클라우드 컴퓨팅 파라다임을 통한 멀티미디어 컨텐츠 관리 설계

Randy Tolentino*, 김용태**, 정윤수***

A Design of Multimedia Content Management through Cloud Computing Paradigm

Randy Tolentino*, Yong-Tae Kim, Yoon-Su Jeong*****

요 약 사용 조절 모델은 보호된 컨텐츠의 사용에 대한 포괄적인 기술을 허용하는 새로운 접근 조절 모델의 시초이다. 이 범례에서 객체로의 접근에 관련된 결정은 요청 시간에만 제한되어있지 않다. 그것은 보호된 객체의 사용과 결합되며 사용과 병렬식으로 진행되는 지속적 처리가 된다. 사용 조절의 실현은 오랫동안 보안 문서의 전파에 있어서 조절 능력을 잃게 되는 문제를 해결하려한 연구 과제이다. 클라우드 컴퓨팅의 발현으로 문서들이 클라우드에 저장이 되고 문서를 보거나 편집할 수 있는 프로세서들이 클라우드안에 상주하며 문서들은 브라우저와 같은 신 클라이언트에 의해 접근이 가능해진다. 우리는 그러한 시나리오가 이해 당사자의 정책에 기반을 둔 문서 사용 보안에 대한 사용 조절의 실행에 있어 이상적인 기회를 제공하는 사실에 주목한다. 본 논문에서는 클라우드 기반의 어플리케이션에서 더 나은 멀티미디어 컨텐츠를 실행하기 위한 멀티미디어 컨텐츠 관리(MCM)를 제안한다. 그리고 클라우드 컴퓨터의 발현과 사용을 통해 보안된 객체의 사용에 있어 매끄러운 조절을 제공하기 위한 강력한 구성을 설계한다. 우리는 이러한 실현을 위해 설계 원칙을 기술하고 제안 구조를 논한다.

주제어 : 멀티미디어 컨텐츠 관리, 보안, 클라우드 컴퓨팅

Abstract Usage control models are the new breed of access control models that allow description of comprehensive policies for usage of protected content. In this paradigm, decisions regarding access to objects are not limited to request time only. It is coupled with the usage of the protected objects and becomes a continuous process carried out in parallel to the usage. The realization of usage control has been a long standing research problem to overcome the issue of loss of control in secure document dissemination. With the emergence of cloud computing, documents are stored in the cloud, the document viewers and editors themselves reside in the cloud and are accessed from thin clients such as browsers. We note that such scenarios provide an ideal opportunity for the realization of usage control for securing the usage of documents based on the stakeholders' policies. In this paper, we proposed Multimedia Content Management (MCM) for a better realization multimedia content in the cloud based applications. We designed a robust architecture to provide fi ne-grained control over usage of protected objects through the use of emerging cloud computing paradigm. We present the design principles for this realization and discuss our proposed architecture.

Key Words : Multimedia Content Management, Security, Cloud Computing

※ 본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음
*한남대학교 멀티미디어학과
**한남대학교 멀티미디어학과 조교수(교신저자)
***목원대학교 정보통신공학과 조교수
논문접수: 2012년 10월 23일, 1차 수정을 거쳐, 심사완료: 2012년 11월 20일

1. 서 론

Widespread use and distribution of multimedia content over the Internet in the forms of TV programming, user-generated videos and other rich media has made efficient and secure multimedia content dissemination a highly relevant and pressing matter for the research community and industry alike [1]. Allowing content owners to specify and associate fine-grained and highly expressive policies regarding their content is a rich research topic. Most of the deployments of secure content distributions make use of partial content release i.e. only part of the content is released freely with the rest of the content released after the user makes payment of some sort. This very crude mechanism only allows a rudimentary set of high-level policies to be applied on the content that is delivered to the users thus reducing the level of control over how the content may be used. Moreover, the existing mechanisms are mostly proprietary thus reducing the possible domain of target audience that may benefit from the content. This scenario requires that research in the area of authorization be extended and applied in the area of secure content distribution. Due to this reason, for the past few years, the focus of security research in the domain of authorization has shifted from access control models to usage control in which two distinct enhancements have been made - mutability of attributes and continuity of access decisions [2]. This allows object owners to define not only the users that may be allowed to access their content but also how the content might be used after it is released to the client platform.

