A Method for Trusted Usage Control over Digital Contents Based on Cloud Computing

Tao Huang, Zhiyong Zhang*, Qingli Chen, Yanan Chang
Electronics Information Engineering College, Henan University of Science and Technology, Luoyang 471023, China
E-mail: z.zhang@ieee.org

Abstract

Digital Rights Management (DRM) of multimedia contents in the open network environment is a hot research spot in recent years, and DRM controller in client has been facing versatile attacks, such as break and alteration. Based on cloud computing and remote certification, this paper proposed a usage control architecture and bidirectional integrality verification security protocol of multimedia digital contents in cloud environment. DRM controller is set in cloud multimedia server by as a service, and user calls DRM controlling function through client GUI. By comparisons and analyses on the schemes available, the novel approach realizes enhanced secure, trusted and controllable digital rights protection mechanism, in combination with trusted computing enabled high security terminal platforms, ensures bidirectional trust relation between the multimedia contents providers and the end users, and meanwhile satisfies the basic privacy protection and security requirement of the user end platform configuration.

Keywords: *Digital Rights Management, Cloud Computing, Remote Attestation, Usage Control, Security Protocol*

1. Introduction

The development and application of cloud computing, communication network technology and information technology, and the disposition and application of wireless mobile communication networks such as 3G and 4G as well as next-generation high-speed broadband Internet enable people to access and utilize multimedia digital contents such as texts, graphics, images, animations, audios and videos by various access modes. This brings substantial changes to the life, work and study of people. Multimedia digital contents are convenience to be replicated, distributed and transmitted, however, when the technology brings convenience to people's life, work and study, there is also the phenomenon that the multimedia digital contents and products protected by intellectual property right are replicated in mass quantities either intentionally or unintentionally via computer networks with the help of information technologies. Then these digital contents are disseminated and abused. The lack of digital copyright protection that has attracted people's attention due to such phenomena is detrimental to the sound development of multimedia digital industry. Traditional methods for intellectual property right protection can not satisfy the demand of the intellectual property right protection of multimedia digital contents. Thus, Digital Rights Management (DRM) is invented. In the whole life cycle of multimedia digital contents, which consists of the production, storage, publication, reception, broadcasting and display of multimedia digital contents, DRM can protect the intellectual property right of the multimedia digital contents by using software and hardware technologies, to ensure the legal usage and controlled dissemination of the multimedia digital contents [1, 2].

With the emergence and rapid development of cloud computing in recent years, the usage control on multimedia digital contents can be realized by cloud computing. Due to its advantage of direct, rapid and flexible transmission of multimedia digital contents, it provides a strong infrastructure service platform for the establishment of multimedia communication network and the wide-range transmission of multimedia digital contents. In addition, the appearance and development of trusted computing secures the applicability and interoperability of the safe distribution of DRM protected multimedia digital contents and the usage control of multimedia digital contents on high safety terminal platforms [3].

The DRM controller is facing the probability to be cracked and tampered on terminal in an open network environment. The present paper combines the cloud computing and the remote attestation

technology of trusted computing to construct the mechanism of usage control on multimedia digital contents. We propose a usage control framework regarding multimedia digital contents in cloud environment and bidirectional integrity checking protocol.

2. Related research

2.1. Usage Control models for DRM

As the next-generation access control architecture, Usage Control (UCON) makes up for the deficiencies of traditional access control, and expands the traditional way in many ways. It is a basic access control architecture that can be applied on digital right management (DRM). Three basic components, authorization (A), obligation (B) and condition (C) are incorporated into this infrastructure. Therefore, UCON is known as $UCON_{ABC}$ model. This architecture combines the features of continuous access control and describes the dynamic changes of every entity property in the utilization of resources. In the $UCON_{ABC}$ model, every entity property changes before, during and after the implementation of rights. The family of $UCON_{ABC}$ models for usage control (UCON) is illustrated in Figure 1(a), (b), (c) and (d). This architecture is capable of implementing three access control strategies: discretionary access control, mandatory access control and role-based access control. It has been proved formally [4].

