EURASIP Journal on Information Security

RESEARCH Open Access

A new usage control protocol for data protection of cloud environment

Kefeng Fan[1*], Xiangzhen Yao[1], Xiaohe Fan[2], Yong Wang[2] and Mingjie Chen[2]

Abstract

With the rapid development of the cloud computing service, utilizing traditional access control models was difficult to meet the complex requirements of data protection in cloud environment. In cloud environment, the definition of data and its protection are gradually varied when contents shifting from one virtual machine to another; in these new scenarios, the multi-tenancy pattern has been taken as a core attribute. For this reason, many users need to change their roles according to different situations; certifications has impact much more complicated challenges in cloud environment while access control was suitable for the static status but no longer for the changing situation. In this paper, a new usage control protocol model—multi-UCON (MUCON) based on usage control (UCON), combined with encryption technology and the digital watermarking technology, is proposed with the characteristics of flexible accrediting, feature binding, and off-line controlling. The analysis and simulation experiments indicate that the proposed protocol model is secure, reliable, and easy to be implemented, which can be deployed in cloud computing environments for data protection.

Keywords: Cloud computing, Data protection, UCON, Rights transfer, Fair using

1 Introduction

Cloud computing is a more flexible, cost effective, and proven delivery platform for providing business or consumer service over the internet and intranet compared with traditional network platforms. Cloud computing supports distributed service-oriented architecture and multi-user and multi-domain administrative infrastructure which is based on open networks, and the users' data is stored in cloud that the consumer cannot control their private data fully and thoroughly. As a result, data security issues become the primary concern of users in cloud computing environment. Meanwhile, access controls take a significant role of data protection nowadays, but traditional access controls cannot authorize users to fully and thoroughly control their data anytime and anywhere across platforms and networks. Therefore, some researchers propose usage control (UCON) to resolve data security issues [1–4]; nowadays, the development of UCON technologies has been approached through two stages, namely traditional access control stage and modern usage control stage [5–9]. The former is a static pre-authorization model and focuses on the authorization policy, which is depended on qualifying accounts to allow the access of the protected objects [10]. With the increasing popularization of the internet and cooperating with a bunch of cross-platform applications, this model has been unable to adapt itself to the security requirements of open distributed network systems [11, 12], for example, a permission denied can only be implemented in a certain system in which a user has no right to read a file, but if the content is shifting from another valid user, the permission denied operation will not be implemented; thus, the piracy will be easy and non-stoppable. UCON is a new model proposed on the basis of trust management and DRM [13–16], which extend the traditional access control and turn the three technologies into an integrate one. Meanwhile, two key attributes, continuity and mutability, which can fit the model itself to the multi-tenancy environment, have been proposed in UCON. Therefore, UCON can be more effective to control unauthorized accessing and copying, can be more secure to distribute digital content, and can be adaptable in complex using permission validation. In UCON model, the usage of the digital content in the process can be tracked dynamically [17],

* Correspondence: fankf@126.com
[1]Research Center of Information Security, China Electronics Standardization Institute, Beijing 10007, China
Full list of author information is available at the end of the article

the authorization of the contents can be effectively controlled, and the permissions can be reduced, terminated, or canceled accordingly [18] due to the content owner's will.

However, most of the researches of UCON are concentrated on the basic conceptual level at present, where the theory is almost not considered of cloud computing. Therefore, it will be great significance to resolve the existing questions of secure access control in cloud computing by building a usage control model with dynamic license certification [19, 20] and security access control mechanism. In this paper, we proposed a new usage control protocol model, namely multi-UCON (MUCON) with secure dynamic authentication and authorization mechanisms, including three authorization models, machine to machine coding, sharing with one user domain, and making the rights transfer under controlled as well as flexible accrediting which can be applied. Permissions monitor embedded in the client is used to monitor and control the user's activity; when the user accesses beyond his rights, the monitor will cooperate with the content server to investigate and affix the responsibility of the user's illegal activity, so as to reduce pressure on servers and prevent illegal violations of user privacy. Meanwhile, embedded in the digital content with digital watermarking of strong robustness for copyright information is to ensure that digital content is illegal in cracking the case of the responsibility of the user, thus making the protection of digital content more completeness.

