to the internet is constantly deepening.

As shown in Figure 3, the management of critical resources includes root server management, IP address allocation, and domain name resource allocation and management. At the same time, the participants in the formulation of key resource management policies include a wide range of sectors, such as the private sector, the public sector, governments, and international organizations. Economic trade and market competition: Due to the growth of internet e-commerce and communication networks, business, marketing, and market competition are becoming more complex, and these complexities are reflected on the internet. The purpose of all parties has expanded from professional standards and key resource management to cross-border internet business, e-commerce, and other businesses.

At present, most of the rules in Figure 3 are extensions of the relevant rules formulated by the World Trade Organization on the internet, as well as protocols reached in bilateral and multilateral negotiations. In order to better study the rules of internet governance, utilizing the MSM to institutionalize rules in the context of global digital contracts is a way or approach to solve problems [24,25]. The MSM typically requires the participation of government agencies, private organizations, civil society groups, and international organizations to negotiate and formulate internet rules. Therefore, in the context of the

global digital contract, the MSM is used to formulate internet governance rules, which can take into account the interests and requirements of all parties, follow the jointly formulated governance rules and norms, and adopt the same solution measures for problems in the same field through activities. The multiple-stakeholder mechanism is shown in Figure 4.

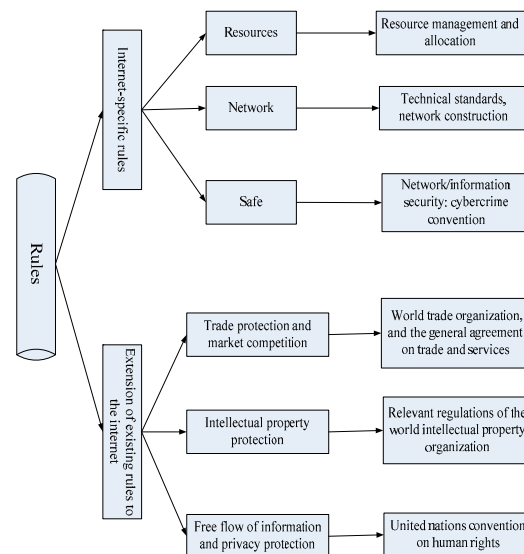


Figure 3. Attribute classification of international internet governance rules.

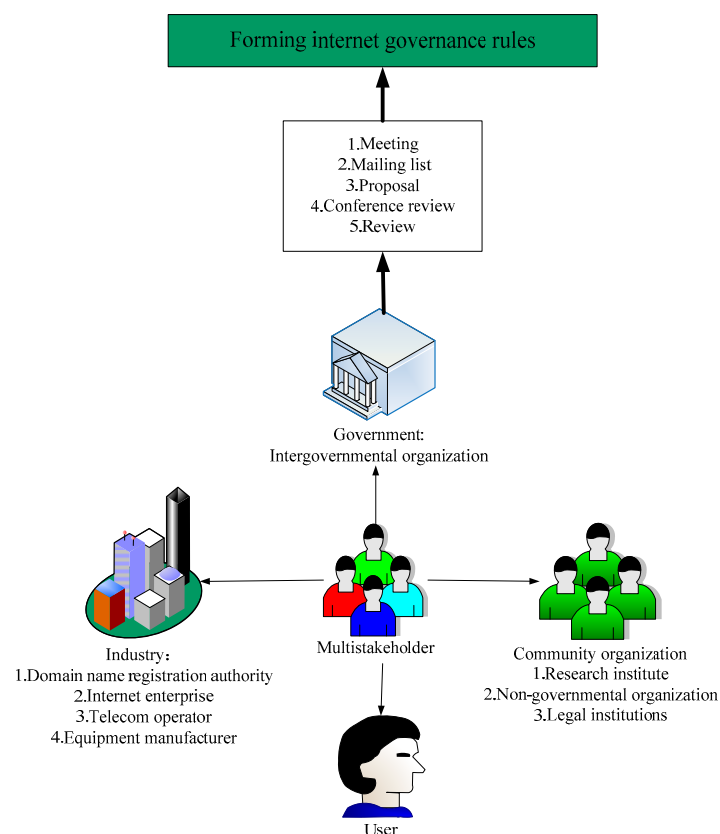


Figure 4. Internet governance based on multiple-stakeholder mechanisms.

The formation of the core rules of the internet is determined by the participation of multiple stakeholders and follows established processes. As shown in Figure 4, the openness of non-governmental platforms is generally very high, and all governments, organizations, enterprises, and individuals worldwide can participate in activities on non-

governmental platforms. On this platform, all parties participate in the formulation of rules and regulations in a certain way and procedure. The processes and procedures they follow include multiple ways and means.

The use of multilateral mechanisms has always been a common practice among governments around the world in international trade events. Although there have always been voices in the internet community opposing the use of multilateral mechanisms to formulate internet governance rules, governments of various countries are representatives of the public interest, and their mission is to provide public services and safety for their own people, safeguard their legitimate rights and interests, and ensure that the public can use the internet safely and reliably. Therefore, in some areas of internet governance rulemaking, multiple approaches still need to be taken. However, for different levels of problems, different decisions should be appropriately chosen. For example, the government should play an important role in policymaking in areas such as managing critical internet resources, maintaining cybersecurity, preventing cybercrime, and protecting citizens. According to the above analysis, the “multilateral mechanism” and the “multi-stakeholder” mechanism are not mutually exclusive. As long as they are properly operated, both can play a role and effectively address the complex issues of the global internet.

In global internet governance, the importance of specific internet rules is higher than the extension of existing internet rules. Among the special rules of the internet, the rules of internet resources are more important as they are the foundation for the development of the internet. Therefore, the special rules of the internet are the main rules of the global internet, and the key resource rules of the internet are the core rules of international internet governance. The quadrant diagram of global internet governance rules and methods is shown in Figure 5.

