International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.11 (2015), pp.43-56
http://dx.doi.org/10.14257/ijmue.2015.10.11.05

Development of a User Management Module for Internet TV Systems

Kangjai Lee[1] and Jaegeol Yim[2*]

[1]*Dept. of Computer Information, Suwon Science College, Hwaseong, Gyeonggi, Korea*

[2]*Dept. of Computer Engineering Dongguk University, Gyeongju, Gyeongbuk, Korea*

kjlee@ssc.ac.kr, yim@dongguk.ac.kr

Abstract

The first step of accessing computer systems is typing in a user ID and a password. The user management system of the computer system then authenticates the user. Only after authentication is the user allowed to access the computer system. In addition to authentication, authorization is also performed by user management systems. For Internet TV systems, authorization is extremely important because Internet TV channels and videos should only be accessed by authorized users. Furthermore, user management systems record who accessed which TV channels and videos when and how long. This information is used by the billing system. Therefore, we develop a user management system for Internet TV systems. Our user management system controls accessing resources based on the roles of the user.

Keywords: *User Management; Access Control; Internet TV; Authentication; Authorization*

1. Introduction

There is no practical computer application software that does not have a user management component. It is the user management component that allows users to login to the system and to permit users to access resources. Therefore, a user management performs extremely important roles of protecting classified information from unauthorized individuals and of keeping track of who accessed what resources and when. For example, a user management system protects credit card numbers and passwords of the cards in a customer database from malicious persons.

On the other hand, a user management system should also allow all resources to be used by authorized persons. To this end, a user management system has to be able to authenticate and authorize users [1]. In other words, it should be able to confirm the identity of a person and control authenticated users' access to system resources.

Reflecting the roles of user management system, we can notice that it is closely related to access control and security. This paper reviews the techniques that are useful for designing user management systems and develop a user management system for Internet TV systems.

[*] Corresponding Author

ISSN: 1975-0080 IJMUE

2. Techniques for User Management

2.1. Policy-Based Access Control [2-3]

The authors of [2] introduced a policy-based access control to solve security and privacy problems of social networking. It controls access based on privacy policies. A Policy-Based Access Control (PBAC) consists of an Integrated Authentication, an Access Control Handler, and a Privacy Policy Controller. Integrated Authentication is based on identifying the user and his/her mobile device. This identifies a user with a combination of user authentication (user's name/password) and device authentication. Access Control Handler assigns an authority to an authenticated user based on the user's role, purpose, and condition. Privacy Policy Controller securely manages the personal data disclosed by a user in the social network environment. Privacy Policy Controller issues privacy notices when Personal Information Protection Act is violated.

Combining a relational database management system and a policy evaluation engine, the authors of [4] introduced a new access control system for large databases [3-4]. The system has several advantages including:

- Rules are stored, evaluated, and enforced by the database system
- This system allows access control for entire rows as well as individual fields.
- This system is DBMS-independent
- Applications need not be aware of the new access control module.
- Policy rules follow common trust management approach for writing policy rules.

The authors of [5] introduced a policy-based access control model to support access control based on privacy policies. This system is a systematic and comprehensive privacy policy based on the purpose, condition, and role of the user and helps to protect users from potential dangers in social network environments [3].

The proposed system consists of IAM (Integrated Authentication Mechanism), ACHM (Access Control Handler Mechanism), and PPCM (Privacy Policy Controller Mechanism).

IAM is based on identifying the user and the mobile device, such as a cellular phone, a smartphone, or a tablet PC. This is a method of identification that combines user authentication based on certificates or a username/password with device authentication based on dynamic information.

ACHM is given authority according to that of the authenticated user through the IAM. Access control is enabled based on the role, purpose, and condition defined below.

PPCM securely manages the personal data disclosed by a user in the social network environment. The purpose of collecting personal or sensitive information is clearly stated by SNS, and it is important to gather a minimum level of data on SNS users. Unique identifying information, such as a social security number, is not stored, or, in the case of Korea, is only used for encryption. PPCM issues privacy notices when Personal Information Protection Act is violated.

Users can set up a privacy policy for their desired security level, and this is automatically managed when making, using, and collecting personal data. The privacy policy in this mechanism is built on XACML [5]. This policy document indicates the status of access control and specifies the privacy protection policies.

2.2. Light-Weight Access Control Mechanism [3]

Authorization specifies the authenticated user's right to access resources. Legacy authorization mechanisms can be categorized into two models: centralized authorization model and distributed authorization model. In centralized authorization model, a centralized trusted authority is responsible for controlling access. The centralized trusted authority is overloaded when the system is a relatively large-scale network. On the other hand, in the distributed authorization model, each subject manages its own policy for authorization and maintaining consistency is difficult.

The authors of [7] introduced Light-Weight Access Control mechanism as an alternative for the existing methods. In this mechanism, an authorization server issues an authoricate that is a certificate for authorization and contains rules for authorization. The process of the authorization consists of the following six steps: maintaining authorization policy, key distribution, issuing authoricate, request for service, verify the authoricate, and permit or prohibit.

2.3. Access Control for Cloud Computing Systems [3]

Cloud computing architectures can make full use of powerful machines by creating virtual machines on them and rearrange the computing power for different applications [8]. In cloud systems, infrastructure, platform and software are regarded as services. Infrastructure as a service (IaaS)/ platform as a service (PaaS)/ software as a service (SaaS) corresponds to hardware/operating system/application software of traditional computer systems [9].

After analyzing security in traditional systems and cloud system, the authors of [9] introduced access control architecture for cloud computing systems. In the architecture, light weighted services are implemented on virtual machines, core applications run on powerful servers or clusters, and the administrator node is kept in a secure environment.