2 Access control model overview

2.1 Traditional access control

Traditional access control technology originated in the 1970s; its core is the authorization policy. The technology stipulates whether the subject can access to the object through the authorization policy. There are three main strategies: discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). All of them have been widely used in various fields of DRM [7]. They are based on the subject-object passive security model, as shown in Fig. 1 [7].

However, with the development and extensive application of network technology, the large digital work spread on the network became easier. There are some drawbacks in the traditional access control policy on the protection of the copyright of digital products. First, its permission is static. Second, it can only be authorized before performing a task but cannot realize unauthorized access control continued or prevent the resources being freely copied and transmitted to other users. Third, it barely focused on the protection of digital works in a closed environment, by setting reference monitors servers based on server-side to realize access control of the digital resource. Finally, it just handles recognized users' identity and attributes.

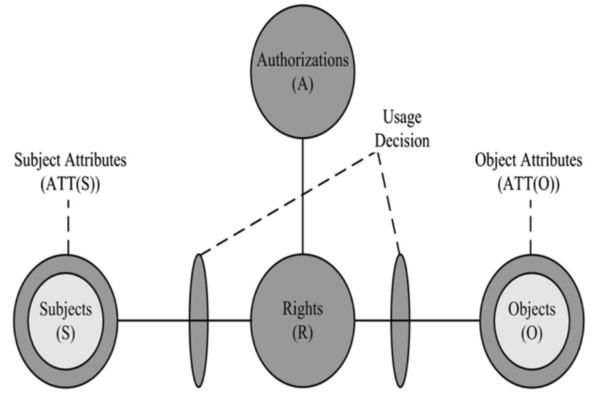

Fig. 1 Traditional access control model. The technology stipulates whether the subject can access to the object through the authorization policy. There are three main strategies: discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). All of them have been widely used in various fields of DRM. They are all based on the subject-object passive security model

2.2 Usage control

At the beginning of the twenty-first century, the famous information security experts Ravi Sandhu and Professor Jaehong Park first proposed Usage Control. As a conceptual model of the new generation of access control, it amends the shortness of the traditional as well as it has been adapted to new security requirements in many aspects by expanding and extending. The UCON defined three elements: authorization, obligation, and condition, and it proposed two important properties which are essential for accessing control in an open network environment of continuity and variability [12]. The core model of UCON is ABC model, as shown in Fig. 2 [21–23]. It expounds a fundamental concept and authorization policy of usage control. UCON model consists of five basic elements: subjects, subject attributes, objects, object attributes, and rights, and it contains three usage decision elements: authorizations, obligations, and conditions.

However, UCON model is just a conceptual model; there is neither a precise definition of the relevant elements of authorizations nor accurate explanation of the status to the authorization policy of UCON. The model did not give a specific definition of the concept nor gave the derivation process about what conditions are required before, during, or after a visit in a content accessing, while how to manage transition relationships between states has become the focused issue nowadays. When describing the volatility, it just illustrates subject and object attributes can be changed at the phase of before, during, or after the visits but not illustrate a specific definition of the concept or the derivation process about how to change or the impact of changes in a certain system. Furthermore, none of