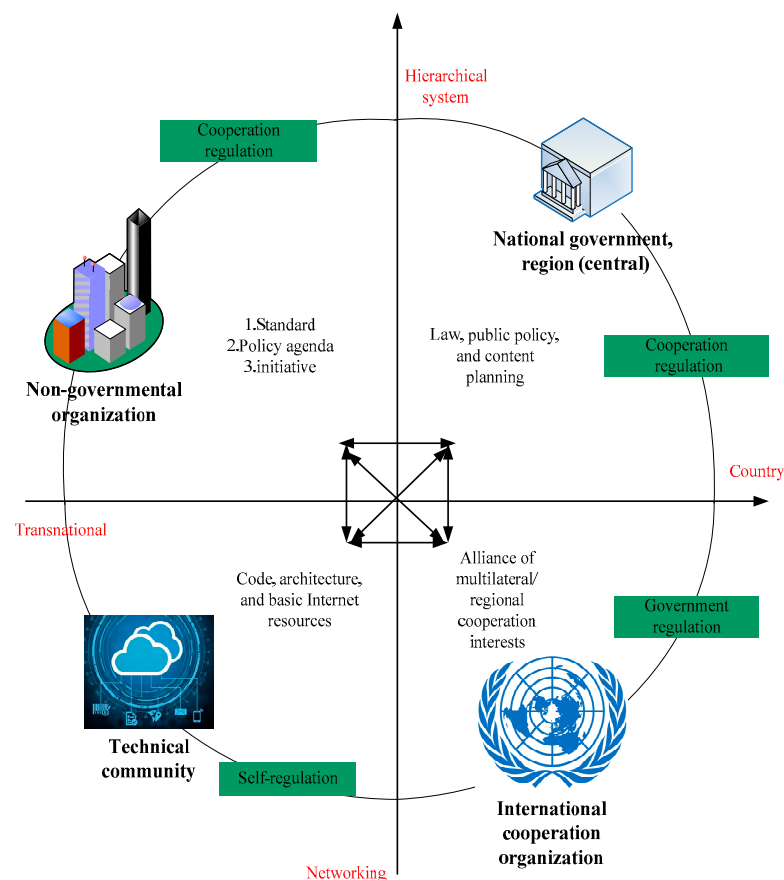


Figure 5. Quadrant diagram of global internet governance rules and methods.

As shown in Figure 5, by setting up management platforms and governance rule categories horizontally and vertically, a four-quadrant analysis matrix can be obtained to analyze the main controls and their corresponding regulations mentioned above. It can be seen that in the formulation of governance rules in some special areas of the internet, the number of government cooperations is limited, while the scale of non-intergovernmental platforms is still very large. Many non-governmental platforms have specific rights on the internet, responsible for developing internet resources and formulating network technology standards and rules. Unlike the organizational approach and rules of intergovernmental platform processes, the cooperation approach of non-governmental platforms involves all stakeholders, and their organizational approach and rulemaking are often based on the principle of multiple stakeholders.

2.4. Legal and Policy Development

Creating and developing a legal and policy framework that adapts to the global digital contract can protect user privacy and data security, enable internet governance legislation to have relatively high liquidity, and enable legislation to involve data protection laws, cybersecurity laws, digital identity verification systems, and more. Legal reform is a way of social change, but as a relationship with the implementation of national coercive force, it has stability and lag. In contrast, the internet seeks more innovation, and the governance ideas and methods of internet platforms are adjusted according to the new models and functions that have emerged on the internet. Therefore, legal regulations are very limited in the field of the internet, and it is necessary to find ways to ensure that they can help internet governance play its due role and make up for the failure of platform governance. Among them, the most important task is to address the legal issues related to internet governance, as shown in Table 2.

Table 2. Legal issues in internet governance.

Number	Legal Dilemma	Category	Explain
1	The dilemma in legislation	Lawmaking lags behind the development of internet governance	The legal system of network governance is still being improved.
		Imbalance of rights of the internet governance platform	1. There is a lack of statutory rules to divide the power of different attributes. 2. The scientific structure of the authority and responsibility of the network platform is lacking.
2	The dilemma of regulatory enforcement	There is a problem with the supervision system of administrative outsourcing	1. The division of authority within the government is not clear. 2. Regulatory and law enforcement agencies are not scientific enough in setting up.
		Imperfect regulatory mechanism	The prevention mechanism is not sound.
		Complex regulatory and law enforcement environment	1. Sufficient culture of the rule of law in cyberspace has not been established. 2. The pattern of collaborative governance of network information content needs to be strengthened.
3	Insufficient privacy protection	Data collection infringes on citizens' privacy rights	Internet platforms pose a threat to users' privacy rights during data collection.
		Governance platform infringes on privacy	With the continuous development of the internet, violations of rights that have brought physical and mental trauma to different groups of people are more common, infringing on the privacy rights of consumers.
		Problems in the data security protection phase	The instability of the internet has led internet companies to infringe on consumer privacy.

As shown in Table 2, there are many problems in the process of internet governance, which are not conducive to the formulation of laws and regulations related to internet governance. In order to address the above issues, it is necessary to leverage the global digital contract to help laws better safeguard the privacy of users in various countries and protect personal and national information through new forms of contracts. At the same time, it also helps global networks to share and develop, allowing multiple parties to participate in the formulation of internet governance laws and regulations and formulate more reasonably and in line with the development of the internet. The specific measures are as follows.

2.4.1. Privacy Protection

In the process of internet governance, public privacy protection is very important [26]. In the process of collecting network data, it is necessary to improve data protection work and expand the scope of protection laws based on the primary protection of user data rights. In the process of protecting users' right to know, more effective ways should be created to clarify data content, while rejecting the use of personal data as an additional condition for customers' right to refuse. It is also necessary to enhance the ability to handle erroneous information and enhance the ability to collect information by modifying or deleting learning materials. In addition, the public's willingness to seek security in online information governance can affect competition in the internet market, thereby encouraging the internet industry to meet higher security standards, enhance privacy protection, and meet customer needs [27].

