교육과학연구, 제14권 제1호, pp. 113-123 (2012. 05)

온라인상 어린이 보호를 위한 불법 유해콘텐츠 파일공유 접근제어 방안 연구

박 남 제*

본 논문은 유비쿼터스 환경의 핵심 기기인 개인 스마트폰 서비스 환경에서의 온라인상 학생 보호를 위한 불법 유해콘텐츠 파일공유 접근제어 방안에 관한 것으로, 기존의 인터넷에서 행하고 있는 단순한 유해정보 차단의 단점을 극복하기 위하여, 콘텐츠의 내용에 기반한 등급 분류 체계를 갖추고, 이를 통한 새로운 불법 유해콘텐츠 파일공유 접근제어 방안을 제안한 것이다. 우선 기존의 어린이들에게 유해 정보가 노출되는 것을 막기 위한 콘텐츠 내용에 기반한 등급 분류 기준에 대하여 알아본다. 그리고, 제안하는 불법 유해콘텐츠 파일공유 접근제어 방법의 구성을 살펴본 후, 적용 방안을 제안하고 결론을 맺는다.

* **주제어:** 유해콘텐츠, 콘텐츠 기반 등급분류, 접근방지, 유해정보 차단

Ⅰ. 서 론

스마트폰이 현대인의 필수품으로 자리매김하면서 이를 이용한 다양한 서비스가 제공되고 있고, 이러한 추세는 앞으로도 지속적으로 이루어질 것으로 전망된다. 하지만 이러한 환경에서 어린이는 인터넷상에서 여러 폭력물과 음란물 등 유해 콘텐츠 등에 심각히 노출되어 있고, 이러한 노출로부터 어린이 또는 청소년을 보호하는 것은 모든 나라의 주요 관심사가 되고 있다. 그러나 이 문제를 해결하기 위해선 국가의 법제도적 대책과 더불어 기술적 대책의 마련이 선결되어야 하며, 이는 서비스 제공자, 부모, 어린이 등 주요 주체, 그리고 정부의 공동 노력에 의해 해결될 수 있다.

새로운 융합 서비스와 스마트 기기 환경에서 편리한 서비스를 제공받기 위해서는 유해정보 콘텐츠의 접근제어가 반드시 필요하다. 즉, 성인이 아닌 청소년들이 갖고 있는 스마트폰에 다양한 온라인 정보가 지원될 경우, 성인 콘텐츠 등에 무방비로 노출될 수 있기 때문에 불법 유해콘텐츠의 접근을 방지하기 위한 방안이 반드시 필요하다. 현재 유선 인터넷에서 시행하고 있는 성인 인증은 주민

* 제주대학교 교육대학 초등컴퓨터교육전공 교수(email: namjepark@jejunu.ac.kr)
◎ 접수일(2012년 5월 1일), 수정일(1차: 2012년 5월 18일), 게재확정일(2012년 5월 22일)

등록번호를 이용하는 방식으로, 주민등록번호만 갖고 주민등록번호 알고리즘으로 계산하는 단순 계산 방법, 이름과 주민등록번호를 갖고 금융정보기관에 문의하여 확인하는 방법, 이름을 입력하여 로그인(log-in) 했을 때의 실명 이름을 이용하여 별도 입력을 받지 않는 등의 방법이 사용되고 있다. 이러한 단순한 방법 외에도 휴대전화 번호, 주민등록번호, 공인인증서 등 세 가지 정보의 조합으로 성인임을 확인하는 단계적 성인 인증 방법도 사용되고 있다. 하지만, 신규 융합 IT 서비스와 스마트 기기 환경에서 온라인상 어린이 보호를 위한 새롭고 효율적인 불법 유해정보 콘텐츠에 대한 접근방지 방안이 필요하다. 본 논문에서는 기존 멀티미디어 콘텐츠에 적용되고 있는 사용자 연령별 단순 등급 표현 대신 콘텐츠 내용을 세분화하여 표현하는 불법 유해콘텐츠의 접근제어에 대한 방안을 제시한다.