In a virtual cluster based Cloud Computing environment, the sharing of infrastructure introduces two problems on user management: usability and security [10]. The authors of [10] proposed a uniform user management system that is fit for the scale expansion and interconnection of dynamic virtualization environment. The user management system supplies a global user space for different virtual infrastructures and application services in one cloud, and allows user system interconnection among homogeneous cloud instances.

The authors of [11] proposed an access control model for negative authorization to provide the user with the ability and flexibility of specifying the objects to which access is not desired through the means of negative authorization. Compared to the filtering mechanism that blocks unwanted information and services, negative authorization has the advantage of saving precious computation and network resources because access control happens prior to actual access in negative authorization.

2.4. Other Related Works [3]

Virtual environments have recently gained a lot of attention. The concept of avatars and the introduction of social abilities in virtual environments have recently encouraged people to participate in creativity while having fun. The authors of [12] proposed a novel joint hierarchical node based user management infrastructure for the development of scalable and consistent virtual worlds.

3. Design

3.1. System Requirements

Our user management system allows the system manager to register, delete, update, and retrieve user information. It also classifies users into groups depending on their roles and assigns resource access levels to groups. It is a unified ID management system in that a user may not log in again in order to access another sub-system. The system requirements are itemized as follows:

- Unified ID management.
- Create, delete, update, and retrieve information of users
- Create, delete, update and retrieve information of user groups

- Establishing the relationships between users and user groups
- Assigning access levels to user groups
- Authentication with a token
- Logging (recording) all events

3.2. Context Diagrams

3.2.1. Management of My Information

As is shown in Figure 1, a system user can retrieve, update, and delete his/her information and password with user management system.

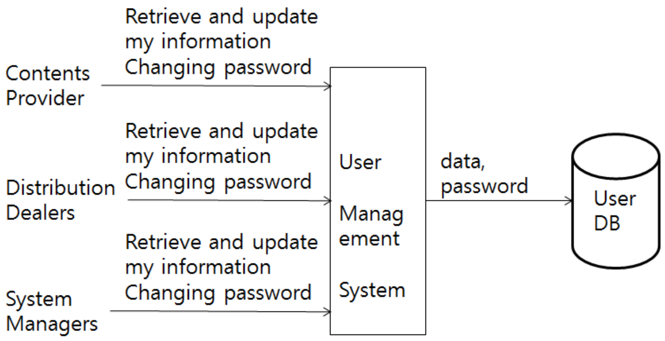


Figure 1. A Context Diagram for Management of my Information

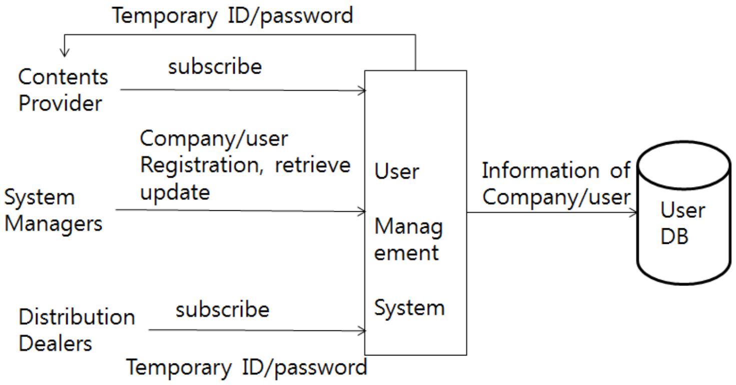


Figure 2. A Context Diagram for the Management of Users

3.2.2. Management of Users

When a user accesses our user management system for the first time, the user obtains a temporary account as is shown in Figure 2. Users should login with their temporary account and change their IDs and passwords immediately.

3.2.3. Login/Logout

User login and logout can be requested through the registration system. The registration system delivers the user ID and password to the user management system, then the user management system gets a token and transfers it to the registration system as shown in Figure 3.

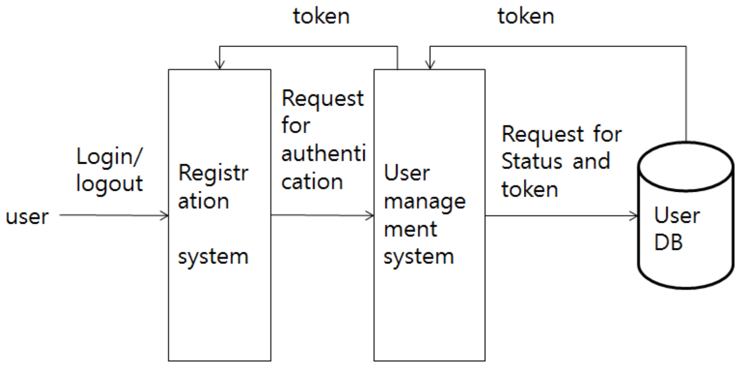


Figure 3. A Context Diagram for Login/Logout

3.2.4. Unified ID Management

An Internet TV system consists of a content management system, content registration system, broadcast management system, metadata management system, distribution management system, log (trace) system and others. When users access these component systems, they use their tokens for authentication as shown in Figure 4. Whenever a request for authentication with a token arrives, the expiration date of the token is extended.