2.4.2. Personal Information Protection

Personal information security is the most important security requirement for users on internet platforms and also the most concerning issue for internet users [22]. Internet platforms are indeed unable to fulfill their responsibility to protect users' personal data. When the number of internet platform users is large, various internet platforms may face public security issues in terms of personal information protection. Therefore, in the context of the global digital contract, it is necessary to better govern the internet through various means and legislative methods to protect personal information, taking China as an example. In order to successfully govern the internet and combat crime, China saves information about its citizens in internal public security institutions. Public information is held by government departments, and citizens are very confident about it. However, with the development of the internet, the information about users on the internet is also more complex and ever-changing. Therefore, relying solely on internet platforms for user data protection cannot guarantee user data security. In this case, legal regulations are needed to address issues related to user information security.

3. Practical Path of Internet Governance

3.1. International Cooperation and Multilateral Consultation

International cooperation is crucial for global internet governance in the context of the global digital contract. Countries should strengthen international cooperation, formulate rules and standards through mutual consultation and cooperation, and solve cross-border internet problems. International organizations such as the United Nations and the World Trade Organization play an important role in internet governance. Under the influence of the global digital contract, international cooperation has been utilized to study the implementation of internet governance practices, mainly in the following three steps. Firstly, the private sector, the internet technology community, and individual citizens are united to negotiate multiple interests. Secondly, developing countries should

use multilateral consultations and combine with international organizations such as the United Nations to govern the internet. Thirdly, developed countries collaborate with their own governments and citizens to carry out internet governance through a multi-agent governance approach.

Utilizing multilateralism is a way to address various common human challenges, resolve international conflicts, and provide good guarantees for global internet governance [28]. As the most representative and authoritative international government in the world today, the United Nations should be the best place for the international community to practice many things. After years of competitive gaming in internet governance, technological standards and key internet resources are still held by a few developed countries, while developing countries are still in an unequal position in technological standards and related governance. Therefore, international governance of the internet should pay more attention to fairness and justice, involve more participants, and establish accountability mechanisms and legal frameworks. By utilizing multilateralism, it is easier to help the global internet formulate governance practice rules and paths. At the same time, due to the multilateral system of the United Nations, the universal support of all member states has been received, and the internet governance rules designed for international standards have unique authority.

3.2. Data Privacy Protection

Standards and rules related to privacy protection have been established to ensure the proper storage of personal information and data involved in digital contracts. Differential privacy (DP) is a method of protecting privacy in cryptography, with the goal of creating a method that improves the accuracy of requested information while collecting as much information as possible and reduces the likelihood of recording errors when searching for data [29,30]. In other words, while ensuring commonality, personal characteristics are removed to maintain the privacy of internet users. DP's privacy protection mainly relies on accurate data provided by information providers when attackers impersonate users. Based on this, the user's original privacy data is inferred. Based on the inferred results, a pattern of adding different types of noise interference to the original privacy data has been derived to achieve data modification, thereby preventing internet attackers from obtaining effective data and protecting the privacy of internet users. Using DP can predict the future development trend of internet privacy management. It can also protect various types of privacy of internet users, predict the probability of attackers attacking, and further propose methods to prevent such predictive inference attacks, thereby better governing the internet.

The core terms used in this study are defined as follows: "Privacy budget" refers to a total threshold for measuring privacy leakage risks in differential privacy protection, which controls the degree of data perturbation; a smaller value indicates a higher level of privacy protection. "Global sensitivity value" represents the maximum difference in the output results of the same query function between adjacent datasets, serving as a key parameter to determine the amount of noise required for privacy protection. "Global Digital Compact" is a UN-led international cooperation framework aimed at establishing open, secure, and inclusive digital governance rules through multilateral negotiations to address global issues such as the digital divide and data security. "Certificateless Cryptography (CC) algorithm" is an encryption technology that enables key management without certificates, ensuring secure data transmission through the collaborative generation of users' public keys and partial private keys.

By adding noise to the output results of the original data, it is ensured that even if the data in the original data is deleted or changed, the results are still generated, and the results are the same as the actual results. The specific expression is

$$Pr[N(X_1) \in Q] \leq \exp(\mu) * Pr[N(X_2) \in Q] \quad (4)$$

Among them, Q represents a possible set of outputs, and μ represents privacy budget parameters. From the formula, it can be seen that the smaller the privacy budget μ , the higher the degree of privacy protection.

Differential privacy mainly protects the personal information of users in the data by adding some noise, which is very important for noise control. It is necessary to protect user privacy while avoiding too much noise affecting the effectiveness of data usage. The expression for calculating the global sensitivity of noise is as follows:

$$SF_k = \max_{X_1, X_2} \|k(X_1) - k(X_2)\|_1 \quad (5)$$

When the global sensitivity value is high, a large number of noises need to be added to the function query results to confirm the user's identity, resulting in poor data availability.

The amount of noise is very important. The amount of noise in the dataset can cause too much interference, resulting in the unavailability of the data. The noise density is

$$q(j) = \frac{1}{2\gamma} \exp\left(-\frac{|j|}{\gamma}\right) \quad (6)$$

Among them, $\gamma = \Delta k / \mu$. The amount of noise is directly proportional to the value of function sensitivity Δk and inversely proportional to privacy budget μ . γ represents the noise density parameter, which is determined by the function sensitivity Δk and the privacy budget μ . j represents the discrete index value in the noise sequence, which is an integer, used to quantify the distribution state of the noise; i represents the number of iterations or sample index, which is a positive integer and represents the budget share of the i -th iteration in the privacy budget allocation.

