Secure Method of Managing Digital Content in Ubiquitous Computing Environment

Akihiro Tsutsui[†] *and Tomoko Sawabe*

Abstract

A research project for building a remote collaboration environment based on technologies for handling large-scale digital content is being undertaken by NTT Network Innovation Laboratories. This article briefly reviews collaborative research with Keio University on a secure method of managing digital content in a ubiquitous computing environment.

1. Introduction

NTT Network Innovation Laboratories has developed a digital cinema system and related technologies based on ultrahigh-definition video coding and content delivery technologies. We are currently using these technologies in research and development (R&D) of a networked remote collaboration environment and in its application for the creation of content such as movies [1]–[3].

Keio University has developed several technologies for digital content delivery through basic research on digital media creation, editing, and usage. It is also engaged in R&D of permanent archiving and digital media handling.

In a collaboration program between NTT Network Innovation Laboratories and Keio University, my colleagues and I are designing a platform that enables secure remote access to large-scale digital media. We are also planning demonstration experiments using this platform. These goals can be achieved by applying the previous research outcomes and know-how associated with digital content handling of both parties. Another aim of the collaboration program is to clarify the technical problems of building a network supported cooperative work (NSCW) environment. So far, in the program's first year, we have investigated an authentication mechanism that enables secure and flexible access to digital content via a network. In this article, we discuss security issues related to large-scale digital content.

2. NSCW

NSCW is an advanced concept based on computer supported cooperative work (CSCW). Compared with CSCW, the aim with NSCW is to build a distributed cooperative working environment that makes maximum use of networks. NTT Network Innovation Laboratories has developed several key technologies for processing and transmitting ultrahigh-definition images and videos stably and securely. We are now striving to achieve an NSCW environment that consists of high-quality audio/video communication with high reality, effective data sharing, and interactive work spaces among distributed workers. Some examples of the application of NSCW are shown in **Fig. 1**. One example is collaborative film making, such as digital cinema. Currently, digital cinema creation and editing processes are done all over the world as a result of ongoing globalization, so they are conducted in a networked distributed environment. To promote research on NSCW, it is essential to build practical experimental environments. By studying an actual use case such as film making, we can consult with experts in this area and clarify their requirements. More comprehensive technologies are required for

† NTT Network Innovation Laboratories
Musashino-shi, 180-8585 Japan

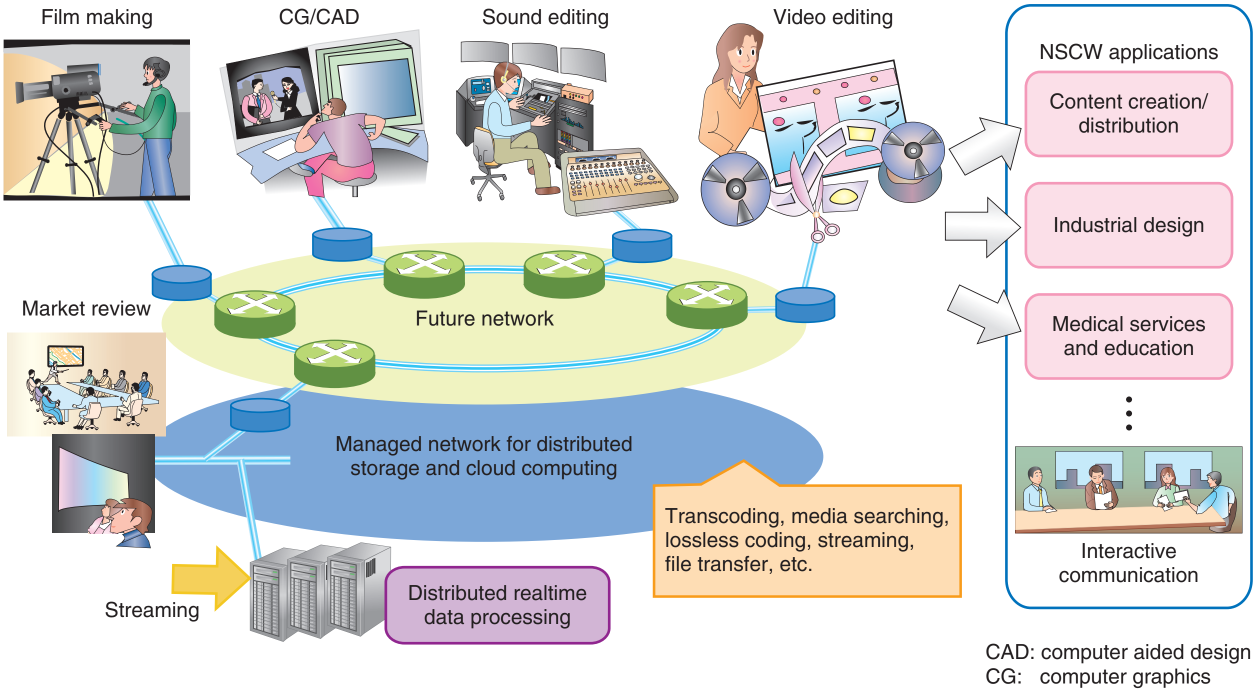
Film making
CG/CAD
Sound editing
Video editing
NSCW applications
Content creation/ distribution
Industrial design
Medical services and education
Interactive communication
Market review
Future network
Managed network for distributed storage and cloud computing
Transcoding, media searching, lossless coding, streaming, file transfer, etc.
Streaming
Distributed realtime data processing
CAD: computer aided design
CG: computer graphics

