韓國IT서비스學會誌
第12卷 第2號
2013年 6月, pp.103-118
http://dx.doi.org/10.9716/KITS.2013.12.2.103

안드로이드에서 로컬 프록시를 이용한 유해 컨텐츠 차단에 관한 연구*

김인재** · 양민수***

A Study for Blocking Harmful Contents through a Local Proxy on Android*

Injai Kim** · Min-Su Yang***

■ Abstract ■

Harmful contents on a mobile platform are becoming serious problems to young people due to the prevalence of smart phones with the fast development of mobile technology. Mobile applications and contents are so much optimized on the mobile environment that young men are exposed to many harmful contents.

A system for blocking harmful contents is suggested in this study. The system includes a local proxy function, filtering module, and local database in order to increase the blocking efficiency. The local proxy function and the filtering module are implemented on an Android platform, and the local database are running on a PC-based server. The suggested system perfectly blocks harmful contents, and shows relatively high speed.

Keyword : Android, Local Proxy, Harmful Contents, Blocking Methods

논문투고일 : 2013년 01월 25일 논문수정완료일 : 2013년 04월 05일 논문게재확정일 : 2013년 04월 10일
* 본 연구는 2013학년도 동국대학교 논문게재장려금 지원으로 이루어졌음.
** 동국대학교 경영대학 경영학부
*** (주)펜타시큐리티

1. 서 론

IT 기술이 급속도로 발전하고 인터넷이 널리 보급되면서 우리의 삶은 더욱 편리하고 윤택해 졌다. 정부기관, 기업, 교육기관 등 모든 것이 인터넷을 통해서 연결되고, 인터넷이 널리 보급되면서 오프라인 생활이 점점 온라인화 되었다. 게임, 행정업무, 쇼핑, 은행업무 등 생활의 대부분이 온라인으로 가능할 정도로 삶이 편리해진 것이다. 하지만 온라인에도 이러한 편리함만 있는 것은 아니다. 오프라인에 퇴폐업소가 사회적 문제이듯이 온라인에도 수많은 유해 사이트 및 유해 컨텐츠가 사회적으로 큰 문제를 일으키고 있다. 특히 유해 컨텐츠가 모바일 디바이스 환경에서 개인 정보유출을 목적으로 하는 악성 바이러스 설치 도구로 활용되고 있다는 점에서 매우 우려할 만한 점이며 개인정보 보호에도 큰 악영향을 주고 있다.

현재 유해사이트는 전 세계적으로 563만 개 정도가 될 정도로 많으며 그 중에서 음란 사이트는 95.5%나 된다. 또한 음란, 폭력, 피싱 등의 유해 사이트가 하루 평균 1600개씩이나 생겨나고 있다[1]. 이렇게 생겨나는 수많은 음란 사이트는 사회적으로 큰 문제를 일으킨다. 수많은 아동 성폭행 범죄에서 이를 입증해 주고 있다. 아동 성폭행 범인의 대부분이 인터넷을 통해서 다운로드 받은 음란물과 연관되어 있다[4, 6]. 이러한 음란물은 성인사이트 뿐만 아니라 P2P 사이트를 통해서도 유포되고 있는데 P2P 사이트는 방송통신위원회에 따르면 110여 개가 등록되어 있으며 등록되지 않은 사이트까지 포함하면 250여 개에 달한다고 밝혔다. 또한, 평균적으로 개당 2분에 한 개씩 한 시간에 30여 개의 음란물이 업로드 된다고 밝혔다. 전체 사이트에 한 시간에 총 7500여 개의 음란물이 업로드 되고 있는 것이다[2]. 사실상 거의 통제가 불가능한 수준에 다다를 정도로 음란물이 무분별하게 유통되고 있다.

국내 스마트 폰의 보급률은 2011년 하반기 스마트 폰 보급률 53%에 이를 정도로 많이 보급되어 있다[3]. 이렇게 스마트 폰의 보급률이 매년 늘어나면서 스마트 폰의 기술 또한 빠르게 발전하고 있다. 모바일 게임, 모바일 뱅킹, 모바일 쇼핑, 모바일 업무 등 애플리케이션이 날로 발전하고 있는 것이다. 스마트 폰이 빠르게 발전하면서 일반적인 애플리케이션뿐만 아니라 음란물과 같은 유해 컨텐츠가 자연스럽게 스마트 폰을 통해서 유포되기 시작했고, 스마트 폰에서의 유해 컨텐츠 문제가 사회적으로 더 큰 이슈가 되게 되었다. 스마트 폰의 유해 컨텐츠에 관한 문제가 사회적으로 이슈가 되고 있는 이유는 바로 청소년들 때문이다. 스마트 폰을 가지고 있지 않은 청소년들을 찾기 힘들 정도로 대부분의 청소년들이 스마트 폰을 사용하고 있고, 시간과 장소를 가리지 않고 게임, 채팅, 전화 등을 이용하고 있다. 이렇게 청소년들이 스마트 폰을 점점 많이 사용하게 되면서 청소년들이 스마트 폰을 통해서 유해 컨텐츠에 점점 노출되기 시작했다. 많은 유해 사이트들이 PC 웹 사이트 뿐만 아니라 모바일 웹 사이트로 음란 사이트를 제작하여 배포하고, 전용 애플리케이션을 만들어 배포하는 등 너무나 쉽게 이러한 정보가 노출되어 있다.

PC 환경에서는 유해 컨텐츠를 차단하는 프로그램 및 시스템은 많이 출시되어 있다. 하지만, 스마트 폰 환경에서는 유해 컨텐츠를 차단하는 시스템이 많이 부족한 것이 현실이다. 앞으로 스마트 폰의 보급률은 점점 늘어나며, 스마트 폰은 우리의 삶에 중요한 부분을 차지할 것이다. 그렇기 때문에 본 논문에서는 보다 안전하고 건전한 스마트 폰 이용을 위한 스마트 폰에서의 유해 컨텐츠 차단에 대한 기술을 제시하고자 한다.

2. 이론적 배경

2.1 유해정보 현황

2.1.1 음란 사이트 현황

경찰청의 “자살 · 도박 · 음란 사이트 적발 현황” 자료에 따르면 2009년도부터 올해 8월까지 총 72,133곳의 불법 사이트가 적발되었으며, 이 중에

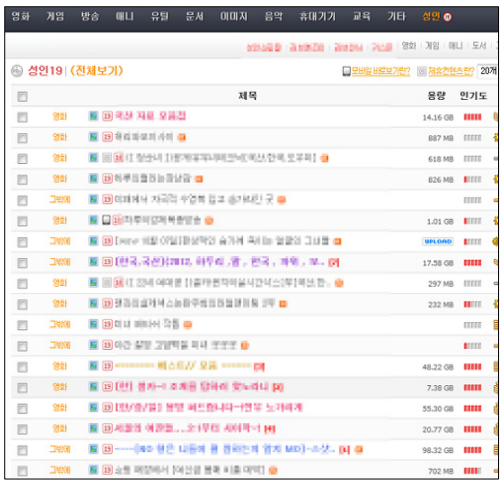
서 음란 사이트가 30,912건으로 큰 비중을 차지하고 있다. 2009년에 5909건에서 2011년도 10,352건으로 2배가 증가 했으며, 2012년도에 다시 30,912건으로 다시 2배 가까이 증가했다[4].

유해정보 차단 서비스 전문 업체 “플랜티넷”은 2007년부터 2012년 6월 말까지 집계된 세계 유해 사이트는 총 563만 개라고 분석했다. 2007년의 240만 건에서 133%인 321만개가 증가 했고, 2012년 1월부터 6월까지는 약 30만 건이 증가했다. 유해 사이트 언어별로는 영어가 55%로 가장 많이 증가했고, 중국어가 23.3%, 독일어가 7%, 한국이 5.4%로 4위를 차지하고 있다. 8.5%가 음란 사이트였고 1.3%가 도박 사이트, 폭력과 엽기 사이트가 0.03%로 나타났다. 음란 사이트는 2007년부터 전체 유해사이트의 98%이상을 차지하고 있으며, 도박, 폭력사이트도 점차 증가하고 있다[1].

