RADIUS 서버를 이용한 사용자 인증 기반 URL 필터링 시스템의 설계 및 구현

김태웅°, 류호연, 김성조
중앙대학교 컴퓨터 공학과
{twkim°, deux9745, sjkim}@konan.cse.cau.ac.kr

A Design and Implementation of URL Filtering System Based on User Authentication Using RADIUS Server

Tae Woong Kim°, Ho Yeon Ryu, Sung Jo Kim
Dept. of Computer Science & Engineering, Chung-Ang University

요 약

엄청난 양의 정보를 제공하는 인터넷은 사람들에게 편의성을 제공해 주고 있다. 그러나 다른 한편으로는 인터넷으로 인하여 청소년들이 유해한 정보에 무방비로 노출되고, 회사에서는 업무와 관련이 없는 인터넷 사용으로 업무 능률이 저하되며 네트워크 자원이 낭비되는 등의 여러 가지 문제가 발생하고 있다. 본 논문에서는 이러한 문제를 해결하기 위해 개인별로 인증을 받은 후에 각 개인에 따라 설정된 필터링 정책에 의해 인터넷을 사용하는 시스템을 제안한다. 기존의 시스템은 시스템 구성 및 성능, 사용자 관리의 어려움 등의 문제로 ISP 등의 대단위 네트워크에 적용하기 어렵다. 본 논문에서는 대단위 네트워크에 적용 가능하고 사용자 관리가 용이한 URL 필터링 시스템을 제안한다. 이러한 시스템을 사용하면 학교나 가정 및 직장에서 개인별로 다양한 필터링 정책을 적용할 수 있어 유해한 정보로부터 청소년을 보호할 수 있으며, 업무 능률의 상승과 네트워크 자원을 효율적으로 활용할 수 있는 장점이 있다.

1. 서론

과거에 소수 사람들의 전유물로 인식됐던 인터넷이 최근에는 학교나 회사뿐만 아니라 일반 가정에서까지 쉽게 접근하여 원하는 정보를 얻을 수 있을 정도로 확산되었다. 사용자 및 호스트의 수가 급격히 증가하는 인터넷은 엄청나게 많은 양의 정보를 제공하고 있으며, 이로 인해 우리의 생활은 더욱 편리하고 윤택하게 되었다. 그러나 다른 한편으로는 인터넷으로 인하여 여러 가지 사회적 문제가 야기되는 부작용이 발생하고 있다. 어린 학생들은 음란물, 마약, 폭력, 도박 등의 유해한 정보에 무방비 상태로 노출되어 있으며, 회사에서는 직원들의 업무 외의 불필요한 인터넷 사용으로 인해 생산성이 감소하고 네트워크 비용의 증가하는 문제점이 발생하고 있다.

이러한 문제점을 해결하기 위한 방법으로 인터넷 내용등급제[1]와 같은 방안이 고려되고 있으나, 이는 자율적인 규제 방안일 뿐 확실한 대안이 될 수 없다. 또 다른 방법으로는 클라이언트 컴퓨터에 인터넷 필터링 소프트웨어를 설치하는 방법이 있으나 이는 프로그램 조작 및 삭제 등이 쉬운 단점을 가지고 있다. 가장 신뢰성 있는 방법은 네트워크 단위에서 인터넷 필터링을 수행하는 것이다. 또한 개인별 필터링 정책을 설정함으로써 사용자에게 알맞은 인터넷 컨텐츠를 제공할 수 있다.

본 논문에서 제안하는 필터링 시스템의 목적은 다음과 같다. 첫째, ISP(Internet Service Provider)와 같은 대단위 네트워크 차원에서 개인 혹은 그룹 단위의 필터링 정책을 적용할 수 있는 URL 필터링 시스템을 설계·구현함으로써 보다 효율적인 필터링 정책을 세울 수 있도록 한다. 둘째, 캐싱 서버를 이용한 프록시 형태의 필터링 시스템을 구현함으로써 높은 성능과 확장성을 달성한다.

본 논문의 구성은 다음과 같다. 2장에서는 URL 필터링 방법론과 기존 연구의 문제점을 알아보고, 3장에서는 본 논문에서 제안하는 RADIUS를 이용한 사용자 인증 기반의 URL 필터링 시스템의 설계 및 구현에 대해 설명한다. 4장에서는 본 논문에서 제안한 시스템에 대한 결론을 맺는다.

