Abstract

This document proposes the Internet of Governance (IoG), a new technology supporting platform for cyberspace collaborative governance. This document illustrates IoG definition, two roles and four functionalities, and develops architectural models to carry out these functionalities. This document provides the design of IoG framework and the collaboration life-cycle and uses some practical applications as examples.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 October 2024.

Copyright Notice

Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the
1. Introduction

With the development of the Internet, Cyberspace governance has extended from key resource allocation to various aspects. Cyberspace governance today faces two new problems: the lack of collaboration and the difficulty of implementation. Cyberspace needs a new technology supporting platform to resolve these problems. This document proposes the Internet of Governance (IoG), a new technology supporting platform for cyberspace collaborative governance. IoG is an open and interconnected platform that facilitates inter-domain and international collaboration to resolve cyberspace governance issues. As infrastructure, IoG achieves facility and data sharing. As community, IoG achieves interpersonal coordination and rule consensus. This document provides IoG architectural design and provides practical use cases.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].
2. Terminology

Internet of Governance (IoG): Refers to a supporting platform that connects entities involved in cyberspace governance, such as ISPs, ICPs and IT companies.

Governance Domain: Refers to entities that join the Internet of Governance.

Governance Data: Refers to data collected by governance domains. The sources of the governance data can be traditional network information such as routing information, DNS information and IP information. The sources of the governance data can also be structured information such as IP credit information and AS rankings, and non-structured information such as model parameters of learning-based active measurement.

Governance Service: Refers to services provided by governance domains, such as looking glasses, virtual machines or containers.

Governance Metadata: Refers to the metadata that describes governance data or governance service, such as network address, index and access level. It can be used to address and route governance data and governance service.

Governance Center: Refers to a facility that holds management functionalities of IoG, such as routing, authentication, identity management, etc.

Governance Gateway: Refers to software systems that execute IoG-related functionalities. Governance gateways are deployed in governance domains. Governance gateways should be able to access local devices and resources. Governance gateways connect to each other and to the governance center.

3. The Internet of Governance (IoG)

3.1. Definition

IoG is an open and interconnected platform that facilitates inter-domain and international collaboration to resolve cyberspace governance issues. IoG contains multiple cyberspace governance entities, such as Internet organizations, ISPs and ICPs.
3.2. Two Roles

IoG serves as both infrastructure and community. As infrastructure, it provides automated collaboration procedures, so that participants can share data and access services in an efficient and automated manner. As a community, it provides an organizational structure and agenda, so that participants can communicate and share information efficiently and conveniently.
3.3. Four Functionalities

As infrastructure, IoG carries out two functionalities, facility sharing and data sharing. As a community, IoG carries out another two functionalities, interpersonal coordination and rule consensus.

Facility sharing means that after authentication, a governance domain can access or operate monitoring or control facilities owned by another domain. IoG provides a higher level of facility sharing than Looking Glasses (LG). LG sites execute simple commands (ping, trace, bgp, etc.), while IoG domains can execute more complicated operations on other participants, such as obtaining network probers, executing scrutinized programs, or applying for a virtual machine. These operations are exposed and accessed as services.

Data sharing means that governance domains share governance data while ensuring privacy and security. Data sharing can benefit many cyberspace governance problems, such as IP traceback, network attack tracing and defense. To address privacy and security concerns of data sharing, IoG follows the rules that data are usable yet invisible. Governance data are stored locally by its owner, and other governance domains launch remote operations on these data and obtain the results without accessing raw data.

Interpersonal coordination means to construct an official platform for collaboration negotiation and information sharing. Participants negotiate practical details of facility sharing and data sharing, such as methods of calling, service exposure, authentication, etc. Participants share cyberspace governance information, such as 0-day
network attacks or sudden network failures, taking measures to mitigate losses.

Rule consensus means to consolidate consensus reached during the collaboration process of facility sharing, data sharing and interpersonal coordination. In IoG, new governance methods can emerge to complement current rule-based cyberspace governance.

3.4. Architectural Model

This document proposes architectural models to achieve IoG's two roles described in 3.1. Functional model, communication model and information model are required to achieve IoG's role as infrastructure. Organization model, credit model and incentive model are required to achieve IoG's role as community.

Functional model defines mandatory functionalities that IoG participants need to implement to achieve streamlined and automated collaboration. IoG collaboration, such as data sharing and facility sharing are implemented with API (Application Programming Interface) calls. An IOG domain (provider) can expose or publish services as APIs in an API catalog managed by IoG governance center. Another domain (caller) can search and call these APIs, providing API parameters and authentication information. The provider executes these APIs by manipulating its facilities or operating on local databases, and only returns the result of the API. No extra data movement is involved, so that privacy is protected.

Communication model defines how IoG domains communicate each other and how to publish and access service metadata. IOG domains form an overlay network with VPN (Virtual Private Network) to meet the security requirement. A centralized API catalog is managed by IoG governance center to store published service metadata.

Information model defines homogeneous information structure of governance data so that IoG domains deployed with different underlying local management systems can understand each other. IoG collaborations are all performed by API calls, and the participants do not exchange data but service results. IOG domains are obliged to translate raw data into understandable, formatted parameters and results of API calls, so that mutual-understanding can be achieved even with heterogeneous local management systems.