When calculating the privacy budget under a fixed number of iterations scenario, the implementation method is to evenly allocate the privacy budget in each iteration, that is, h value, $0 < h < 1$. When the initial budget allocation is determined, the entire budget sequence is fixed and adjustable and meets the requirements of differential privacy protection. The privacy budget allocation formula is shown in Formula (4), and the evaluation function is shown in Formula (5).

$$\mu_i = \frac{h\mu}{(i-1)!} \left(\ln \frac{1}{h}\right)^{i-1}, i \in N^+ \quad (7)$$

$$F(n) = \sum_{j=1}^n \left(\frac{1}{\mu_i}\right)^2 = \frac{1}{h^2 \mu^2} * \sum_{j=1}^n \left(\frac{[(i-1)!]^2}{\left(\ln \frac{1}{h}\right)^{2(i-1)}}\right)^2 \quad (8)$$

Among them, μ_i is the privacy budget for each score search, and μ is the total budget.

With the continuous development of the internet, personal and national information is easier to publish on the internet. In the context of global digital contracts, understanding privacy protection in internet governance is crucial. In order to ensure data security during data transmission, the use of cryptographic technology has been strengthened in practice. A secure and effective certificate without a signature can be established based on the Certificateless Cryptography (CC) system [31]. When generating partial private keys, this scheme uses a secure hash function to bind the user's public key with the generation of partial private keys, making it impossible for attackers to delete the results of the hash function by changing the user's public key. By analyzing the effectiveness of this strategy, compared with other strategies, it is found that this strategy reduces the number of bilinear and exponential operations, improves computational efficiency and accuracy, and reduces

communication overhead, ensuring that data can only be accessed and used by authorized individuals.

This method continuously optimizes the virtual gradient value to approach the real gradient value, which can make the virtual data approach the user's real data. The formula is as follows:

$$(a^*, b^*) = \underset{a', b'}{\operatorname{argmin}} \|\nabla M' - \nabla M\|^2 = \underset{a', b'}{\operatorname{argmin}} \left\| \frac{\delta \vartheta(H(a', M), b')}{\delta M} - \nabla M \right\|^2 \quad (9)$$

When virtual gradient $\nabla M'$ continuously approaches real gradient ∇M , the false information created by malicious attackers approaches the user's true information, leading to indirect leakage of user privacy to the attacker.

Each participant negotiates keys with other participants to generate a joint mask, and then the local gradient parameters are converted. The specific expression is as follows:

$$\hat{m}_i = m_i + \sum_{j \in V: i < j} \operatorname{PRG}(f_{i,j}) - \sum_{j \in V: i > j} \operatorname{PRG}(f_{i,j}) \quad (10)$$

The server receives gradient parameters from various participants but cannot obtain the correct gradient parameters from the user. Therefore, attackers are unable to recover the user's data, thereby ensuring the privacy and security of the user's data.

Differential privacy controls the risk of privacy leakage by adding noise, and the CC algorithm improves encryption efficiency by optimizing key management. These technologies provide practical tools for the ongoing research on "Data Security Governance under the Global Digital Contract Framework".

3.3. Transparency and Accountability

On a global scale, the number of international internet governance platforms is constantly increasing, and these governance platforms are all different. Choosing the correct partitioning method is a necessary foundation for using governance platforms to govern the internet. When a user conflicts with a platform company, the government and industry need to supervise the governance policies formulated by the platform company to protect the legitimate rights of users. In order to urge users to consciously comply with market behavior, the government and public organizations should clarify the boundaries of governance, jointly improve policies, and create a healthy online environment. The governance mechanism diagram of the internet supervision platform is shown in Figure 6.

To ensure more openness and transparency in internet governance, an internet governance supervision platform is established to monitor the behavior and information of internet service providers. Platform enterprises need to create business information networks, connect key personnel, and carry out a series of value activities. At the same time, in order to better govern the behavior of various groups, enterprises can develop a comprehensive policy system as operators and supervise as platform supervisors to ensure the effectiveness of policy implementation and timely revise and supplement the governance policy system. Due to the virtual nature of the internet, governance is mainly achieved through the unilateral formulation of governance rules by enterprise platforms in order to avoid attacks from other platforms and solve the problem of threats to user information caused by significant changes in the macro environment. By analyzing Figure 6, it can be seen that creating a cohesive business and a strong business ecosystem requires the platform to maintain a high degree of neutrality in overseeing governance policies during formulation and implementation.

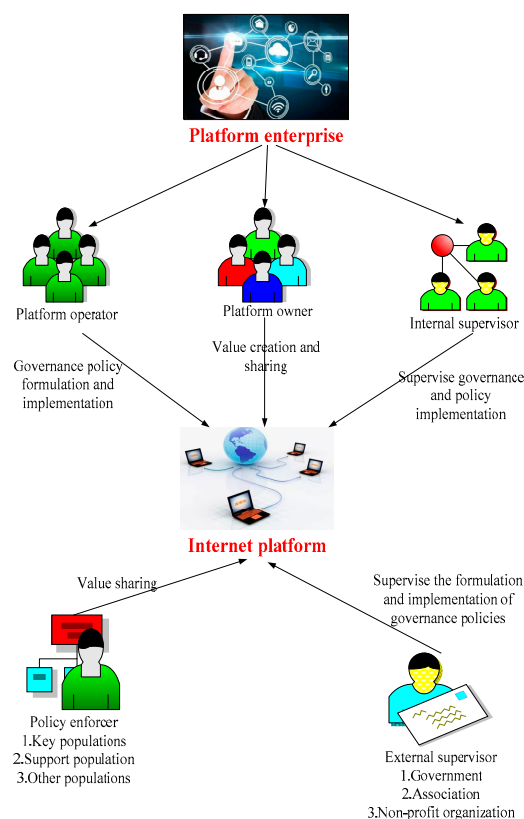


Figure 6. Governance mechanism of internet supervision platform.