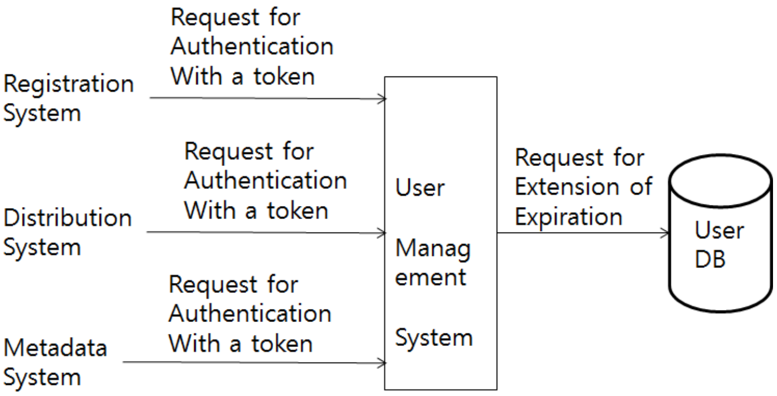


Figure 4. A Context Diagram for Unified Access Management [1]

3.3. Workflows

3.3.1. The Process of Our User Management System

Users of our Internet TV system can be classified into content providers, content distributers, and system managers. Figure 5 shows the process of accessing component systems of our Internet TV system. A subscribed user accesses the system through the context registration component and types in his/her valid ID and password in order to get a token. After this moment, the user shows this token to other component systems such as metadata management system, distribution management system, and others whenever the user wants to access those systems. These systems evaluate the user's authority for accessing resources with the token.

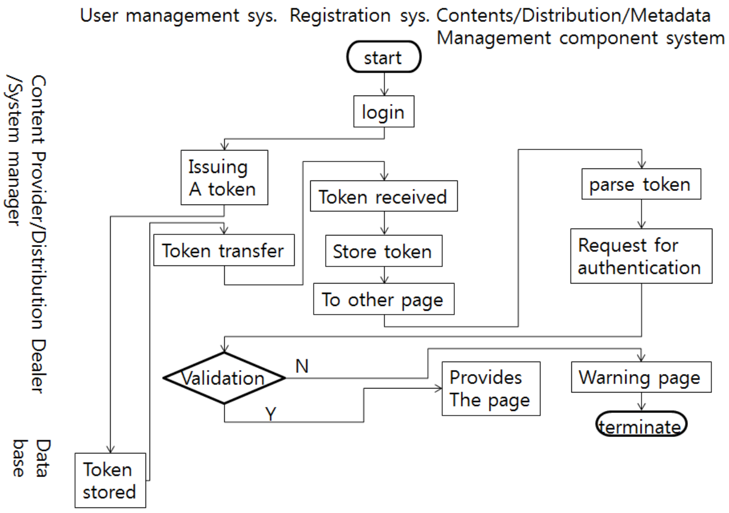


Figure 5. The Process of Our User Management System [1]

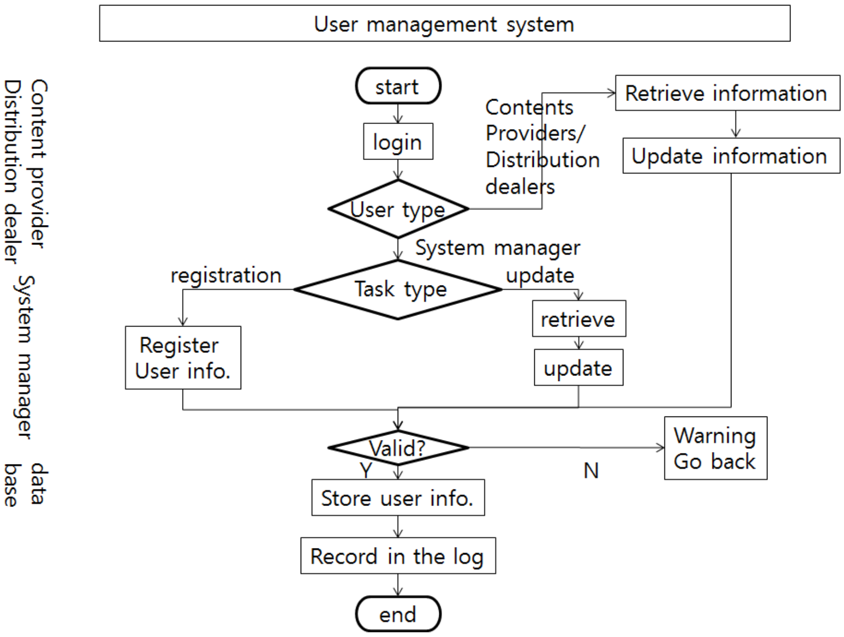


Figure 6. The Process of User Registration Component

3.3.2. Workflow of User Registration

Our user registration component allows system managers to register new users and retrieve and update user information. It also allows contents providers and distribution dealers to retrieve and update their information as shown in Figure 6.