II. 어린이 불법 유해정보들의 분류 기준 방안

기존의 멀티미디어 콘텐츠에 적용되고 있는 단순한 등급 체계를 탈피하기 위하여 콘텐츠 등급을 사용자 나이로 구분하지 않고 단어(word), 신체노출(nudity), 성행위(sex) 및 내용(content) 등 4개의 분야로 콘텐츠 내용을 세분화하여 해당 제공 서비스의 내용 기반 분류 등급을 표현하도록 하였다 (김영수 외, 2009; 황승흠 외, 2003; C.Burges, 1998).

<표 1> 서비스 콘텐츠 내용기반 분류 등급 표현

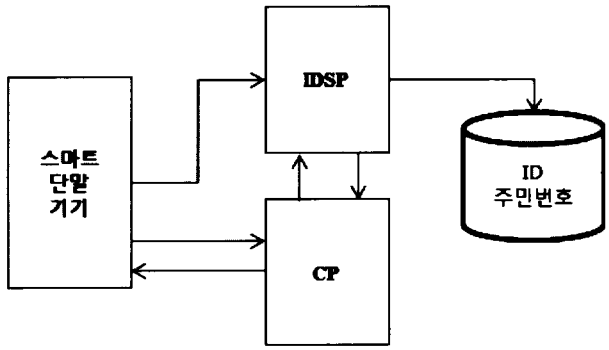
분류	0등급	1등급	2등급	3등급
단어	어느것과도 상관없음	성상담/성교육에 사용되는 성행위 묘사 단어	정상적인 성행위 묘사 단어	비정상적인 성행위 묘사 단어
신체노출	어느것과도 상관없음	노출 복장, 남성 상반신 노출 등	여성 상반신 노출 등	남녀의 성기 또는 음모 노출, 전신노출 등
성행위	어느것과도 상관없음	격렬한 키스 등	착의 상태의 성적 접촉 등	노골적 성행위 또는 성범죄 등
내용	어느것과도 상관없음	상식적 내용	불륜적인 내용	패륜적 내용 및 상식 이하의 내용

<표 1>은 4가지 항목에 대한 등급별 구분 기준이다. 비정상적 성행위 묘사 단어를 사용하거나, 남녀의 성기 또는 음모 노출, 노골적 성행위 또는 성범죄, 그리고 노골적인 저속어를 사용하였을 경우에는 3등급으로 지정한다. 정상적 성행위 묘사 단어를 구사하거나, 여성 상반신 노출 사진, 착의 상태의 성적 접촉, 또는 심한 비속어나 혐오적 표현을 사용한 데이터에 대해서는 2 등급으로 지정한다. 성적인 내용을 담고 있으나 성상담 및 성교육 등에 사용되는 성행위 묘사 단어를 담고 있거나 가벼운 비속어를 사용한 콘텐츠는 1등급으로 지정하고, 위의 경우에 모두 속하지 않는 경우에는 0

등급으로 지정한다. 이러한 새로운 등급 기준이 신규 융합 서비스 환경에 적용되면, 상기한 4개의 분야별로 등급 값이 기록되고 이들 각 등급의 조합으로 최종 등급이 결정되게 된다. 이러한 세분화된 등급 기준을 통해 대상이 되는 멀티미디어 콘텐츠 등급을 분야별로 표현할 수 있게 되고, 단어, 신체노출, 성행위, 내용 등의 항목에 각각 가중치를 달리하여 최종 종합 등급을 조절하는 것이 가능하게 된다(김지연, 2003; F.Sebastiani, 2002).

Ⅲ. 제안된 유해콘텐츠 서비스 접근제어 방안

유해정보 인증 기능 처리부를 포함하는 스마트 단말기(스마트폰)와 서버에서 유해정보 인증 등급 확인부를 포함하는 IDSP(Identification Server Provider) 시스템과, 상기 스마트 단말기와 IDSP 시스템 간 전송되는 메시지를 프로토콜 변환하는 게이트웨이로 구성된 서비스 구성도를 제안한다.



