C-*i*UMS: Context Based Smart and Secure Multimedia Service in Intelligent Ubiquitous Home*

Jong Hyuk Park[1], Sangjin Lee[1], and Sung Hee Hong[2]

[1] CIST, Korea University, 5-Ka, Anam-Dong, Sungbuk-Gu, Seoul, Korea
{hyuks00, sangjin}@korea.ac.kr
[2] KETI, Yatap-Dong 68, Boondang-Gu, Seongnam-Si, Kyunggi-Do, Korea
shhong@keti.re.kr

Abstract. In this paper, we propose multimedia service system, called *C-i*UMS (*Context based intelligent* Ubiquitous Multimedia Service), for smart and secure service based on context in intelligent ubiquitous home. The proposed system provides user centric multimedia service based on context including user location, user preference and device status information. In addition, the proposed system supports ubi-home super-distribution which contents can distribute safely and consume from the central intelligent and secure media center to the end terminal in intelligent ubi-home. Furthermore, we propose and apply a VTD*i*C algorithm for customized contents to multimedia players. Finally, a prototype of USN device is designed and implemented to realize intelligent Ubi-home supporting smart service.

1 Introduction

In Ubiquitous Computing (UC), many invisible computers are interactively connected through networks, allowing users to access computer anytime, anywhere. It aims for computing environments where users can easily access computers following their needs. In addition, it is smart environments where computing needed by users is aware by itself. In UC, various computing devices are dispersed for specific users with specific purposes. Furthermore, computing devices are connected without interruption through networks. Being invisible, users only feel the human characteristics of the interface, and such space is not virtual spaces in internet, but spaces of the real world [1, 2].

Intelligent Ubi-Home (IUH) will be made possible through Ubiquitous Computing, and it offers useful services to users. In addition, the area of multimedia services is likely to face increasing demands for user-centric smart and secure services that do not require manual commands from the user [3, 4]. Moreover, the intelligent service becomes available through context awareness technology. This technology is an interaction between users and computers, and its aim is to make such interaction be just as

---

communication among humans. The context mean situation information for at least one object. Moreover, it is subjects that could be the object of situations and they are suitable factor between users or applications. For example, it's person, place, location, light, sound, movement, touch, temperature, user's goals, tasks, work context, business processes, etc. [5, 6, 14].

Projects related to ubiquitous computing include Oxygen of MIT [8], Aura project of CMU [9], Cooltown from HP [10, 11], and TRON project of Japan [12, 13]. The projects are aimed at providing user centric intelligent services.

In [7], we have proposed a user centric intelligent IPMPS in Ubi-home. As an intelligent and secure multimedia copyright protection system in Ubi-home, this system was rather limited in functional aspects.

In this paper, we propose a C-*i*UMS based on [7] and add user context and device context for the intelligent multimedia service appropriate for IUH. In other words, in the proposed system, Intelligent and Secure Media Center (ISMC) receives the current status context of multimedia player located near through ubiquitous sensor network communication between the ISMC and user / device. Afterwards, it provides customized contents through intelligent video transcoding which is suitable for such status. The system also provides Ubi-home super-distribution which contents can distribute safely and consume from the ISMC to the end terminal in IUH.

This paper is organized as follows. In Section 2, system design and implementation are discussed, including architecture, protocol, and analysis. A conclusion is presented in Section 3.

2   *C*-*i*UMS

The proposed system is based on [7] and is composed to provide an intelligent service with ubiquitous features through user context and device context. In this Section, we discuss *C*-*i*MUS architecture, design, protocol, prototype implementation and analysis.

The proposed system consists of two parts, as depicted in Figure 1. One is contents creation and distribution part in extra wire / wireless communication environments, while the other is multimedia service part in IUH. We roughly discuss the front part, and then review *C*-*i*MUS in detail from subsection 2.2.

2.1   *C*-*i*UMS Architecture

The front area of C- *i*UMS consists of CKMA, CP, and CDC.

The Certificate / Key Management Authority (CKMA) issues a certificate to users (contents provider, contents distributor, contents consumer, device, and domain). It provides system validation and authentication functions of the user or device. In addition, it generates and manages key for packaging and communication. Moreover, it provides accounting management for multimedia contents consumption.

