Contribution ID: **20** Type: **Poster Presentation**

Towards Privacy and Accessible Through Resource Integration

Due to the rapid development of edge devices and existing infrastructure in the post-5G era, a significant flood of large and diverse data is streaming into cloud infrastructure via services on edge devices. Consequently, many cloud infrastructure providers must develop methods for efficient resource allocation and scheduling to support service deployment with high availability and reliability. However, existing infrastructure providers often overlook efficient resource provisioning to preserve data privacy from edge device services. Typically, every service employs high-security mechanisms to preserve data privacy, but this comes at the cost of high resource usage, such as with fully homomorphic encryption. On the other hand, employing low-security mechanisms may pose a high risk of violating data privacy. Therefore, we propose the creation of an infrastructure focused on ensuring high availability and reliability of service deployment, coupled with effective security mechanisms tailored to each individual service, all while minimizing financial costs for service developers.

We propose an infrastructure to categorize the transferred data from edge devices to the cloud for each service into four protection levels based on privacy violation. The first level is high protection, including data such as government-issued identification numbers, financial account information, personal medical and health-related data, biometric authentication data, usernames or email addresses combined with passwords, and genetic data. The second level is moderated protection, covering security camera recordings, body-worn video system recordings, cameras recording cash handling or payment card handling areas, and building entry records. The third level is low protection, encompassing licensed software/software license keys and library paid subscription electronic resources. The fourth level is minimal protection, including published research, press releases, and public event calendars.

As each data category requires a different protection level, the infrastructure provides different security mechanisms to efficiently preserve data privacy. For services requiring high security and developers with high financial costs, the infrastructure suggests applying quantum key distribution (QKD) to protect data transmission. Alternatively, for service developers with lower financial capacity, the infrastructure suggests applying zero-knowledge encryption to protect data transmission. Moreover, this paper investigates the resource utilization of security mechanisms such as AES, DES, Diffie-Hellman, ECC, Blowfish, Twofish, ChaCha20, RC4, Camellia, and Serpent. These encryption algorithms serve various purposes and are chosen based on factors such as security requirements, performance considerations, and the specific use case. We analyze patterns of data transmission based on privacy violation levels and transmission frequency to prevent over or under resource allocation, ensuring high availability, reliability, and security.

Primary authors: Dr THONGLEK, Kundjanasith (Cybermedia Center, Osaka University, Japan); Prof. LEE, Chonho (Cybermedia Center, Osaka University, Japan); Dr ABE, Hirotake (Cybermedia Center, Osaka University, Japan); Prof. ENDO, Arata (Cybermedia Center, Osaka University, Japan); Mr TANIGUCHI, Kohei (Cybermedia Center, Osaka University, Japan); Prof. DATE, Susumu (Cybermedia Center, Osaka University, Japan)

Presenter: Dr THONGLEK, Kundjanasith (Cybermedia Center, Osaka University, Japan)

Track Classification: Track 8: Infrastructure Clouds and Virtualizations