Cloud computing provides data ubiquity and wide accessibility. It also lends itself to better control over data from the perspective of the service providers [3]. It is quite possible that rather than allowing users to download data, they are given access to the same data using a cloud operating system through browser. It has been previously noted that once data is released outside the domain of the data owner, it becomes very difficult to control as dictated by the policies of the owner.

In this paper, we argue that since it is extremely difficult to control access to objects released outside the domain of the owner, it is more feasible to keep the objects under the control through cloud computing while still giving full access to the intended audience through usage control models. Our focus is to introduce a usage control framework at the cloud in the Software as a Service (SaaS) [4] level of abstraction.

Most of the unique and defining usage control features can better be realized using cloud computing technologies. Such features include attribute updates, continuity of access decisions and revocation of content etc. We provide concise arguments regarding how each of these features can be supported by the cloud computing paradigm and provide a framework that can do so in an effective manner.

Contributions: Our contributions in this paper are the following:

1) We provide a vision for enabling usage control frameworks in and through cloud computing to enable secure content distribution while still enabling fine-grained control over who may access the content and under continuous usage control restrictions, and

2) We provide a detailed architecture of the realization of our usage control framework in the cloud

Outline: The rest of the paper is organized as follows. Section II covers the previous efforts and realizations of secure dissemination of multimedia content. Section III describes our architecture towards realization of the usage control requirements for distribution of multimedia content and through cloud computing. Section IV discussed the multimedia content security within cloud and the paper is concluded in Section VI.

2. Related Works

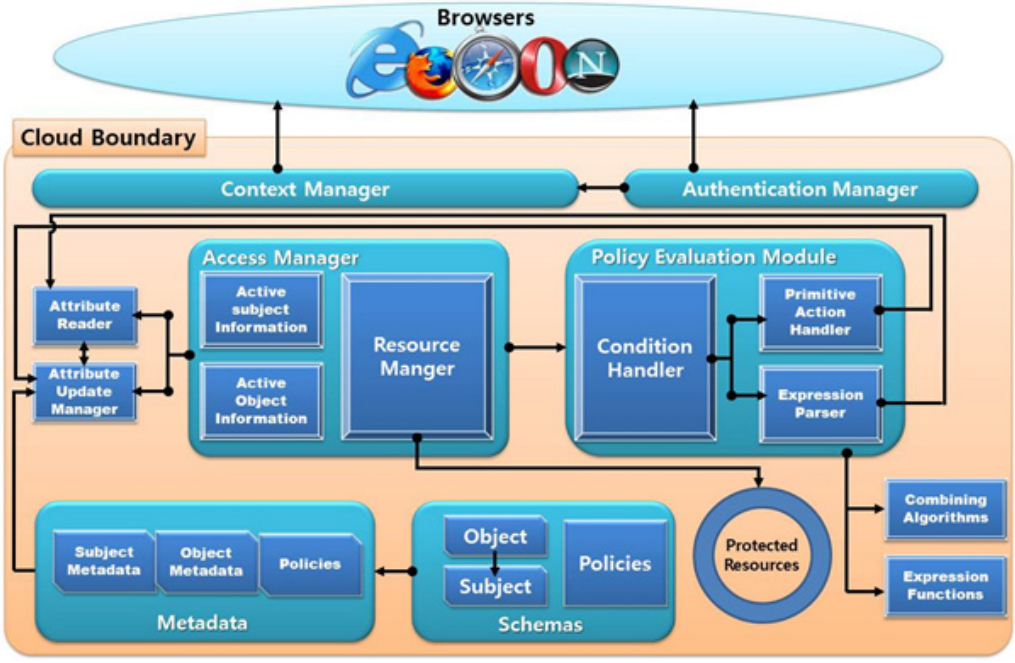
Multimedia content dissemination and control over