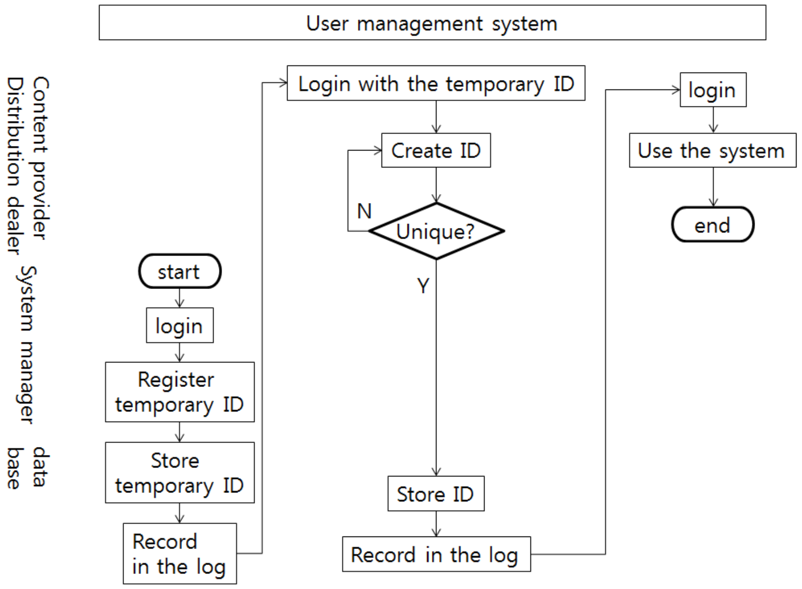
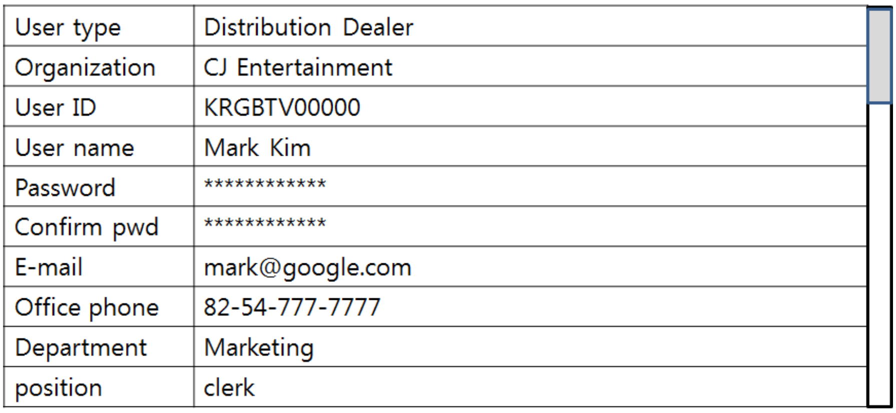


Figure 7. The Process of Issuing a User ID

3.3.3. Workflow of System Access for New Users

New users access the system with temporary IDs as shown in Figure 7. A new user has to login the system immediately after getting a temporary ID and create a unique ID.



User type	Distribution Dealer
Organization	CJ Entertainment
User ID	KRGBTV00000
User name	Mark Kim
Password	************
Confirm pwd	************
E-mail	mark@google.com
Office phone	82-54-777-7777
Department	Marketing
position	clerk

Figure 8. User Interface for Updating my Information [1]

3.4. User Interface Design

A typical user interface of our user management system is shown in Figure 8. In the screen, the user information is listed in text boxes so that the user can modify listed data. The list is associated with a scroll bar with which the user can scroll the list.

3.5. Database Design

We define "UserTable" (OSP_USRM_USER) in order to store user information including user ID and password for authentication. The attributes of the table are: USER_ID, USER_SEQ, USER_Code, COMPANY_ID, USER_Name, USER_pwd (password), EMAIL, PHONE_NO, DEPARTMENT, POSITION, JOB, STATE_Code, REG_ACT_Date(registration date), REG_ACT_ID, UPD_ACT_Date (updated date), UPD_ACT_ID (ID of the person who made last update), DEFAULT_TF.

An example query to retrieve a person's information with his/her ID is as follows:

```
SELECT T1.USER_ID, T1.USER_CD, 'common.code.Z08.' || T1.USER_CD AS
USER_CD_NM, T1.COMPANY_ID, T1.USER_NM, T1.USER_PASS, T1.EMAIL,
T1.PHONE_NO, T1.DEPARTMENT, T1.POSITION, T1.JOB, T1.STATE_CD,
T2.COMPANY_NM, T2.COUNTRY_CD,
" AS RESULT, " AS MESSAGE, T1.USER_SEQ, T1.DEFAULT_TF, " AS
SERVICE_AREA_CD
FROM UserTable T1, CompanyTable T2
WHERE T1.COMPANY_ID=T2.COMPANY_ID
ANDT1.USER_ID='KRGBTV00000'
```

Most of the users of our Internet TV are working for an organization or a company. Information of those organizations and companies is stored in "CompanyTable" consisting of the following attributes: COMPANY_ID, COMPANY_NM, COUNTRY_CD, COMPANY_Code, BUSINESS_NO, REPR_Name (name of the representative of the company), CATEGORY, SECTOR, Number_Employees, Sales, CompanyRatingCode, Homepage, Phone_No, Fax_No, eMail, Zipcode, Address, Bank, AccountNo, AccountName, StateCode, RegActDate (Date of registration), RegActID (the person who registered), UpdateActDate, UpdateActID, DefaultTF, ServiceAreaCode

Whenever a user logs in, our user management system issues a unique token and records the time when the token is used in "LoginTable" consisting of the following attributes: Token, UserID, and ConnectDate. ConnectDate represents the time when the token is used most recently. If the difference between the current time and ConnectDate is greater than a certain threshold, then our user management system invalidates the token and forbids the user from accessing the system. Then, the user has to log in again in order to obtain another token. Note that users do not notice they use tokens; they just click buttons in order to express their intention. Then, the listener associated with the button invokes the function in the business layer with the token implicitly. The following is an example code needed for authentication:

```
SELECT USER_ID, CONNECT_DT

FROM LoginTable

WHERE TOKEN = '93D71AED2DAB4C0EA3AFDF8348B12A1A'
```