[그림 1] 제안 기능에 대한 서비스 구성도

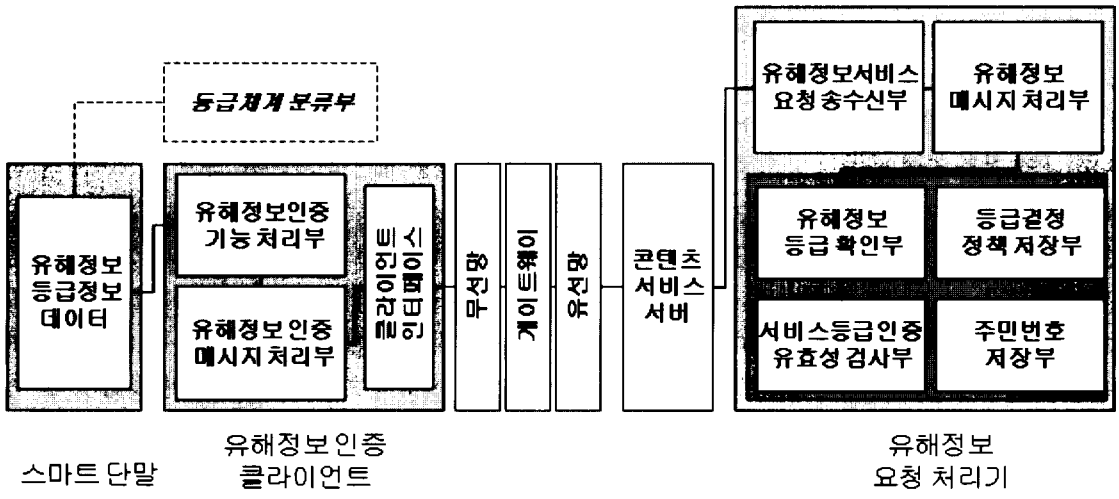
제시된 유해정보 서비스 구성도는 종래의 유해 콘텐츠 접근방지 방안과는 달리 유해 콘텐츠 인증 등급 확인 및 ID 메시지를 처리하는 IDSP 서버가 추가되어 인증기능을 강화한 구성을 갖추고 있다.

위의 그림은 내용기반 등급분류기준에 따른 유해콘텐츠 정보인증 서비스의 기능도이다. 그림에서 나타나는 것과 같이 유해정보 인증 기능 처리부, 유해정보 인증 메시지 처리부, 유,무선 프로토콜 변환 기능을 하는 게이트웨이, 콘텐츠를 제공하는 콘텐츠 서비스 서버, 그리고, 유해정보 인증 등급 분류부, 주민번호 저장부 등의 기능을 더 포함한다. 서비스 클라이언트 측의 각 기능 모듈로는 유해정보 인증 기능 처리부와 유해정보 인증 메시지 처리부가 있으며, 유해정보 인증 요청 처리기 측의 각 기능 모듈로는 유해정보 인증 서비스 요청 송수신부, 유해정보 인증 메시지 처리부, 그리고 사용자 연령 확인부가 있다. 또한 사용자 연령 확인부는 유해정보 인증 등급 확인부, 서비스 등급 인증 유효성 검사부, 등급 결정 정책 저장부, 그리고 주민 번호 저장부 등으로 구성된다.

사용자 단말에 내장된 유해정보 인증 기능 처리부가 유해정보 콘텐츠의 유해정보 인증 등급 정보를 독출하면, 유해정보 인증 메시지 생성부는 ID와 유해정보 인증 등급 정보를 포함한 유해정보 인

증 요청 메시지를 생성하여 CP에게 전송하게 된다. 유해정보 인증 시스템의 인증 처리 절차는 다음과 같다.

