The Journal of Digital Policy & Management 2013 Sep; 11(9): 189-194

시맨틱 웹을 위한 권한부여 정책 관리에 관한 연구

조선문*
배재대학교 IT교육*

A Study on Authorization Policy Management for Semantic Web

Sun-Moon Jo*
Dept. of Computer Information Technology Education, Paichai University*

요 약 시맨틱 웹은 웹에 있는 정보를 컴퓨터가 좀 더 이해할 수 있도록 도와주는 기술을 개발하여 검색, 데이터 통합, 자동화된 웹 서비스를 지원하는 것이다. 정보의 양이 증가하고 다양해지면서 사용자의 요구에 적합한 정보만을 효율적으로 추출 가공하여 제공하는 문제가 있다. 시맨틱 웹은 기존의 웹과 완전히 구별되는 것은 아니다. 현재 웹을 확장하여 웹에 게시되는 정보에 잘 정의된 의미를 부여하고 이를 통해 컴퓨터와 사람이 협동적으로 작업을 수행하게 한다. 시맨틱 웹을 구축하기 위해서는 HTML의 한계를 극복해야 한다. 기존의 접근 권한부여는 HTML 때문에 정보와 의미론을 고려하지 못하였다. HTML을 사용하여 여러 관련 문서를 확장하거나 통합하는 것은 어렵다. 사람이 아닌 프로그램이나 소프트웨어 에이전트가 자동으로 문서의 의미를 추출할 수가 없다. 본 연구에서는 시맨틱 웹 환경에서 접근 권한부여 정책 관리하는 방법을 제안한다. 따라서 본 연구에서 설계한 정책이 기존의 방법보다 권한부여 과정을 개선하였다.

주제어 : 시맨틱 웹, XML, 권한부여, 정책, 보안

Abstract Semantic Web is what supports a search, data integration, and automated web service by developing technology of giving help so that a computer can understand information a little more on the web. As amount of information gets growing and diverse, there is a problem of offering by efficiently extracting and processing only information proper for users' demand. Semantic Web isn't what is distinguished completely from the existing web. It gives a meaning, which was well defined, to information of being inserted on web by expanding the current web. Through this, a computer and a person come to perform work cooperatively. To implement Semantic Web, the limit of HTML needs to be overcome. The existing access authorization has not taken information and semantics into account due to the limitations of HTML. It is difficult to expand or integrate many relevant documents by using HTML. Program or software agent, not a person, cannot extract a meaning of document automatically. This study suggests a method of Access Authorization Policy Management that is in the Semantic Web configuration. Accordingly, the policy, which was designed in this study, improved the authorization process more than the existing method.

Key Words : Semantic Web, XML, Authorization, Policy, Security

Received 30 July 2013, Revised 2 September 2013
Accepted 20 September 2013
Corresponding Author: Sun-Moon Jo(Paichai University)
Email: sunmoon@pcu.ac.kr

ISSN: 1738-1916

1. 서론

3세대 웹은 시맨틱 웹 서비스이다. 에이전트 기반으로 이용되며 사용자와 애플리케이션 기반이고 특정한 목적을 지향하고 있다. 웹 서비스도 기존의 웹에서 사용되던 HTTP, HTML, URL과 같은 기술을 통해 발전하고 있다[1]. 웹은 널리 알려진 클라이언트와 서버 개념과 간단한 HTML 언어를 이용하여 편리성을 추구한 덕분에 사용자 누구나 정보를 접근하거나 게시할 수 있다. HTML의 단순성은 현재 웹의 성장을 가져온 중요한 열쇠가 되었다. 그러나 이런 단순성이 정보가 방대해진 상황에서는 문제가 된다. 정보의 양이 증가하고 정보의 형태가 다양해지면서 사용자의 요구에 적합한 정보만을 효율적으로 접근, 추출하여 제공해야 하는 문제가 되었다[2,7].