The Contents Provider (CP) is a copyright holder that creates secure contents with packager. CP creates PC (Packaged Content) by adding metadata that describes the raw multimedia file in the packaging process, and establishes usage rules.

The Contents Distribution Center (CDC) manages the PCs which are distributed by the copyright holder, and provides an interface which the user consumes the contents. The CDC consists of CMS, LMS, and CSS. The Contents Management System (CMS) manages multimedia which is safely packaged by the CP. It provides related information by using multimedia metadata. The License Management System (LMS) manages licenses used to unlock the user's file lock system in order to play PCs, and gives a license to the end user (consumer) when the right payment has been made. The Contents Streaming Server (CSS) provides contents streaming service to IUH or the end user.
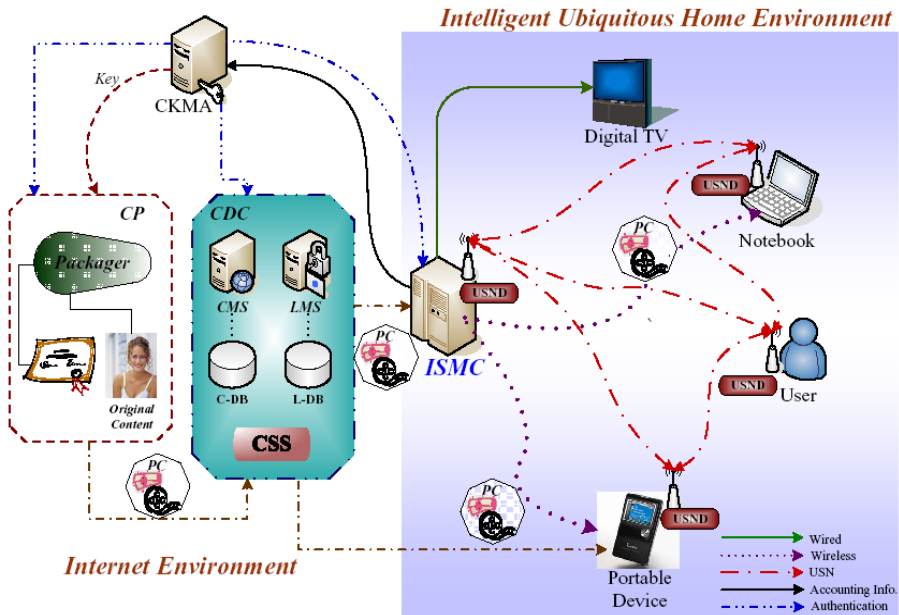

Fig. 1. *C-i*UMS Architecture

2.2 System Design

In this subsection, we discuss components for each block depicted in Figure 2.

The proposed system consists of four main components roughly, which are ISMC, *i*UMP, USND, and End User. In this paper, we assume that an *i*UMP is matched one user (consumer) for facility of the implementation.

- ISMC: It is a core component of the C-*i*UMS architecture. It consists of the SCAM, MMM, DRMSM, CMM, SPMM, and CM.

The Simple Certificate Authority Module (SCAM) registers and manages user or device to the ISMC. In addition, it authenticates the *i*UMP (*intelligent* Ubiquitous Multimedia Player) by acting as a private CA that has authenticated from the extra CKMA.

The Multimedia Management Module (MMM) can serve customized contents among incompatible *i*UMPs by applying a MPEG-21 DIA and intelligent video transcoding.