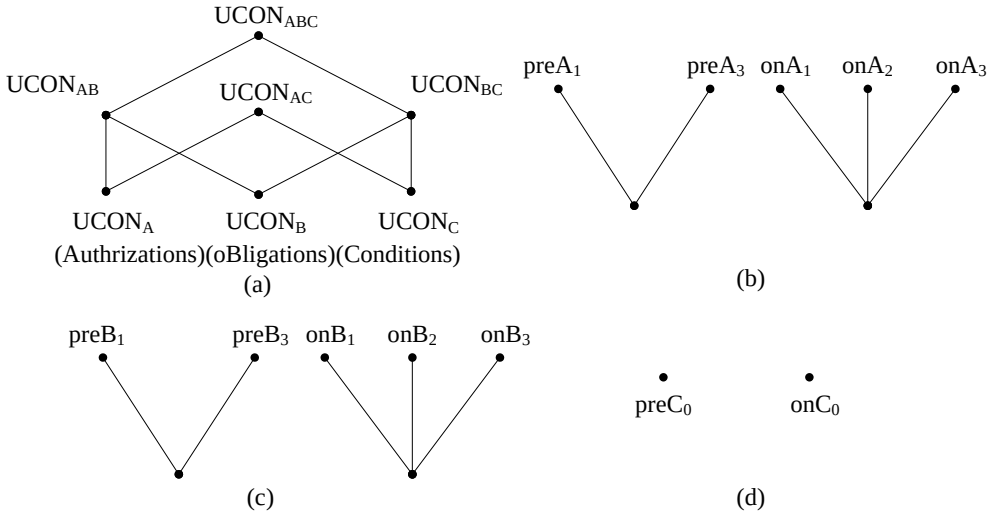

Figure 1. Family of $UCON_{ABC}$ models

Regarding the temporal and spatial extension of DRM, reference [5] added “location restriction” to the traditional right usage control, and realized the access control on sensitive resources for mobile client devices.

Reference [6] puts forward the $UCON_D$ model, a formalized UCON model with delegation features based on next-generation access control architecture UCON for DRM application. It also introduced the realization based on delegation certificate (DC). $UCON_D$ is an extension model of $UCON_{ABC}$ in the aspect of delegation authorization, making the latter more complete.

2.2. Basic characteristics of cloud computing

Due to the development of information and communication technologies, the computing model has experienced the transition from collectively delivering the tasks to a large processor to a distributed task processing model based on network, and then to the recent cloud computing model based on demand. Cloud computing virtualizes the service online, and the user does not have to care about the

internal realization of “cloud”. The goal is that a user can maximize the virtual resource pool on the internet at any time and any place, and deal with computing problems in large quantities.

Cloud computing is essentially a new service model providing service on demand and a new type of Internet data center service. According to the hierarchy of service, “cloud” can be divided into three forms: infrastructure cloud, platform cloud and application cloud. The three “clouds” respectively correspond to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

- IaaS is the service of the lowest hierarchy. The user disposes the computing resources such as processor and storage system, and runs the operation system and application softwares on his/her own way. It is related to the storage service and computing ability.
- PaaS is the service above IaaS. It is the development and running environment of softwares. The provider provides various programming languages and tools, by means of which the user writes application softwares and then runs them on the cloud computing platform.
- SaaS is the software applications developed by IaaS and PaaS. The providers run applications on cloud computing devices and the users use these softwares on thin-client interface of various client devices.

Reference [7] comes up with a digital rights management (DRM) concept for cloud computing and show how license management for software within the cloud can be achieved in a privacy-friendly manner. In the scenario, users who buy software from software providers stay anonymous. At the same time, the approach guarantees that software licenses are bound to users and their validity is checked before execution. Reference [8] proposes an optimal cloud resource provisioning (OCRP) algorithm by formulating a stochastic programming model. The OCRP algorithm can provision computing resources for being used in multiple provisioning stages as well as a long-term plan, e.g., four stages in a quarter plan and twelve stages in a yearly plan. In this paper, different approaches to obtain the solution of the OCRP algorithm are considered including deterministic equivalent formulation, sample-average approximation, and Benders decomposition.