시맨틱 웹의 궁극적인 목적은 웹에 있는 정보를 컴퓨터가 좀 더 이해할 수 있도록 도와주는 표준과 기술을 개발하여 의미 검색, 데이터 통합, 자동화된 웹 서비스 등을 지원하는 것이다[3]. 시맨틱 웹에서 다수의 응용은 데이터에 대한 선택적 접근 제공을 요구한다. 접근은 데이터를 설명하는 데 사용되는 언어와 검색과 브라우징에 실행할 수 있는 타입의 액션들에 맞추어야 한다. 이는 XML이 웹에서 교환되는 정보를 제공하기 위한 언어로 사용되는 일이 증가하고 있기 때문이다. 그러므로 접근 정책을 명세하고 실행할 수 있는 방법이 요구된다[4,5,6]. 첫 번째는 문서는 민감도가 다양한 정보를 포함하여 다양한 보호 입상 수준을 지원해야 한다는 사실이다. 어떤 경우에는 여러 문서에 같은 접근 정책이 적용될 수 있다. 또 어떤 경우에는 같은 문서의 부분마다 다른 접근 정책이 적용될 수 있다. 다른 많은 중간 상황도 발생할 수 있다. 접근을 모든 입상 수준을 지원할 만큼 충분히 유연해야 한다. 두 번째는 문서가 항상 정의된 문서 타입에 맞는 것은 아니다. 접근 정책은 문서 타입과 관련하여 명세될 가능성이 매우 높으므로, 문서가 기존의 접근 정책에 의해 다루어지지 않는 상황은 적절하게 관리해야 한다. 웹에서는 문서 교환 및 수집 과정이 빈번할 수 있으므로, 접근 방법은 이러한 상황에 매우 자주 대처해야 한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 연구에 관하여 설명과 문제점에 대하여 기술한다. 3장에서 제안하는 접근 권한부여 방법과 알고리즘에 대하여 기술한다. 4장에서 실험 결과를 기술하고, 5장에서 결론 및 향후 연구에 대하여 기술한다.

2. 관련 연구

XML 문서에는 문서 타입 선언이 추가되어 문서가 따라야 할 규칙이 있다. 이러한 규칙은 일괄적으로 문서 타입 정의라고 한다[7,8]. 예를 들면, [그림 1]은 문서에 대한 DTD를 보여준다. DTD는 두 부분(요소 선언과 속성 목록 선언)으로 이루어져 있다. 요소 선언 부분은 문서에 들어 있는 요소들의 구조이다. 특히 요소의 경우에는 그 하위 요소와 순서, 임의의 선택인지 여부('?'), 더 나타낼지 여부('*' or '+'), 하위 요소들이 서로 대체할 수 있는지 여부('|'), 데이터 내용 타입이 있다.

```
<?xml version="1.0" encoding="EUC-KR" ?>
<!DOCTYPE department[
<!ELEMENT department (employee>*>
   <!ELEMENT employee (name, address, resume, salary, medical-dossier)>
<!ELEMENT name (fname, lname)>
<!ELEMENT address (street, tel*, email)>
<!ELEMENT resume (education, previous-job*, hobby?, skills*)>
<!ELEMENT salary (#PCDATA)>
<!ELEMENT medical-dossier ANY>
<!ELEMENT fname (#PCDATA)>
<!ELEMENT lname (#PCDATA)>
<!ELEMENTstreet(#PCDATA)>
<!ELEMENT tel (#PCDATA)>
<!ELEMENT email EMPTY>
<!ELEMENT previous-job (#PCDATA)>
<!ELEMENT education (#PCDATA)>
<!ELEMENT hobby (#PCDATA)>
<!ELEMENT skills ANY>
<!ATTLIST department id ID #REQUIRED>
<!ATTLIST employee id ID #REQUIRED manager IDREF #IMPLIED>
<!ATTLIST email mailto CDATA #IMPLED> ]>
```

[Fig. 1] XML DTD Example

Hada는 권한부여 정책을 7-튜플로 구성하였다. 조건부 액션 개념을 전통적 권한부여 의미론으로 통합함으로써 보다 유연성 있는 권한부여를 할 수 있도록 하였다[9,10]. 그러나 XPath 언어를 활용하지 않았다. 접근에서는 권한부여의 평가 과정이 복잡하고 응답시간이 느리다. 그 이유는 DTD 검증 과정에서 문서의 파싱과 검색 때문이다.

XACML은 정책, 요청, 응답으로 구성되어 있다. 정책은 가장 기본이 되는 규칙, 여러 규칙들을 포함하는 정책의 집합인 정책셋으로 구성된다. 그러나 특정 규칙의 타깃이 요청 문맥에 해당되더라도 규칙에 포함되어 있는 조건에 어긋나면 요청 문맥에 대한 규칙의 결과는 비적용으로 된다. 요청 문맥에 대한 정책에 대한 평가는 규칙에 대한 평가보다 복잡하다[11].