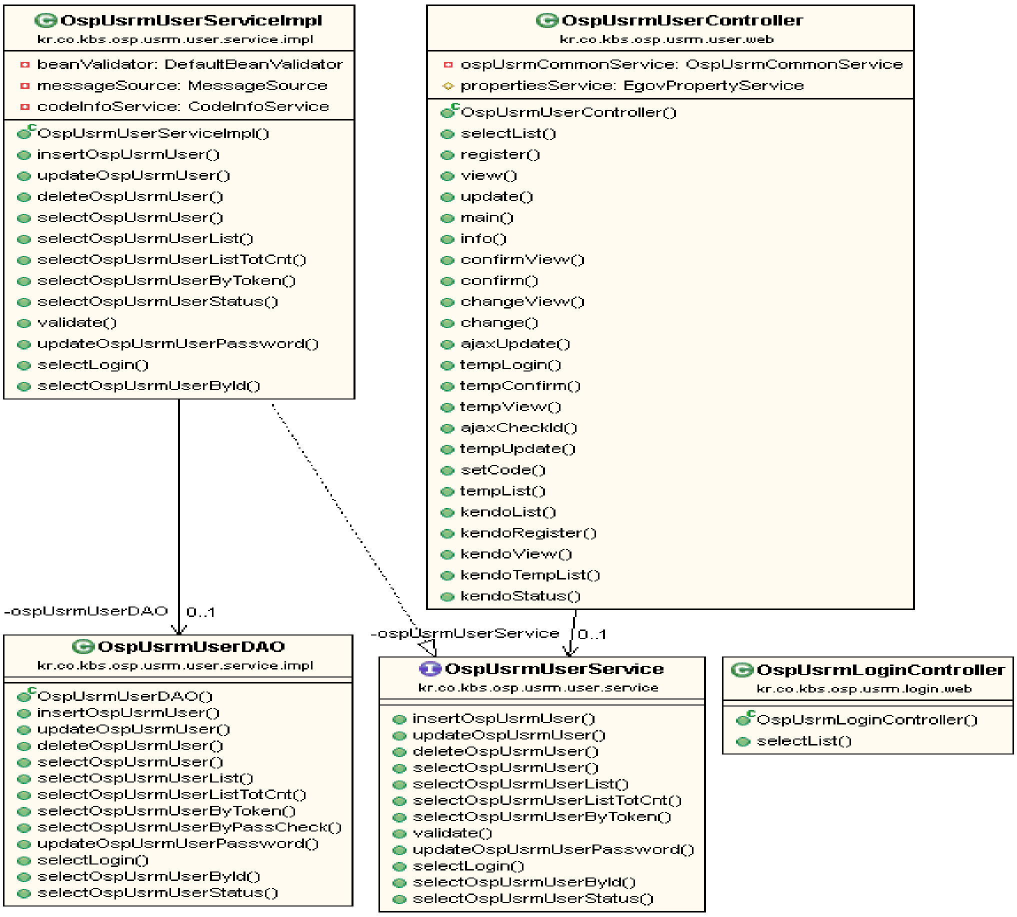


Figure 9. Part of the Classes Implemented in the Server [1]

By this moment, readers would have found that we need a table where all the codes appear in "UserTable" and others are defined. We define "CommonCodeTable" consisting of the following attributes: Code, CodeGroupCode, CodeName, and CodeNameEng. An example query to retrieve codes that belong to a code group is:

SELECT TRIM(' ' FROM UPPER(CODE)) AS CODE,

UPPER(CODEGROUPCODE) AS CODEGROUPCODE, CODENAME

FROM CommonCodeTable

WHERE CodeGroupCode='Z12'

Since we have "CodeGroupCode" in "CommonCodeTable," we have to define "commonCodeGroup" table consisting of CODEGROUPCODE, CODEGROUPNAME, CODEGROUPNAME_ENG, and CODENAME_ENG. The following is a sample query to obtain about a CODEGROUPCODE.

SELECT CODEGROUPNAME, CODEGROUPNAME_ENG

FROM CommonCodeTable

WHERE CODEGROUPCODE = 'Z01'

4. Implementation

We have implemented Web Services for login, logout, and info. The info service retrieves information of a user. Web Service "login" authenticates the user with userID and password. Then it issues a token if the user is successfully authenticated. It can be invoked by the following sentence:

http:// .../api/user/login (userId, userPass).

It returns a character (result: S if succeed, E otherwise), a string (message: detail description of the result), and a token (32 character).

Web Service "logout" is invoked when a user clicks the "logout" button or closes the web browser. It can be invoked by the following sentence:

http:// ……/api/user/logout (token).

In order to retrieve the information of a user, we can use Web Service "info" with the following sentence:

http:// ……/api/user/info (token)

Web Service "info" returns result, message, userId, userName, userCode, companyId, companyName, countryCode, serviceAreaCode, and so on.

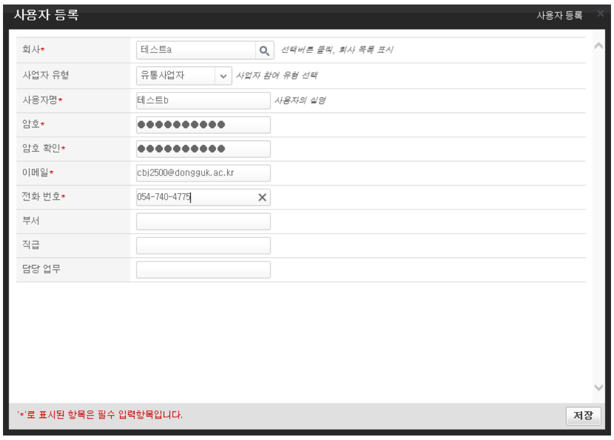
We have discussed the typical user interface of our system in the previous section. The user interfaces have been implemented in jsp. For example, the user interfaces for user information retrieval, basic information update, and password change have been implemented in /web/user/info.jsp, web/user/myinfo.jsp, and web/user/change.jsp, respectively.

The user interface for company information retrieval and a list of registered companies has been implemented in /web/kendo/company/list.jsp. The user interface for registration of a new company and update of detail information of companies has been implemented in /web/kendo/company/register.jsp.

A part of the classes implemented in the server are shown in Figure 9. OspUsrmUserController controls the requests for inserting, deleting, updating or retrieving user information, OspUsrmUserServiceImpl defines methods that perform the requested services, and OspUsrmUserDAO has methods that access the database. In a similar manner, classes to manage company information, login information, and user information have also been implemented.