Fig. 1. Application examples of NSCW.

building such an experimental environment, e.g., content archiving and distribution. In addition, technical studies from the ubiquitous computing viewpoint are requiring in order to consider remote collaboration in various distributed networks.

3. Content and security management in ubiquitous environment

The Internet is utilized in various business fields. Therefore, information security must be ensured during content distribution. A major theme of this collaboration program is the security of digital content. Currently, some security-sensitive remote collaborations that handle digital assets operate a safe working space and use a dedicated leased line, which ensures network security. However, excluding open networks, such as the Internet, sacrifices the convenience and expandability of the remote collaboration itself. Many kinds of wired and wireless network access services are available nowadays. Though there may be variations in the communication quality, we can get online anywhere anytime. In Japan, because of the spread of broadband services using optical fiber, high-speed network access is available in almost all offices and homes at low cost. WiMAX and Long Term Evolution (LTE) wireless network access services are provided in public in downtown areas, which enables large-scale content distribution to mobile devices.

In this context, two keys to investigating a flexible remote collaboration environment are ubiquitous computing and cloud computing using open networks. If we assume remote collaboration over the Internet, it is important to create a platform that enables collaborative work via the network anywhere. Of course, communication quality and working circumstances are not uniform because there are various types of access networks. However, content creation can be divided up into many kinds of work. Each kind has its own networking requirements. Enhancing the ubiquitous features of remote collaboration can lead to improved efficiency of all the work.

Ensuring information security in the ubiquitous environment of the Internet is a difficult task. In particular, unauthorized access must be prevented and copyright protection technologies are indispensable for valuable content (e.g., commercial audio and video).

With today's rapid development of cloud computing and business globalization, it is necessary to use the Internet for remote collaboration. Therefore,

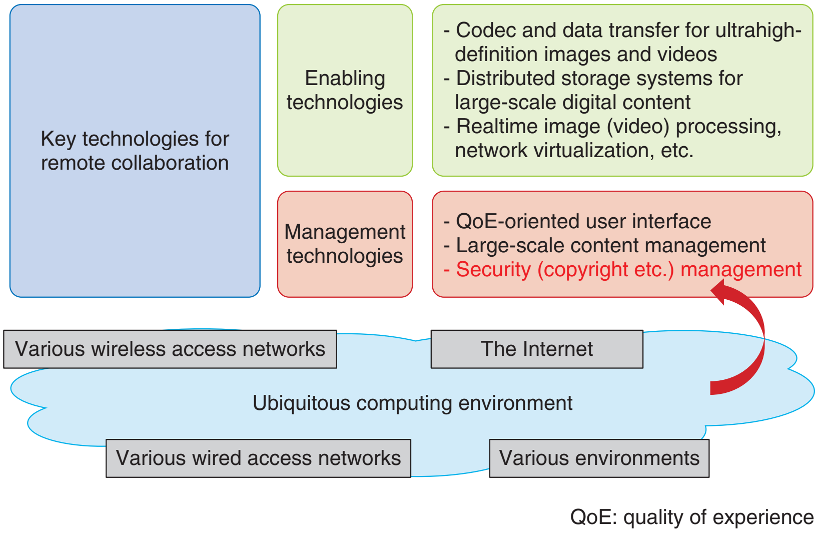
Key technologies for remote collaboration
Enabling technologies
- Codec and data transfer for ultrahigh-definition images and videos
- Distributed storage systems for large-scale digital content
- Realtime image (video) processing, network virtualization, etc.
Management technologies
- QoE-oriented user interface
- Large-scale content management
- Security (copyright etc.) management
Various wireless access networks
The Internet
Ubiquitous computing environment
Various wired access networks
Various environments
QoE: quality of experience

Fig. 2. Key technologies for remote collaboration environment in ubiquitous networks.

security will become more important in this research area in the future (**Fig. 2**).