The Digital Right Management Server Module (DRMSM) is responsible for the security of multimedia downloaded from the CDC. In addition, it saves encrypted contents, protect from illegal copy or falsification of the licenses, and checks right of the certificate and validity of the license. Furthermore, the Accounting Management Engine (AME) receives information occurred by a license usage event based on the usage policy by managing the license usage policy in *i*UMP, and then processes payment in IUH.
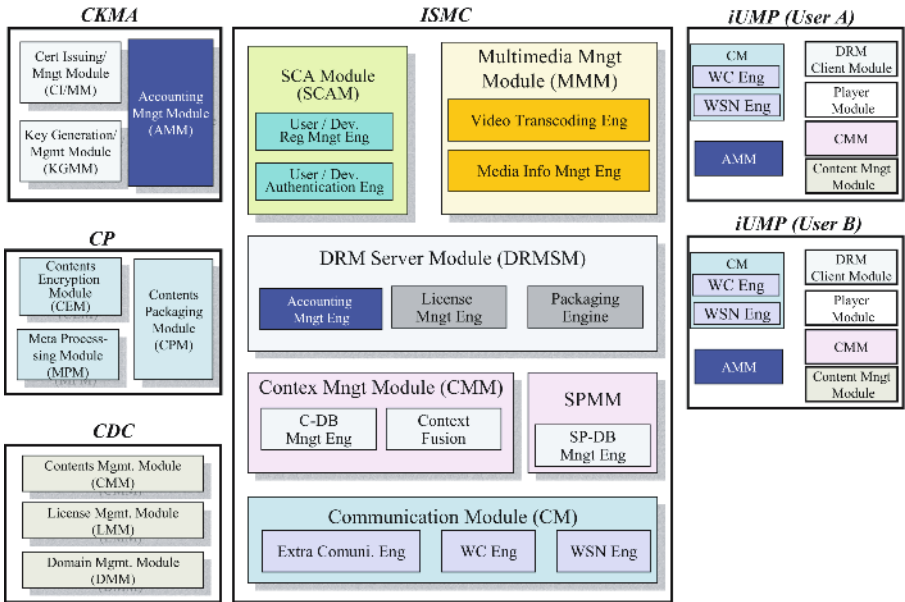

Fig. 2. Components Block-diagram in the *C-i*UMS

The Context Management Module (CMM) stores and controls context information collected into the C-DB (Context – Database) through the USND (Ubiquitous Sensor Network Device). In addition, when a new list of contents arrives at the ISMC, the CMM compares it with user's preference information in C-DB, and then requests the content.

The Security Policy Management Module (SPMM) sets and manages security policy such as authorization (access control) role configuration.

- **USND:** The USND collects context on each *i*UMP and communicates with the ISMC. In other word, this is an interface which provides USN communication between the ISMC and the *i*UMP through the Communication Module (CM). The USND consists of five layers such as follows: the low power manager, sensor parts and a RF communicator, an operation system, protocol engine supporting the network construction among sensor nodes, and application.

- *iUMP:* The *i*UMP is a smart multimedia player with intelligent functions by embedding the USND to the existing multimedia players. Similar with the ISMC, it compares the new contents list (CL) with the preference list (PL) based on user preference context using the CMM. When the lists are matched, it intelligently performs downloading. Content' playing is available after checking the license of the downloaded contents in 2nd terminal – *i*UMP.

- *Improved Location Recognition Method:* In [7], we proposed a user location recognition algorithm based on triangulation using the relationship between RSS (Radio Signal Strength) and location information for the intelligent service. However, the accuracy of the algorithm was influenced too much by the interference of surrounding environments, such as limited power sources or low-power wireless communication. To overcome such shortcoming, we propose an improved location recognition method by applying the Maximum Likely-hood method based on LQI (Link Quality Indicator).

2.3   Two Protocols of the *C-i*UMS

The operation process of the proposed system consists of two protocols. The notations in Table 1 are used throughout this paper.

Table 1. Notations

Notations	Meanings
Rand_1, rand_2	Random number
Pac_k	Key for Packaging
K / K'	Symmetric key pre-shared between the ISMC and User / *i*UMP for each session
ws_k	Symmetric key pre-shared in ubiquitous sensor network communication
A.Request	Request Action 'A'
A_Reg( );	Register User / Device 'A'
A_Cert( );	Certificate of the User / Device 'A'
A_Auth	Authentication of the User / Device 'A'
$E_k(A);$	Encrypt A with a key 'k'
ISMC_SN	Serial number of the ISMC
CL / PL	Contents List / User preferred contents list
N_CL_down( );	New content list downloading
N_Cont_down( );	New content downloading
Comp(A,B);	Compare A with B
$Adv_k(B);$	B is encrypted with a key *k,* and then transmits to each *i*UMP
Reg / Resp	Request and Response
New_Cont_Request( );	Request New contents
iUMP_Sts_Info	Current status of the *i*UMP
VTC(A);	Video Transcoding of the content *A*
$Pack_B (A);$	Package content *A* with a key *B*
$DePack_B(A);$	De-package content *A* with a key *B*
Check(Lice);	Check the license
Play(A);	Play content *A*