2.1.2 음란물 유통 현황

음란물은 음란 사이트, 카페나 블로그, 동영상 사이트, 웹 하드나 P2P 같은 파일 공유 사이트에서 대부분 유통되며, 일부 정상적인 사이트의 성인게시판을 통해서 일부분 유통되고 있다. 여성가족부에서 발표한 2012년 6월부터 8월까지의 인터넷상의 음란게시물 유통 경로 분석 결과 6월에는 857건, 7월에는 1,152건, 8월에는 1,648건으로 매월 신고 건수가 증가하고 있다[5]. 3개월 동안의 음란 사이트 신고 건수는 총 683건이며, 온라인 카페는 1,620건이다. 은라인 블로그는 581건, 불법게시물 773건이 신고 되었다. 음란 사이트, 온라인 카페, 온라인 블로그, 불법게시물 모두 매일 신고 건수가 증가 하였으며, 3개월 동안 총 3,657건의 음란 게시물이 신고가 될 정도로 음란물 유통이 심각한 상황이다.

인터넷 속도가 빠르게 발전하면서 웹 하드 및 P2P와 같은 파일 공유 서비스가 급증하였다. 파일 공유 서비스가 급증하면서 더불어 음란물 유통이 점점 심각해졌다. 웹 하드 및 P2P 사이트는 현재 114개가 등록되어 있으며 등록되지 않은 사이트까지 포함하면 250여개가 넘는다. 음란물로 인한 사회적 심각성이 증가하자 정부는 청소년 음란물 차단 대책을 확정하고 인터넷 뿐만 아니라 TV에서까지 성인인증을 강화하고, 음란물 차단 기술을 갖추도록 의무화하고 있다. 이러한 음란물 차단수단을 적극적으로 적용하여 음란물 필터링, 음란물 업로드에 대한 제재 등을 모범적으로 시행하고 있는 업체도 있지만 그렇기 않은 업체도 많다. 음란물 필터링 기술을 갖추었다 하더라도 쉽게 우회가 가능하기 때문에 사실상 도입의 의미가 없다고도 불 수 있다.



[그림 1] 웹 하드에 업로드 된 음란물

인터넷의 속도 빠르게 증가하면서 음란물의 유통 또한 심각해졌다. 노골적인 음란물이 1분에 적게는 30개에서 많게는 60~70개, 하루에 수백 개, 수천 개의 음란물이 업로드 되고 있다([그림 1] 참조). 2006년 혼자서 웹 하드를 통해 약 1만 4,000여 편의 음란 동영상을 퍼트린 사건이나, 지난해 7월부터 8월까지 파일 공유 사이트를 통해 약 4,000여 편의 음란물을 유통시킨 사건은 음란물 유통 실태를 단적으로 보여준다. 이들을 ‘헤비 업 로더’라고 부르는데 업 로더 들은 자신이 웹 하드나 P2P 사이트에 올린 음란 동영상의 다운로드 횟수가 많을수록 많은 이윤을 챙길 수 있다. 헤비 업 로더의 경우

는 한 달 수익이 수천 만 원에 달하는 것으로 알려졌다. 웹 하드의 이윤 창출 구조가 사용자는 증가시켜서 웹 하드 업체는 수익은 증가시켰지만 반대로 음란물의 유통을 더욱 부추인 결과가 되었다.

웹 하드의 음란물 유통의 심각성은 아동 음란물 유포로 인해서 더욱 심각해지고 있다. 2010년 경찰청이 6개의 파일공유 사이트의 아동 음란물을 전수 조사한 결과, 국내에서 만들어 진 것은 383건, 해외에서 만들어 진 것은 274건이었으며, 이중에서 약 58%가 한국에서 생산되고 있는 것으로 파악됐다. 아동음란물의 유포는 청소년뿐만 아니라 성인의 성의식까지 심각한 영향을 주며, 아동 성폭행 범죄로까지 이어져 사회적 심각성이 더해지고 있다.

대부분의 사이트에서 성인인증을 거쳐야 접근이나 다운로드가 가능하도록 서비스를 제공하고 있지만, 주민등록번호만으로 인증을 사용하기 때문에 주민등록번호만 도용하면 얼마든지 음란물에 접근할 수 있는 문제점이 있다. 뿐만 아니라 웹 하드 업체가 음식점, 카페, PC방, 택배 등을 통해서 무료로 배포하는 무료 다운로드 쿠폰을 인하여 청소년들이 별도의 결재가 없이도 음란물을 다운로드할 수 있게 되었다.

2.1.3 모바일의 음란물 유통

국내 스마트폰 사용자가 2천만을 넘을 정도로 스마트폰 이용자가 있어 이른바 “모바일 시대”라고 해도 과언이 아니다. 스마트폰은 언제 어디서나 필요한 정보를 얻을 수 있어 매우 편리하다. 지도를 보거나 게임을 하고, 교통정보를 확인하거나 인터넷 검색도 마음대로 즐길 수 있다. 하지만 이렇게 편리한 스마트폰에도 음란물에 대한 부작용이 심각하게 발생하고 있다. 스마트폰은 사적이고 개인적인 공간이기 때문에 주위 사람들 모르게 은밀하게 사용이 가능하기 때문이다. 또한 스마트폰은 인터넷이 자유롭고 다른 사람들과의 소통이 편리하기 때문에 PC 환경보다 빠르게 음란물이 유통될 수 있다.

스마트폰에서는 음란물이 웹 사이트, 메신저, 웹 하드, 음란 앱 등을 통해서 유통되고 있다. 스마트폰의 사용이 점점 늘어나고 보편화 되면서 PC 환경의 대부분의 기능이 스마트폰으로 넘어오고 있기 때문이다. 웹 사이트, 메신저, 웹 하드와 같은 PC에서 자주 이용하던 서비스가 모두 스마트폰용으로 만들어지고 있으며, 많은 사람들이 이용하고 있다. 따라서 이러한 서비스 등을 통해서 음란물이 유통될 수 있다.

스마트폰을 통한 웹 사이트 이용률이 점점 늘어나면서 많은 웹 사이트에서 모바일용 웹 사이트를 별도로 제공하고 있다. 모바일 웹 사이트가 증가하면서 모바일 음란 사이트 역시 늘어나게 되었다. 음란 사이트들은 모바일 환경에 최적화된 사진, 동영상을 제공하여 접속자를 늘리고 있다. 이러한 모바일용 음란 사이트들은 인터넷 검색만으로 얼마든지 쉽게 찾을 수 있기 때문에 청소년들에게 쉽게 노출될 수 있다.

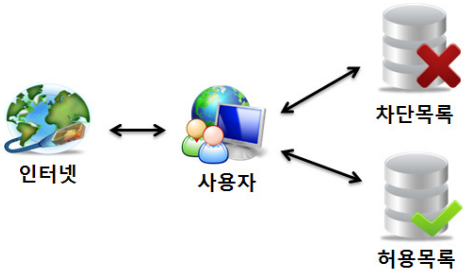
스마트폰을 이용하는 많은 사람들이 “카카오톡”과 같은 모바일 메신저를 사용한다. 모바일 메신저는 언제 어디서든지 실시간으로 커뮤니케이션이 가능한 장점이 있다. 하지만 이런 모바일 메신저들이 음란물 유통으로 사용되고 있다. 행정안전부의 “청소년 성인물 이용실태 조사”에 따르면 “48.8%”의 청소년들이 모바일 메신저를 이용한 스마트폰으로 사람들과 음란물을 공유하거나 전달해봤다고 조사되었다. 또한 남자는 파일공유 사이트를, 여자는 스마트폰을 통해서 음란물을 공유하며, 초등학생들은 직접만나서 전달하는 경우가 “77.1%”, 고등학생은 스마트폰을 통해서 전달하는 경우가 “52.3%”로 조사되었다[6].