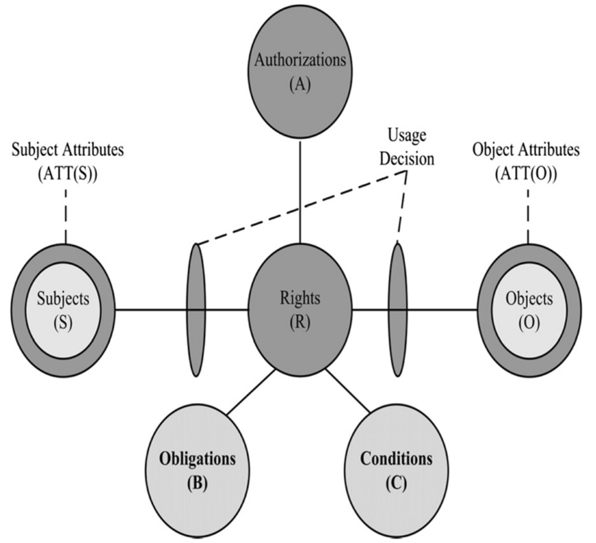

Fig. 2 UCON conceptual model. The UCON defined three elements: authorization, obligation, and condition, and it proposed two important properties which are essential for accessing control in an open network environment continuity and variability

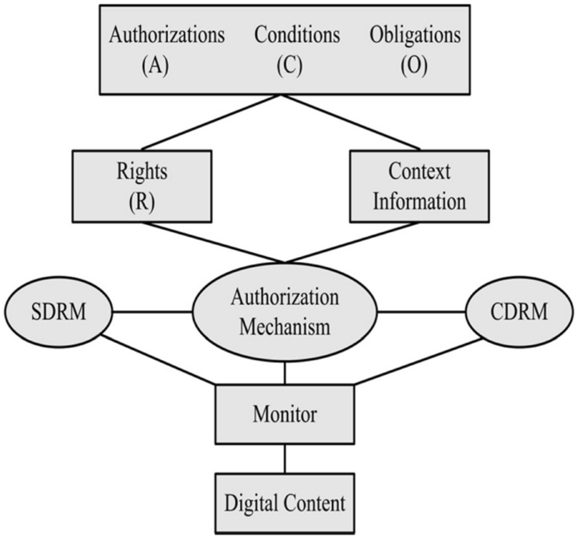

Fig. 3 MUCON conceptual model. MUCON model inherited two principal characters of UCON: continuity and variability. At the same time, it established more secure and reliable authorization mechanism sitting on top of the UCON framework

the specific formal description and the reasoning process of authorization was proposed in the model. Due to the openness and extensibility of the cloud computing environment, the requirement of authorization management in UCON model become more and more complex, and the existing UCON model is no longer applicable in cloud computing environment.

3 The framework of usage control protocol model

In this paper, based on UCON and combined with encryption technology and the digital watermarking technology, we propose a new usage control protocol model called multi-UCON (MUCON), which has the characteristics of flexible accrediting, feature binding, and off-line controlling.

3.1 MUCON conceptual model

MUCON model inherited two principal characters of UCON: continuity and variability. Meanwhile, it established a supplemental secure and reliable authorization mechanism sitting on top of the original UCON framework, the renewed conceptual model is shown in Fig. 3, and its enhancement of main mechanism is described below:

Firstly, in our proposed model, the clients of DRM (CDRM) could select different authorization models of the DRM server (SDRM) according to their needs and submit the machine identifier CID and its application information CINFO to the SDRM before using the protected digital content; this course is called feature binding. Secondly, SDRM encrypt each digital content needed to be distributed when the digital watermark has been embedded in with its copyright information, and then, packaged it with SID, CID, content verification code, and digital content. Finally, after generating license and distributing it to user, SDRM store CID and CINFO into the rights database. When the digital content is accessed, CDRM uses the rights monitor to monitor and control user's access activity and track the users' dispatching behavior or unauthorized accessing behavior. In this case, once the user accesses beyond his right according to the license, for example, touching the unauthorized content, monitor will log the record of use and feed it back to the SDRM.

3.2 Data definition

In order to ensure the MUCON protocol model's accuracy and make it unambiguous, we give an accurate necessary formalized description for the model.

3.2.1 Symbol convention

(a) Entity identifier defined, as shown in Table 1.
(b) Relevant parameters of protocol defined, as shown in Table 2.

3.3 MUCON entity function defined

Definition 1 SDRM: It is responsible for processing distributional digital content (include: encrypting, scrambling, and packing), distribution, and management of licenses.