4. Experiments Related to Internet Governance

The term “Software updates over the Air”, or “SOTA”, describes the updating of apps via communication without establishing a connection with the programmer. For the following reasons, nevertheless, it is not appropriate for internet administration within the framework of the Global Digital Compact: (1) there are several domains and tiers involved in internet governance under the framework of the global digital agreement. The SOTA baseline approach finds it challenging to completely address all facets of internet governance because it primarily concentrates on the most recent advancements and industry best practices in a certain subject or technology. (2) The process of internet governance is dynamic in nature, with new practices, laws, and technologies always emerging. It is challenging to modify the SOTA baseline method to accommodate the quickly evolving governance environment since it frequently concentrates on summarizing and evaluating currently used technology and processes. (3) The game of internet governance requires the cooperation and coordination of several parties. Effective solutions are hard to come by when using the SOTA baseline approach, which typically solely concentrates on technical and practical problems while neglecting the demands and conflicts of interest of stakeholders. (4) A wide range of considerations, including social impact, economic cost, and technical viability, must be thoroughly taken into account when governing the internet. The SOTA baseline approach frequently ignores the impact of other elements in favor of concentrating solely on the development and efficacy of technology, making it challenging to offer thorough direction and assistance for internet governance.

The OSI model, multilateralism, international agreements, and traditional methods, as core elements of internet governance, have three significant commonalities: First, they all have “regulating network behavior and ensuring interconnection” as their core goal, aiming to solve the problem of disorder in cyberspace through a standardized framework or rule system. Second, they rely on a multi-subject participation mechanism. Whether

it is the layered collaboration of the OSI model, the intergovernmental coordination of multilateralism, or the cross-border cooperation of international agreements, they all emphasize the division of rights and responsibilities among multiple parties. Third, they have certain timeliness limitations. With the iteration of the digital economy and technology, their adaptability to new issues such as privacy protection and cross-border data flow has gradually decreased, and it is necessary to improve governance effectiveness through innovation and optimization.

A questionnaire survey was conducted among all users, primarily collecting user ratings through scoring. The user rating scale uses a 1–10 scale, with 1 representing the lowest rating and 10 representing the highest. Scores are determined based on users' actual experience, understanding, and needs regarding internet governance standards/rules. Specifically, the scores cover three core dimensions: satisfaction, reflecting users' recognition of the standards/rules' effectiveness in protecting privacy and balancing the interests of all parties; practicality, measuring the operability of the standards/rules in actual internet governance scenarios; and applicability, assessing their alignment with the Global Digital Compact framework, including whether they are adapted to the economic development levels of different regions and meet the differentiated needs of multiple stakeholders. During the scoring process, users independently rated the governance standards/rules under different models based on their own experience in internet usage, governance practices, or research. The average value was then calculated to present an overall evaluation.

The experimental data for this article comes from a randomly selected user sample from an international online research platform. This sample covers regions with varying levels of economic development worldwide, taking into account the proportion of users in both developed and developing countries. The sample is categorized by identity, including individual users, internet company technicians, government network regulators, and academic researchers. All participants signed informed consent forms to clarify their understanding of internet governance rules. Data selection strictly adhered to the principles of coverage and randomness, excluding samples with regional or identity biases. During data processing, statistical analysis was performed on user ratings, and averages were calculated to reflect user evaluations of different governance models. For algorithm performance testing, the performance of different algorithms was compared on metrics such as encryption time and feature extraction accuracy, by controlling for variables such as data volume, to ensure that the data effectively supports the rationality of the experimental conclusions.

This article used digital contracts and the OSI model to study global internet governance standards. For this purpose, 15 internet users were randomly selected, and the governance standards studied in this article were rated with a score of 1–10. The higher the score, the higher the level of evaluation and satisfaction. In order to better demonstrate the superiority of the OSI model, the experimental results were compared and analyzed with internet governance standards based on multilateralism, international protocols, and traditional methods (that is, before using the OSI model). The specific results are shown in Table 3.

As shown in Table 3, different models were utilized to study internet governance standards. Through the comparison of experimental results, it can be found that in the context of global digital contracts, the OSI model was used to formulate internet governance standards. The user rating was much higher than the internet governance standards developed based on other methods. Among them, the user rating of the internet governance standard based on the OSI model was above 8.99 points, and the average score of 15 users was 9.2 points. The internet governance standards based on multilateralism, international protocols, and traditional methods had user ratings below 8.91, 8.96, and 8.71, respectively, and the average scores were 0.6, 0.54, and 0.72 points lower than the internet governance

standards studied in this article. The average user rating of internet governance standards developed using the OSI model in this article was the highest compared to traditional methods. This once again indicates that in the context of global digital contracts, using the OSI model to study internet governance standards can effectively improve the rationality of governance standards. The opinions of multiple parties are integrated to develop more scientific governance standards, so that the global internet can be shared more securely.

Table 3. User ratings of internet governance standards under different models.

Number	OSI	Multilateralism	International Protocol	Traditional Method
1	9.2	8.4	8.5	8.2
2	9.3	8.5	8.6	8.6
3	9.4	8.5	8.8	8.4
4	9.3	8.7	8.5	8.6
5	9.2	8.9	8.5	8.6
6	9.1	8.8	8.85	8.5
7	9.1	8.8	8.95	8.4
8	9.1	8.4	8.8	8.3
9	9.3	8.6	8.6	8.6
10	9	8.7	8.75	8.4
11	9.1	8.7	8.85	8.5
12	9.2	8.6	8.4	8.5
13	9.2	8.5	8.65	8.6
14	9.3	8.5	8.45	8.7
15	9.2	8.4	8.7	8.3
Average value	9.2	8.6	8.66	8.48

In the context of the global digital contract, the rules of internet governance were studied. By utilizing digital contracts and combining multiple-stakeholder mechanisms (MSMs), global internet governance rules were studied. For this purpose, 20 internet users were randomly selected, and the governance standard rules studied in this article were rated with a score of 1–100. The higher the score, the higher the level of evaluation and satisfaction. In order to better demonstrate the superiority of the MSM model, the experimental results were compared and analyzed with internet governance rules based on multilateralism, international protocols, and traditional methods (that is, before using the MSM model). The specific results are shown in Figure 7.