2.3. Trusted computing and remote attestation

The trusted remote attestation scheme proposed by Trusted Computing Group (TCG) introduces a security chip architecture in computer hardware platforms, which increases the security of the terminal system by providing security features [9, 10].

As one of the key technologies in trusted computing, Remote Attestation (RA) involves the confirmations of the identity of remote certifier, the platform status configuration information and the trustworthiness of dynamic operation environment, by inquirer who sends the attestation request. It enables the inquirer to examine the changes of the certifier’s computers, which avoids sending private information or important commands to insecure or damaged-security computers.

Reference [11] proposes the attestation proxy party-supported remote attestation (AP^2RA). AP^2RA introduces a trusted third party which is called attestation proxy party (APP) to improve the existing remote attestation models. The APP validation component is used to validate the integrity and security of the attestation platform. Then the result is send to the inquirer in the form of RA report. As the inquirer does not get the details of the verifier's platform configuration and security property characteristics, it resolves the privacy protection problem of the inquirer's platform and increases the survivability of the attestation system. If the certifier is captured, APP still can provide remote attestation service, and the result of attestation is still kept safely.

3. Trusted usage control of multimedia digital contents based on cloud computing

In the open network environment such as cloud computing, multimedia digital contents are more likely to be distributed freely, disseminated maliciously and spread illegally. To ensure users access to multimedia digital contents on a safe, trusted and controlled basis while protecting the privacy of the terminal platform, it needs a trusted computing environment which is under hardware supported security, anti-copying and anti-tampering, what’s more, it also requires a control model and security mechanism regarding the multimedia digital contents based on remote attestation.

3.1. Trusted usage control framework of multimedia digital contents based on cloud computing

Figure 2 describes a trusted usage control framework of multimedia digital contents based on cloud computing between a cloud multimedia server and mobile client users. This framework consists of cloud multimedia server, mobile client users, cloud security server, cloud audit server, attestation proxy server (APP), certificate and license server, integrity measurement reference and security strategy database, and finally trusted measurement logging (TML). The two terminal platforms are the client devices that support trusted computing. The mobile client users access the multimedia digital contents on the cloud multimedia server based on the DRM certificate submitted by the graphic user interface (GUI), of the DRM controller on the mobile client platform. The cloud multimedia server platform runs the DRM controller and implements the usage control on the DRM controller via DRM certificate. The cloud security server is responsible for the management of various security strategies and usage control rules of cloud; the cloud audit server is responsible for logging, surveillance and auditing of the multimedia usage control and service; the attestation proxy server is the initiator of the remote attestation, i.e. It is used to verify the trusted third party of bilateral platforms or object; the integrity measurement reference and security strategy database is used to store the platform provided by the device producer or the integrity measurement and security strategy values of the object device, which is regarded as the reference values of APP with respect to the platform or object; the trusted measurement logging (TML) is used to store the local integrity measurement of the platform or object and the whole process of accessing the security properties.