Table 1 The entity identifiers of MUCON protocol

Entity identifier	Real meaning
C	Client
AS	Identification authentication server
CS	Content server
S_rdb	Server-side rights database
LS	License server
C_rdb	Client-side rights database
Res	Reserve of digital content
PL	Play license
Clog	Client usage log

Definition 2 CDRM: Also known as DRM client. Having their own access right to the content, users can access the digital content in CDRM. And CDRM is responsible for descrambling, decrypting, and monitoring, in one word, controlling the usage of users.

Definition 3 Res: Resources can be shared in an open environment, mainly video and audio files, in this paper.

Definition 4 Authorization: This mechanism unified the management by SDRM, based on attributes of the licensor and user, as well as the required permission. And SDRM is responsible for the authority according to authorization rule set. It mainly contains four types of authorization mode: binding users, domain sharing, rights transferring, and fairing usage. The user can choose the digital content licensing modes according to what their need.

Definition 5 Monitor: It monitors and controls use cases of the digital content, logs the illegal activity, and then informs the SDRM to processor.

Definition 6 Context: MUCON context information including the current system environment, right attributes, and users' using information. They collaborate with the CDRM to use the monitor to monitor and control users.

Table 2 Relevant parameters of MUCON protocol

Parameter identifier	Real meaning
SID	DRM substance identifier
CID	Client identifier
Fair_use	Fair use
L_transfer	Limits of authority transfer
Key_w	Watermark key
Key_c	Content key
Playcode	Play password
Key_seq	Sequence key
Lifetime	Certificate's lifetime
Ka, ka'	Public key and private key of a
E	Encrypt
D	Decrypt

Definition 7 SID: It generally attached to the head of encrypted digital content and binds it with the player. Users only use the dedicated client software to playback of digital content normally.

Definition 8 CID: The user's computer hardware identifier, usually is the LAN MAC address, CPU serial number, or hard disk ID. It is used to bind the user's machine to the digital content.

Definition 9 CINFO: The serialized data which users submit it to SDRM; it is also called the request vector, denoted as: Req. Req = {Req_model, Req_t Req_d, Req_m, of R_1, R_2, … R_n}, among them Req_model is the authorization mode of request, Req_t is the usage count of request, Req_d is the usage date of request, Req_m is the used minutes of request, and R_i ($0 \leqq i \leqq n$) is a reserved word.

Definition 10 PL: Complex data structure that contains the SID, CID, and CINFO authentication information and is formed through encryption and digital signature.

Definition 11 RINFO: Used to protect copyright watermark; the watermark with its copyright information is embedded in the distribution of audio and video files and consists of mainly of the CID, CINFO, and copyright notice.

In particular, MUCON protocol includes four sub-protocols: license application protocol (LAP), content packing protocol (CPP), content usage protocol (CUP), and rights control protocol (RCP).

(1) License application protocol (LAP). Firstly, user C initiates a content download request to CS, then CS submits the application information to LS. Once the user's application information has been approved, LS will store the information into S_rdb and issue a license to user C.

(2) Content packing protocol (CPP). Digital content will be encoded by CS firstly, then CS encrypts user's information, calculates the hash value of these contents, and signatures the hash value, finally, CS pack all above information and send it to the requestor.

(3) Content usage protocol (CUP). Before use the received content, the client application at user end will check the authenticity and integrity of the license from LS. If that is correct, it will verify the authenticity and integrity of the received content. Once these authentications at user end passed, CDRM will start and continue the monitor process in parallel with the contents' consuming procedure and the monitor logs necessary information all the time in its existing period.

(4) Rights control protocol (RCP). This sub-protocol controls usage activities according to the owner's selected permission pattern. There are four patterns that can be selected: ID binding, which requests user to only use digital content in a specific machine and cannot copy the content to others; sharing with other users in the same domain, which requests the user to mark a domain with several machines in it, which constrain the sharing scope and user will not be allowed to use these contents outside the chosen domain; restrict transferring, which constrains the license using times in a limited number; and rational using, which allows the user to use the digital contents without tampering with the copyright.