① 유해정보 인증 기능 처리부가 클라이언트인 스마트 단말 태그 내에 포함된 유해정보 인증 등급 정보 데이터를 읽어온다. 이 데이터의 각 카테고리 값은 등급 체계 분류부로부터 획득할 수 있다.
② 유해정보 인증 메시지 처리부는 ID와 유해정보 인증 등급정보를 담은 질의 메시지를 생성하여 콘텐츠 서비스 서버에게 전송한다.
③ 콘텐츠 서비스 서버는 유해정보 인증 요청 처리기의 유해정보 인증 서비스 요청 송수신부에 이 메시지를 전송하여 유해정보 인증을 요청한다.
④ 수신한 메시지를 유해정보 인증 메시지 처리부에서 해석한 후, 각 카테고리 값을 획득한다. 유해정보 인증 메시지 처리부는 이 카테고리 값들을 유해정보 인증 등급 확인부로 전송한다.
⑤ 유해정보 인증 등급 확인부에서는 등급 결정 정책 저장부의 최종 등급 결정 정책을 참조하여 최종 등급과 ID를 서비스 등급 인증 유효성 검사부에 넘긴다.
⑥ 서비스 등급 인증 유효성 검사부는 휴대단말 사용자에게 ID 입력을 요청한다.
⑦ 휴대단말 사용자의 ID를 입력받으면, 주민번호 저장소에서 해당 ID에 해당하는 고객의 주민번호를 확인하여 고객의 나이를 산출하게 된다. 서비스 등급 인증 유효성 검사부는 최종 등급과 사용자의 나이를 통해, 콘텐츠 서비스 서버가 해당 콘텐츠를 사용자에게 제공해도 되는지 여부를 판단한다. 콘텐츠 서비스 서버는 판단 결과를 유해정보 인증 메시지 처리부에게 전달한다.
⑧ 유해정보 인증 메시지 처리부는 유해정보 인증 서비스 요청 송, 수신부를 통해 콘텐츠 서비스 서버에 판단 결과를 통보한다.
⑨ 콘텐츠 서비스 서버는 수신한 유해정보 인증 요청 처리기의 유해정보 인증 판단 결과에 따라 콘텐츠를 제공하거나 제공하지 않는다.



[그림 2] 내용기반 등급분류기준에 따른 유해콘텐츠 정보인증 서비스 기능도

Ⅳ. 제안된 불법 파일공유에 대한 응용 보안적용 방안

본 장에서는 앞장의 유해정보 인증서비스 구조에서의 불법 파일공유에 대한 응응 보안 적용방안을 제안한다. 많은 인터넷 응용에서 인증 및 메시지 무결성을 제공하기 위해 PKI(Publish Key Infrastructure)를 기반으로 서비스를 제공하고 있다. 이 경우 송신되는 메시지는 전송자의 서명을 포함하고, 수신자는 CA(Certificate Authority)의 도움을 받아 전송자의 서명을 검증하게 된다. 현재 PKI 기반의 서비스를 제공하는 많은 응용들이 있지만, 인터넷에서 개인과 개인이 직접 연결되어 파일을 공유하는 P2P(peer to peer)에 실제적으로 적용된 사례는 없다. 이는 P2P의 다양한 특성 때문이기도 하며, 특히 국가간 PKI 상호 운용성을 제공하지 못하는 것도 전 세계적인 사용자가 존재하는 P2P에 적용을 현실적으로 어렵게 만드는 요소이기도 하다. 또한 PKI 인프라의 구축, 인증서 발급 및 관리를 위한 비용도 만만치가 않다(조동욱, 2004; Namje Park, Youngsoo Kim, 2010).