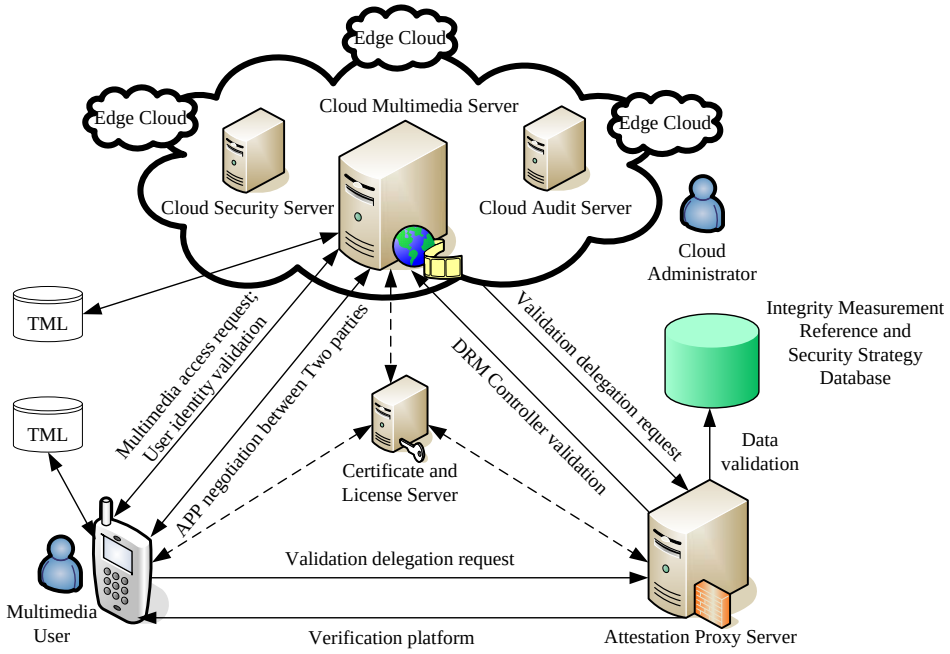

Figure 2. Trusted usage control framework of multimedia digital contents based on cloud computing

3.2. Bidirectional security protocol based on remote attestation

Based on the framework described in Figure 2, this remote attestation protocol contains three entities: the multimedia server based on cloud computing environment (Server), the mobile client (MC) and APP, which respectively correspond to the inquirer, the verifier and the attestation proxy in AP^{2}RA. In addition, DRM controller (DRMC) is the attestation object on the Server. The signature algorithm for the bidirectional integrity attestation security protocol is the RSA algorithm based on asymmetric turbo code system and SHA-1 algorithm is adopted as the hash algorithm. Before the RA conversation, Server, MC and APP are presumed to have acquired the AIK certificate of identity key from the

certificate and license server. K(APP-Server) and K(APP-MC) are respectively the shared secret keys between APP, Server and MC that has been generated before the RA conversation.

The process of bidirectional integrity attestation protocol is defined as follows:

1. The negotiation process between Server, MC and APP is shown in the steps (1)-(3) in Figure 3.

(1) MC submits the digital certificate and sends a request for accessing the multimedia digital contents on the Server.

(2) Upon the reception of request, Server verifies the identity of MC platform and prepares APP negotiation.

(3) Then two parties begin APP negotiation, and finally settle on a proxy service for platform attestation, which protects the privacy of MC.

2. The verification process of Server on MC is shown in steps (4)-(12) in Figure 3.

(4) If the negotiation fails, then protocol is terminated; if the negotiation succeeds, then Server sends a attestation delegation request to APP, which contains the names of the attested objects on MC platform with signature by AIK secret key (AO_Names, SK(Sever.AIK)), the attested object's names (AO_Names) and AIK certificate Cert(Server.AIK) , and a random number Nonce locally produced.

(5) After APP receives the request, it verifies the platform identity of Sever via the AIK certificate and decides whether it accepts or declines the attestation delegation request of Server.

(6) Send the delegation result. If APP accepts the attestation delegation of server, then protocol continues; if not, the protocol is terminated.

(7) APP sends a message of inquiring RA about the platform to MC, including the random number Nonce produced in step (4).

(8) MC measures the local integrity of the platform. The hash value and the corresponding order of measurement are stored in PCRs. Meanwhile the security property eigenvalue of AO secure Attributes is also accessed. This process is written into TML.

(9) MC uses the platform to verify the AIK secret key SK(MC.AIK) , and makes a signature to PCRs, secure Attributes, Nonce and TML containing the platform identifier value. Meanwhile, it sends the above information along with PCRs, secure Attributes, Cert(MC.AIK), K(APP-MC) and TML as a response message to APP via secure channel.