2.2 유해정보 차단 방법

2.2.1 목록기반 차단 방법

[그림 2]의 목록기반 차단 방법은 유해목록을 이용하여 유해 정보를 차단 또는 허용하는 방법으로, 차단목록 기반 차단 방법과 허용목록 기반 차단 방

법으로 나누어진다. 차단목록 기반 차단 방법은 차단하고자 하는 유해정보만 선별적으로 차단하는 방식으로 유해 사이트에 접속하거나 동영상, 사진 같은 유해 정보 파일들을 실행했을 때 차단목록과 일치하는 정보가 있으면 사이트에 접속이나 유해 정보 파일들의 실행을 차단하는 방식이다.



[그림 2] 목록기반 차단 방법

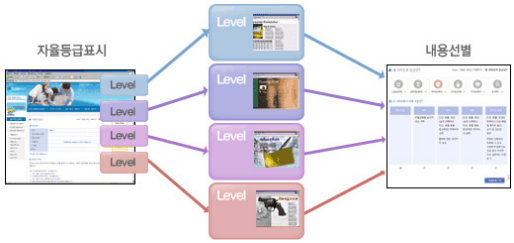
허용목록 기반 차단 방법은 기본적으로 모든 정보를 차단하고 허용하고자 하는 유해 정보만 허용하는 방식이다. 이 방법은 허용하고자 하는 유해 사이트나 유해 정보 파일들만 허용하는 방법이기 때문에 기본적으로는 모든 정보를 차단해야 하고, 유해 사이트에 접속하거나 유해 정보 파일들을 실행했을 때 허용목록과 일치하는 정보가 있으면 허용하고 아니면 차단하는 방법이다.

2.2.2 등급기반 차단 방법

등급기반 차단 방법은 인터넷 내용등급 서비스를 이용해서 차단하는 방법으로, 각각의 웹 사이트들에 등급을 부여하여 사용자가 해당 웹 사이트에 접속했을 때 해당 등급을 보고 판단하여 웹 사이트의 이용을 결정할 수 있도록 한다.

우리나라에서는 현재 좀 더 건전하고 믿을 수 있는 인터넷 문화를 만들기 위해서 방송통신위원회에서 “인터넷 내용등급 서비스”를 제공하고 있다([그림 3] 참조). “인터넷 내용등급 서비스”는 정보제공자가 자신의 웹 사이트에 자율적으로 등급을 표시하고, 정보이용자가 적정한 등급 이용수준을 정하여 원하지 않는 정보를 선택적으로 거를 수 있도록 하는 서비스 이다[7].

등급기반 차단 방법을 위해서는 인터넷 내용분류 표준은 PICS(Platform for Internet Content Selection)을 사용해야 한다. PICS는 인터넷의 내용을 선별적으로 분류할 수 있도록 도와주는 기술적 표준으로 1995년 W3C(Word Wide Web Consortium)에 의해서 개발되었다.



자료 : www.safenet.ne.kr.

[그림 6] 인터넷 내용등급 서비스

정보제공자는 HTML 코드 상에 컨텐츠의 등급 표시를 삽입하면 웹 브라우저는 이 등급을 통해서 컨텐츠를 선별적으로 차단할 수 있으며, 차단된 정보에 대한 등급기준은 사용자가 선택할 수 있도록 하고 있다. 이러한 노력의 하나로 방송통신위원회에서 인터넷 내용등급 서비스인 “SafeNet”을 제공하고 있다. “SafeNet”은 5개 범주에 5등급의 분류 기준을 사용하고 있는데, “노출”, “성행위”, “폭력”, “언어”, “기타” 등 5가지 범주에 대해서 0부터 4까지 총 5단계의 등급을 설정할 수 있다. 등급기반 필터링은 유해정보에 대해서 등급을 제시함으로써 효과적으로 유해정보를 차단할 수 있고, 사용자가 스스로 판단하여 차단할 수 있도록 한다.

2.2.3 도메인기반 차단 방법

도메인기반 차단 방법은 “레드 존(Red-Zone)”, “그린 존(Green-Zone)”과 같이 인터넷 주소 체계를 청소년들에게 유해한 영영역과 그렇지 않은 영역으로 구분하여 인터넷의 수많은 유해정보로부터 청소년을 보호하는 것이다. 레드 존은 음란, 폭력 등과 같은 청소년에게 유해한 사이트이고, 그린 존

은 청소년에게 유해하지 않은 사이트이다. 레드 존과 그린 존 관리를 위해 “국제 인터넷 주소관리기구(ICAAN : Internet Corporation for Assigned Names and Numbers)”가 포르노 사이트 전용 도메인인 “.xxx”와 어린이 전용 도메인인 “.kids”의 사용을 승인했다. 프로노 사이트 전용 도메인 “.xxx”는 성인 사업에 대한 명확한 아이덴티티를 부여하고, 청소년으로부터 유해 정보를 차단하며 웹 사이트의 접근을 높일 수 있다는 장점을 가지고 있다. “국제 인터넷 주소관리기구”에서 “.xxx”의 도메인을 승인함으로써 이 도메인은 “.com”과 같은 최상위 도메인의 가치를 가지게 됐다. 어린이 사이트 전용 도메인인 “.kids”는 어린이 및 청소년들을 폭력물이나 음란물 등의 유해 정보로부터 보호하기 위해서 사용되며, 현재 미국에서 “.us” 도메인 아래에 두어 “.kids.us”와 같은 도메인으로 상용되고 있다. 도메인을 청소년에게 유해한 “레드 존”과 청소년에게 유해하지 않은 “그린 존”으로 구분하여 차단하는 방법을 사용하면 사이트를 효과적으로 필터링할 수 있다.

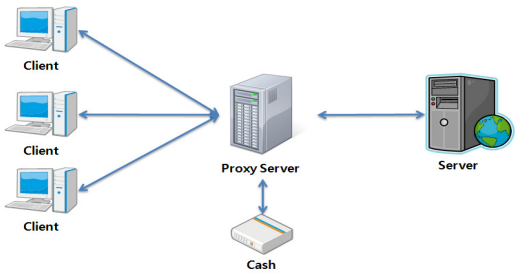
2.3 프록시 서버

2.3.1 정의와 목적

“프록시 서버”란 클라이언트와 서버 사이의 중계시스템이다. 프록시 서버는 컴퓨터의 익명성 유지, 캐시를 사용한 빠른 리소스 전달, 네트워크 서비스나 컨텐츠의 접근 정책 적용, 데이터 유출 보호 등의 여러 가지 장점이 있지만 보안 및 접근 통제를 우회하거나 바이러스 및 악성코드 전파, 정보 유출, IP 추적 방지 등의 단점도 있다([그림 4], [그림 5] 참조).

2.3.2 캐쉬 기능

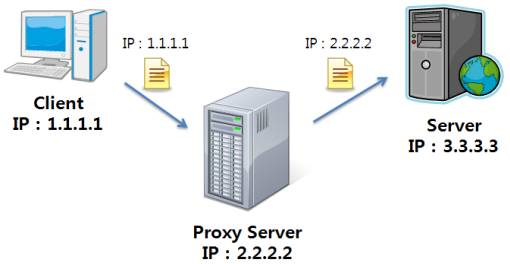
프록시 서버는 성능향상을 위한 캐쉬 서버로 사용할 수 있다. 프록시 서버를 사용하지 않는 경우 클라이언트 서버에 직접 요청해서 정보를 받게 된다. 하지만 캐쉬를 사용하는 프록시 서버가 있는 경우 클라이언트가 요청한 문서를 프록시 서버에서 캐쉬에 저장하여 같은 요청에서는 서버에 요청을 하지 않고 캐쉬의 정보를 전달하여 속도를 향상시키게 된다.



[그림 4] 프록시 서버 캐쉬 사용

2.3.3 IP 숨김 기능

프록시 서버를 사용하면 IP를 숨길 수 있다. 일반적으로 클라이언트가 서버에 접속하면 클라이언트의 IP가 기록되지만 프록시 서버를 사용하면 클라이언트의 IP가 아닌 프록시 서버의 IP가 기록된다. 클라이언트가 서버에 접속하기 위해서 프록시 서버에 문서를 요청하면 프록시 서버가 클라이언트를 대신하여 서버에 문서를 요청하기 때문에 클라이언트의 IP가 기록되지 않고 프록시 서버의 IP가 기록된다.