In Figure 7, the x-axis represents different governance rule models, and the y-axis represents the scores scored by users. The dotted elements in the figure represent the specific scoring of the 20 internet users selected, and the horizontal line in the middle represents the average scoring of these 20 users. As shown in Figure 7, it can be clearly observed that in the context of global digital contracts, user ratings for internet governance rules formulated using the MSM model were much higher than those based on other models. Among them, the rule users based on the MSM model scored above 91.49 points, and the average score of 20 users was 93.3 points. However, users scored governance rules based on multilateralism, international protocols, and traditional methods below 91.01 points, 89.01 points, and 86.51 points, respectively. The average score of 20 users was 6.3 points, 6.55 points, and 10.7 points lower than the average score of users based on the MSM model.

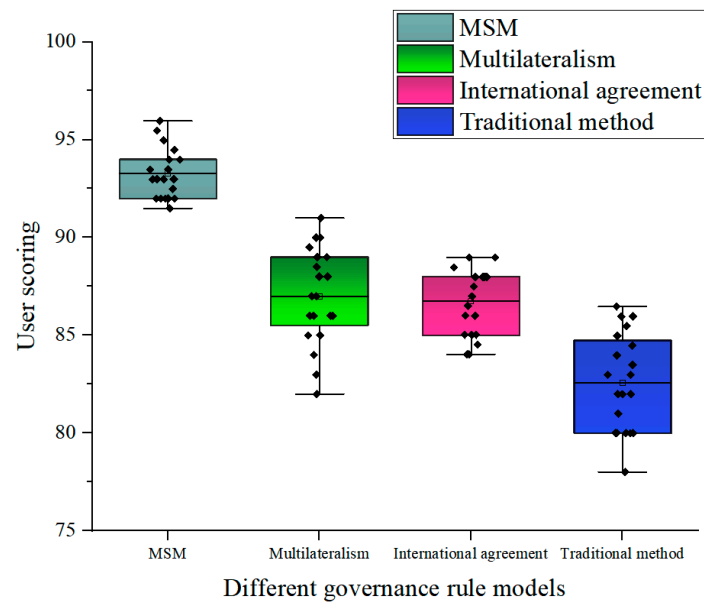


Figure 7. User ratings of internet governance rules formulated under different methods.

In the practical path of internet governance, special attention should be paid to the privacy protection of internet data. In the context of the global digital contract, the Certificateless Cryptography (CC) algorithm was utilized to encrypt data generated during the practice of internet governance. This has not only enhanced privacy protection and the security of internet governance but also increased the speed of encryption and saved encryption time. In order to further demonstrate the superiority of internet data encryption based on the CC algorithm, the experimental results obtained were compared with the Data Encryption Algorithm (DEA), Homomorphic Encryption (HE), and Secure Hash Algorithm (SHA). The comparison results are shown in Figure 8.

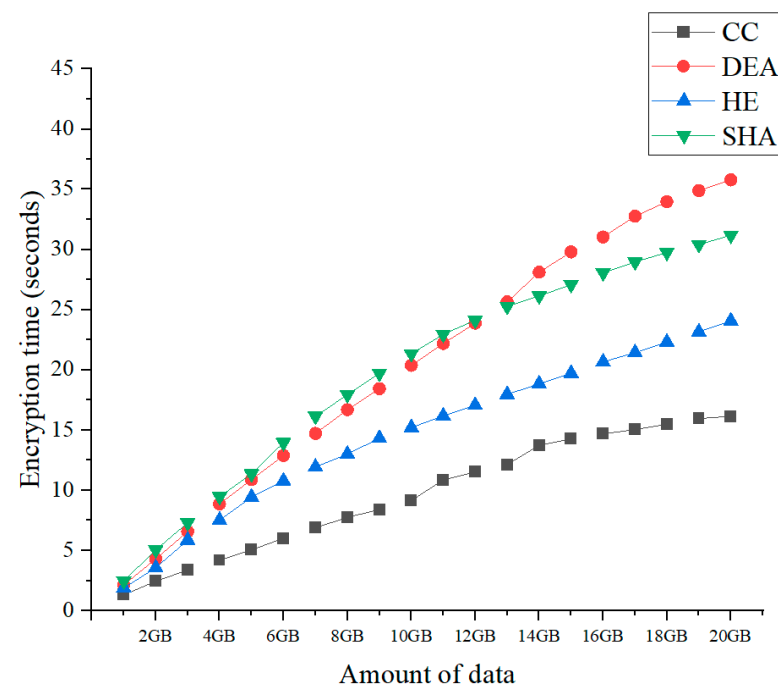


Figure 8. Internet governance dataset encryption time under different algorithms.

In Figure 8, the x-axis represents the amount of internet governance data, ranging from 1 GB to 20 GB, and the y-axis represents the time required to encrypt the data. As

shown in Figure 8, it is clear that using the CC algorithm to encrypt internet governance data required much less time than other algorithms, and the encryption speed was faster. Among them, encrypting data based on the HE algorithm required more time than the CC algorithm, but less time than encrypting data based on the DEA and SHA. When the amount of data was below 12 GB, the time required for data encryption based on the DEA was lower than that required for encryption based on the SHA, but higher than the time required for encryption using the other two algorithms. However, when the amount of data exceeded 13 GB, the time required for data encryption based on the DEA was much higher than the other three algorithms. When the data quantity was 1 GB, the encryption time based on the CC algorithm was 1.31 s, which was 0.83 s, 0.57 s, and 1.16 s lower than the encryption time based on the DEA, HE, and SHAs. When the data quantity was 20 GB, the time required for encryption based on the CC algorithm was 16.14 s, which was 19.64 s, 7.94 s, and 15.05 s lower than the time required for encryption based on the DEA, HE, and SHAs.