2.3.1   Authentication Protocol in the *C-i*UMS

Figure 3 represents an authentication process between the SCAM (ISMC) and the *i*UMP. The process consists of 10 steps as follows.
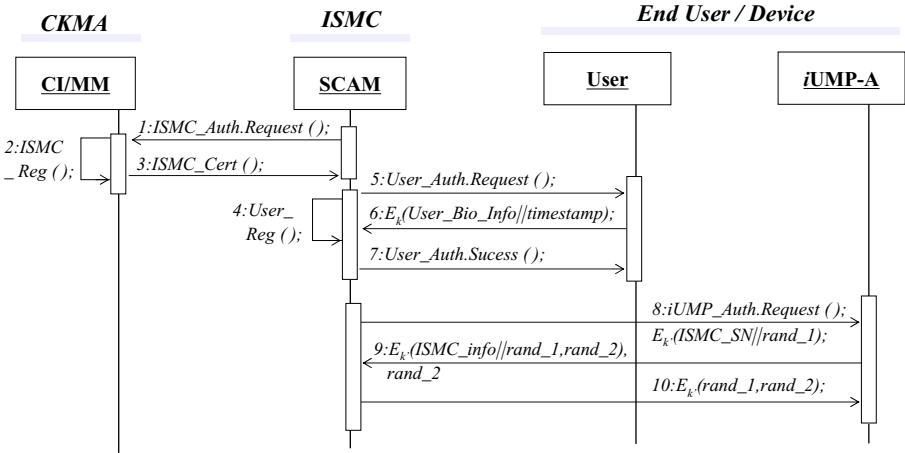

Fig. 3. Authentication Protocol between the *ISMC* and End User / *i*UMP

- **[Step 1-3]:** This step is the ISMC authentication process. The CI/MM (CKMA) authenticates the ISMC with the certificate of the ISMC.
- **[Step 4-7]:** This step is authentication process between the ISMC and user. The user registers to the ISMC, and then requests user authentication. User's biometric information and timestamp are encrypted with session key k, and then transmit to the ISMC. The ISMC confirms user's information, then responses message of the user authentication success.
- **[Step 8-10]:** This step is authentication process between the ISMC and the *i*UMP. The ISMC requests the *i*UMP authentication. In addition, ISMC generates *ISMC_SN* and random number *rand_1* and encrypts them with session key *k'*, and then transmits to the *i*UMP. The *i*UMP generates random number *rand_2* and encrypts the information including it, and then transmits to the ISMC. The ISMC confirms random number *rand_1* and transmits encrypted final message including *rand_1* and *rand_2*.

2.3.2   Smart Multimedia Service Protocol Between the ISMC and the *i*UMP

Figure 4 shows the smart multimedia service protocol between the ISMC and the *i*UMP. This protocol provides user-centric service based on the user preference context. In addition, the protocol provides the customized contents to the *i*UMP based on the current status context of the 2nd terminal - *i*UMP. The process consists of 13 steps as follows
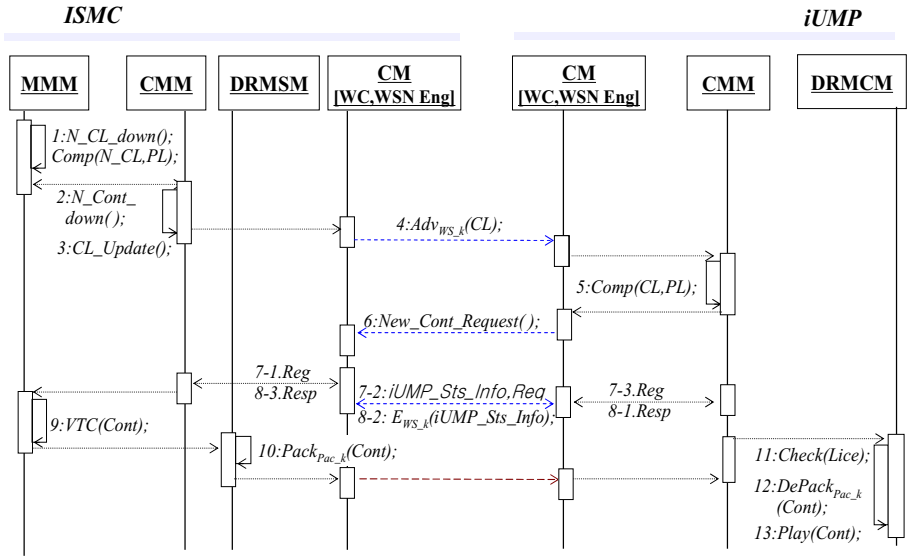
Fig. 4. Smart Multimedia Service Protocol between the *ISMC* and the *iUMP*