[그림 5] 프록시 서버의 IP 변경

2.3.4 프록시 서버 유형

프록시 서버의 유형은 클라이언트의 요청을 처리하는 방식에 따라서 Transparent, Anonymous, High Anonymous 3가지가 있다.

Transparent는 Transparent라는 이름에서 알 수 있듯 순수하게 캐쉬 서버나 사용자 요청을 대행하는 서버로만 동작한다. Anonymous 프록시 서버를 사용할 경우 사용자의 IP와 일부 정보가 숨겨진다. 보통 대형업체에서 제공하는 프록시 서버가 여기에 해당된다. High Anonymous 프록시 서버는 어떠한 사용자 정보도 전송되지 않으며, VIA와 같은 HTTP 헤더도 전송하지 않으므로 프록시를 경유했는지 어떤 IP에서 접속했는지를 알 수 없는 경우가 많다. 따라서 자신의 IP를 숨기는 경우 가장 좋은 방법은 High Anonymous 프록시를 사용하는 것이다.

2.4 안드로이드 구조

2.4.1 안드로이드 이해

안드로이드는 스마트폰, 태블릿 등과 같은 휴대용 장치를 위한 모바일 운영체제로써 운영체제, 미들웨어, 사용자 인터페이스, 표준 응용 프로그램 등을 포함한다. 안드로이드는 C/C++과 자바 언어로 구성되어 있으며, 개발자들은 자바 언어로 응용 프로그램을 작성할 수 있다. 또한 안드로이드 소프트웨어 개발 키트(SDK : Software Development Kit)를 통해 응용 프로그램을 개발하기 위해 필요한 각종 도구들과 응용 프로그램 프로그래밍 인터페이스(API)를 제공한다.

안드로이드는 리눅스 커널 기반으로 동작하고 있으며, 커널 위에 동작하는 다양한 시스템 구성요소는 C/C++ 라이브러리로 구성되어 있다. 안드로이드는 자바 가상 머신으로 동작하는데, 기존의 자바 가상 머신과는 다른 달빅 가상 머신을 사용하여 응용 프로그램과 기타 프로세스들을 실행하는 방식을 사용한다.

2.4.2 안드로이드 구조

안드로이드는 리눅스 커널 기반 위에 C/C++로 만들어진 시스템 라이브러리와 자바 기반의 달빅 가상 머신으로 구성되어 동작한다. 안드로이드는 리눅스가 아닌 리눅스 커널 기반이다. 그렇기 때문에 X윈도우와 같은 내장 윈도우 시스템을 포함하지 않는다. 즉, 표준 리눅스 유틸리티 전체를 포함하지 않고 있는 것이다. 안드로이드 내장 라이브러리는 C/C++로 구성되어 있고 임베디드 리눅스 기반 기기들을 지원하기 위해 표준 C 시스템 라이브러리를 지원하고 있다.

안드로이드에는 하드웨어 추상화 계층이 있는데 이 계층에서는 그래픽, 오디오, 카메라, 블루투스, GPS, 라디오, WiFi와 같은 하드웨어를 직접적으로 지원한다. C/C++ 라이브러리 계층에 속하며, 하드웨어 인터페이스로부터 안드로이드 플랫폼의 로직을 분리하는데 사용된다.

안드로이드는 자바 기반의 달빅 가상 머신을 사용하고 있는데 이는 안드로이드 런타임 계층에 속해 있다. 안드로이드 런타임 계층에서는 달빅 가상 머신과 코어 라이브러리로 구성되어 있는데 응용 프로그램과 많은 시스템 프로세스들이 이 계층을 통해서 실행되게 된다.

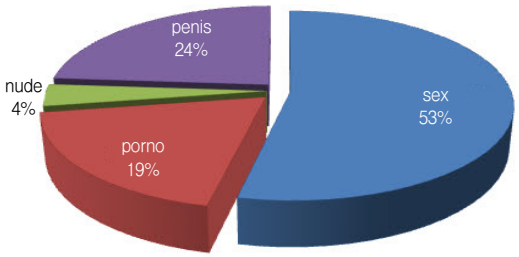
커널과 시스템 라이브러리와 같은 하위 레벨에서는 C/C++ 기반으로 되어 있지만, 사용자 레벨에서는 자바 기반으로 되어 있다. 따라서 자바 기반의 다양한 프레임워크를 지원하고 있는데 이 프레임워크는 대부분이 JNI(Java Native Interface)를 통해 Native C/C++ 코드로 작성되어 있다. 사용자에 의해서 교체될 수 있으며 재사용을 손쉽게 할 수 있도록 디자인되어 있다.

3. 안드로이드 유해 컨텐츠 차단 문제점

3.1 안드로이드 유해 애플리케이션 현황

방송통신심의위원회에서 발표한 “안드로이드 오픈마켓 내 유해 애플리케이션 2차 유통실태 조사”에 따르면 안드로이드용 유해 애플리케이션이 31.6배 증가하였다. 안드로이드 마켓에서 특정단어 “sex”, “porno”, “nude”, “penis”로 검색한 결과 총 18,101

개가 검색되었으며, “prono”는 313.6배, “penis”는 253.8배, “sex”는 20.4배, “nude”는 9.4배가 증가하였다[8]. 이러한 애플리케이션에는 성기를 노출하거나 성행위를 하는 사진이나 동영상, 노골적인 성행위에 관한 정보 등의 정보가 포함되어 있다([그림 6] 참조).



자료 : 방송통신심의위원회의 유해 애플리케이션 실태 조사.

[그림 6] 음란 · 선정성 애플리케이션 분포

안드로이드에 음란 동영상이나 음란 정보 등의 유해 애플리케이션 외에 최근에 룸싸롱, 키스방과 같은 청소년유해업소 애플리케이션의 유통이 증가하고 있다. 이러한 애플리케이션은 가격 정보, 검색 기능, 업종 분류, 사진 등의 정보가 포함되어 있어 청소년 보호에 심각한 문제점이 되고 있다([그림 7] 참조).

[그림 8] 유해업소 애플리케이션

이러한 유해 애플리케이션은 청소년 유해성 표시 또는 문구가 재대로 제공되지 않고 있어 문제가 되고 있다(<표 1> 참조). 방송통신심의위원회의 조사에 따르면 총 18,101개의 애플리케이션 중에서 14.8%인 2,673개의 애플리케이션만이 청소년 유해성 표시 또는 문구를 제공하고 있는 것으로 나타났다[7].

〈표 1〉 청소년 유해성 표시 현황

구 분	sex	porno	nude	penis	합계
애플리케이션 수	9,666	3,450	670	4,315	18,101
청소년 유해성 표시 또는 문구	1,923 (19.9%)	241 (7.0%)	486 (72.6%)	23 (0.5%)	2,673 (14.8%)

자료 : 방송통신심의위원회의 유해 애플리케이션 실태 조사.

안드로이드에는 구글에서 제공하는 정식 마켓 외에 “블랙마켓”이라고 불리는 애플리케이션 불법 유통 마켓들이 존재한다. 블랙마켓은 정식 안드로이드 마켓에서 판매되는 유료 애플리케이션을 무료로 다운로드 받아서 설치할 수 있기 때문에 많은 사람들이 사용한다. 블랙마켓들은 유료로 판매되는 애플리케이션을 무료로 제공하고 있기 때문에 저작권 침해의 문제를 일으키지만, 그것보다 악성코드나 바이러스에 더 심각한 문제점을 가지고 있다. 블랙마켓의 애플리케이션들은 안전성이 검증되지 않은 애플리케이션들이기 때문에 블랙마켓에서 다운로드 받아서 설치할 경우 악성코드나 바이러스에 감염되어 개인정보가 노출되거나 기기에 문제가 발생하는 등의 심각한 문제가 발생할 수 있다.