To verify the technical advantages of the Transformer and SAR data fusion method proposed in this paper in network infrastructure governance, CNN, BiLSTM, SVM, and random forest algorithms commonly used in the current internet governance field were selected for comparison. Experiments were conducted from multiple dimensions, such as feature extraction accuracy, load prediction error, and abnormal warning response time. The datasets used and the performance comparison results of each algorithm are shown in Table 4.

Table 4. Performance comparison of different algorithms.

Evaluation Metrics	Transformer + SAR	CNN	BiLSTM	SVM	RF
Feature Extraction Accuracy (%)	96.2	90.5	88.7	82.4	89.1
Load Forecast Error (MAE)	3	4.9	3.6	6.8	5.7
Anomaly Warning Response Time (ms)	16.8	28.3	23.5	40.2	34.7
Encryption Compatibility (%)	91.5	78.6	75.3	62.5	73.8
Spatial Feature Long-Distance Correlation Capture Rate (%)	93.8	72.6	76.4	56.8	70.3
Multi-Source Data Fusion Efficiency (GB/s)	2.6	1.7	2.1	1	1.4

Judging from the results in Table 4, in internet governance under the background of the global digital contract, the Transformer + SAR fusion method shows significant advantages in all evaluation indicators. Its feature extraction accuracy reaches 96.2%, far exceeding SVM's 82.4%, and higher than CNN's 90.5%, BiLSTM's 88.7%, and random forest's 89.1%. This is due to the Transformer's multi-head attention mechanism's accurate capture of the spatial characteristics of SAR data and the network runtime characteristics; the load prediction error is only 3.0, lower than other algorithms, reflecting the ability to accurately predict dynamic network loads; the anomaly warning response time is 16.8 ms, which can quickly respond to network anomalies and ensure the timeliness of governance; the encryption compatibility is 91.5%, which has strong synergy with certificateless encryption algorithms and meets the needs of privacy protection; the spatial feature long-distance correlation capture rate of 93.8% and the multi-source data fusion efficiency of 2.6 GB/s also highlight its advantages in integrating multi-dimensional and cross-regional network data, fully verifying the effectiveness of this method in improving the accuracy, security, and efficiency of internet governance.

5. Discussion

Theoretically, this article offers a thorough understanding and methodology for an examination of internet governance within the framework of the Global Digital Compact. Even though internet governance is discussed in the literature that is now available, it is performed within the larger framework of the Global Digital Compact, which highlights recent advancements and trends in the field. This offers an alternative viewpoint for comprehending the guidelines, policies, and procedures of internet governance. In actuality, it offers legislators, internet firms, and pertinent stakeholders a useful resource. The swift advancement of digital technology has presented previously unheard-of difficulties for internet administration. Not only have the governance models and procedures already been examined in use, but also, specific, doable routes have been suggested to offer direction for real-world operations.

Despite the fact that internet governance is the subject of a lot of current work, the majority of studies tend to begin from a single national or regional viewpoint. In order to analyze the issues of internet governance more thoroughly and take into account the differences and similarities between various countries and regions, this article highlights the history of the Global Digital Compact. This makes it more thorough and in-depth than research that only stays at the theoretical level or concentrates on a single practice. This article's primary output is a thorough examination and debate of internet governance's guidelines, policies, and best practices within the framework of the Global Digital Compact. This offers direction for the realm of practice as well as fresh theoretical insights for academics. Additionally, it can offer academics fresh viewpoints and research techniques that can advance the field of internet governance research and growth. Policymakers, internet corporations, and other pertinent stakeholders can find great inspiration and reference value in the research findings. In order to make better decisions and more informed choices, it can assist these entities in better understanding their duties and obligations within the framework of the Global Digital Compact.

So, the primary focus of this paper is a thorough analysis and discussion of internet governance within the framework of the Global Digital Compact, which has both theoretical and practical significance. This article is deeper and more comprehensive in perspective and content than previous works. The findings have guiding implications for the realm of practice in addition to having a significant impact on academia.

6. Conclusions

In the context of the global digital contract, this paper constructs the standards, rules, and practice paths of internet governance by integrating SAR data processing and the Transformer model, combining differential privacy protection and certificateless cryptographic algorithms. This study shows that the governance standards based on the OSI model, the rules of the multi-stakeholder mechanism, and the data encryption of the CC algorithm are superior to traditional methods in terms of efficiency and satisfaction and effectively improve privacy protection and network security. However, there are shortcomings in this study: the core relationship between SAR and internet governance is not explained enough, and the innovative expansion of the existing framework is limited. Future research can deepen the integration mechanism of SAR data and network governance, optimize sample design to enhance repeatability, and explore new governance frameworks to break through the limitations of the existing model and further improve the internet governance system under the global digital contract.

Author Contributions: X.F., W.Z. and Z.L.; Writing, Editing, and Software, Z.L.; Data Analysis, X.F. Resources, Z.L. and W.Z.; Data Analysis and Software. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the National Social Science Fund of China ‘The Practical Dilemmas and Chinese solutions of Global Governance of Cross-border Data Flows (Grant: 24BXW043)’.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