- **[Step 1-3]:** This step is the process which new contents are intelligently stored into M-DB. The MMM (ISMC) receives recent contents lists from the extra CDC, and then compares it with user preference from the CMM. If they were matched, new content will be downloaded (or stored) into the ISMC. In addition, the contents list of the ISMC was updated.

- **[Step 4-8]:** This step is a preparing process for smart multimedia service based on context (user preference, device current status information) between the ISMC and the *i*UMP. The CM of ISMC encrypts updated contents list *CL* with a key *WS_key*, and then transmits it to each *i*UMP. CMM of the *i*UMP compares it with user preferred list *PL*. If the list is matched, it requests the new content downloading. In addition, The CM collects current its status contexts - device kind, OS information, CPU clock speed, memory size (main / video), and then transmits them to the ISMC.

- **[Step 9-10]:** This step is video transcoding and re-packaging process. According to intelligent video transcoding decision algorithm based on current status context of the *i*UMP received through step 7-8, video transcoding level (HD / SD) is determined. After then, these contents are packaged with key *pac_k* and transmitted to *i*UMP through wireless communication.

- **[Step 11-13]:** This step is consumption process of the multimedia contents in *i*UMP. After checking the license, the customized PCs are de-packaged and played.

2.3.3 Video Transcoding Decision Algorithms for C-*i*UMS: VTD*i*C Algorithms

In this subsection, we propose the VTD*i*C (Video Transcoding Decision based on *i*UMP Context) algorithm which decides the intelligent video transcoding level (SD/ HD) in C-*i*UMS.

The VTD*i*C algorithm decides the level of video transcoding based on the current status context of *i*UMP collected to the ISMC through the USND.

Input values (*DEV_KIND, OS, CPU_CLK, VIDEO_MEM, and MAIN_MEM*) are the critical elements that decide the content level of the video transcoding. In this algorithm, empirical average values were set as the critical value to provide customized service to *i*UMP. The *DEV_KIND* means the types of device (PC, Notebook, Portable device, etc.) that plays the contents after video transcoding. Playing HD level contents is difficult in OS such as Window CE or Embedded Linux. The *CPU_CLK* means the clock speed of the CPU. Generally, HD level contents are smoothly played in computers better than Pentium IV 1.2 GHz. Finally, memory size is an important element. The *VIDEO_MEM* means video memory size, while the *MAIN_MEM* means main memory size. The HD level contents are smoothly played when the memory size is more than 128 MB, 1024 MB, respectively.

Algorithm 1. Video Transcoding Decision based on *i*UMP Context

```
SubProcedure VideoTranscodingbyDecisioniUMP_Context: VTDiS( )
    Input Context: {DEV_KIND, OS, CPU_CLK, VIDEO_MEM, MAIN_MEM};
    Output: {Function Call};
{
      if((DEV_KIND ne PC) and (DEV_KIND ne  NOTEBOOK)){
         if(OS ne (WIN_CE or EMB_LINUX)){
             if(CPU_CLK gt 1.2G){
                 if((VIDEO_MEM gt 128M) and (MAIN_MEM gt 1024M)) {
                   VideoTranscoding_HD( );
                   }
                   else VideoTranscoding_SD( );
   }
             else VideoTranscoding_SD( );
             }
         else VideoTranscoding_SD( );
            }
      VideoTranscoding_SD( );
}
```

2.4 Prototype Implementation and Analysis

In this subsection, we discuss the prototype implementation of the proposed system, and review the differences between the proposed system and the exiting systems.