4. Importance of authentication technology

Security is the key to handling valuable digital content in a ubiquitous computing environment. In particular, an access control method for digital content is especially important. From the network security viewpoint, there are several technologies for protecting digital content from illegal tapping, unauthorized access, and tampering. These include encryption, authentication, and digital watermarking [4]. The main focus of this article is authentication technology.

Robustness against unauthorized access and resistance to tampering are important features of authentication for digital content distribution. They enable distribution of appropriate content to identified people. In terms of security, ideal content distribution would be the delivery of specific content (containing an embedded identifier) by hand from the copyright holder to a user in a closed room. This would require face-to-face confirmation and a physically closed space for absolute authentication. Meeting both conditions in content distribution over a network is impossible. They may be almost met by using high-definition videoconferencing systems and network security technologies. However, this approach is impractical because it is costly. Thus, the general use of password authentication is currently a reasonable solution. In addition, the trade-off between authentication strength and user-friendliness of the authentication process must be considered. The implementation and operational cost of an authentication mechanism should be balanced against the value of the content.

If the authentication process is complicated and difficult for users to understand, they may try to access target content through illegal or unexpected methods. In that case, authentication strength degrades drastically. We focus on this security hazard and describe an easy implementation example of multifactor authentication.

5. Multifactor authentication

Authentication via a network can be broken down into identification, judgment, and authorization processes. In each process, the authentication strength can be enhanced by using multiple methods and information. This is the concept of multifactor authentication. For example, the combination of a specific device and secret knowledge possessed by users can act as a highly secure key for authentication. Using multiple communication methods can also enhance authentication strength. For example, some online banking transactions these days require confirmation by phone.

In particular, mobile phones are useful for multifactor authentication because they are widely used, are used predominantly by one individual, and have a