2. 관련연구

사용자의 인터넷 사용을 차단할 수 있는 방법은 실제 전송되는 내용을 기반으로 그 내용이 어느 분류에 속하는지 결정하여 차단 여부를 판단하는 내용 기반 차단 방식과 HTTP, TCP/IP 등과 같은 프로토콜의 헤더 정보를 이용해 차단 여부를 결정하는 URL 기반 차단 방식으로 나눌 수 있다. 내용 기반 차단 방식은 내용을 정확하게 분류하기 어렵기 때문에 신뢰성이 떨어진다. URL 기반 차단 방식은 프로토콜 헤더 정보를 이용하여 차단 여부를 결정하기 때문에 내용 기반 차단 방식에 비해 빠르고 부하가 적어 대단위 네트워크에 적용이 쉽다. 그러나 프로토콜 헤더에서 얻어오는 클라이언트의 정보에는 실제 컴퓨터를 이용하는 사용자에 대한 정보가 없기 때문에 사용자별로 인터넷 필터링을 수행하는 것이 불가능하다.

URL 기반 차단 방식을 사용하여 사용자별 인터넷 필터링을 수행하는 기존의 시스템[2]은 사용자 ID와 비밀번호로 사용자를 인증하고, 인증된 세션의 사용자 정보를 이용해 사용자별 인터넷 필터링 시스템을 구현했다. 그러나 이 시스템은 다음과 같은 문제점이 있다.

▸확장성이 적은 시스템 구성 : 웹 요청 분석 모듈, 사용자

관리 모듈, 사용자 인증 모듈, 필터링 모듈 등 각 모듈이 한 서버에서 동작한다. 컴퓨팅 파워(computing power), 메모리 등의 제한된 자원(resource)을 각 모듈이 공유해야 하기 때문에 많은 양의 인터넷 트래픽을 처리하기가 어렵다. 또한 클러스터 기능이 지원되지 않기 때문에 인터넷 트래픽이 많은 대단위 네트워크에 적용할 수 없다.

- 비표준 인증 시스템 : 사용자를 인증하는데 있어서 RADIUS(Remote Access Dial-In User Service)나 LDAP(Lightweight Directory Access Protocol)와 같은 표준 인증 시스템을 사용하지 않았다. 따라서 기존에 구축되어 있는 사용자 정보 DB를 이용하지 못하며 이 시스템을 위한 사용자 DB를 따로 구축해야하는 문제점이 있다.

3. RADIUS를 이용한 사용자 인증 기반 URL 필터링 시스템의 설계 및 구현

이 장에서는 2장에서 언급했던 문제점을 해결하기 위해 전체 시스템을 재구성한다. 새롭게 설계한 시스템의 구성과 IP 탐색 방법에 대해서 알아본다.

3.1 전체 시스템 구성

본 논문에서 설계한 사용자 인증 기반 URL 필터링 시스템의 구성은 그림 1과 같으며 각 구성요소의 역할은 다음과 같다.

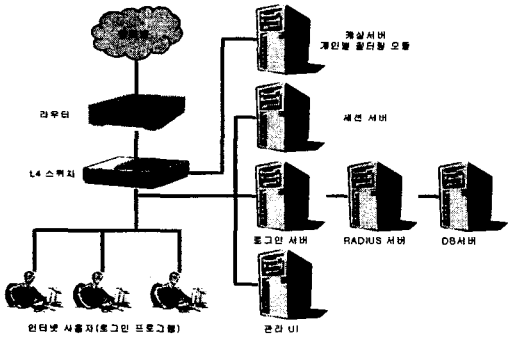

그림 1. 전체 시스템 구성

- 캐싱서버 : 사용자가 자주 사용하는 웹 자원을 캐싱하여 네트워크 부하를 줄이고 인터넷 검색 속도를 높일 수 있다. 또한 플로그인(plug-in)을 지원해주어 개인별 필터링 모듈이 동작할 수 있도록 한다.
- L4(Layer-4) 스위치 : 라우터 앞단에 위치하여 외부 네트워크로 나가는 모든 URL 요청을 캐싱서버로 리다이렉트(redirect)한다. 네트워크 단위에 설치되기 때문에 신뢰성 있는 필터링이 가능하다.
- 로그인 프로그램 : 사용자 컴퓨터에 설치된 프로그램으로서 사용자 ID와 비밀번호를 로그인 서버에 전달한다.
- 로그인 서버 : RADIUS 서버의 클라이언트인 NAS(Network Access Server)로서 동작을 하며, 로그인 프로그램으로부터 받은 사용자 ID와 비밀번호를 RADIUS 프로토콜에 적합한 형태로 만들어 RADIUS로 전송한다.
- 세션 서버 : 인증 받은 사용자에 대한 정보를 가지고 있으며, 일정기간 동안 인터넷을 사용하지 않은 경우 개인별 필터링 모듈의 부하를 줄이기 위해 해당 세션을 종료한다.
- RADIUS 서버 : 로그인 서버로부터 받은 인증요청 정보와 사용자 DB를 이용해 인증 여부를 결정한다. 인증 여부에 대한 결과를 로그인 서버를 통해 사용자, 개인별 필터링 모듈, 세션 서버에 전달한다.
- 관리 UI : 웹을 통하여 사용자의 필터링 정책과 비밀번호, 그룹 필터링 정책 등을 설정할 수 있도록 한다. 시스템 설정에 관련한 설정도 관리 UI를 통해 가능하다.