3.2 안드로이드 유해 사이트 차단 현황

안드로이드 유해 사이트 차단에는 크게 “자녀 스마트폰 관리”와 “Safe Browser”가 있다. 자녀 스마트폰 관리는 유해 사이트 차단, 애플리케이션 관리, 음란 동영상 차단 등과 같이 전체적으로 스마트폰을 관리하기 위한 기능으로 되어 있다. 음란, 유해 정보들을 차단하고 관리하는 것뿐만 아니라 스마트폰의 사용시간 제어, 위치전송 등 스마트폰

의 사용을 제어할 수 있는 다양한 기능들을 제공한다. 뿐만 아니라, 웹 사이트 또는 애플리케이션의 부모모드 등을 통해서 자녀들의 스마트폰을 관리할 수 있는 관리 인터페이스를 제공하고 있다.

Safe Browser란 음란, 유해 웹 사이트 차단기능을 내장하고 있는 웹 브라우저로써 바이러스/피싱 사이트, 음란 사이트, 온라인 게임 사이트 등과 같은 유해 사이트들을 차단할 수 있다. Safe Browser는 별도의 필터링 애플리케이션을 실행시킬 필요 없이 웹 브라우저 자체적으로 웹 사이트 차단 및 필터링을 제공하기 때문에 어떠한 면에서는 빠르고 편리하다고 할 수 있다. 유해 및 음란 웹 사이트를 차단하는 기능도 있지만 차단할 사이트를 별도로 추가할 수 있기 때문에 필요에 따라서 개인적인 목적으로도 사용할 수 있다. 음란 사이트/음란 컨텐츠, 무기/마약 등의 유해 사이트를 차단하며, 악성코드/바이러스/스팸 등의 보안 문제도 지원한다. 또한, 온라인 게임 사이트, 프록시 서버, 스팸 웹 서버, P2P 및 웹 스토리지, 소셜 네트워크 등 다양한 종류의 차단도 가능하다.

3.3 안드로이드 유해 컨텐츠 차단 문제점

안드로이드의 유해정보 차단은 웹 사이트 차단, 애플리케이션 차단, 동영상, 스팸 문자 또는 전화 등의 차단이 있다. 유해정보를 차단하기 위한 많은 애플리케이션들이 있는데 대부분은 안드로이드에 설치되는 유해 애플리케이션의 설치를 차단하거나 검사하는 기능을 가지고 있다. 악성 애플리케이션을 검사하거나 설치를 차단하는 애플리케이션과 기술은 이미 많이 알려져 있다. 대부분의 유해 차단 애플리케이션은 안드로이드에 설치되는 유해 애플리케이션만 관리할 뿐 웹 사이트의 유해 컨텐츠까지는 차단하지 않는다. 자녀 스마트폰 관리 애플리케이션들이나 웹 브라우저에 음란 및 유해 웹 사이트 차단 기능이 추가된 Safe Browser에서 일부 기능을 제공하고 있지만 자녀 스마트폰 관리 애플리케이션이나 Safe Browser, 그리고 기타 일부 유해 차단 애플리케이션에서 지원하고 있는 웹 사이트 차단 기능은 웹 사이트의 주소를 웹 브라우저에 입력하면 차단목록(Black List) 기반으로 웹 사이트의 접속 자체를 차단하는 기능이다. 이러한 기능은 웹 사이트의 접속은 차단할 수 있지만 정상적인 사이트에 포함된 음란, 유해 컨텐츠는 차단이 어렵다. “sex.com”과 같이 음란 사이트에 접속을 하면 쉽게 차단이 가능하지만 정상적인 사이트의 게시판에 음란물 링크는 차단 차단되지 않는다.

기존의 웹 페이지 접속뿐만 아니라 웹 페이지의 유해 컨텐츠까지 차단하기 위해서는 안드로이드로 유입되는 네트워크 패킷을 수정하거나 웹 브라우저의 HTML 소스 코드를 수정해야 한다. 네트워크 패킷을 수정하기 위해서는 운영체제에서 이러한 기능을 제공해야 하는데, 일반 데크스 탑 환경에서는 이러한 기능이 가능하기 때문에 차단이 가능하지만 안드로이드에서는 네트워크 패킷을 수정할 수 있는 기능을 제공하지 않기 때문에 네트워크 패킷을 수정할 수 없다. 또한, 안드로이드에서는 웹 브라우저에 대한 정보를 가져오거나 수정할 수 있는 기능도 제한되어 있다.

따라서 본 연구는 위 문제점들을 해결하고 웹 사이트 뿐만 아니라 웹 사이트 내의 유해 컨텐츠를 효과적으로 차단하고자 한다. 본 연구는 안드로이드 내에 로컬 프록시 서버를 구현함으로써 네트워크 패킷을 통한 웹 사이트 접속 차단뿐만 아니라 웹 페이지의 유해 컨텐츠까지 차단하는 시스템을 제안하고자 한다.

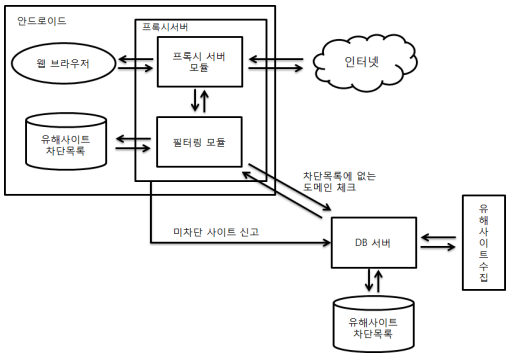
4. 로컬 프록시를 이용한 유해 컨텐츠 차단 시스템

4.1 유해 컨텐츠 차단 시스템 설계

4.1.1 유해 컨텐츠 차단 시스템 구성

제안된 유해 컨텐츠 차단 시스템은 프록시 서버 모듈, 필터링 모듈, DB 서버 등 3가지로 구성된다

([그림 8] 참조). 프록시 서버 모듈은 본 시스템에서 가장 중요한 부분으로 로컬 프록시를 동작하는 기능을 담당하고, 필터링 모듈은 음란 사이트와 유해 컨텐츠들을 차단하는 역할을 한다. DB 서버는 필터링 모듈에서 확인되지 않은 사이트에 대한 추가적인 차단 여부를 확인하기 위해서 사용된다. 사용자가 웹 브라우저로 웹 사이트 접속을 시도하면 접속할 사이트에 대한 패킷이 프록시 서버 모듈에 전달된다. 프록시 서버 모듈은 패킷을 필터링 모듈에 전달하여 사이트를 차단할지 여부를 판단한다. 정상 사이트라 하더라도 웹 사이트의 응답 패킷을 필터링 모듈을 통해서 다시 분석하여 유해 컨텐츠가 포함되었는지 확인한다.

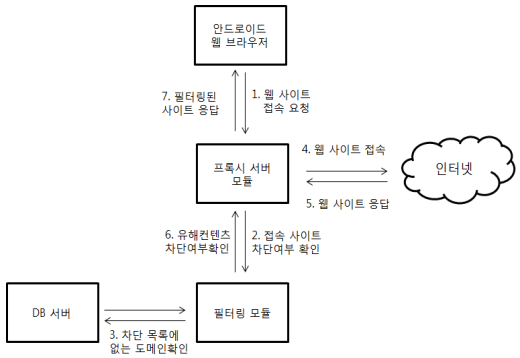


[그림 8] 유해 컨텐츠 차단 시스템 구성

본 연구에서 제시하는 프록시 서버 모듈 장점은 안드로이드 플랫폼에 장착되어 차단속도를 높이고 추가적인 차단을 위해서는 필터링 모듈과 협업하도록 설계되었다. 기존의 레거시 시스템과는 달리 스마트폰 환경에서는 제한된 컴퓨팅 자원을 효율적으로 활용할 수 있도록 시스템이 구성되어야 하기 때문이다. 본 연구의 제안 시스템은 유해 컨텐츠 차단 효과를 극대화하는 안드로이드 환경에서 새로이 시도되는 유해 컨텐츠 차단 프로그램이다.