4 Model performance analysis and simulation

4.1 Security analysis

Firstly, entity mutual authentication in LAP based on the license distribution decision function fPL, if and only if the (Fee==true)&&(Trust==true)&&(CINFO==true) is true, LS distributes a unique license to user C to access the content in a certain period, and other users cannot apply the same digital content license before an expired date, so as to effectively curb the replay attack. Besides, if a user has adverse his credit, LS can refuse to continue the permission in his subsequent licenses; therefore, the content will no longer be accessed by him after the current license expired. In another way, in order to prevent users' abuse of their rights, CRM side can verify the license to ensure the integrity of the content of the permission. In addition, the whole process of LAP are encrypted in transmission, and security encryption algorithm ensures that the communication process is secured. The Monitor combined with data encryption and file hiding techniques can effectively prevent the user to modify a backup of the license.

Secondly, CPP uses the copyright owner's fingerprint information as a key seed, which combined with AES and circulating XOR to ensure the key's security and make it unpredictable; thus, CPP can prevent users from deciphering the key. Furthermore, watermarking algorithm of the protocol with strong robustness embeds the watermark after key encryption; the user will not able to extract or tamper the watermark information from protected content, thus ensuring the legal rights of copyright owners. In addition, the users can also verify the signature of the contents at the LS side in order to authenticate the authenticity and integrity of the content sources.

Thirdly, the CUP executive entity is monitored in CDRM. The monitor is mainly composed by C_rdb, Clog, and controller, where in C_rdb and Clog are encrypted and hidden files which ordinary users could not read and modify. Before the user playback digital content, Monitor will verify the integrity of user licenses and digital content previously in order to prevent users from tampering with them. And then, the licensed content and C_rdb records will be updated accordingly after being used; thus, backing up and restoring the license can be prevented effectively. This is ensuring the CUP security and implementing the control functions effectively.

Finally, the total number of the master license is limited by RCP in order to prevent uncontrolled migration permissions to other clients. If the master license is not restricted by RCP, the total number of distribution of the license can be limited to make a true reasonable sharing of digital content. In addition to the use of the Monitor's log system to record the abuse of legitimate-user's rights, combining with digital watermarking technology is going to prepare for prosecution to ensure protocol security.

In summary, the MUCON protocol is secure and with a characteristic of flexible accrediting, feature binding, and off-line controlling.

4.2 Performance analysis

MUCON protocol is based on public key cryptography technology, and Client and CDRM ensure the legitimacy of the process of protocol communication by the mutual authentication of the SDRM. The amount of computation, storage space, and communication traffic are three key elements which are used to measure the quality of the protocol performance. The following are genetically analysis and simulation of them.

In the simulation of computational analysis, we use a Lenovo workstation as a service entity SDRM with Windows XP, 1 GB memory, and DRM software system software. Microsoft Visual VC++6.0 is chosen as compiler tool. The measured time of signatures and authentication are 2.76 s/1000 times and 13.99 s/1000 times, respectively. We use another Lenovo workstation as client side and install DRM software system instead of SDRM, running the monitor and the client software; the measured time of signature and verification are 6.98 s/1000 times and 36.8 s/1000 times, respectively. The measured results show that the protocol procedure runs 1000 times spend 71.0 s, and it authenticates 41.5 users in 1 s. As we know, user access number is dynamic in a wide range in cloud computing environment. This protocol can authenticate user quickly so that it can be applied into the cloud environment which is accessed by a large number of users simultaneously.

Storage space is actually describing the space complexity, which includes three aspects. The storage space is occupied by the algorithm, the storage space is occupied by the input and output data of the algorithm, and the temporary occupation of storage space during operation. In the protocol, DES combined with RSA is used as an encryption and decryption method, the space complexity of the DES is O(n), and the RSA algorithm to encrypt the object is always used as a DES encryption session key, which is a 64-bit pseudorandom number, so the space complexity is constant O(1). Thus, MUCON protocol's space complexity price is low when ensuring the security of content protection.