(10) After receiving the response to the RA inquiry, APP determines the validity of Cert(MC.AIK) combining with certificate and license server and then attests the current integrity of the platform by inquiring the integrity measurement reference and security strategy database. At the same time, it verifies the security configuration of the platform (including OS, key components and system security level) combining the security strategy established previously in the database.

(11) After verifying MC, APP sends the platform integrity description and its signature value as well as APP certificate Cert(APP.AIK) to Server as RA report via secure channel.

(12) Based on the RA report of APP, server makes the access decision.

3. The attestation process of MC on the DRMC object on the Server platform is shown in steps (13)-(22) in Figure 3.

(13) MC sends an attestation delegation request to APP. The sent message includes the attested object on the Server with signature by AIK secret key Signature(DRMC, SK(MC.AIK)), the attested object DRMC, AIK certificate Cert(MC.AIK), and a random number Nonce produced locally.

(14) Upon the reception of the request, APP verifies the identity of MC platform via its AIK certificate and accesses the attested object DRMC and then decides whether to accept or decline the attestation delegation request of MC.

(15)APP sends the delegation result. If APP accepts the attestation delegation request of MC, the protocol continues; if not, the protocol is terminated.

(16) APP sends inquiry about the RA of DRMC to Server, including the random number Nonce produced locally in step (13).

(17) Server measures the local integrity of DRMC, whose hash value and the corresponding order of measurement are stored in PCRs. Meanwhile the security property eigenvalue of DRMC secure Attributes is also accessed and stored. This process is written into TML.

(18) Server uses the AIK private key SK(Server.AIK) to make signature on PCRs, secure Attributes, Nonce and TML containing the platform identifier value. Meanwhile, the information above along with PCRs, secure Attributes, Cert(Server.AIK), K(APP-Server) and TML as a response message are send to APP through secure channel.

(19) After receiving the response to the RA inquiry, APP determines the validity of Cert(Server.AIK) via the certificate and license server and then attests the current integrity of DRMC by inquiring the integrity measurement reference and security strategy database. At the same time, it verifies the security configuration of DRMC with the security strategy established previously in the database.

(20) After the attestation by APP on DRMC object on Server platform, it sends the DRMC integrity and security status and its signature value as well as APP public key certificate Cert(APP.AIK) to MC as RA report via secure channel.

(21) Based on the RA report of APP, MC makes the access decision.

(22) MC accepts or declines the access to the multimedia digital contents on Server. The usage control based on digital license is executed.

