Network Working Group
Internet-Draft
Intended status: Informational
Expires: 5 January 2026

L. Li
Huawei
F. Liu
Huawei Singapore
4 July 2025

Future Requirements of Fine-Grained Privacy for the Network
draft-li-6gip-fine-grained-privacy-network-00

Abstract

This draft describes some potential new privacy requirements for the future network. We start from the data lifecycle and propose that the privacy needs to be considered during the data is processing. We also introduce some new academic research results. Some use cases are proposed. The goal is to attract IETF working or interest groups in researching to these new requirements in protocol level for the future network.

Table of Contents

1. Introduction

As mentioned in ITU-R "Framework and Overall Objectives of the Future Development of IMT in 2030 and beyond", new services in future network will be very likely to use computing power for data processing instead of only data transmission [ITU2083]. However, privacy issues may occur in the data processing and management phase. Possible scenarios can be sensing services and/or data analytics services, where user-related data will be collected and processed for example to derive sensing/analytic results, which may touch the sensitive information contained in the data. As shown in Figure 1, 5G networks do consider protecting user privacy with mechanisms like identity concealment, user consent and so on. However, existing mechanisms do not cover privacy preserving consideration happening in heavy data processing and management services provided in network system.

Given that the latest legal regulations (e.g., Data Act [DATAACT] and eIDAS2.0 in EU [EUDI]) force stronger privacy protection and full sovereignty of the data ownership , the lifecycle privacy-preserving consideration and management should be further enhanced.

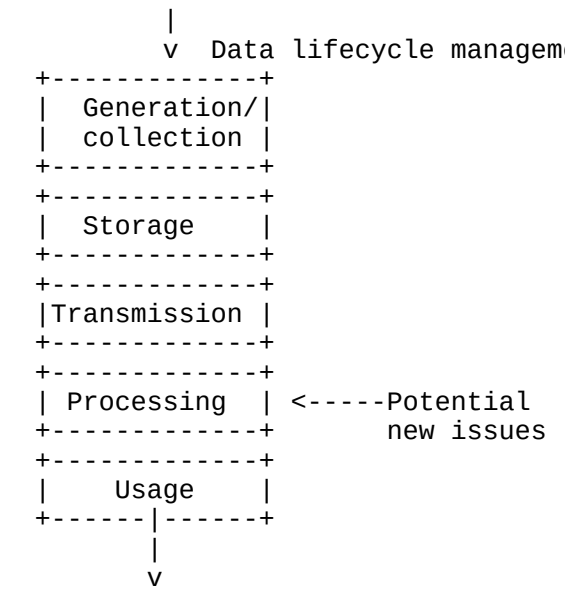

Figure 1: Vulnerability of privacy in data lifecycle

In future telco network, individual users may want their data being processed in their favorable way. First of all, depending conditions such as whether the user is at home, in public, or consumes certain types of services, a user may either relax or escalate the privacy preserving level. Second, a user may want to indicate at where his data shall be processed, e.g., centralized at the operator side or partly exposed to third parties. Third, a user may want to specify what type of data processing techniques shall be used to process his data to guarantee the privacy preserving strength. In general, a user expects a stronger but more fine-grained privacy-preserving consideration for data processing and management services.

Same issues have also been raised in internet apps, Regarding to the processing privacy, such as the privacy information retrieval (PIR) mentioned by Apple at WWDC25. Through PIR, a device can retrieve and return data through a server, but the server cannot associate the device with the specific returned content. This is achieved through homomorphic encryption and is open-sourced at link: https://github.com/apple/swift-homomorphic-encryption. Besides, We also see the potential of new technologies, such as private set intersection (PSI), which is very useful in cloud computing, such as in the field of federated learning. These drive us to research how new privacy-preserving technologies can be used in future networks in protocol level.

2. 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 [RFC2119].

3. AIML Use case for privacy reqirements in future network

TODO

4. Potential New Requirements of Privacy as a serivce(PrivaaS)

Several users request services where their data will be processed by the network. Given individual preferences indicated by the users, the network should provide fine-grained privacy-preserving schemes during the service time for the users. This could for example based on service types, user subscriptions/context, network states, etc.