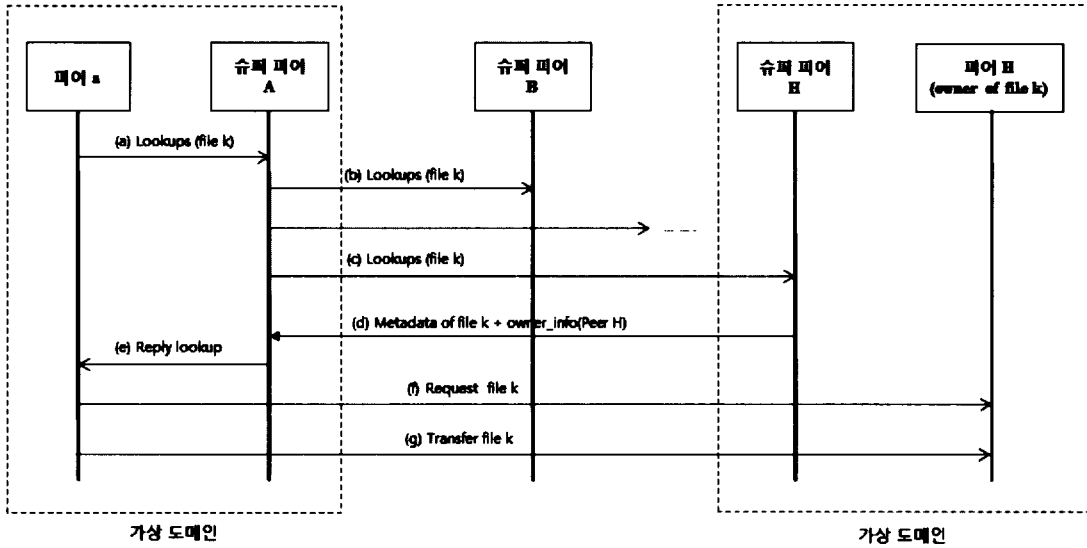
파일공유 오픈소스 프로젝트인 JXTA(Juxtapose) 프레임워크의 경우에도 PKI를 사용하지않고 공개키를 이용하는 방식을 채용하였다. 이 구조에서 각각의 피어는 공개키가 포함된 자신의 인증서를 스스로 생성한 후 Peer advertise 메시지 전송과정에서 배포한다. 비교적 간단한 방법이지만 이 방식은 공개키를 인증하는 제 3의 신뢰기관이 존재하지 않기 때문에 MITM(Man-in-the-Middle) 공격 발생시 적절히 대응할 수가 없다. 예를 들어 중간의 공격자가 피어 A가 보낸 Peer advertise 메시지를 위변조하여 피어 A의 공개키를 자신의 공개키로 대치한다고 해도 이를 감지할 수 없기 때문이다.

본 연구에서 제안하는 방안은 PKI를 사용하지 않으면서도 안전한 파일공유 응용을 구축할 수 있는 방법으로 PKI를 사용하지 않고 안전하게 자가 생성한 공개키를 분배하기 위한 기술이다. 본 제안 방법은 각 피어는 자신의 공개키/비밀키 쌍을 스스로 생성하고 분배하는 기본 구조를 가지며 MITM 공격에 대해서도 안전성을 가진다(한국전자통신연구원, 2008; S.Kang, 2002).

1. 제안 보안 구조에서의 대상 응용 기본 동작

본 연구에서 대상으로 하는 파일공유 응용은 슈퍼 피어 기반의 2계층 구조를 갖는다. 이 구조에서 각각의 피어는 유일하게 구분되는 ID를 가진다. 그리고 각각의 피어는 서비스 네트워크에 참여하기 위해 자신의 ID와 패스워드를 서버로부터 인증 받아야 한다. 이 단계에서 각각의 피어는 서버로부터 슈퍼 피어의 정보들을 수신하며, 이 정보를 기초로 슈퍼 피어를 선정하여 Join 메시지를 전송한다. Join 메시지를 성공하면 피어는 슈퍼 피어에게 자신이 보유한 파일들의 메타 정보를 전달한다. 본 논문에서는 자가 생성한 공개키/비밀키 쌍을 사용하며, 인증서버는 PKI에서 CA 서버의 기능을 가진 서버가 아닌 단지 ID와 패스워드를 인증하는 서버이다.

대상으로 하는 파일공유 응용의 기본적인 동작은 아래의 그림과 같다. 그림의 슈퍼 피어는 자신의 가상 도메인 상에 존재하는 각 피어가 소유한 파일에 대한 메타 정보를 보유한다. 자원 검색을 요청하는 피어는 자신의 슈퍼 피어에게 검색 요청을 하고, 슈퍼 피어는 다른 슈퍼 피어들에게 파일 검색 요청을 전달하여 검색을 수행하는 방식을 따른다.



[그림 3] 파일공유 보안 응용의 기본 동작

2. 신뢰적인 파일공유 응용을 위한 보안 구조

<표 2>는 보안구조 설계에 사용된 기호들이다. 슈퍼 피어는 응용에 의해 미리 선택되어 있는 것으로 가정한다. 또한 각 슈퍼 피어는 서버의 공개키와 현재 서비스 네트워크에 참여하고 있는 다른 슈퍼 피어의 공개키를 가지고 있다고 가정한다(Youngsoo Kim etl., 2009).