- **Implemented the USND:** The USND is a communication module based on a 900MHz band to enable wireless communication, and is comprised of MCU Atmega 128 and RF module CC1000. The RF module CC1000 measures the RF signal strength, which it outputs to the RSSI port. The USN Module also has self-organizing capability.

- Tests for the improved location recognition method: Figure 5 is graphs showing the relationship between the distances in the previous location recognition algorithm [7] based on the RSSI triangle measure and the improved location recognition method based on the LQI, which is currently developed and researched on its prototype stage. Compared to the RSSI, the LQI shows a result more proportionate to distance. However, In IUH, location information with physically relative concept such as user, device and room is more important than the absolute value. Thus, connective improvements are being made to build network and provide service when user come close to electric device or service machines, rather than measuring the absolute distance using the LQI.
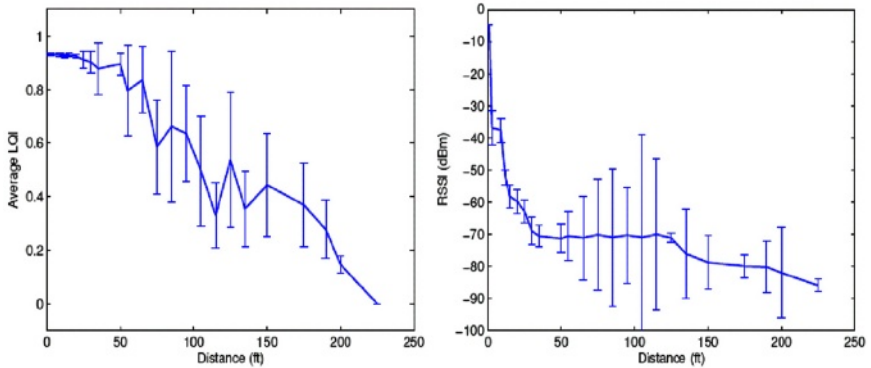

Fig. 5. Graphs showing the relationship between the distances in the previous location recognition algorithm [7] based on the RSSI triangle measure] and the improved location recognition method based on the LQI

- Multimedia Contents Consumption in *i*UMP: In Figure 6, the left shows a screen that contents isn't played due to missing license, while the right shows a screen that customized downloaded content is played after the valid license checking.
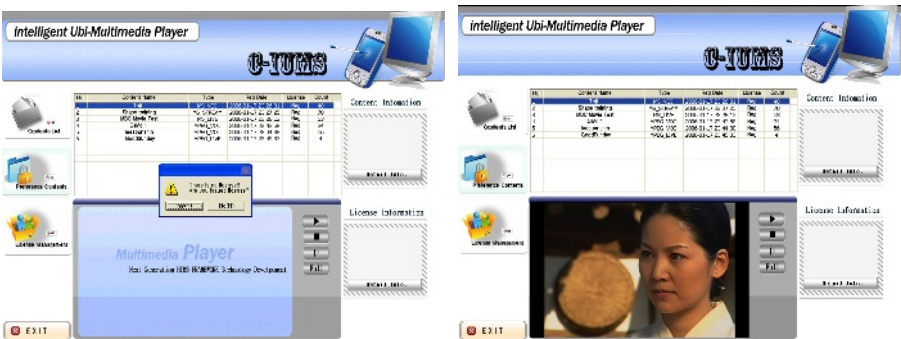

Fig. 6. License Checking and Preference Contents Play

In the next, we discuss the characteristics of the proposed system by comparing it with research areas related to this paper. Up to now, it is difficult to find researches of context-based smart and secure multimedia service in IUH. The proposed system has distinguished characteristics as follows; supporting of user-centric service based on user location recognition, supporting of contents customized to device status, supporting of multimedia service based on user preference context, support on super-distribution in IUH, supporting of efficient authentication and device management within IUH