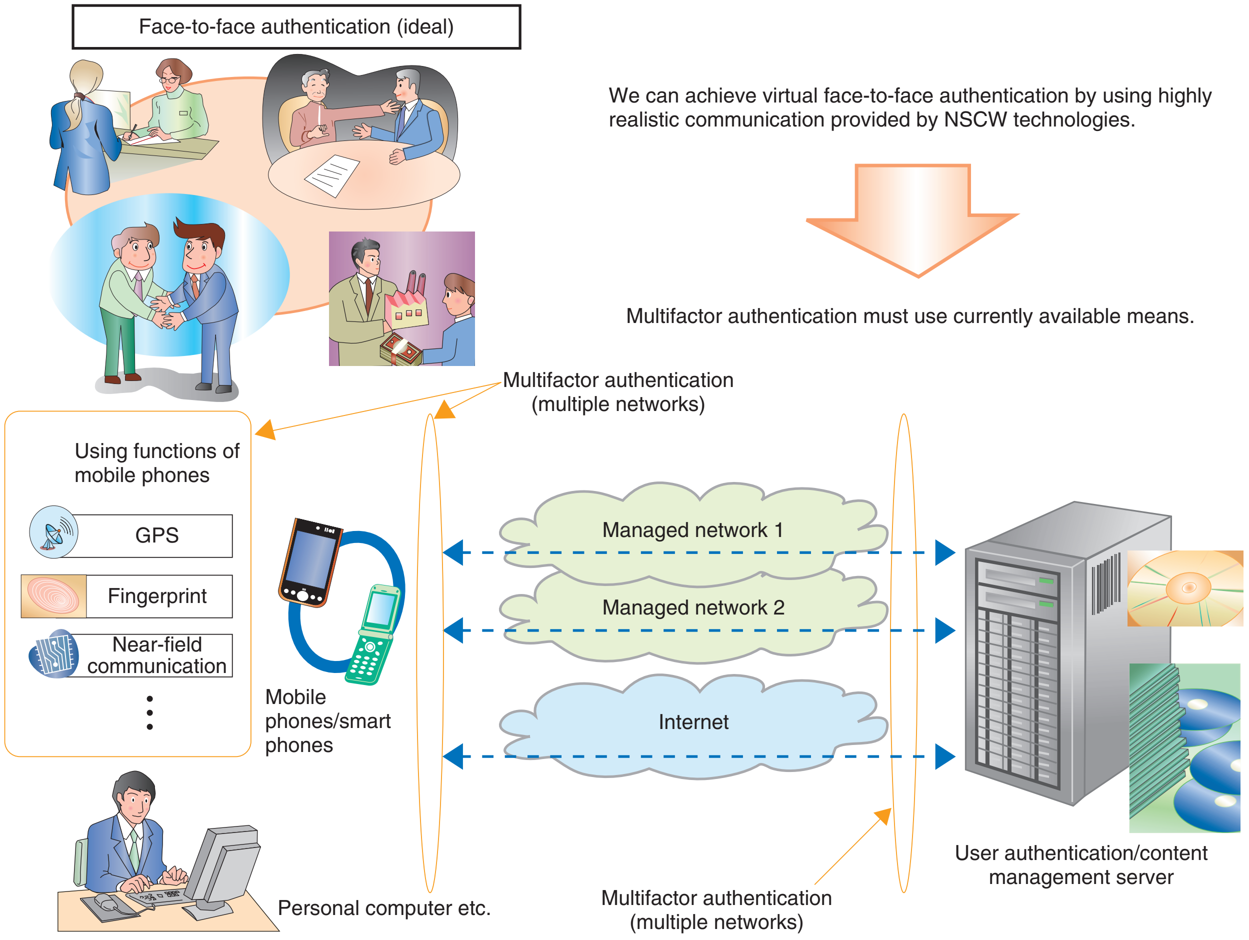
Face-to-face authentication (ideal)
We can achieve virtual face-to-face authentication by using highly realistic communication provided by NSCW technologies.
Multifactor authentication must use currently available means.
Multifactor authentication (multiple networks)
Using functions of mobile phones
GPS
Fingerprint
Near-field communication
⋮
Mobile phones/smart phones
Managed network 1
Managed network 2
Internet
User authentication/content management server
Personal computer etc.
Multifactor authentication (multiple networks)

Fig. 3. User authentication and multifactor authentication technologies.

specific identifier (e.g., phone number). Moreover, the physical hardware cannot be copied and the carrier (operator) can detect illegal usage and tampering and some mobiles contain biometric sensors and GPS (global positioning system) functions. In addition, mobile phones use closed carrier network services (telephone and social networking system (SNS) services), which are independent of other open networks such as the Internet.

One existing example of multifactor authentication for large-scale digital content management is the Arianna System [5]. It is a practical implementation using the Internet (web service) and mobile phone services. However, it cannot support smartphones, which are becoming increasingly popular. We are investigating and developing a new multifactor authentication method using a smartphone as an authentication device (**Fig. 3**). Our method combines multiple authentication keys (users' secret knowledge), biometrics, and geographical information to enhance authentication strength.

6. Future work

NTT Network Innovation Laboratories is promoting research activities for creating an advanced remote collaboration environment through NSCW. The next step is to build an experimental testbed for demonstration experiments on handling large-scale digital content in networks. This will let us examine key technologies such as content storage & archiving and content transmission (**Fig. 4**). We are planning to test multifactor authentication technologies and demonstrate an actual remote collaborative application, such as film making.