이러한 시스템 구성은 시스템으로 들어오는 부하를 최대한 분산시킬 수 있다. 또한 대단위 네트워크에서 사용될 경우, 다수의 개인별 필터링 모듈, 로그인 서버, 세션 서버 등을 설치하고 이에 대한 정보를 설정함으로써 클러스터 기능을 지원할 수 있다.

본 시스템은 신뢰성 있는 사용자 인증을 위해 원격 접속 사용자를 위한 인증 프로토콜인 RADIUS[3]를 이용한다. RADIUS 서버는 사용자의 인증 정보를 일반 DB에 저장하는 것이 일반적인데, 본 논문에서 제안하는 시스템은 인증에 사용될 새로운 사용자 DB를 구축하는 대신 기존에 구축되어 있던 사용자 DB를 이용할 수 있도록 설계되었다. 사용자 인증 정보가 담겨있는 DB 이름, 테이블 이름, 필드 이름 등을 설정 파일에 저장하여 이 파일에 저장된 정보를 바탕으로 인증을 시도한다. 다음 그림 2는 관리 UI를 통해 사용자 DB 정보를 설정하는 화면이다.

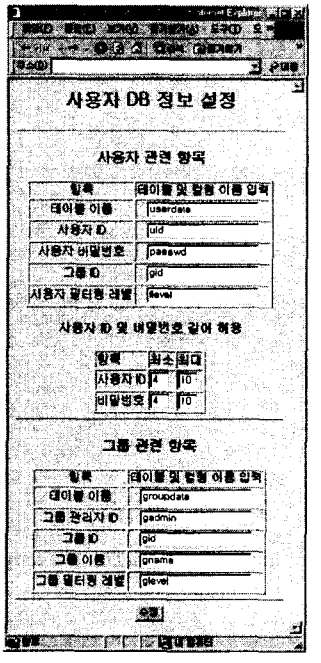

그림 2. 사용자 DB 정보 설정

3.2 개인별 필터링 모듈

사용자 인증 성공 후, 실질적인 개인별 인터넷 필터링을 수행하는 개인별 필터링 모듈의 구성은 그림 3과 같다.

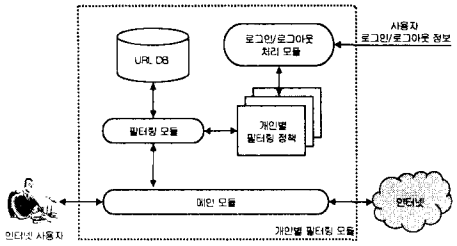

그림 3. 개인별 필터링 모듈의 구성

사용자가 요청한 URL의 필터링 여부를 결정하기 위해서는 미리 설정되어 있는 사용자의 필터링 정책을 검색해야 한다. 최근의 웹 페이지는 이미지, 동영상 등의 멀티미디어 자원을 많이 포함하고 있기 때문에 한 번의 사용자 URL 요청이 매우 많은 양의 자동 URL 요청을 발생시킨다. 따라서 사용자의 필터링 정책을 검색하는 빈도가 굉장히 높아 빠른 검색 기법이 필요하다.

본 논문에서 제안한 검색 기법은 IP 주소를 키(key)로 하는 완전해쉬(perfect hash)이다[4]. 해쉬 함수는 실행시간이 짧은 장점이 있으나, 충돌(collision)이 발생하는 경우 검색 속도가 느려지는 단점이 있다. 완전해쉬는 일반 해쉬와 다르게 검색 시 충돌이 일어나지 않기 때문에 빠른 검색이 가능하다. 완전해쉬는 키로 쓰일 입력 값을 미리 정의하고, 이를 이용해 충돌이 일어나지 않는 해쉬 함수와 해쉬 테이블을 생성하기 때문에 입력 값이 미리 정의되어야 한다. 본 논문에서 제안한 시스템에서는 완전해쉬를 생성하기 위한 입력 값으로 IP 주소를 사용한다. 왜냐하면 LAN 환경의 고정 IP 주소나 DHCP를 이용한 동적 IP 주소 모두 사용할 수 있는 IP 주소 대역이 정해져 있고, 사용자의 웹 요청에서 얻는 발신지 IP 주소를 이용해 로그인 된 사용자의 정보를 얻기 때문이다. 완전해쉬의 생성 및 이를 이용한 사용자별 필터링 정책 검색 방법은 그림 4와 같다.