this distribution has been well studied in the past literature. Control over distributed content is often referred to Digital Rights Management (DRM) [5]. Liu et al. [1] have described a comprehensive review of the problems and possible solutions to the problem of DRM. They have covered both hardware and software-based solutions to the problem in brief and have also identified user privacy and usability as the major concerns regarding DRM deployments. However, almost all the solutions they have proposed are those related to cryptographic assurances and partial dissemination of files. The need for association of high-level expressive policies is not directly addressed in this work. Novelli et al. [6] have described a mechanism for content distribution over a content distribution network which is realized using grid infrastructure. However, this too is a purely distribution mechanism which does not address secure distribution of content in terms of the policies associated with the content by the originator or copyrights holder.

One of the most recent works in terms of securer content distribution has been carried out by Thomas et al. [7]. This work proposes the use of digital watermarking and cryptographic mechanisms to ensure that not only is content distributed to the intended target but also that the security concerns of the content owner as well as the different parties involved in the dissemination (such as sellers and re-sellers) are protected. However, as with previous works, no high-level security policy about the usage of the content is covered by this work and is thus unable to dictate how the content might be used once it reaches the intended target machine. This type of policies has been covered by Pretschner et al. [8] in a project which aims at the deployment of usage control models at different levels of abstraction. However, due to the complexity of the policies and enforcement requirements at the different machines have made it difficult to realize the high-level goals set forth by the project. To-date, no implementation plan has been made available by this project in terms of the realization of usage control. The approach closest to the implementation of usage control models has been proposed by Katt et al. [9]. However, due to the reliance of the approach on XACML and the lack of functional details, this approach has been unable to demonstrate technical feasibility and we consider it to be too crude to deploy in a commercial setting. It is our belief that using the cloud computing paradigm would open new avenues for realization of usage control models and would speed up the efforts aimed at this goal.

3. Proposed Architecture

Several concepts of document and protected object dissemination through the cloud exist today such as Google Books for online book reading and YouTube for video sharing. In either of these cases, the concept of access control is employed. For example, Google Books allows limited previews of some books, which is limited to certain pages of the book. However, the access control models employed do not employ the concept of revocation. Even those services that have this concept tend to employ revocation using adhoc techniques. In the context of video sharing sites, this becomes more pronounced as the prevalent models of digital rights management involve attributes such as the time duration for which a video can be watched, the number of times it can be viewed etc. There is a need to provide architecture for explicitly specifying the requirement for usage of these protected objects in any of the object dissemination systems in the cloud. By enabling usage control models in the cloud, it would be possible to deploy these and other novel scenarios for fine-grained usage control over content disseminated through cloud based applications. However, for such control over data, there are several requirements that must be fulfilled by the cloud based usage control application.



[Fig. 1] MCM Architecture

We define the following criteria for any usage control engine implementation:

1) Expressive power: The usage control domain encompasses some of the most highly expressive policy models. It is, by nature, capable of specifying a myriad of policies and covers many real-world scenarios. Any implementation of this domain must therefore be able to accommodate special usage control features like attribute mutability and decision continuity.

2) Efficiency: The continuity feature of usage control models requires a constant policy execution model. This requires a highly efficient implementation scheme both in terms of time as well as space complexity.

3) Ease-of-use: End users are not likely to interact directly with any policy engine. However, the ease-of-use in terms of how easy it is to specify policies is an important concern for any implementation. The policy language should therefore be easy to implement and not give rise to redundant markup.

4) Standardization: What might be considered somewhat difficult to achieve in light of the above requirement, our final requirement is that the policy language should be based on a standardized syntax. A proprietary or esoteric syntax is highly unlikely to be accepted by the

community at large and will severely hinder adoption, especially in the case of our target domain i.e. cloud computing.

In the following, we describe how we have catered to these requirements in a platform independent, object-oriented architecture of a usage control model for the cloud application. We base our architecture on the most widely accepted usage control model - UCON [2] - that divides a usage session in different states. The different modules of our architecture are discussed fig 1.

1) Context Manager: The most important aspects of our design reside within the context manager. These include the capability to manage user requests and conveying them to the different MCM constructs. The context manager also caters to the requirement of

continuity by keeping record of the information about different subjects and objects. It communicates with the access manager to allow state transitions and to receive notifications of decisions from the access manager.