Gabi에서는 권한부여의 의미론을 다양한 것으로 정의하였다. 권한부여 규칙은 4-튜플로 구성되는데 주체의 집합, 객체의 집합, 접근, 우선권이다[12]. 객체는 주체 시트의 요소 주체와 관련하여 주체의 위치 경로로 표현하고 있는 객체의 XPath 트리 노드이다. 접근에 대한 값은 허가와 거부 중 하나이다. 이 방법은 모든 종류의 노드를 보호할 수 있는 가능성을 제공하지 않는다. 또한 충돌 해결 정책과 권한의 평가 과정이 느리다.

3. 문서 권한부여 정책

3.1 접근 권한부여

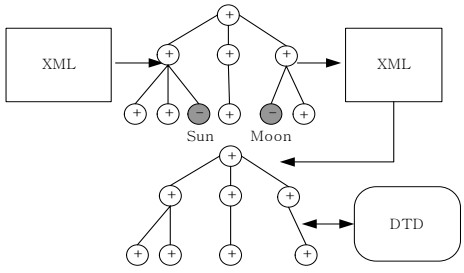
권한부여 규칙은 보안 정책의 표현이다. 보안 관리자는 보안에 대한 요구사항과 정책을 권한부여 규칙들로 구성된다. 일반적인 사용자나 객체에 대한 권한을 부여할 때뿐 아니라, 동일한 객체에 대한 여러 주체들의 권한 충돌이 발생할 때, 또는 동일한 주체에 대한 객체에 대한 여러 권한들이 중첩될 때에도 이용된다.

권한부여는 개별 문서와 요소들을 비롯하여 모든 입상 수준에서 권한부여를 지원한다. 권한부여를 명세할 수 있는 객체의 범위가 DTD에서 개별 문서 내의 단일 요소와 속성에 이른다. 여기서 요소와 속성은 path expression에 의해 참조될 수 있다[13]. 허가나 거부 권한부여의 이유는 예외를 지원하면서 주체와 객체들에 적용할 수 있는 권한부여를 단순하게 제공하기 위해서다.

본 연구는 문서의 권한부여 규칙을 subject, object, action, sign, type으로 구성한다. 권한의 Subject는 id나 접근을 요청한 위치로 기술 된다. Object는 권한이 주어지는 객체로 XPath로 표현한다. Action(write, delete)은 주체가 수행할 수 있는 연산으로 이루어진다. Sign ∈ {+, -}은 권한의 부호를 의미한다. Type ∈ {L, R, LDH, RDH, LD, RD}은 권한의 속성 값을 의미한다.

요소에 명세한 권한부여는 요소의 속성에만 적용하거나, 재귀 접근에서는 하위 요소와 그 속성에 적용할 수 있는 것으로 정의한다. 어떤 요소에 대한 로컬 권한부여는 요소의 직접적인 속성에는 적용되지만 하위 요소의 속성에는 적용되지 않는다. 보안 측면에서 재귀 권한부여는 트리에 있는 노드에서 자손으로 허가나 거부를 전파함으로써 요소의 전체 내용에 해당하는 권한부여를 쉽게 명세서하는 방법을 기술한다.

권한 접근 중 묵시적 권한은 상위 구성요소에 한 번의 권한부여로 하위 구성요소에 권한을 부여한다. 반면에 명시적 권한 기법은 각각의 요소 마다 권한의 정보를 저장하는 기법으로 묵시적 권한 기법에 비하여 저장 공간의 오버헤드가 있지만, 각 구성 요소가 권한의 정보를 가지고 있다.



[Fig. 2] DTD Check

예를 들면, XML 접근제어에 연산자가 추가 하면 DTD 검증 과정이 필요하게 된다. DTD 검증 과정은 DOM 기반의 접근 시스템에서 발생한다. 다음은 구조 변경을 허용하지 않는 환경에서 가정하면 [그림 2]와 같은 DTD 검증과정이 이루어진다.

3.2 전파 규칙 및 권한 정책

전파 규칙은 요소에 다른 권한이 설정되어 있을 경우나 충돌이 생긴 권한들 사이의 우선순위를 결정하여 권한을 설정하는 방법이다.