In this paper, we analyze the communication traffic of the protocol with the user's response time and throughput of data. Among them, user's response time refers to the sum of time before the user and network to establish the physical connection or before the user establish the DRM server security communication. The user's response time is denoted as T. Data throughput refers to the amount of exchange data between the server and the client during user interacting with the system. It is measured by (Mbps) = ((Byte)*8)/(μs) and is denoted as S(max). Data transmission process of the MUCON protocol is using direct methods. In different data transmission rates, the user's response time and throughput is measured as in Table 3. The experimental data shows that MUCON can reflect a good performance in cloud environment. In case of massive data are stored in cloud and data exchanges rapidly, the high traffic processing ability of the MUCON protocol can satisfy the access control demands of users in cloud computing environment perfectly.

Table 3 The user response time and throughput of the MUCON protocol

Data transmission rates (Mbps)	The user's response time (μs)	Data throughput (Mbps)
1	20,460	0.6001
11	11,896	2.1360
55	10,996	2.5136

4.3 Comparison of related schemes

At present, the main technical characteristics of the mainstream commercial digital content protection system or software are packer/unpack, serial number, registration code, function control, limit of the times of using, and time limits, while based on MUCON, protocol system can control the usage rights off-line in real time, with flexible licensing models, and it can also track the transaction with watermarking technology, which can more effectively curb illegal copying of digital content and proliferation. It can ultimately achieve the data protection in cloud environment. Table 4 is a comparison table of the MUCON protocol with other data protection schemes [12].

Table 4 The comparison of MUCON protocol with other scheme

Scheme	Machine binding	Usage control	Off-line control	Support distribution	Consequent tracking
MUCON	YES	YES	YES	Optional	YES
CDKey	NO	NO	NO	YES	NO
Keyfile	NO	NO	NO	YES	NO
Floppy	YES	YES	NO	NO	NO
Rom	NO	YES	NO	NO	NO
Disk	YES	NO	NO	NO	NO
Puresoft	YES	YES	NO	NO	NO
CSpec	YES	YES	NO	NO	NO

5 Conclusions

Based on UCON and according to its deficiency, we proposed a distributed security control protocol model with features of flexible accrediting, feature binding, and off-line controlling. Finally, through the security assessment of the protocol and the performance analysis and simulation, it has been proved that the MUCON protocol is effective, secure, reliable, and easily implemented. Usage control is not only an old topic but also a new challenge as the key technology in system security. With the development of cloud computing technology, the users' data protection of cloud environment has become a hot area of study. Because of the dynamics and complexity of cloud computing environment, access control has become a more difficult task, and it will catch more and more attention from the researchers and industries.

As we all know, social network is widely applied in our daily life. With the increasing amount of data for social network, many network companies put users' data onto cloud platform. For privacy considerations, social network companies may require cloud service providers to make related access control strategy. This proposed model will help network companies ensure the security of users' data.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

KF and XZ carried out the main research of this work. MJ performed the experiments. XH and YW contributed to the writing of the manuscript. All authors read and approved the final manuscript.

Acknowledgements

The authors extend their thanks to the reviewers for the comments and suggestions which helped in improving the overall quality of this article. This work was supported in part by a grant from the National Natural Science Foundation of China (No.61172053, No.61202266).

Author details

[1]Research Center of Information Security, China Electronics Standardization Institute, Beijing 10007, China. [2]School of Electronic Engineering and Automation, Guilin University of Electronic Technology, Guilin 541004, China.