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

References

1. Liu, J.; Liu, L.Y.; Tu, Y.; Li, S.X.; Li, Z.M. Multi-stage Internet public opinion risk grading analysis of public health emergencies: An empirical study on Microblog in COVID-19. *Inf. Process. Manag.* **2022**, *59*, 2–21. [\[CrossRef\]](#)
2. Li, Z.; Zhang, W.Y.; Zhang, H.T.; Gao, R.; Fang, X.D. Global Digital Compact: A Mechanism for the Governance of Online Discriminatory and Misleading Content Generation. *Int. J. Hum.-Comput. Interact.* **2024**, *3*, 1381–1396. [\[CrossRef\]](#)
3. Mancuso, I.; Petruzzelli, A.M.; Panniello, U. Digital business model innovation in metaverse: How to approach virtual economy opportunities. *Inf. Process. Manag.* **2023**, *60*, 103457. [\[CrossRef\]](#)
4. Putz, B.; Dietz, M.; Empl, P.; Pernul, G. Ether Twin: Blockchain-based Secure Digital Twin Information Management. *Inf. Process. Manag.* **2021**, *58*, 102425. [\[CrossRef\]](#)
5. Khan, S.D.; Basalamah, S. Multi-Branch Deep Learning Framework for Land Scene Classification in Satellite Imagery. *Remote Sens.* **2023**, *15*, 3408. [\[CrossRef\]](#)
6. Wang, J.S.; Yang, G.H. Data-driven methods for stealthy attacks on TCP/IP-based networked control systems equipped with attack detectors. *IEEE Trans. Cybern.* **2018**, *49*, 3020–3031. [\[CrossRef\]](#)
7. White, P.A. Cyberpeace: Why Internet Governance Matters for Global Peace and Stability. *Peace Change* **2019**, *44*, 441–467. [\[CrossRef\]](#)
8. Tjahja, N.; Trisha, M.; Jamal, S. Who do you think you are? Individual stakeholder identification and mobility at the Internet Governance Forum. *Telecommun. Policy* **2022**, *46*, 102410–102411. [\[CrossRef\]](#)
9. Flonk, D.; Markus, J.; Anke, S.O. Authority conflicts in internet governance: Liberals vs. sovereigntists? *Glob. Const.* **2020**, *9*, 364–386. [\[CrossRef\]](#)
10. Malcic, S. Proteus online: Digital identity and the Internet governance industry. *Convergence* **2016**, *24*, 205–225. [\[CrossRef\]](#)
11. Guan, S.; Xie, Y.; Zhai, Y.M. The Model Selection and Optimization of Global Internet Governance—Based on Reflection on the Multi stakeholder Model. *Gov. Res.* **2018**, *35*, 112–113.
12. Zhang, J.W. How to Regulate Digital Financial Assets: Cryptocurrency and Smart Contracts—Review of the Draft Law on Digital Financial Assets of the Russian Federation. *J. Shanghai Univ. Political Sci. Law Rule Law Ser.* **2018**, *33*, 14–23.
13. Jiang, L. New Trends and Policy Implications for Global Digital Economy Regulation. *J. Beijing Norm. Univ. Soc. Sci. Ed.* **2023**, *3*, 58–65.
14. Wylde, A. The UN Global Digital Compact (GDC), Achieving a trusted, free, open, and Secure Internet: Trust-building. *Eur. Conf. Cyber Warf. Secur.* **2023**, *22*, 544–551. [\[CrossRef\]](#)
15. Saravistha, D.B.; Sukadana, I.K.; Suryana, K.D. Urgency of Contract Model Settings in the Global Digital Market Related to Tourism Business: A Study on Consumer Protection and Electronic Information and Transactions. *Bp. Int. Res. Crit. Inst.-J. BIRCI-J.* **2022**, *5*, 4549–4556.
16. Ong, J.P. The Enforceability of Digital Contract: A Comparative Analysis on Indonesia and New Zealand Law. *Lawpreneurship J.* **2021**, *1*, 30–42. [\[CrossRef\]](#)
17. Tjahja, N.; Meyer, T.; Shahin, J. What is civil society and who represents civil society at the IGF? An analysis of civil society typologies in internet governance. *Telecommun. Policy* **2021**, *45*, 102141. [\[CrossRef\]](#)
18. Cheung, M.; Chen, Z.T. Power, Freedom, and Privacy on a Discipline-and-Control Facebook, and the Implications for Internet Governance. *IEEE Trans. Prof. Commun.* **2022**, *65*, 467–484. [\[CrossRef\]](#)
19. Abood, A.M.; Hussein, M.S.; Faisal, Z.G.; Tawfiq, Z.H. Design and simulation of video monitoring structure over TCP/IP system using MATLAB. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *24*, 1840–1845. [\[CrossRef\]](#)
20. Wang, L.M. Harmony but Difference: The Rule Boundary and Application of Privacy and Personal Information. *Leg. Rev.* **2021**, *39*, 15–24.
21. Feng, W.B.; Hong, Z.; Wu, L.F.; Fu, M.L. Overview of Network Protocol Recognition Technology. *Comput. Appl.* **2019**, *39*, 3604–3605.

22. Zharova, A. Ensuring the information security of information communication technology users in Russia. *Int. J. Cyber Criminol.* **2019**, *13*, 255–269.
23. Joseph, I.; Ituabhor, O.; Zhimwang, J.T.; Ikechi, R. Achievable Throughput over Mobile Broadband Network Protocol Layers: Practical Measurements and Performance Analysis. *Int. J. Adv. Netw. Appl.* **2022**, *13*, 5037–5044. [[CrossRef](#)]
24. Raha, A.; Hajdini, I. Franchisees with multiple stakeholder roles: Perceptions and conflict in franchise networks. *J. Strateg. Mark.* **2022**, *30*, 160–179. [[CrossRef](#)]
25. Daigo, E.; Kevin, F. Exploring the value sponsors co-create at a charity sport event: A multiple stakeholder perspective of sport value. *Sport Manag. Rev.* **2022**, *25*, 656–678. [[CrossRef](#)]
26. Dai, L. On the Protection of Personal Privacy Rights in the Context of Digital Trade. *Contemp. Law* **2020**, *34*, 148–160.
27. Isaak, J.; Hanna, M.J. User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer* **2018**, *51*, 56–59. [[CrossRef](#)]
28. Cheng, S. Multilateralism: A New Phenomenon in International Politics. *J. Soc. Sci. Jilin Univ.* **2020**, *60*, 127–133.
29. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 746–789. [[CrossRef](#)]
30. Feng, D.; Zhang, M.; Ye, Y. Research on location trajectory publishing technology based on differential Privacy Model. *J. Electron. Inf. Technol.* **2020**, *42*, 74–88.
31. Qiao, Z.; Yang, Q.; Zhou, Y.; Zhang, M. Improved secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments. *IEEE Syst. J.* **2021**, *16*, 1842–1850. [[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.