4.1.2 유해 컨텐츠 차단 절차

[그림 9]는 본 논문에서 제안하는 유해 컨텐츠 차단 시스템의 유해 사이트 및 유해 컨텐츠 차단



[그림 9] 유해 컨텐츠 차단 절차

처리 절차이다. 안드로이드 기반 로컬 프록시 서버를 이용하여 웹 브라우저의 음란 사이트 및 유해 컨텐츠를 차단하는 방식으로 그 절차를 자세히 서술하면 다음과 같다.

① 사용자가 안드로이드 웹 브라우저를 통해서 웹 사이트의 접속을 시도하면 웹 사이트 접속 요청이 프록시 서버 모듈에 보낸다.

② 웹 사이트 접속 요청을 받은 프록시 서버 모듈은 필터링 모듈을 통해서 접속 요청을 받은 웹 사이트의 접속을 차단할지 확인한다.

③ 접속하려는 웹 사이트의 정보가 스마트폰의 차단 목록에 없다면 DB 서버에 해당 정보를 보내어 차단할지 여부를 확인한다.

④ 정상적인 사이트일 경우 접속 대상 웹 서버에 접속 요청을 보내고 음란 사이트로 판단될 경우 사용자에게 차단 메시지를 보낸다.

⑤ 정상적인 사이트로 판단되어 접속 대상 웹 서버에 접속 요청을 보내면 요청을 받은 웹 서버에서는 응답 메시지를 프록시 서버로 보내게 된다.

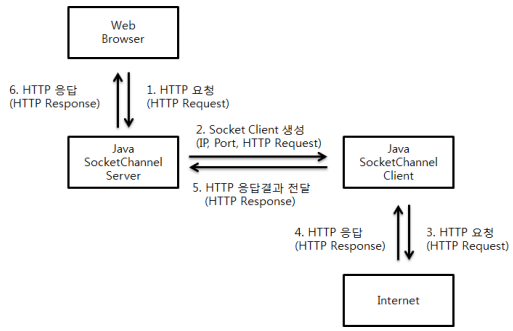
⑥ 웹 서버에서 응답 메시지를 받은 프록시 서버는 응답 메시지에 포함된 음란 정보를 차단하기 위해서 응답 메시지를 필터링 모듈로 전달한다.

⑦ 마지막으로 정상 응답 메시지 또는 음란 정보가 필터링된 응답 메시지를 웹 브라우저에 다시 전달하면 웹 사이트 접속 요청 처리가 마무리된다.

4.2 유해 컨텐츠 차단 시스템 구현

4.2.1 안드로이드 기반 로컬 프록시 서버

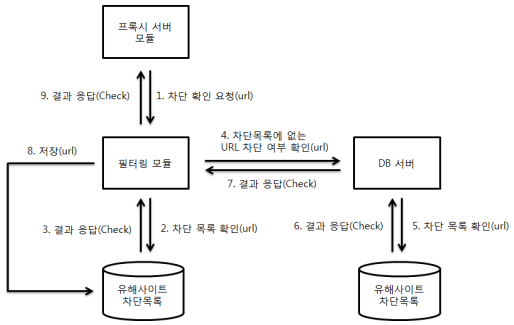
웹 브라우저에서 웹 사이트 접속을 시도하면 접속할 웹 사이트의 HTTP Request 패킷이 프록시 서버의 SocketChannel Server에 전달되고, Server는 전달받은 HTTP Reuqest 패킷의 Host 헤더에서 접속하고자 하는 웹 서버의 IP와 Port를 추출한다. Server에서는 연결을 끊지 않은 상태에서 추출한 IP와 Port로 새로운 SocketChannel Client를 생성하여 전달받은 HTTP Request 패킷을 원래 목적지로 정상적으로 전달한다. 패킷을 전달하면 해당 웹 서버에서는 HTTP Response 패킷을 Socket Channel Client에게 전달하게 되고, SocketChannel Client는 응답받은 HTTP Response 패킷을 그대로 SocketChannel Server에게 전달한 후 연결을 종료한다. SocketChannel Server 역시 SocketChannel Client에게 받은 HTTP Response를 보냄으로써 요청을 마무리한다. 이 과정을 여러 번 반복하면서 웹 사이트의 내용을 웹 브라우저를 통해서 볼 수 있도록 한다([그림 10] 참조).



[그림 10] 프록시 서버 처리 과정

4.2.2 유해 컨텐츠 필터링

유해 컨텐츠 차단을 위한 필터링 모듈은 DB 서버와의 적절한 통신을 통해서 차단 목록으로 인한 성능 저하를 방지한다. 안드로이드의 차단 목록에서는 많이 접속할 수 있는 차단 목록만 가지고 있고, 목록에 없는 사이트는 DB 서버를 통해서 실시간으로 확인하는 방식을 사용한다. 프록시 서버 모듈이 차단 확인 요청을 위해서 필터링 모듈에게 접속할 사이트의 URL을 전달하면 필터링 모듈은 차단 목록에 URL이 있는지 확인하고 차단 목록에 URL이 있으면 차단 메시지를 전달하고, 차단 목록에 URL이 없으면 DB 서버에 추가 차단 여부 확인을 위해서 URL을 전송한다. 요청을 받은 DB 서버는 DB 서버의 차단 목록에 전송받은 URL이 있는지 확인하여 결과를 필터링 모듈에게 보낸다. DB 서버의 차단 목록에 URL이 있으면 필터링 모듈은 안드로이드의 차단 목록에 해당 URL을 추가하고 DB 서버 모듈에 차단 메시지를 전달한다([그림 11] 참조).



[그림 11] 필터링 모듈 처리 절차

```
filters.add(new RequestFilter() {
   public boolean filter(Request request) {
      //필터링 모듈의 차단목록 확인
      if( pListCheck( request.getUrl() ) ) {  //차단목록에 있다면
         ...
         request = SetDenied(request);   //차단 설정
         ...
      } else {
         //차단목록에 없으면 DB 서버에서 확인
         if( sListCheck(request.getUrl()) )  {
            ...
            pListAdd(request.getUrl()); //차단목록에 추가

            request = SetDenied(request); //차단 설정
            ...
         } else {
            return false;
         }
      }
      return false;
   }
});
```

[그림 12] 필터링 모듈 소스 코드

[그림 12]는 유해 컨텐츠를 차단하기 위한 필터링 모듈의 소스코드의 일부이다. 필터링 모듈의

차단 목록에서 URL을 검사하기 위한 pListCheck() 함수의 Return 값이 True이면 차단 대상 URL로 판단하여 SetDenied() 함수로 URL을 차단하고, False이면 DB 서버의 차단 목록에서 URL을 검사하기 위해 sListCheck() 함수를 호출한다. sListCheck() 함수의 Return 값이 True이면 차단 대상으로 판단하여 pListAdd() 함수로 필터링 모듈의 차단 목록에 URL을 추가하고, SetDenied() 함수로 URL을 차단한다.

4.2.3 DB 서버

DB 서버는 Apahce 웹 서버 기반의 PHP로 동작하며, DB 서버의 차단 목록은 MySQL 기반으로 동작한다. 필터링 모듈에서 차단 여부 확인을 위해서 url을 전송하면 DB 서버는 해킹 시도 차단을 위해서 파라미터 검사를 수행한다. MySQL 기반의 차단목록에서 url을 조회하여 url이 검색되면 차단 대상으로 판단하여 필터링 모듈에게 차단 메시지를 전달하고, url이 검색되지 않으면 정상적인 사이트로 판단하여 필터링 모듈에게 미차단 메시지를 전달한다.

4.2.4 차단 목록 관리

필터링 모듈의 차단 목록은 안드로이드 기반 SQLite를 사용하며, 기본 키와 차단할 사이트 주소, 사이트의 종류로 컬럼이 구성된다(<표 2> 참조).

〈표 2〉 필터링 모듈의 차단 목록 DB 구조

DB 종류	테이블 이름	컬럼명	컬럼타입	설명
SQLite	blacklist	no	integer primary key	기본키
		url	text	차단 사이트 주소
		type	numeric	차단 사이트 종류

DB 서버에서의 차단 목록은 MySQL을 사용하며, 기본 키와 차단할 사이트 주소, 사이트의 종류로 컬럼이 구성된다(<표 3> 참조).