<표 2> 신뢰적인 파일공유 응용에 사용된 기호

기호	의미
ID_k	피어 K의 ID
IP_k	피어 K의 IP 주소
K^u_k	피어 K의 공개키
K^r_k	피어 K의 개인키
K^u_s	ID 인증서버의 공개키
K^r_S	ID 인증서버의 개인키
PW_k	피어 K의 비밀번호
$E_k(m)$	암호화 함수(메시지 m을 암호화 키 k로 암호화)
$D_k(c)$	복호화 함수(암호문 c를 복호화 키 k로 복호화)
$S_k(m)$	전자서명 (서명키 k로 메시지 m)

본 논문에서 제안된 프레임워크에서 각 피어는 공개키를 생성하여 인증서버에 등록을 한다. 본 절에 나오는 수식 중 P_a, P_b는 각각 ID가 a, b인 피어를 의미하며, SP_A, SP_B는 ID가 A, B인 슈퍼 피어를 의미한다. S는 ID 인증 서버를 의미한다. 각각의 단계에 대한 자세한 설명을 다음과 같다.

• **단계 1: ID, 패스워드 인증 및 공개키 등록**

① ID, 패스워드 인증

② (피어 a → 서버) a의 공개키 등록

$E_{K^u_s}$ ("Publish key registration" | ID_a | IP_a | PW_a | K^u_a) | S_{PWa} (m)

③ (서버) 피어의 ID 검증

- 서버의 개인키로 복호화
- 메시지에 저장된 패스워드의 피어가 등록한 패스워드와 비교를 통한 검증
- 피어의 패스워드를 통한 서명 검증

④ (서버 → 피어 a) 공개키 등록의 성공/실패 여부 반환

$E_{K^u_a}$ ("*Publish key registration Success*" | ID_a | "*SP_Info*" |
{IP_A | ID_A | K^u_A} | {IP_B | ID_B | K^u_B} | ...) | S_{Krs} (m)

- 슈퍼피어의 목록과 IP, ID, 공개키 정보도 함께 전송
- 피어 a의 공갯니로 암호화하여 전송

⑤ (피어 a) 인증서버의 ID 검증

- 자신의 개인키로 복호화
- 서버의 공개키로 서명 검증

단계 1까지는 피어를 패스워드 기반으로 인증하게 되며, 단계 1에서 피어의 공개키를 서버에 등록한 이후로 피어의 공개키가 사용가능한 상태가 된다.

• **단계 2: Join 요청**

① (피어 a → 슈퍼피어 A) Join 요청

$E_{K^u_A}$ ("*Join Request*" | ID_a | IP_a | K^u_a) | $S_{K^r_a}$ (m)

- Join 요청 시 자신의 공개키도 함께 전송
- 슈퍼 피어의 공개키로 암호화하고 자신의 개인키로 서명하여 전송

• **단계 3: 피어 a의 공개키 요청과 응답**

① (슈퍼피어 A → 서버) 피어 a의 공개키 요청

$E_{K^u_S}$ ("*Request publish key*" | ID_a | IP_a) | $S_{K^r_A}$ (m)

② (서버) 슈퍼피어 A의 ID 검증

- 서버의 개인키로 복호화
- 슈퍼피어 A의 공개키로 서명 검증

③ (서버 → 슈퍼피어 A) 피어 a의 공개키 반환

$E_{K^u_A}$ ("*Reply publish key*" | {ID_a | IP_a | K^u_a}) | $S_{K^r_S}$ (m)

④ (슈퍼피어 A) 서버의 아이디 검증

- 자신의 개인키로 복호화
- 서버의 공개키로 서명 검증

⑤ (슈퍼피어 A) 단계 2에서 수신한 메시지에 포함된 피어 a의 서명 검증

• **단계 4: Join 성공 및 실패**

① Join 성공/실패 여부 회신

$E_K^u{}_a$ ("*Join sucess*") | $S_K^r{}_A$ (m)