Organization model defines the organization structure and agenda of IoG. IoG consists of participants, an advisory group and a secretariat. Participants are entities that collaborates via IoG. An advisory group are selected representatives of IoG responsible for making decisions. The secretariat performs administrative and management tasks.
Incentive model defines how to encourage IoG collaboration and how to increase collaboration efficiency and effects. IoG community is designed to be relatively loose, so that incentive mechanisms are needed to balance cooperativeness and selfishness of the participants.

Credit model defines how to translate participant behaviors and attributes to credits. Credits can be used to assess participant performance and cooperativeness.

4. Components and Collaboration Life-cycle

This section provides an IoG framework consisting of three major components. The interaction of these components are illustrated through the collaboration life-cycle figure.
4.1. Components

IoG consists of three components: governance center, governance gateway, and governance domain. The governance center stores service metadata and runs administrative and management tasks. The Governance gateway is usually deployed at the entrance to the governance domain's network, performing IoG-related functionalities. The governance gateway can communicate with each other and the governance center. The Governance domain contains all governance-related entities inside the domain's network, including governance databases, monitoring and control facilities, and network management systems. The governance gateway is given permission to access the governance domain to implement service APIs.

4.2. Collaboration Life-Cycle

The IoG component design leads to the collaboration life-cycle illustrated in Figure 2 and the following procedures.

1. An IoG domain (provider) decides to expose one of its services by publishing service API metadata to the governance center. The service API metadata includes the API name, parameter format, parameter descriptions, the provide hostname/IP and calling methods (such as URL or REST). The provider should also implement the API with its facilities.

2. Suppose another domain (caller) generates demand for the services from the provider in step 1.

3. The caller searches API catalog in the governance center of the demanded service and obtain a list of APIs related to the service. The caller selects one or more APIs.

4. The caller calls these APIs by providing proper parameters and authentication information.

5. The provider receives the API calls and runs local implementation.

6. The result is returned to the caller.
5. Supporting Cyberspace Governance Applications

The following subsections provide examples of IoG supporting practical cyberspace governance applications based on the component design and collaboration life-cycle described in Section 4.

5.1. DDoS Tracing and Defense

IoG can provide a reliable supporting platform for DDoS tracing and defense. Tracing an IP source requires coordination among multiple ASes (Autonomous Systems). IoG provides automated procedures to access IP traceback data maintained by ASes in their own infrastructures. The following steps are performed to enable IP traceback data sharing within the IoG architecture defined in section 4.

1. An IoG domain(A) decides to expose the IP traceback service. It announces service metadata in the API catalog in the governance center.

2. Another IoG domain(B) decides to trace a certain IP.

3. B search the API catalog of the IP traceback services and obtain available services provided by other domains, including A. The identity of B is certified by the governance center and obtains authentication token.

4. B initiates API calls according to the service metadata from A, providing proper parameters and authentication token.
5. A accesses local IP traceback databases if A receives API calls from B and B is certified.

6. A returns the IP traceback information to B.

5.2. IP Geolocation and Verification

The following steps are performed to implement CPV [CPV] algorithm to verify IP geolocations within the IoG framework. CPV is an advanced IP geolocation verification method that requires more complex operations on probers to achieve better accuracy than simple commands like ping or traceroute. Suppose an IoG participant A decides to verify that the geolocation of a certain IP is O.

1. A selects other participants B and C that provides CPV service APIs. According to CPV algorithm, B and C should be selected so that O is located inside the triangle formed by A, B and C.

2. A initiates multiple API calls to measure the delay between AO, BO, CO, AB, AC, BC.

3. A calculates the size of triangle ABC, AOC, BOC and AOB.

4. A checks whether the summation of the size of triangle AOB, AOC, BOC equals to the size of triangle ABC. If so, then A decides the location of O is correct in this iteration and record the result. A then starts another iteration, performing step 1 again with new choices of B and C.

5. After all iterations, A calculates the ratio of correct results to decide whether O is the correct geolocation.

6. Security Considerations

6.1. Authentication

Authentication checks are carried out throughout the collaboration life-cycle of IoG to ensure security. The governance center maintains identity information of each governance domain. Each governance zone needs to be authenticated when they communicate with the governance center in step 1 and step 3 described in section 4.2. Besides, in step 3, the caller zone obtains a token from the governance center and uses this token when API calls are initiated in step 4. The provider checks the token before responding.

6.2. Secured Transport

As discussed in [RFC7861], measures are taken to satisfy RPC security. All communications involved in IoG collaboration life-cycle described
in section 4.2 should use secured protocols such as HTTPS where TLS [RFC8446] is mandatory.

6.3. Privacy Protection

In section 3.2, privacy protection has been discussed. The key issue of data sharing is to exchange information with minimal privacy risks. In IoG framework, all communications between governance domains are remote API operations, where only parameters and results are exchanged. The raw data can only be locally accessed.

7. Acknowledgements

The authors would like to thank the support of Tsinghua University and Joint Research on IPv6 Network Governance: Research, Development and Demonstration under Grant 2020YFE0200500.

8. IANA Considerations

This memo includes no request to IANA.

9. Normative References


Authors' Addresses

Jilong Wang (editor)
Tsinghua University
Beijing
100084
China

Email: wjl@tsinghua.edu.cn

Yi Qiao (editor)
Tsinghua University
Beijing
100084
China

Email: qiaoy21@mails.tsinghua.edu.cn