문서에 대해 정의하고 유지할 권한부여의 수를 제한하기 위해 문서의 그래프 구조를 이용하여 권한부여 전파를 시행할 수 있다. 전파라는 개념은 그래프 구조의 보호 객체들 사이에 존재하는 관계를 토대로 한다. 문서와 DTD를 제시하는 그래프에서는 권한부여 전파를 위해 다음과 같은 관계를 기술한다.

권한부여는 XML의 DTD와 관계가 있으며, DTD 대 인스턴스 전파 관계로 인해 DTD 인스턴스에 전파한다. DTD의 다양한 입상 수준(문서, 요소, 속성, 링크)에서 정의되어 DTD의 유효 문서 인스턴스 내용에 다양한 보호를 제공한다. 전파를 시행할 보호 요구사항에 따라 DTD에 대한 다양한 권한부여를 명세함으로써 문서 보호를 실행할 수 있다. 예를 들어, 문서와 관련된 DTD에 대해 DTD 수준에서 한 가지 권한부여만 기술하고, 요소 대 하위 요소 및 요소 대 속성이나 링크 관계로 인해 DTD의 모든 하위 요소, 속성, 링크로 전파되고 DTD 대 인스턴스 관계로 인해 DTD의 모든 문서 인스턴스로 전파함으로써 주체에게 보호 요구사항이 동질적인 문서에 접근할 권한을 부여할 수 있다.

각각의 접근 권한부여 상태는 주체가 요소나 속성에 접근할 수 있는지 여부를 표시한다. 인스턴스나 스키마 수준에서 해당 객체에 대한 각각의 권한부여와 관련된 타입은 객체의 구조와 관련이 있다. 앞에서 논의한 원리에 따라 문서에 대한 권한부여를 시행하기 위해서는 문서의 요소와 속성에 허가 권한부여가 적용되는지(+), 거부 권한부여가 적용되는지(-), 아니면 어떠한 권한부여도 적용되지 않는지(Ɛ)를 제시해야 한다. 본 연구에서는 권한 설정과 권한의 충돌을 해결하는 제어 알고리즘을 기술한다.

```
Input: T: Dom Tree, ur: User-requester,
       ap: Authorization Policy(auth.dtd, xml.xas)
Output: T: modified Dom Tree
Procedure label
begin
   for each c ∈ children(T.root) do
 // L is local, R is recursive, LDH is Local DTD Hard
 // RDH is Recursive DTD Hard, LD is local DTD   level,
 if c.parent.type in (L, R, LDH, RDH, LD, RD) then
     if auth.dtd ∩ xml.xas == ∅  then
        c.label ← c.parent.label
     else
        c.label ← propagation_rule
     fi
  else if ap.auth.dtd ∩ ap.xml.xas == ∅ then
        c.label ← default()
      else
        c.label ← propagation_rule
      fi
  fi
 end
```

[Fig. 3] Control Algorithm

[그림 3]에서 XML 문서에 해당하는 접근 권한을 a.xml에 하고, DTD에 해당하는 접근 권한을 a_dtd로 분리한다. auth.dtd ∩ xml.xas == ∅이면, 즉 접근 권한 정보가 없다면 auth.dtd에 미리 정해진 접근 권한 값을 설정한다. 그렇지 않다면 권한들 중 우선순위가 가장 높은 권한을 설정한다. propagation_rule()은 동일한 모드에서 충돌이 발생한 경우 정해진 규칙에 의해 우선순위가 높은 권한을 설정한다. 이러한 과정은 전위 순서로 실행한다. default()는 명시적 권한 설정이 없을 때 권한을 반환한다.

```
<!DOCTYPE authorizations [
<!ELEMENT authorizations    (authorization)+>
<!ELEMENT authorization (subject,    object, action,
              sign, type)>
<!ELEMENT subject (#PCDATA)>
<!ELEMENT object (#PCDATA)>
<!ELEMENT action EMPTY>
<!ELEMENT sign EMPTY>
<!ELEMENT type EMPTY>
<!ATTLIST authorizations about    CDATA #REQUIRED>
<!ATTLIST action value #REQUIRED>
<!ATTLIST sign value (+|-)    #REQUIRED>
<!ATTLIST    type    value    (L|R|LDH|RDH|LD|RD)
#REQUIRED>
]>
```

[Fig. 4] Authorization Syntax

권한부여가 있는 xas와 함께 사용자가 요청하는 유효한 문서를 입력으로 받는다. 출력은 사용자가 접근할 수 있는 정보만을 포함하는 문서이다. xas 정보를 표현하기 위해 [그림 4]를 이용한다. 접근을 정의하는 라인 외 링크 목록은 자체가 XML 문서이며, 관리자에 의해 쉽게 관리 및 업데이트될 수 있지만 표준 파일 시스템 수준의 접근에 의해 쉽게 보호된다.