② (피어 a) 슈퍼피어 A의 ID 검증

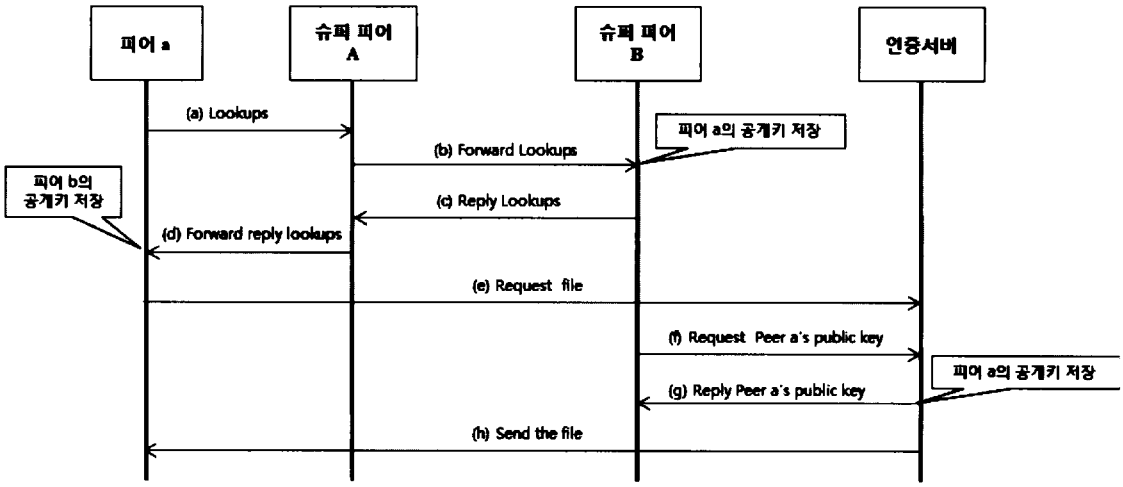
- 자신의 개인키로 복호화
- 슈퍼피어 A의 공개키로 서명 검증

• **단계 5: 피어 a의 파일공유의 메타데이터 전송**

위의 5 단계 내용은 서비스 네트워크의 Join 단계이다. 이를 기반한 안전한 파일공유 보안의 응용 과정의 동작을 살펴보면 다음과 같다.

본 메커니즘은 각 피어의 공개키를 저장하고 제공하는 등의 관리 기능이 각 슈퍼 피어에 분산되어 있는 구조로 서버의 부하를 줄여준다. 또한 각 피어가 파일을 검색하고 결과를 반환하기 위한 메시지 전달과정에서 자연스럽고 안전하게 공개키가 분배되는 구조를 갖는다. 만약 슈퍼피어의 오류가 발생한 경우에 각 피어는 자신의 ID 인증 서버로의 인증과정에서 수신한 슈퍼 피어의 목록 중 다른 슈퍼피어를 하나 선정하여 Join 메시지를 보내어 새로운 가상 도메인에 가입을 처리하도록 한다.

위의 그림은 신뢰적인 파일공유 응용에서 네트워크 Join 이후의 단계에서 파일 검색 과정을 보여준다. 각 단계에서 전송되는 메시지 형식은 다음 <표 3>과 같다.



[그림 4] 신뢰적인 파일공유 보안 응용 동작 과정

<표 3> 주요 메시지 형식

	메시지 형식
a	$E_{K^u_A}$ ("*looup_req*" | {"*beyonce*"}) | $S_{K^r_u}$ (m)
b	$E_{K^u_B}$ ("*looupfile*" | {"*beyonce*"}) | "*requester*" | {ID_a | IP_a | K^u_a}) | $S_{K^r_A}$ (m)
c	$E_{K^u_A}$ ("*replylooup*" | {"*beyonce*"}) | *fileid* | "*owner*" | {ID_b | IP_b | K^u_b}) | $S_{K^r_B}$ (m)
d	$E_{K^u_a}$ ("*replylooup*" | {"*beyonce*"}) | "*owner*" | *fileid* | {ID_b | IP_b | K^u_b}) | $S_{K^r_A}$ (m)
e	$E_{K^u_b}$ ("*requestfile*" | *fileid* | $S_{K^r_a}$ (m)
f	$E_{K^u_B}$ ("*request_pkey*" | *fileid* | ID_a | $S_{K^r_b}$ (m)
g	$E_{K^u_b}$ ("*reply_pkey*" | {ID_a | K^u_a}) | $S_{K^r_B}$ (m)