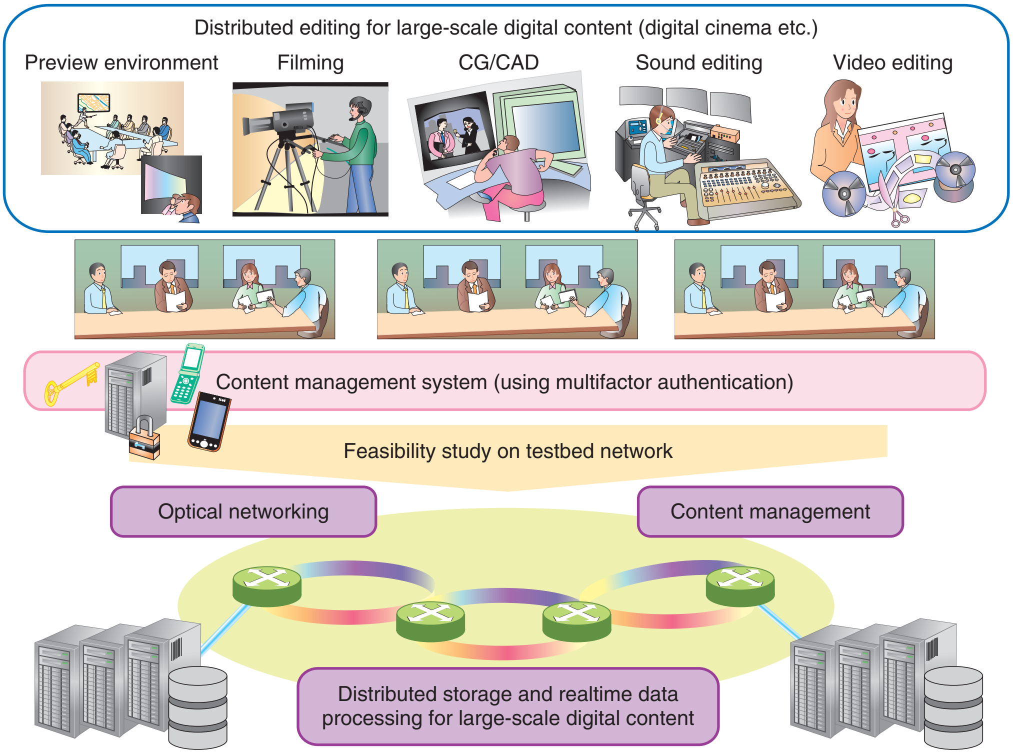
Distributed editing for large-scale digital content (digital cinema etc.)
Preview environment
Filming
CG/CAD
Sound editing
Video editing
Content management system (using multifactor authentication)
Feasibility study on testbed network
Optical networking
Content management
Distributed storage and realtime data processing for large-scale digital content

Fig. 4. Feasibility study of remote collaboration environment for content creation.

7. Conclusion

We think that multifactor authentication is suitable for handling large-scale digital content in a ubiquitous computing environment on open networks. In general, component technologies, such as authentication, encryption, and digital watermarking, are required for the security management of large-scale digital content. Applying these technologies to an actual remote collaboration system handling digital content is a future challenge.

Standardization activities for encryption and digital watermarking are under way and de-facto standards already exist. However, the standardization of authentication technologies is not yet mature. In particular, discussion of the user interface is an open issue.

In this collaboration program between NTT Network Innovation Laboratories and Keio University, we have so far focused on security for remote collaboration and investigated a multifactor authentication mechanism using a mobile phone (a typical ubiquitous device). In the future, we intend to build a testbed and further investigate this topic.

References

[1] D. Shirai, M. Kitamura, and T. Fujii, “4K Super High Definition Video Streaming System Using JPEG 2000 Codec,” IEICE Technical Report, Communication Systems, Vol. 107, No. 244, pp. 43–48, 2007 (in Japanese).

[2] S. Y. Kim, M. Ogawara, T. Fujii, Y. Kamamoto, N. Harada, and T. Moriya, “Requirements for Developing Ultra-realistic Live Streaming Systems,” Proc. of the IEEE ISPACS 2009, pp. 175–178, Kanazawa, Japan.

[3] D. Shirai, M. Kitamura, T. Fujii, A. Takahara, K. Kaneko, and N. Ohta, “Multi-point 4K/2K layered video streaming for remote collaboration,” Elsevier, Future Generation Computer Systems, Vol. 27, No. 7, pp. 986–990, 2011.

[4] B. Schneier, “Beyond Fear: Thinking Sensibly About Security in an Uncertain World,” Springer, 2003.

[5] http://www.dcin.or.jp/actives/ip003/c01.html (in Japanese).

Akihiro Tsutsui

Senior Research Engineer, Supervisor, NTT Network Innovation Laboratories.

He received the B.E. and M.E. degrees in systems engineering from Kobe University, Hyogo, in 1988 and 1990, respectively. Since joining NTT in 1990, he has been researching programmable network devices, high-performance Internet protocols, and home networking. His current interests include data management technologies in networks.

Tomoko Sawabe

Senior Research Engineer, NTT Network Innovation Laboratories.

She received the B.S. and Dr.Eng. degrees from Keio University, Kanagawa, in 1987 and 1996, respectively. She joined NTT in 1987. She has been engaged in research on parallel digital signal processing, multi-DSP architectures, and super-high-definition image processing.