Received: 16 February 2015 Accepted: 14 March 2016
Published online: 24 March 2016

References

1. HY Tsai, Threat as a service: virtualization's impact on cloud security. IT Professionals **14**(1), 32–37 (2012)
2. Nashaat, Hossam, A proposed model for enhancing data storage security in cloud computing system. J Emerg Trends Comp Inform Sci **3**, 970–974 (2012)
3. P Kalpana, S Singaraju, Data security in cloud computing using RSA algorithm. Int J Res Comp Commun Technol **1**(4), 143–146 (2012)
4. Prashant Srivastava and et al., An architecture based on proactive model for security in cloud computing, IEEE-International Conference on Recent Trends in Information Technology, pp.661-666, 2011
5. Danmei Niu, Zhiyong Zhang and Lili Zhang, A DRM system for home network based on RBAC and license chain, 2010 Fourth International Conference on Genetic and Evolutionary Computing, pp.530-533.2010.
6. Z Zhiyong, H Tao, N Danmei, Z Lili, Usage control model for digital rights management in digital home networks. J Multimedia **8**(6), 376–383 (2011)
7. EM Hinkes, Access controls in the digital era and the fair use/first sale doctrines. Santa Clara Comput High Technol Law J **4**(23), 685–726 (2007)
8. T Masue, T Hirai, T Shikama, Transfer acceleration of content usage control information by using base-values reference method, Consumer Electronics. Consumer Electronics **8**(57), 1141–1147 (2011)
9. Li Fen, Liu Quan, Pei Qingqi, Pang Liaojun, On trust degree-based usage control in DRM System, Computational Intelligence and Security (CIS 2010), pp.298-301. 2010
10. SG Lian, *Multimedia content encryption: techniques and applications* (Auerbach Publication, Taylor & Francis Group, UK, 2008)
11. Bai qinghai, Zheng ying, Study on the access control model, Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), pp.830-834.2011
12. YY Yu, Z Tang, A survey of the research on digital rights management. Chin J Comput **28**, 1954–1968 (2005)
13. Ta Minh Thanh, Iwakiri, M. Nonspecific DCT-block fingerprinting based on incomplete cryptography for DRM system. Advanced Technologies for Communications (ATC), 2012 International Conference on, pp.300-303. 2012.
14. K Seong-Jun, P Kyung-Won, L Kyung-Taek, C Hyung-Jin, Digital tuner implementation using FM tuner for DRM plus receivers. IEEE Trans Consumer Electronics **2**(58), 311-–317 (2012)
15. Z Zhixin, W Xianrong, Z Delei, C Feng, An experimental study of HF passive bistatic radar via hybrid sky-surface wave mode. IEEE Trans Antennas Propagation **1**(61), 415–424 (2013)
16. Rantakokko, J., Handel, P., Fredholm, M., Marsten-Eklöf, F. User requirements for localization and tracking technology: a survey of mission-specific needs and constraints. Indoor Positioning and Indoor Navigation (IPIN), 2010 International Conference on, pp.1-9.2010
17. LM Ni, Z Dian, MR Souryal, RFID-based localization and tracking technologies. Wireless Communications. IEEE **2**(18), 45–51 (2011)
18. M Raine, A Valentin, M Gaillardin, P Paillet, Improved simulation of ion track structures using new Geant4 models—impact on the modeling of advanced technologies response. Nuclear Science. IEEE Trans **6**(59), 2697–2703 (2012)
19. C Mingyu, G AlRegib, J Biing-Hwang, Feature processing and modeling for 6D motion gesture recognition. Multimedia IEEE Trans **3**(15), 561–571 (2013)
20. S Elling, L Lentz, M de Jong, Combining concurrent think-aloud protocols and eye-tracking observations. An Analysis of verbalizations and silences. Professional Communication, IEEE Trans **3**(55), 206–220 (2012)
21. Zhang Zhiyong, Yang Lin, Pei Qingqi, Ma Jianfeng. Research on usage control model with delegation characteristics based on OM-AM methodology. 2007 IFIP International Conference on Network and Parallel Computing, in Conjunction with IFIP International Workshop on Network and System Security, Dalian, China, Sep, 2007
22. Z Zhang, K Wang, A trust model for multimedia social networks. Soc Networks Analysis Mining **3**(4), 969–979 (2013)
23. Park J, Sandhu R. Towards usage control models: Beyond traditional access control. In: Proc. of the 7th ACM Symp. on Access Control Models and Technologies (SACMAT 2002). pp.57 – 64. 2002.[doi:10.1145/507711.507722]