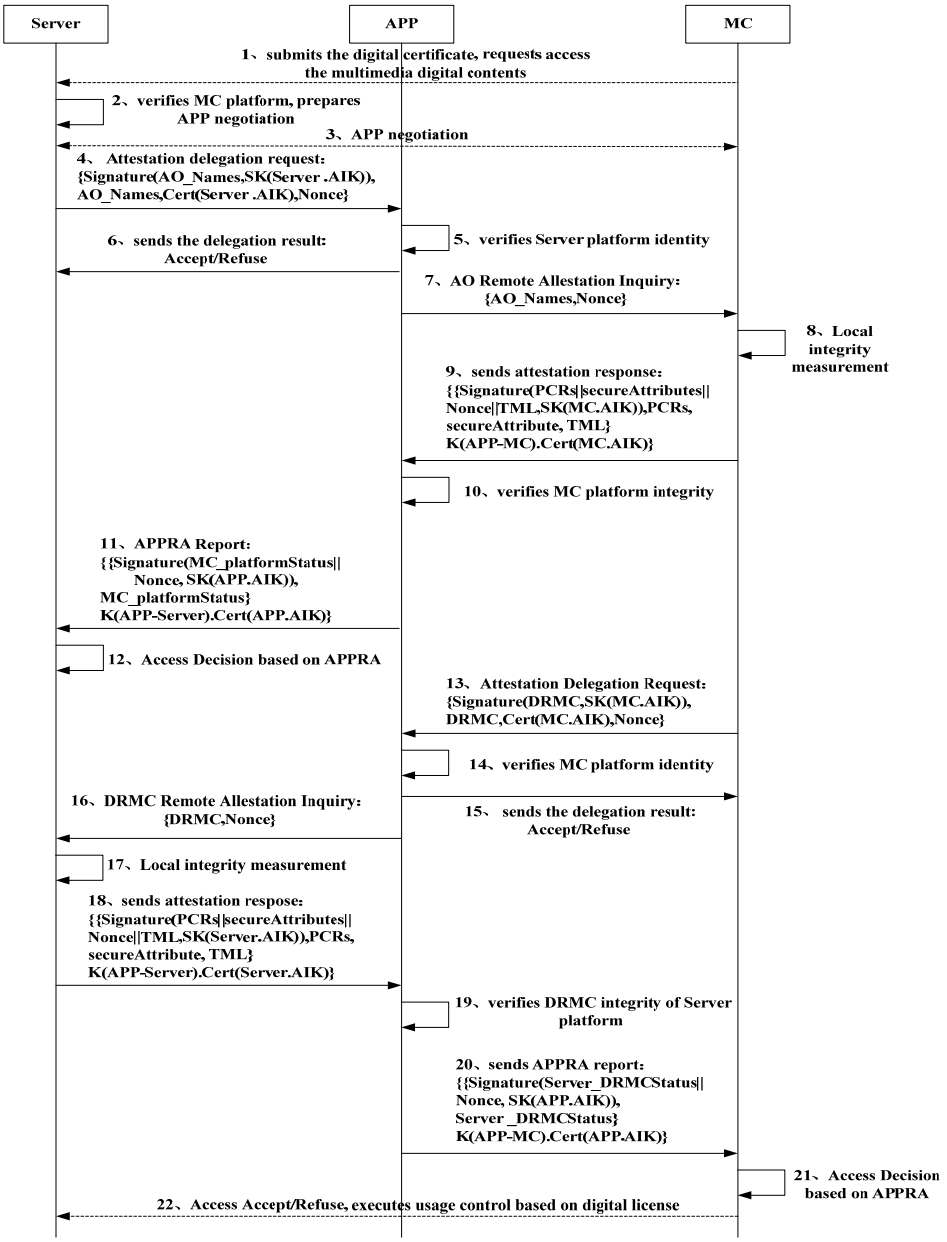

Figure 3. Sequence diagram of bidirectional integrity attestation protocol

3.3. Comparisons and Analyses

Comparisons are done between the solution provided by this paper with the existing representative solutions, such as OMA DRM, Authorized Domain introduced by reference [12], LDM (local domain manager) in reference [13] and CPSec DRM system in reference [14], in the aspects of functionality and security mechanism. The result is shown in Table 1.

Table 1. Comparisons of functionality and security mechanism between the present solution and relevant solutions

Functionality and security mechanism	OMA Solution	Reference [12] solution	Reference [13] solution	Reference [14] solution	Ours
Secure distribution of Digital contents	Contents encryption	Contents encryption	Contents encryption	Contents encryption	AP^2RA remote attestation
Secure distribution of digital certificate	Based on ordinary security domain	Authorized domain	LDM and delegation certificate	Based on user certificate	AP^2RA remote attestation
cryptography method	PKI	Symmetric cryptography	PKI	Asymmetric cryptography	PKI
Client terminal	Ordinary terminal	Ordinary terminal	Ordinary terminal	Ordinary terminal	Trusted computing terminal
Copyright protection mechanism	License authorization	License authorization and transfer	License authorization and transfer	Temporal and spatial restriction	Remote attestation security enhancement
System cost	Medium	Low	High	Medium	High
Suitable environment	Ordinary security domain	Digital family network	Digital family network	Ordinary network application	Cloud computing environment

This paper proposes a remote attestation method based on AP^2RA. It combines the trusted computing platform to realize the safe and trusted usage control on multimedia digital contents. In terms of cost, as it adopts a third-party trusted platform, it costs more but is more compatible with the cloud computing environment.