2) Authentication Manager: MCM is an authorization model and like all such models, it assumes the presence of an authentication mechanism to provide identity of the different stakeholders. The actual implementation (or selection) of this mechanism remains outside our scope. The authentication module, however, provides an interface that allows us to abstract away the details of authentication from the rest of the engine.

3) Access Manager: The highly expressive nature of MCM allows the specification of different types of policies. These policies are evaluated using the 'policy evaluation module' through the access manager. The context manager requests the access manager to evaluate

the different policies associated with their respective states. The access manager also handles the creation and management of attribute update manager and attributes reader to change and retrieve the attributes associated with subjects and objects.

4) Policy Evaluation Module: The access manager sends Browser Fig. 1. MCM Architecture

Primitive Action Handler Expression Parser Combining Algorithms Expression Functions requests to this module requesting the evaluation of an individual policy based on the state of the system. The policy evaluation module is responsible for parsing the policies, evaluating the predicates and calculating update values. Attributes are retrieved using attribute readers and updated using update managers passed by the access manager. These updates are synchronized with the usage of objects in the browser through AJAX for seamless integration.

5) Schemas: In accordance with the requirement of standardization, the policies and attributes for subjects and objects are defined through the widely adopted standard of inter-operability - XML. The policies and metadata must adhere to the schemas defined for their respective types. Note that subjects are a subset of objects in MCM and therefore, their schemas are derived from that of the objects.

6) Resource Manager: Resources under protection by the MCM engine must be resistant to different attacks. For this reason, we propose the use of a hardware-based security mechanism. Specifically, this is the Trusted Platform Module (TPM) [10]. This cryptographic coprocessor comes built-in to many off-the-shelf systems and is capable of providing strong security. One of the security features provided is termed as binding which allows an object to be associated with a specific machine. In this case, only that machine can be used to decrypt the object.

4. Content security within Cloud

The second aspect of our architecture for secure dissemination of multimedia content is concerned with the "middlemen" in the content distribution chain. When content is released by its owner to a third-part (in this case, the cloud computing platform), she needs some form of assurance that the content will be used and distributed in compliance with her policies. She also needs assurance that the content will not be compromised while hosted on the third-party servers. The increasing number of hosted cloud computing services such as Amazon's EC2 [13] provides a lot of motivation to host content and services outside one's own domain of control. The obvious benefits are lower-costs and smaller maintenance overhead both in terms of human resource and in monetary terms. However, by hosting services on such cloud computing platforms opens up a can of worms in the form of security and privacy concerns. The question of how a cloud platform might be trusted is still a very open research issue. Santos et al. [11] have described a detailed infrastructure for the implementation of a trusted cloud computing platform using the constructs

of Trusted Computing and the security coprocessor called the Trusted Platform Module (TPM)[12]. The TPM is a specialized security chip which allows, among other things, a mechanism to provide assurance to remote authorized parties that a platform is trustworthy and that it will behave as expected. The mechanism proposed by Santos et al. provides a detailed architecture for using the TPM to securely deploy VMs in a cloud and provide assurance that the data released to a specific VM will only be accessible to that VM. However, no mechanism for the establishment of trust on the execution of policies attached to the protected content is provided in the architecture. We have described in detail a mechanism for establish trust on distinct VMs running on the same platform as is the case with cloud computing platforms. Using our proposed architecture, the cloud computing platform can provide assurance to the content owner that the VM is behaving as expected and thus the security that the policies of the object owner will indeed be enforced as expected.

5. Conclusion

The dissemination of multimedia content faces several issues with regards to its complexity because of the multitude of policy types that providers may wish to associate with their content. In this paper, we have proposed a framework for the use of cloud computing for secure dissemination of protected multimedia content as well as documents and rich media. We have leveraged the MCM model for enforcing fine-grained continuous usage control constraints on objects residing in the cloud. Our framework allows for the object owner to specify her policies regarding usage of the protected objects ensuring the enforcement of her policies including those specifying say, the duration of each use, the number of times the object can be used etc. For our future studies we are aiming to apply the detailed architecture for the deployment along with our ongoing work in this area. Trustworthy execution of the policies within the cloud forms part of our future plans for this contribution.