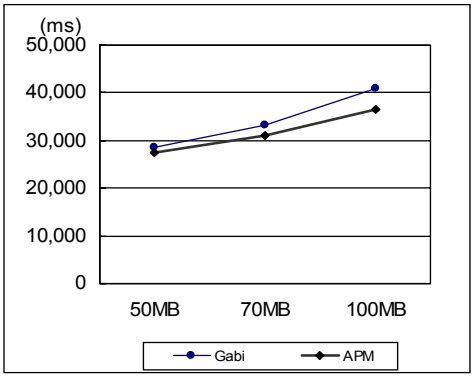
4. 실험 및 평가

4.1 평가

성능 평가의 대상은 Gabi의 방법과 제안하는 APM (Authorization Policy Management)에 대하여 접근 시간을 비교하였다. Auth.xas는 XML 문서로 작성되어 있으므로, 접근 정보를 참조하기 위해서는 Auth.xas를 파싱

하고 트리를 검색해야 한다. Auth.xas의 파싱 작업은 제어 알고리즘에서 접근 권한 정보를 참조하기 위해 필요하다. 접근 시간을 측정하기 위한 매개 변수를 구성하였다. 매개 변수의 시간 단위는 밀리세컨드이다. 문서는 XML 벤치마크로부터 데이터와 문서를 이용하였다[14]. 50MB, 70MB, 100MB와 DTD인 test.dtd- (5KB), 접근 권한 정보인 Auth.xas(195KB)로 구성된다. 문서의 크기가 커짐에 문서의 파싱과 트리의 검색은 증가한다. 그리고 매개 변수들 중에서 문서 파싱이 시스템의 성능에 가장 큰 영향을 미치는 변수가 된다. 아래와 같이 질의를 사용하였다.

/site/people/person/phone



[Fig. 5] Comparison of Access Policy

[그림 5]와 같이 접근 시간을 Gabi와 제안하는 APM을 비교한 결과이다. 문서에서 수정이 포함된 문서와 구조의 변경이 되는지를 검사하기 위해 DTD 검증 과정이 필요하다. Gabi에서는 접근 정보뿐 아니라 문서 자식에 대한 정보가 포함하므로 요구되는 시간은 크다. Gabi에서는 수정을 수행하여 변경된 문서를 파싱하고 새로운 트리의 모든 노드를 DTD와 비교하면서 검색한다. APM은 접근 권한부여를 <subject, object, action, sign, type>으로 구성하여 권한을 설정하므로 문서와 DTD 검증 과정에서 권한부여 과정을 단순하게 한다.

4.2 평가 고찰

시스템은 객체 지향원리에 따라 설계되었으며, 클래스 집합의 명세서에 기반을 두고 있다. 클래스는 그룹으로 구성된다. 첫 번째 그룹은 DOM 클래스 계층이 확장된 것으로서 필수 보안 속성으로 문서의 노드로 설명된다. 이러한 확장은 기존 DOM 실행과의 즉각적인 통합을 허용하는 기법을 활용하였다. 클래스의 두 번째 그룹은 접근 처리와 밀접한 관계가 있으며 권한부여 부호 주체의 개념을 이용하였다.

서비스의 문제는 성능에 중점을 두었다. 다중 스레드 시스템을 확보하기 위해서는 클래스를 스레드에 안전한 타입으로 구현하고, 각 요청의 매개변수들을 모두 특정 방법 호출 환경에 두었다. 성능을 더욱 강화하는 구조적 솔루션은 사용자 계층을 관리하는 스레드를 분리하는 것이다. 해당 사용자에게 권한부여가 적용되는지 여부를 계산하는 서비스는 사용자가 직접, 또는 간접적으로 권한부여 주체에 명세된 그룹에 속하는지 평가해야 한다.