V. 결 론

어린이를 포함한 청소년들은 온라인상에서 포르노그래피, 폭력물, 불건전 정보 노출 등 다양한 위협에 노출되어 있다. 온라인상의 어린이 보호를 위해서는 기술적 보안 수단뿐만 아니라 이를 막기 위한 법, 제도의 개선과 참여자(서비스 제공자, 부모, 정보, 어린이 등)의 인식 제고가 요구된다. 본 논문에서는 네트워크 서비스 환경에서 청소년들의 유해정보 차단 방안에 대해 제안하였다. 제안하는 기법은 콘텐츠 내용에 따른 등급을 이용한 유해방지 기법의 장점을 모두 계승하고 새로운 융합 서비스 환경에서 유해 정보를 차단할 수 있는 서비스 구성과 유해정보 인증 서비스 기반 기능도를 제시함으로써 유해정보 차단을 위한 실질적인 해결 방안에 참고가 될 것으로 사료된다.

참고문헌

김영수·박남제·홍도원·원동호(2009). 모바일 RFID 서비스 환경에서의 성인인증 시스템. **한국콘텐츠학회논문지**, 9(1).

김지연(2003). **인터넷 내용등급시스템에 관한 비교분석.** 숭실대학교 정보과학대학원.

조동욱(2004). 음란콘텐츠에 기반한 유해 음락 사이트의 차단. **한국통신학회논문지**, 29(6B), 531-583.

조동욱·김지영(2004). 음란 유해사이트 차단을 위한 음향 신호처리 및 분석, **한국콘텐츠학회논문지**, 4(2), 1-89.

한국전자통신연구원(2008). **유무선 IPv6 기반 P2P 네트워크 정보보호 기술개발.** 한국전자통신연구원.

황승흠·황성기·김지연·최승훈(2003). **국내외 인터넷 내용등급시스템의 비교분석과 발전방안 연구.** 정보통신윤리위원회/성신여자대학교.

C. Burges(1998). A Tutorial on Support Vector Machines for Pattern Recognition. *Data Mining and Knowledge Discovery*, 2, 121-167.

F. Sebastiani(2002). Machine Learning in Automated Text Categorization. *ACM Computing Surveys*. 43(1), 1-47.

G. Siolas, F. d'Alche-Buc(2000). Support Vector Machines based on a Semantic Kernel for Text Categorization. *Proceeding of IJCNN 2000*, 5(1), 205-209.

Namje Park, Youngsoo Kim(2010). Harmful Adult Multimedia Contents Filtering Method in Mobile RFID Service Environment. *Lecture Notes in Artificial Intelligence*, Vol. 6422.

S.Kang(2002). *Korean Morphological Analysis and Information Retrieval*, Hongreung Science Press.

Support Vector Machine, Wikipedia(2005). the free Encyclopedia, http://en.wikipedia.org/wiki/SVM

Thesaurus, Wikipedia(2008). The Free Encyclopedia. http://en.wikipedia.org/wiki/Thesaurus.

W. Frakes, R. Baeza-Yates(1992). *Information Retrieval: Data Structures and Algorithms*, Prentice Hall, 1992.

Youngsoo Kim, Namje Park, Dowon Hong, Dongho Won(2009). Context-based classification for harmful web documents and comparison of feature selecting algorithms. *Journal of Korea Multimedia Society*. 12(6).

Y. Yang, J. Pederson(1997). A Comparative Study on Feature Selection in text Categorization. *Proceedings of the 14th International Conference on Machine Learning*. 412-420.

<Abstract>

A Study on Access Control of Illegal and Objectionable Contents for Child Online Protection

Park, Nam-Je

(Jeju National University)

This paper is about access control of illegal and objectionable contents for child online protection coming through the combination of smart phone device, as the core technology of ubiquitous environments. To overcome the shortcoming of simple access control of illegal and objectionable contents on current internet, we suggest a framework for content-based classification and propose an access control of illegal and objectionable contents's framework architecture using it. At first, we explain conventional methods for illegal and objectionable contents, and show a criteria of content-based classification for preventing an exposure of illegal and objectionable contents from minors. Additionally, we describe data structure and service for the proposed access control of illegal and objectionable contents, and finish it with concluding remarks.

<Key words> illegal and objectionable contents, content-based classification, Access Control, illegal and objectionable contents's protection