5. Experiments

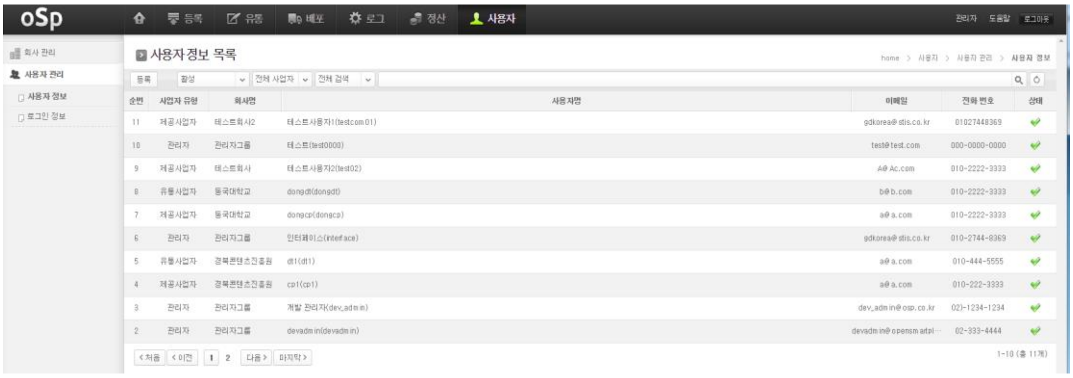
We have performed experiments to test our user management system. User registration has been tested as shown in Figure 10.



회사*	테스트a	선택버튼 클릭, 회사 목록 표시
사업자 유형	유통사업자	사업자 참여 유형 선택
사용자명*	테스트b	사용자의 실명
암호*	●●●●●●●●●●●	
암호 확인*	●●●●●●●●●●●	
이메일*	cbj2500@dongguk.ac.kr	
전화 번호*	054-740-4775	
부서		
직급		
담당 업무		

'*'로 표시된 항목은 필수 입력항목입니다.

Figure 10. A Screen Shot of User Registration



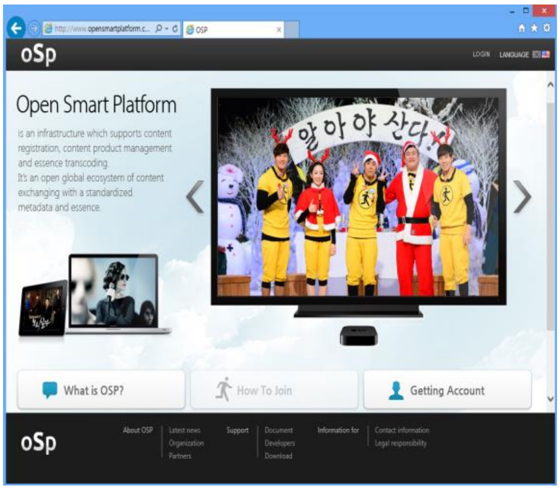
사용자 정보 목록

순번	사업자 유형	회사명	사용자명	이메일	전화 번호	상태
11	제공사업자	테스트회사2	테스트사용자1(testcom01)	gdkorea@stis.co.kr	01027448369	✓
10	관리자	관리자그룹	테스트(test0000)	test@test.com	000-0000-0000	✓
9	제공사업자	테스트회사	테스트사용자2(test02)	A@Ac.com	010-2222-3333	✓
8	유통사업자	동국대학교	dongdt(dongdt)	b@b.com	010-2222-3333	✓
7	제공사업자	동국대학교	dongcp(dongcp)	a@a.com	010-2222-3333	✓
6	관리자	관리자그룹	인터페이스(interface)	gdkorea@stis.co.kr	010-2744-8369	✓
5	유통사업자	경북콘텐츠진흥원	dt1(dt1)	a@a.com	010-444-5555	✓
4	제공사업자	경북콘텐츠진흥원	cp1(cp1)	a@a.com	010-222-3333	✓
3	관리자	관리자그룹	개발 관리자(dev_admin)	dev_admin@osp.co.kr	02)-1234-1234	✓
2	관리자	관리자그룹	devadmin(devadmin)	devadmin@opensmartpl…	02-333-4444	✓

<처음 <이전 1 2 다음> 마지막>

1-10 (총 11개)

Figure 11. A Screen Shot of Retrieving Temporary IDs



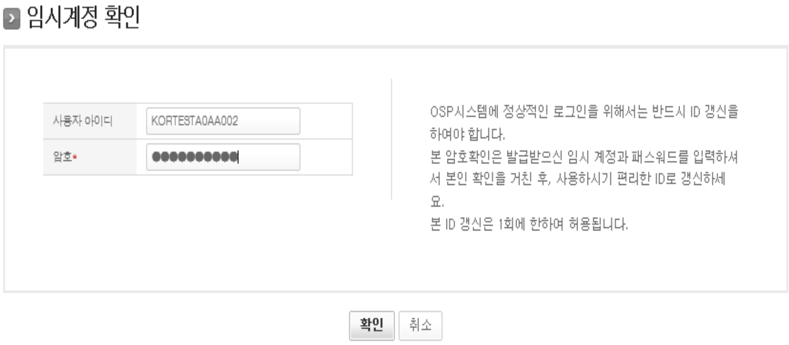
Open Smart Platform

is an infrastructure which supports content registration, content product management and essence transcoding.
It's an open global ecosystem of content exchanging with a standardized metadata and essence.

Figure 12. "Getting Account" is for New Users with their Temporary IDs

Our user management system issues a temporary ID to a new user. A system manager can retrieve temporary IDs as shown in Figure 11 and deliver them to new users.

A new user with his/her temporary ID has to click the "Getting Account" button on the main page shown in Figure 12.



