Privacy Preserving System for Integrated Broadcast-broadband Services using Attribute-Based Encryption
Go Ohtake, Kazuto Ogawa, and Reihaneh Safavi-Naini*
*University of Calgary

Several integrated broadcast-broadband services, such as Hybridcast, have recently been launched which allow viewers to receive content via the airwaves together with additional information about the content via the Internet. By sharing personal preferences such as viewing histories with service providers, viewers can expect more attractive and personalized services. Viewing histories used for the above services must be protected for viewer’s privacy. In this paper, we propose a privacy preserving system for integrated broadcast-broadband service. The system uses an attribute-based encryption (ABE) scheme to encrypt a viewing history to be stored on a cloud server, such that it is decryptable by service providers that possess the required attributes that are approved by the viewer. We implement the system by using JavaScript that runs on an HTML5 (Hyper Text Markup Language 5) application. The implementation result shows that the proposed system can be used in practice in the sense that the required computation for data encryption on the user terminal is small. Using the system, a viewer can safely receive personalized services from a large number of service providers.