- ***Supporting of user-centric service based on user location recognition:*** In [7], RSSI triangle measure was proposed as location recognition algorithm to provide intelligent service in ubiquitous home environment. Being vulnerable to surrounding interference, however, the results weren't satisfying. The proposed system improved such shortcoming, and a prototype of improved user location recognition method based on LQI is being developed. Improvements are shown in Figure 5.
- ***Supporting of contents customized to device status context:*** In previous systems, the level of contents (SD/HD) was fixed to the environment of device. However, the proposed system grasps the status information in *i*UMP and applies the VTD*i*C algorithms described in subsection 2.3 to provide customized contents to device.
- ***Supporting of service based on user preference context:*** As a part of user-centric service provided only in IUH, the proposed system is provided preferred contents based on user preference context, as shown in Figure 6.
- ***Supporting of Ubi-home super-distribution:*** In the existing home multimedia services, the safety of 2nd contents distribution within home was not considered. In the proposed system, however, CP distributes contents and licenses which are considered 2nd distribution in IUH. In addition, the ISMC provides ubi-home super-distribution to make sure 2nd distribution is safely performed.
- ***Efficient authentication and device management in IUH:*** In the existing systems, user and device authentications were provided through PKI algorithm, the management of a new user or a device is complicated. In the proposed system, however, the SCA module is applied in ISMC to authenticate the new user and the device, improving the efficiency of management.

3   Conclusion

As a new paradigm, ubiquitous computing properly combines all components (human, objects, environments, etc.) in the world to realize human-centric services. Currently, worldwide researches on ubiquitous computing are being actively made.

In this paper, we proposed smart and secure multimedia service based on context in intelligent ubiquitous home. The system provides user-centric service based on context to realize more improved multimedia services. In addition, the system provides customized content services to the *i*UMP by proposing / applying the intelligent VTD*i*C algorithm. Finally, to resolve security issues generated during contents distribution in IUH, the system provides Ubi-home super-distribution.

References

1. Mark Weiser: The Computer for the 21st Century, Scientific American (1991), 94-104
2. Mark Weiser: Hot topic: Ubiquitous Computing IEEE Computer (1993), 71-72
3. Jong Hyuk Park, Heung-Soo Park, Sangjin Lee, Jun Choi, Deok-Gyu Lee : Intelligent Multimedia Service System Based on Context Awareness in Smart Home, KES 2005, Springer-LNAI, Volume 3681 (2005), 146-1152
4. K. Carey, D. Lewis, S. Higel, V. Wade: Adaptive Composite Service Plans for Ubiquitous Computing, in proc. 2nd International Workshop on Managing Ubiquitous Communications and Services (MUCS), Dublin (2004), 13-14
5. A.K. Dey and G.D. Abowd: Towards an understanding of context and context awareness, HUC99 (1999)
6. Guanling Chen & David Kotz: A Survey of Context-Aware Mobile Computing Research. Dartmouth College TR2000 381 (2000)
7. Jong Hyuk Park, Jungsuk Song, Sangjin Lee, Byoung-Soo Koh, and In-Hwa Hong: User Centric Intelligent IPMPS in Ubi-Home, ICCSA 2006, Springer-LNCS, Volume 3983 (2006), 245 – 254
8. Project Oxygen web sitehttp://www.oxygen.lcs.mit.edu
9. Project Aura web site, http://www.cs.cmu.edu/~aura/
10. Project CoolTwon Web site, http://cooltown.hp.com/
11. Tim Kindberg, , John Barton, Jeff Morgan, Gene Becker, Debbie Caswell, Philippe Debaty, Gita Gopal, Marcos Frid, Venky Krishnan, Howard Morris, John Schettino, Bill Serra: People, Places, Things: Web Presence for the Real World, HPL-2000-16 (2002)
12. Project TRON web site, http://www.tron.org/
13. http://www.sakamura-lab.org/TRON/overview.html
14. Matthias Baldauf and Schahram Dustdar: A Survey on Context-aware systems, TUV-1841-2004-24 (2004)