4. Conclusions

In order to resolve the problems such as the DRM controller on the user terminal being maliciously cracked and tampered, the present paper proposed a usage control framework and its bidirectional integrity attestation protocol regarding multimedia digital contents in the cloud computing environment based on the cloud computing features and remote attestation technology, which sets DRM controller as a cloud service on the multimedia server. The user could call the DRM control function through the client GUI. This solution ensures the bidirectional trusted relationship between the multimedia digital contents provider and the terminal users and satisfies the demand for privacy protection of terminal platform configuration. Further study will concentrate on formalized verification and analysis on the security protocol proposed by the present paper.

Acknowledgments

The work was sponsored by the National Natural Science Foundation of China (Grant No.61003234), Plan for Scientific Innovation Talent of Henan Province (Grant No.134100510011), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant

No.2011HASTIT015), and Henan University of Science & Technology Doctors Research Fund (Grant No.09001470).

References

[1] Zhang ZY, "Digital Rights Management Ecosystem and its Usage Controls: A Survey", International Journal of Digital Content Technology & Its Applications, vol.5, no.3, pp.255-272, 2011.
[2] Zhang LL, Zhang ZY, Niu DM, Huang T, "A Novel DRM Security Scheme and its Prototype System Implementation", International Journal of Digital Content Technology & Its Applications, vol.5, no.11, pp.334-342, 2011.
[3] Zhang ZY, "Security, Trust and Risk in Digital Rights Management Ecosystem", Science Press of china, china, 2012.
[4] Park J, Sandhu R, "The $UCON_{ABC}$ Usage Control Model", ACM Transactions on Information and System Security, vol.7, no.1, pp.128-174, 2004.
[5] Muhlbauer A, Reihaneh S N, Salim F, Sheppard N P, Surminen M, "Location constraints in digital rights management", Computer Communications, vol.31, no.6, pp.1173-1180, 2008.
[6] Zhang ZY, Yang L, Pei QQ, Ma JF, "Research on Usage Control Model with Delegation Characteristics Based on OM-AM Methodology", In Proceeding(s) of IFIP International Conference on Network and Parallel Computing. Washington DC: IEEE Computer Society Press, pp.238-243, 2007.
[7] Petrlic R, Sorge C, "Privacy-preserving DRM for cloud computing", In Proceeding(s) of 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA, pp.1286-1291, 2012.
[8] Chaisiri S, Lee B S, Niyato, D, "Optimization of resource provisioning cost in cloud computing", IEEE Transactions on Services Computing, vol.5, no.2, pp.164-177, 2012.
[9] Zhang ZY, Pei QQ, Yang L, Ma JF, "Game-Theoretic Analyses and Simulations of Adoptions of Security Policies for DRM in Contents Sharing Scenario", Intelligent Automation and Soft Computing, vol.17, no.2, pp.191-203, 2011.
[10] Zhang ZY, Lian SG, Pei QQ, Pu JX, "Fuzzy Risk Assessments on Security Policies for Digital Rights Management", Neural Network World, vol.20, no.3, pp.265-284, 2010.
[11] Zhang ZY, Pei QQ, Yang L, Ma JF, "Attestation proxy party-supported remote attestation model and its secure protocol", Journal of Xidian University, vol.36, no.1, pp.58-63, 2009.
[12] Popescu B, Crisop B, Tanenbaum A, Kamperman F, "A DRM security architecture for home networks", In Proceeding(s) of 4th ACM Workshop on Digital Rights Management, pp.1-10, 2004.
[13] KIM H, Lee Y, Chung B, Yoon H, Lee J, Jung K, "Digital Rights Management with right delegation for home networks", In Proceeding(s) of 9th International Conference on Information Security and Cryptology, LNCS 4296, pp.233-245, 2006.
[14] Ma ZF, Fan KF, Chen M, Yang YX, Niu XX, "Trusted digital rights management protocol supporting for time and space constraint", Journal on Communications, vol.29, no.10, pp.153-164, 2008.