Users A, B, and C request different network services. For example, user A uses network to browse web pages, and user B uses the network to share data with a third party to obtain third-party services. User C relies on the network to assist his vehicle self-driving, where environment sensing information including privacy content will be collected by the network.

Depending on the user’s requirements and network settings, fine-grained privacy mechanisms will be used correspondingly for each user. For example:

* User A uses anonymization of identity identifiers as a fine-grained privacy protection mechanism, which attackers cannot distinguish network traffic from others.

* User B uses a data pseudonym as a privacy protection mechanism. User data is processed to remove potential privacy risks, such as location scoping instead of precise location information.

* User C uses homomorphic encryption to perform environment sensing information computing and identify the obstacles while the data is encrypted.

By leveraging privacy as a service, both users’ requirements are fulfilled with fine-grained privacy-preserving mechanism supported from the network such as in telecom. User requirements and service data requirements can be adapted at the same time.

4.1. Potential new privacy technique for PrivaaS

As the example shows, homomorphic encryption is just an example of a new technology. Some new technologies have been discussed in academia, and they can all be considered. The following are some examples of new potential privacy technologies for processing privacy.

* Ciphertext computation: It refers to the operation of performing calculations directly on encrypted data without decrypting it first.

* Privacy information retrieval (PIR): It is a technology that enables the querying party to hide the keywords of the queried object or customer ID information.

* Private set intersection (PSI): It is a cryptographic protocol, which is used to compare the intersection of private data sets of two or more parties, while ensuring that the respective data of each party will not be leaked.

* Multi-party computation (MPC): It is a general - purpose cryptographic primitive. Without disclosing the original input data of the participants, it allows distributed participants to cooperate in calculating any function and output accurate calculation results.

#TODO: How the new technology is used at the protocol level is an ffs

5. Existing Privacy Designs in the Telco netowrk.

Requirements for privacy for 5G are defined in 3GPP TS 22.261 [TS22261]: The 5G system shall support a secure mechanism to collect system information while ensuring end-user and application privacy (e.g., application-level information is not to be related to an individual user identity or subscriber identity and UE information is not to be related to an individual subscriber identity).Some design principles have been applied to the solution, such as exposure collection of user information and use consent principles. User identifiers are also protected, such as concealment the user’s permanent identity (SUPI) and using non-permanent identifiers such as GUTI(Globally Unique Temporary Identifier) and GPSI(Generic Public Subscription Identifier) to handle user-related information.

It is worth mentioning that these technologies often use pseudonymization, and the privacy of data and content processing may need to be enhanced.

6. Potential Related IETF/IRTF Groups.

Some potential WGs may be related to the privacy needs mentioned above, as follows:

* 6GIP is a group that specifically discusses the privacy and security issues for the network including 6G

* The Privacy Preserving Measurement (ppm) working group is proposing a protocol for multi-party computation using cryptographic techniques, although use case is limit to information measurement, the charter's goal is to address privacy issues in data collection.

* Privacy Enhancements and Assessments Research Group (pearg) is a general forum for discussing and reviewing privacy enhancing technologies for network protocols and distributed systems in general, and for the IETF in particular.

* Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular. Some of the latest algorithms and academic results may be discussed in CFRG.

TODO: Identifying more WG is ffs

7. IANA Considerations

This document has no IANA considerations.

8. Security Consideration

TODO

9. References

9.1. Normative Reference

[ITU2083] (ITU), I. T. U., "Framework and Overall Objectives of the Future Development of IMT in 2030 and beyond", Group ITU-D SG2, May 2024, <https://www.itu.int/dms_pub/itu-d/oth/07/31/D07310000090015PDFE.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[TS22261] 3GPP, "Service requirements for the 5G system", TS 22.261, Group 3GPP/SA3, June 2025, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107>.

9.2. Informative References

[DATAACT] law, E. U., "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)", 23 February 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0068>.

[EUDI] law, E. U., "European Commission. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.", 3 June 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0068>.

Acknowledgments

TODO

Authors' Addresses

Lun Li
Huawei
Email: lilun20@huawei.com

Faye Liu
Huawei Singapore
Email: liufei19@huawei.com