〈표 3〉 DB 서버의 차단 목록 DB 구조

DB 종류	테이블 이름	컬럼명	컬럼타입	설명
MySQL	blacklist	no	int	기본키
		url	varchar(50)	차단 사이트 주소
		type	numeric	차단 사이트 종류

차단 목록 관리는 사이트 수집이 중요한데 국내에서는 공개된 정보는 없다. 방송통신심의위원회에서 유해 사이트를 관리하며 소프트웨어 사업자에게만 암호화된 DB를 제공한다. 외국 유해 사이트 정보는 urlblacklist 사이트를 통해서 유해 사이트 DB를 구할 수 있다. 이 두 사이트를 통해서 공인된 유해 사이트 DB를 제공받을 수 있으며, 비공인 DB는 사이트 검색을 통해서 수동을 수집한다. 유해 사이트들의 정보는 일반적으로는 수집이 어렵기 때문에 유해 사이트들 안에서의 링크나 랭킹 정보들을 분석하여 다른 유해 사이트들을 수집할 수 있다. 또한 최근 차단된 유해 사이트의 다른 사이트 주소를 알리기 위해서 외국 계열의 트위터나 페이스북 같은 SNS(Social Network Service)를 사용하는 경우가 증가하고 있기 때문에 이러한 SNS를 추적하여 차단되지 않는 최신 유해 사이트들을 수집할 수 있다.

4.3 실험 결과

본 연구에서 제안하는 시스템의 실험을 위해서 스마트폰은 1.5GHz 듀얼코어, 1GB 메모리, 안드로이드 4.0.3 아이스크림 샌드위치로 구성했으며, DB 서버는 쿼트코어 3.00GHz, 8GB 메모리, 64비트 운영체제로 구성했다. DB 서버에 사용된 웹 서버는 Apache 2.2.14, PHP 5.12, MySQL 5.1.39로 구성했다.

실험 내용은 웹 사이트 접속 차단과 웹 페이지 유해 컨텐츠 차단을 실험했다. 각각의 실험 방법에 대해서 필터링 모듈의 차단 목록에 있는 URL과 필터링 모듈의 차단 목록에 없는 URL을 실험하며, 필

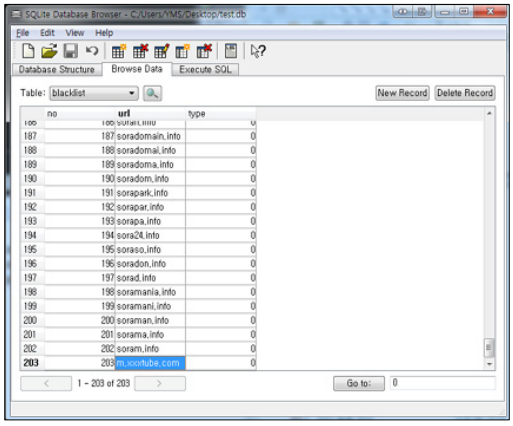
터링 모듈의 차단 목록에 없는 URL이 DB 서버를 통해서 차단되어 필터링 모듈의 차단 목록에 추가되는지 실험했다.

4.3.1 웹 사이트 접속 차단

[그림 13]은 웹 사이트 접속을 차단하는 실험결과로 필터링 모듈에서 사용되는 차단 목록에 포함되어 있는 웹 사이트가 차단되는지 보여준다. [그림 14]는 필터링 모듈에서 사용되는 차단 목록 DB로 안드로이드에서 사용할 수 있도록 SQLite 방식을 사용하고 있다. 이 목록에 포함된 사이트 중 하나인 “m.xxxtube.com”의 웹 사이트 접속을 시도하였더니 필터링 모듈을 통해서 웹 사이트의 접속이 차단되었다.

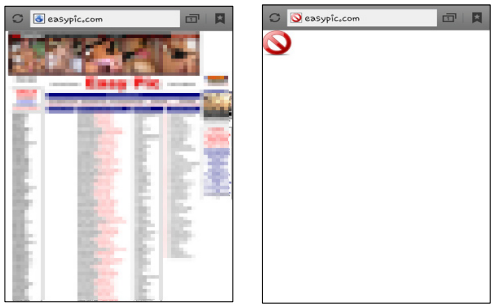
(a) 차단 전 (b) 차단 후

[그림 13] 필터링 모듈의 차단 목록에 있는 웹 사이트 차단



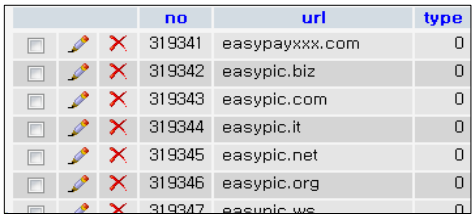
[그림 14] 필터링 모듈의 차단 목록 DB

[그림 16]는 DB 서버의 차단 목록에 의한 차단 실험결과이다. 필터링 모듈의 차단 목록에는 없고, DB 서버의 차단 목록에는 있는 웹 사이트인 “easypic.com” 웹 사이트를 접속을 시도했을 때 DB 서버와의 통신을 통해서 [그림 15]와 같이 차단이 되었다. DB 서버는 Apache와 PHP로 구성되어 있으며, 차단 목록 DB는 [그림 17]와 같이 MySQL 기반을 사용한다.



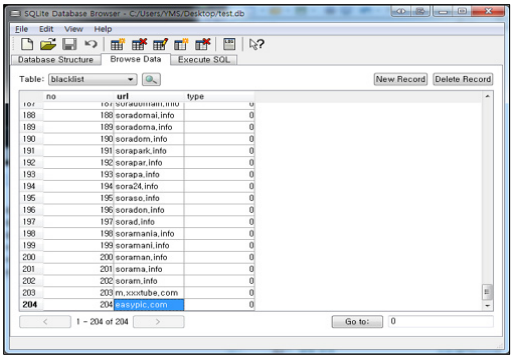
(a) 차단 전 (b) 차단 후

[그림 15] DB 서버의 차단 목록에 있는 웹 사이트 차단



	no	url	type
	319341	easypayxxx.com	0
	319342	easypic.biz	0
	319343	easypic.com	0
	319344	easypic.it	0
	319345	easypic.net	0
	319346	easypic.org	0
	319347	easypic.ws	0

[그림 16] DB 서버의 차단 목록 DB

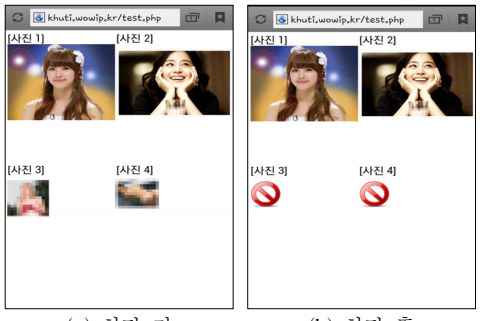


[그림 17] URL이 추가된 필터링모듈의 차단목록 DB

“easypic.com” 웹 사이트가 필터링 모듈의 차단 목록에 없는 사이트로 판단되어 DB 서버와 HTTP 통신을 통해서 차단할 사이트로 판단되었고 [그림 17]과 같이 필터링 모듈의 차단 목록에 “easypic.com” 사이트가 추가 되었다.