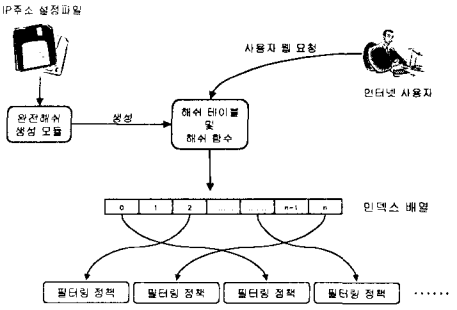

그림 4. 완전해쉬의 생성과 이용

그림 3의 로그인/로그아웃 처리 모듈은 사용자가 로그인/로그아웃 할 때 각각 로그인 서버와 세션 서버로부터 사용자의 정보를 받아 필터링 정책에 사용자 정보를 추가하거나 삭제하는 역할을 수행한다. 개인별 필터링 모듈은 현재 로그인 된 사용자의 정보만을 관리하기 때문에 메모리 요구량을 최소화 할 수 있다. 사용자가 로그인하면 사용자의 자료구조를 메모리에 할당하고 해당 인덱스 배열의 포인터가 그 사용자 자료구조를 가리키게 함으로써 완전해쉬를 이용한 검색이 가능하다. 사용자가 로그아웃 하면 해당 사용자의 자료구조를 메모리에서 해제하고 인덱스 배열의 포인터를 초기화한다. 이러한 기법을 통해 메인 모듈이 인덱스 배열의 포인터 값을 이용하여 사용자의 로그인 여부를 쉽게 판단할 수 있고, 사용자의 필터링 정책에 빠르게 접근할 수 있다.

가정과 같은 작은 단위의 구성원을 쉽게 관리할 수 있도록 하기 위해 사용자를 그룹으로 분류하였다. 시스템 관리자는 그룹을 생성, 삭제 및 관리를 하고 그룹별 필터링 정책을 설정한다. 그리고 각 그룹 관리자는 그룹에 포함되는 일반 사용자의 개인별 필터링 정책을 설정한다. 시스템 관리자가 설정한 그룹별 필터링 정책은 그룹 관리자가 변경할 수 없기 때문에 각 그룹의 특성에 따른 필터링 정책을 설정할 수 있다. 구성원 정책은 관리 UI를 통해 이루어지며 그 구성은 그림 5와 같다.

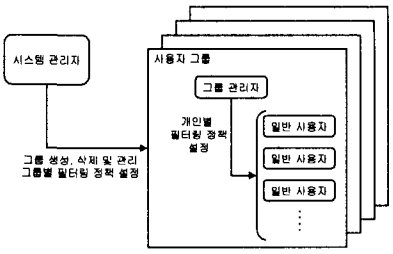

그림 5. 구성원 정책도

4. 결론

인터넷은 현대 사회에 있어서 없어서는 안 될 존재가 되었다. 인터넷이 우리의 생활 깊숙이 들어와 있는 만큼, 그 폐해 또한 날로 커지고 있다. 어린 학생들이 음란, 도박 등 유해한 정보에 노출되어있고, 직장인들은 업무 시간에 개인적인 용도로 인터넷을 이용함으로써 작업 능률의 저하는 물론이고 네트워크 자원을 낭비한다.

본 논문에서 제안한 시스템을 이용하면 이러한 문제를 해결할 수 있다. 각 개인에 알맞은 필터링 정책을 설정함으로써 자신에게 허용되지 않은 웹 사이트로의 접근을 제한한다. 또한 관련이 있는 사용자들을 그룹으로 관리함으로써 사용자 관리의 편의성을 제공한다. 또한 이 시스템은 클러스터 기능을 이용하여 ISP 등 대단위 네트워크에도 적용 가능하도록 구현하였다. 완전 해쉬를 이용한 사용자 정보 검색은 매우 빨라서 시스템의 부하를 줄이고, 사용자가 느끼는 응답 지연시간을 최소화 한다. 사용자의 인증 정보를 새로 구축하지 않고 기존 사용자 DB를 이용하여 동작할 수 있도록 구현하였다.

참고문헌

[1]http://www.w3.org/PICS/,Platform for Internet Content Selection, Jan. 2003.

[2]전해식, "사용자 인증기반 URL 필터링 시스템의 구현", 석사 학위 논문, 중앙대학교, 2001

[3]C. Rigney, S. Willens, A. Rubens, W. Simpson "Remote Authentication Dial-In User Service(RADIUS)" , RFC 2865, Jun. 2000

[4]Bob Jenkins, Minimal Perfect Hashing, http://burtleburtle.net/bob/hash/perfect.html,