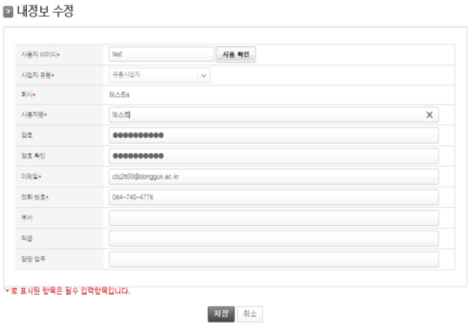
임시계정 확인

사용자 아이디	KORTESTA0AA002
암호*	●●●●●●●●●●

OSP시스템에 정상적인 로그인을 위해서는 반드시 ID 갱신을 하여야 합니다.
본 암호확인은 발급받으신 임시 계정과 패스워드를 입력하셔서 본인 확인을 거친 후, 사용하시기 편리한 ID로 갱신하세요.
본 ID 갱신은 1회에 한하여 허용됩니다.

Figure 13. A Screen Shot of Logging in with a Temporary ID

After clicking the "Getting Account" button, the user has to login the system with his/her temporary ID as shown in Figure 13.

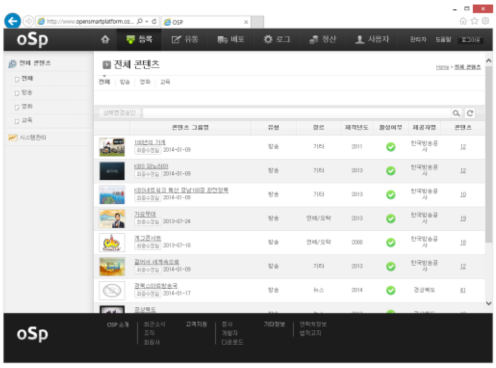


내정보 수정

사용자 아이디•	test 사용 확인
사업자 유형•	유통사업자
회사•	테스트a
사용자명•	테스트
암호	●●●●●●●●●●●
암호 확인	●●●●●●●●●●●
이메일•	cbj2600@dongguk.ac.kr
전화 번호•	064-740-4776
부서	
직급	
담당 업무	

'•'로 표시된 항목은 필수 입력항목입니다.

Figure 14. A Screen Shot of Changing ID and Password

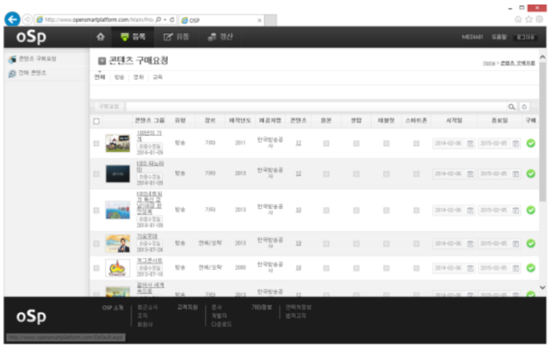


전체 콘텐츠

전체 | 방송 | 영화 | 교육

콘텐츠 그룹명	유형	장르	제작년도	활성여부	제공자명	콘텐츠
100년의 기계 최종수정일 2014-01-09	방송	기타	2011	✓	한국방송공사	12
KBS 파노라마 최종수정일 2014-01-09	방송	기타	2013	✓	한국방송공사	12
KBS네트워크 특선 경남100경 완전정복 최종수정일 2014-01-09	방송	기타	2013	✓	한국방송공사	10
가요무대 최종수정일 2013-07-24	방송	연예/오락	2013	✓	한국방송공사	19
개그콘서트 최종수정일 2013-07-18	방송	연예/오락	2000	✓	한국방송공사	18
걸어서 세계속으로 최종수정일 2014-01-09	방송	기타	2013	✓	한국방송공사	12
경북스마트방송국 최종수정일 2014-01-17	방송	뉴스	2014	✓	경상북도	41
경상북도						

Figure 15. User Interface for System Managers

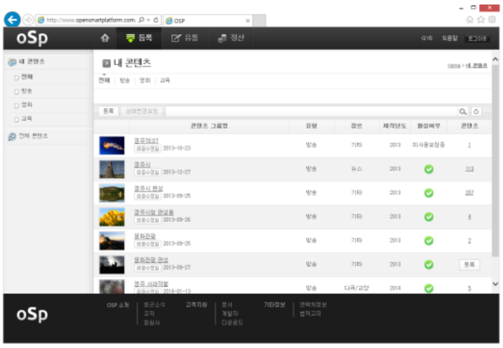


콘텐츠 구매요청

전체 | 방송 | 영화 | 교육

□	콘텐츠 그룹	유형	장르	제작년도	제공자명	콘텐츠	원본	셋탑	태블릿	스마트폰	시작일	종료일	구매
□	100년의 기계 최종수정일 2014-01-09	방송	기타	2011	한국방송공사	12	□	□	□	□	2014-02-06	2015-02-05	✓
□	KBS 파노라마 최종수정일 2014-01-09	방송	기타	2013	한국방송공사	12	□	□	□	□	2014-02-06	2015-02-05	✓
□	KBS네트워크 특선 경남100경 완전정복 최종수정일 2014-01-09	방송	기타	2013	한국방송공사	10	□	□	□	□	2014-02-06	2015-02-05	✓
□	가요무대 최종수정일 2013-07-24	방송	연예/오락	2013	한국방송공사	19	□	□	□	□	2014-02-06	2015-02-05	✓
□	개그콘서트 최종수정일 2013-07-18	방송	연예/오락	2000	한국방송공사	18	□	□	□	□	2014-02-06	2015-02-05	✓
□	걸어서 세계속으로	방송	기타	2013	한국방송공사	12	□	□	□	□	2014-02-06	2015-02-05	✓