Reference

[1] Q. Liu, R. Safavi-Naini, and N. Sheppard(2003), “Digital rights management for content distribution,” in Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21. Australian Computer Society, Inc. Darlinghurst, Australia, Australia, 2003, pp. 49 - 58.

[2] J. Park and R. Sandhu(2002), “Towards Usage Control Models: Beyond Traditional Access Control”, in SACMAT ‘02: Proceedings of the seventh ACM Symposium on Access Control Models and Technologies.New York, NY, USA: ACM Press, 2002, pp. 57 - 64.

[3] F. Krautheim(2009), “Private Virtual Infrastructure for Cloud Computing”, Workshop on Hot Topics in Cloud Computing (HotCloud ‘09).

[4] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica(2009)., “Above the clouds: A Berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28.

[5] P. Kumik(2008), “Digital Rights Management,” Legal Information Management, vol. 1, no. 02, pp. 21 - 23.

[6] G. Novelli(2007), G. Pappalardo, C. Santoro, and E. Tramontana, “A gridbased infrastructure to support multimedia content distribution,” in Proceedings of the second workshop on Use of P2P, GRID and agents for the development of content networks. ACM, 2007, p. 64.

[7] T. Thomas, S. Emmanuel, A. Das, and M. Kankanhalli(2009), “Secure multimedia content delivery with multiparty multilevel DRM architecture,” in Proceedings of the 18th international workshop on Network and operating

systems support for digital audio and video. ACM New York, NY, USA, 2009, pp. 85 - 90.

[8] A. Pretschner, M. Hilty, and D. Basin(2006), "Distributed usage control," Communications of the ACM, vol. 49, no. 9, p. 44.

[9] B. Katt, X. Zhang, R. Breu, M. Hafner, and J. Seifert(2008), "A General Obligation Model and Continuity: Enhanced Policy Enforcement Engine for Usage Control," in Proceedings of the 13th ACM symposium on Access control models and technologies. ACM New York, NY, USA, pp. 123 - 132.

[10] OASIS, "XACML 2.0 Specification Set," 2005, Available at: http://www. oasis-open.org/ committees/tchome.php?wg abbrev=xacml.

[11] "Amazon Elastic Compute Cloud (Amazon EC2)," 2009, available at: http://aws.amazon.com/ec2/.

[12] N. Santos, K. Gummadi, and R. Rodrigues(2009), "Towards trusted cloud computing," Proceedings of Workshop on Hot Topics in Cloud Computing (HotCloud'09).

Randy Tolentino

- 2003년 2월 : Western Visayas 과학기술대학(학사)
- 2005년 2월 : Western Visayas 과학기술대학(석사)
- 2011년 2월 : 한남대학교, 멀티미디어공학과(석박사통합과정 박사)
- 2011년 ~ 현재 : 한남대학교, 멀티미디어공학과 조교수
- 관심분야 : 모바일 웹서비스, 정보 보호, 센서 웹, 모바일 통신보안
- E-mail : daryn2004@yahoo.com

김 용 태

- 1984년 2월 : 한남대학교 계산통계학과(공학사)
- 1988년 2월 : 숭실대학교 전자계산학과(공학석사)
- 2008년 2월 : 충북대학교 전자계산학과(이학박사)
- 2002년 12월 ~ 2006년 2월 : (주)가림정보기술 이사
- 2010년 3월 ~ 현재 : 한남대학교 멀티미디어학부 교수
- 관심분야 : 모바일 웹서비스, 정보 보호, 센서 웹, 모바일 통신보안
- E-Mail : ky7762@hnu.ac.kr

정 윤 수

- 1998년 2월 : 청주대학교 전자계산학 (공학사)
- 2000년 2월 : 충북대학교 대학원 전자계산학 (이학석사)
- 2008년 2월 : 충북대학교 대학원 전자계산학 (이학박사)
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail : bukmunro@mokwon.ac.kr