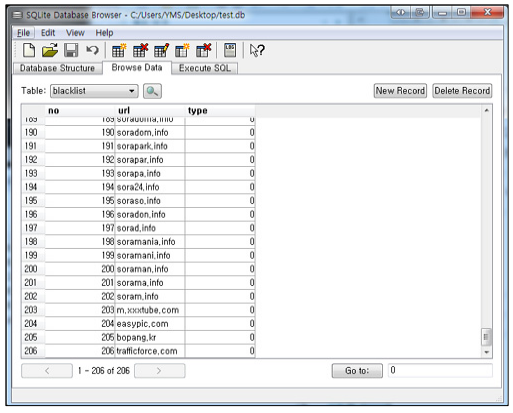
4.3.2 웹 페이지에 링크된 유해 컨텐츠 차단

[그림 18]은 웹 페이지의 유해 컨텐츠 차단에 관한 실험 결과이다 “사진 1”과 “사진 2”는 유해 컨텐츠가 아닌 정상적인 이미지이고, “사진 3”은 해외 사이트에서 링크된 유해 컨텐츠이고, “사진 4”는 국내 사이트에서 링크된 유해 컨텐츠이다. 차단되지 않은 웹 페이지에 링크된 유해 컨텐츠가 [그림 19]와 같은 필터링 모듈의 차단목록 DB로 인해서 정상적으로 차단되었다.



(a) 차단 전 (b) 차단 후

[그림 18] 웹 페이지의 유해 컨텐츠 차단



[그림 19] 차단 후 필터링 모듈의 차단목록 DB

5. 결 론

모바일 기술의 빠른 발전과 스마트폰 보급으로 인해서 우리의 삶은 많이 윤택해 졌지만 데스크 탑 환경에서와 마찬가지로 모바일에서의 유해 컨텐츠 문제가 점점 심각해지고 있다. 청소년들의 스마트폰 사용률 증가, 유해 컨텐츠의 모바일 최적화, 모바일 기기의 자유로운 인터넷 접속 등으로 인해서 그 심각성이 더해지고 있다.

본 연구에서는 이러한 유해 컨텐츠 문제를 개선하기 위해서 안드로이드에서 로컬 프록시를 이용한 유해 컨텐츠 차단 시스템을 제안하였다. 로컬 프록시 방식을 사용함으로써 차단 목록 DB가 탑재된 DB 서버와의 실시간 통신에 따른 속도저하 문제를 개선하였다. 웹 사이트 접속 차단과 웹 페이지에 링크된 유해 컨텐츠 차단을 실험한 결과도 웹 사이트 접속 차단뿐만 아니라 웹 페이지에 링크된 유해 컨텐츠까지 효과적으로 차단하였다. 또한 필터링 모듈의 차단 목록에 없는 유해 사이트는 DB 서버와의 통신을 통해서 정상적으로 차단되었다.

본 연구는 웹 사이트 차단뿐만 아니라 차단되지 않은 웹 페이지 내의 유해 컨텐츠까지 모두 차단하는 것을 목표로 하였다. 하지만 제시한 방안은 HTTP 패킷을 분석하여 URL을 기반으로 차단하기 때문에 정상적인 사이트의 URL을 사용하고 있는 유해 컨텐츠는 차단할 수 없었다. 정상적인 URL을 사용하고 있는 유해 컨텐츠까지 차단하기 위해서는 차단여부가 판단되지 않은 사이트의 유해 정도를 분석하는 내용 기반 차단 방법에 관한 지속적인 연구가 필요하다. 그 외에도 유해 사이트 및 유해 컨텐츠 차단에서 큰 비중을 차지하는 차단 목록의 효과적인 관리 및 수집에 대한 연구가 진행되어야 할 것이다.

본 연구의 결과가 스마트폰 응용 프로그램 개발자에게 주는 시사점은 레거시 시스템의 프록시 서버의 개념을 스마트폰 플랫폼에 장착함으로써 유해 컨텐츠 차단 속도를 높이고 향후 다른 분야에서도 로컬 프록시를 활용한 프로그램 개발에 착안

점을 제시하였다는 점이다. 향후 이런 개념의 응용 프로그램 개발에 더 많은 연구와 관심이 있을 것으로 기대된다.

참 고 문 헌

[1] 플랜티넷, http://www.plantynet.com.

[2] 뉴스, http://news.khan.co.kr/kh_news/khan_art_view.html?artid = 201209032155455&code = 940100.

[3] 뉴스, http://www.mediaus.co.kr/news/articleView.html?idxno = 23533.

[4] 뉴스, http://www.seoul.co.kr/news/newsView.php?id = 20121003006001.

[5] 여성가족부 블로그, http://blog.daum.net/moge-family/5693.

[6] 행정안전부, “청소년 성인물이용 실태조사”, 행정안전부, 2012.

[7] 인터넷내용등급서비스, http://www.safenet.ne.kr.

[8] 방송통신심의위원회, “안드로이드 오픈마켓 내 유해 애플리케이션 2차 유통실태 조사”, 방송통신심의위원회, 2011.

[9] 김미정, 장혜진, “내용 기반 Web 유해 문서 차단을 위한 지능형 에이전트 시스템의 개발”, 「1999년도 한국멀티미디어학회 추계학술발표논문집」, (1999), pp.606-611.

[10] 김용운, 김봉완, 최대림, 김태권, 고락환, 이용주, 「안드로이드 OS 기반 음향정보를 이용한 음란 동영상 검출 서비스 구현」, 2010년도 한국멀티미디어학회 학술발표논문집, (2010), pp.416-419.

[11] 김은실, 김귀정, 김봉환, “고등학생들의 사이버 음란물 접촉과 성범죄와의 관계성 분석”, 「한국콘텐츠학회논문지」, 제11권, 제6호(2011).

[12] 김춘옥, “국내 PC 통신상의 음란정보 유통현황 및 심의의 문제점”, 한국언론학회, (1998), pp.32-40.

[13] 고태규, 양은석, “청소년들의 인터넷 성인사이트 이용행태에 관한 연구”, 「한국체육학회지」, 26권, 제4호(2007).

[14] 노성호, 「컴퓨터통신을 통한 음란물 접촉실태와 대책」, 한국형사정책학회, (1998), 230-245.

[15] 이세용, 「인터넷과 청소년의 성의식」, 한국정보사회학회, (2000), pp.154-182.

[16] 정완, “휴대폰과 인터넷을 통한 음란물 유통의 실태와 대책”, 「한국형사정책학회」, 제22권(2010), pp.51-74.

[17] 정진성, 조동욱, 「음란 사이트 현황과 차단 방법에 대한 고찰」, 한국콘텐츠학회/한국통신학회 추계 종합학술대회 논문집, 제1권, 제2호(2003).

[18] 조성택, “사이버 범죄의 규제에 관한 연구 : 사이버 음란물을 중심으로”, 「한국지역정보화학회지」, 제9권, 제2호(2006).

[19] 최광훈, 고광만, 박희완, 윤종희, “유해 사이트를 접속하는 안드로이드 앱을 문자열 분석으로 검사하는 시스템”, 「정보처리학회논문지」, 제19A권, 제4호(2012), pp.187-194.

[20] 한승완, 김세민, 정병호, 노용만, “내용 기반 유해 멀티미디어 차단 기술 동향”, 「한국정보보호학회」, 제19권, 제5호(2009).

[21] 한승완, 최병철, 임재덕, “유해 멀티미디어 분석 및 차단 기술 동향”, 「정보보호학회지」, 제22권, 제3호(2012).

◈ 저 자 소 개 ◈

김 인 재 (ijkim@dongguk.edu)

동국대학교 경영대학 경영학부 교수로 재직 중이다. 서울대학교 산업공학 학사, 한국과학기술원 경영과학 석사, University of Nebraska-Lincoln 경영정보학 박사 학위를 받았다. LG전자 중앙연구소 전산실 개발팀장으로 재직하였다. 주요 관심 분야는 정보기술의 수용, 정보기술 융합, 정보 보안, 소프트웨어공학, 온라인 커뮤니티 전략 등이다. 기술수용 및 전략, 정보기술 응용, 소프트웨어 품질, 정보보안에 관한 다수의 논문을 국내외에 발표하였다.

양 민 수 (msyang@pentasecurity.com)

국가평생교육진흥원에서 전자계산학 학사를 취득한 뒤, 동국대학교 국제정보대학원에서 정보보호 석사를 취득하였다. (주)잉카인터넷 근무하였고, 현재 펜타시큐리티시스템(주)에서 근무 중이다. 주요 관심분야는 웹 취약점 자동화 탐지, 웹 방화벽, 자동화 기술, 정보보호 등이다.