5. 결론 및 향후 연구 방향

시맨틱 웹에서 권한부여는 사용자나 객체에 대한 권한을 부여할 때 뿐 아니라, 동일한 객체에 대한 여러 주체들의 권한 충돌이 발생할 때 이용된다. 문서와 DTD 모두의 그래프 기반 구조로 인해 접근 요청은 두 가지 방법으로 평가한다. 거부 권한부여의 존재와 보호 요구사항이 관련한 문서가 같을 경우는 DTD와 문서 수준에서 거부 권한부여가 명세될 때에는 상향식을 선택된다. 거부 권한부여가 없을 경우는 보호 요구사항과 관련하여 같은 문서에는 하향식이 바람직하다. 이는 문서에 대한 권한부여는 DTD와 문서 단위의 수준에서 명세된 다음 전파되기 때문이다.

본 연구는 시맨틱 웹 환경에서 문서 접근을 위한 권한부여 정책 관리를 위한 방법을 설계하였다. 문서에서 누가 접근을 행사할 것인가를 고려하면서 그룹 전반에 걸친 정책과 문서 작성자의 요구를 조정한다. 권한부여에서 기술한 요구를 실행하면 의뢰자에게 볼 수 있는 정보만 제공된다. 본 연구에서는 사용자와 연산자를 그룹 단위로 관리할 수 있게 되었다. 그러므로 복잡하고 다양한 접근권한 정보를 체계적으로 관리할 수 있다.

향후 연구를 통해 개선되어야 할 점은 시맨틱 웹에서 보다 자동적으로 권한부여를 설정 방법과 보다 간소화된 절차를 거쳐 접근 정책 방법을 연구하도록 하는 것이다.

References

[1] M. C. Daconta, L. J. Obrst, Kevin T. Smith, The Semantic Web: A Guide to the Future of XML Web Services and Knowledge Management, Wiley Publishing, Wiley Technology Publishing, 2003.

[2] S. A. Mcllraith, T. C. Son, Honglei Zeng, Semantic Web Services, IEEE Intelligent Systems, Vol. 16(2), pp. 46-53, 2001.

[3] J. Hendler, Agents and the Semantic Web, IEEE IEEE Intelligent Systems, Vol. 16(2), pp. 30-36, 2001.

[4] S. M. Jo, H. S. Joo, W. H. Yoo, A Study on Policy Design of Secure XML Access Control, J. of Korea Contents Association, Vol. 7, No. 11, pp. 43-51, 2007.

[5] H. Zhang, N. Zhang, K. Salem, D. Zhuo, Compact access control labeling for efficient secure XML query evaluation, Technical report, Department of Computer Science, University of Waterloo, 2004.

[6] E. Bertino, E. Ferrari, Secure, Selective Dissemination of XML Documents, J. of ACM Transactions on Information and System Security, Vol. 5, No. 3, pp. 290-331, 2002.

[7] L. Sun, Y. Li, DTD level authorization in XML documents with usage control, International Journal of Computer Science and Network Security, Vol. 6, No. 11, pp. 244-250, 2006.

[8] L. Sun, H. Wang, A purpose-based access control in native XML databases, Concurrency and Computation: Practice and Experience, vol. 24, pp. 1154-1166, 2011.

[9] S. Hada, M. Kudo, XML Access Control Language: Provisional Authorization for XML Documents, www.trl.ibm.com/projects/, pp. 1-28, 2002.

[10] M. Murata, A. Tozawa, M. Kudo, S. Hada XML Access Control using Static Analysis, J. of ACM Transactions on Information and System Security, 2006.

[11] Sun's XACML Implementation. http://sunxacml.-Soureefore.net/, 2003.

[12] A. Gabillon, An authorization model for XML database, In Proc. of the 2004 ACM Workshop on Secure Web Service, Fairfax USA, 2004.

[13] S. MOban, A Sengupta, Y. Wu, A Framework for Access Control for XML," J. of ACM Transactions on System and Information Security, pp. 1-38, 2006.

[14] The XML benchmark project, Available form: http://www.xml-benchmark.org.

조 선 문

・1995년 2월 : 충주대학교 컴퓨터공학과(학사)
・2001년 2월 : 인하대학교 컴퓨터정보공학과(석사)
・2007년 2월 : 인하대학교 컴퓨터정보공학과(박사)
・2006년 3월 ~ 현재 : 배재대학교 IT교육 교수
・관심분야 : 시맨틱 웹, 인터넷 응용, 프로그래밍 언어, 보안
・E-Mail : sunmoon@pcu.ac.kr