Figure 16. User Interface for Distribution Dealers



내 콘텐츠

전체 | 방송 | 영화 | 교육

콘텐츠 그룹명	유형	장르	제작년도	활성여부	콘텐츠
경주TEST 최종수정일 2013-10-23	방송	기타	2013	미사용요청중	1
경주시 최종수정일 2013-12-27	방송	뉴스	2013	✓	113
경주시 편성 최종수정일 2013-09-25	방송	기타	2013	✓	207
경주시청 편성용 최종수정일 2013-09-26	방송	기타	2013	✓	4
문화관광 최종수정일 2013-09-25	방송	기타	2013	✓	2
문화관광 편성 최종수정일 2013-09-27	방송	기타	2013	✓	등록
경주 사과작황 최종수정일 2014-01-13	방송	다큐/교양	2014	✓	5

Figure 17. User Interface for Contents Providers

After logging in with a temporary ID, a user can change his/her ID and password as shown in Figure 14. One of the main features of our user management system is role-based access control. As is shown in Figure 15, all main menus including "registration", "circulation", "distribution", "billing", "log", and "user" are available when the user is a system manager. Our user management system recognizes the user as a system manager by investigating the user ID and provides all main menus.

When the user is a distribution dealer, the main menu only shows "registration", "distribution", and "billing" as shown in Figure 16. From the screen, a distribution dealer can purchase contents.

When a content provider accesses the system, all the content items he/she uploaded are listed on the screen. All content items are classified into groups and the group names are listed with the number of content items that belong to the group as shown in Figure 17. From this screen, a content provider can register a group of contents so that the group appears in the user interface for distribution dealers.

7. Conclusions

We have developed a role-based user management system for Internet TV systems. The system has a list of roles. A user has one or multiple roles. Each role is associated with a list of resources that this role is allowed to access. Therefore, a user can access only permitted resources. For example, the “System Management” menu will not be shown to an end user. Another feature of our system is that it handles all kinds of users and controls accessing all component systems. Making use of our user management component, we are developing a practical Internet TV system.

Acknowledgment

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2011-0006942), by ‘Development of Global Culture and Tourism IPTV Broadcasting Station’ Project through the Industrial Infrastructure Program for Fundamental Technologies funded by the Ministry of Knowledge Economy (10037393) and the Dongguk University Research Fund of 2015.

References

[1] J. Yim and G. Lee, “Design and Implementation of a User Management System”, Information, vol.17, no. 10(A), **(2014)**, pp. 5009-5014.

[2] K. Kim, S. Hong and J. Kim, “A Study on Policy-based Access Control Model in SNS”, IJMUE, vol.7, no. 3, **(2012)**, pp. 143-150.

[3] J. Yim, G. Lee and K. Ham, “Review of the Techniques for User Management System”, Advanced Science and Technology Letters, vol. 46, **(2014)**, pp. 87-91.

[4] L. Opyrchal, J. Cooper, R. Poyar, B. Lenahan and D. Zeinner, “Bouncer: Policy-Based Fine Grained Access Control in Large Databases”, IJSIA, vol. 5, no.2, **(2011)**, pp. 1-16.

[5] K. Kim, S. Hong and J. Kim, “A Study on Policy-based Access Control Model in SNS”, IJMUE, vol.7, no. 3, **(2012)**, pp. 143-150.

[6] “OASIS, OASIS: Extensible access control markup language(XACML) V2.0. OASIS Specification”, Available at www. Oasis-open.org/committees/xacml, **(2005)**.

[7] G. Kim and J. Han, “Light-weight Access Control Mechanism based on Authoricate issued for Smart Home”, IJSH, vol. 2, no. 4, **(2008)**, pp. 49-58.

[8] H. Gonz´alez-V´elez and M. Kontagora, “Performance evaluation of MapReduce using full virtualisation on a departmental cloud”, Int. J. Appl. Math. Comput. Sci., vol. 21, **(2011)**, pp. 275-284.

[9] X. Fu, K. Wu and X. Z. Gong, “Implement Access Control Architecture to Enhance Security and Availability of Cloud Computing Systems”, IJSIA, vol. 6, no. 2, **(2012)**, pp. 245-250.

[10] J. Lin, X. Lu, L. Yu, Y. Zou and L. Zha, “VegaWarden: A Uniform User Management System for Cloud Applications”, IEEE Fifth International Conference on Networking, Architecture and Storage (NAS), **(2010)**, pp. 457-464.

[11] X. Li, J. He and T. Zhang, "Negative Authorization in Access Control for Cloud Computing", IJSIA, vol. 6, no.2, **(2012)**, pp. 307-312.

[12] U. Farooq and J. Glauert, "Joint Hierarchical Nodes Based User Management (JoHNUM) Infrastructure for the Development of Scalable and Consistent Virtual Worlds", 13th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications, **(2009)**, pp. 105-112.

Authors

Kangjai Lee, received his M.S. degree in Computer Science from the Dongguk University in 1981 and his Ph.D. degree in Computer Engineering from the Dongguk University at Seoul Korea in 1997, respectively. He is a Professor in the Department of Computer Information at Suwon Science College at Hwaseong Korea. His current research interests include Database applications, Data mining, Knowledge discovery, Multimedia systems.

Jaegeol Yim, received the M.S. and Ph.D. degrees in Computer Science from the University of Illinois at Chicago, in 1987 and 1990, respectively. He is a Professor in the Department of Computer Science at Dongguk University at Gyeongju Korea. His current research interests include Petri net theory and its applications, Location Based Service, AI systems, and multimedia systems. He has published more than 50 journal papers, 100 conference papers (mostly written in Korean Language), and several undergraduate textbooks.