(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0078130
(43) 공개일자 2015년07월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2013-0167247
(22) 출원일자 2013년12월30일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
송지환
경기 성남시 분당구 중앙공원로 54, 228동 1405호 (서현동, 우성아파트)
권은영
서울 강동구 고덕로97길 29, 901동 301호 (강일동, 강일리버파크9단지아파트)
(뒷면에 계속)
(74) 대리인
윤동열

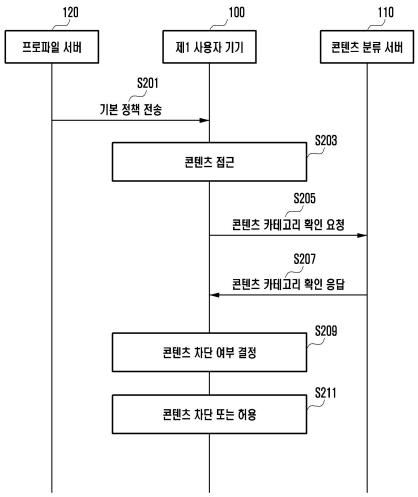
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **콘텐츠 차단 방법 및 시스템**

(57) 요 약

본 발명의 일 실시예에 따른 사용자 기기의 콘텐츠 차단 방법은 프로파일 서버로부터 정책을 수신하는 과정; 콘텐츠 접근 요청을 수신하는 과정; 상기 접근 요청된 콘텐츠가 속하는 카테고리를 확인하는 과정; 상기 확인된 카테고리가 상기 정책에 차단 설정된 카테고리와 일치하는지 결정하는 과정; 및 상기 확인된 카테고리가 상기 정책에 포함된 카테고리와 일치하는 경우, 상기 접근 요청된 콘텐츠를 차단하는 과정을 포함하는 것을 특징으로 한다.

대 표 도 - 도2



(72) 발명자

박진환

서울 성동구 뚝섬로 51, 105동 901호 (옥수동, 옥수강변풍림아이원)

정일웅

경기 수원시 영통구 효원로 363, 130동 2203호 (매탄동, 매탄위브하늘채아파트)

김현수

경기 용인시 수지구 신봉1로330번길 15-14, 108동 201호 (신봉동, 삼성쉐르빌)

송가진

경기 안양시 동안구 귀인로 258, 108동 801호 (평촌동, 꿈마을라이프아파트)

명 세 서

청구범위

청구항 1

사용자 기기의 콘텐츠 차단 방법에 있어서,

프로파일 서버로부터 정책을 수신하는 과정;

콘텐츠 접근 요청을 수신하는 과정;

상기 접근 요청된 콘텐츠가 속하는 카테고리를 확인하는 과정;

상기 확인된 카테고리가 상기 정책에 차단 설정된 카테고리와 일치하는지 결정하는 과정; 및

상기 확인된 카테고리가 상기 정책에 포함된 카테고리와 일치하는 경우, 상기 접근 요청된 콘텐츠를 차단하는 과정을 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 2

제 1항에 있어서,

상기 정책은 상기 사용자 기기 또는 상기 사용자 기기의 사용자가 속하는 지역, 문화와 상기 사용자 기기의 사용자의 연령, 성별, 직업 및 종교에 기초하여 설정되는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 3

제 1 항에 있어서,

상기 접근 요청된 콘텐츠가 속하는 카테고리를 확인하는 과정은,

콘텐츠 분류 서버로 상기 접근 요청된 콘텐츠에 대한 정보를 수신하는 과정; 및

상기 콘텐츠 분류 서버로부터 상기 접근 요청된 콘텐츠가 속하는 카테고리에 대한 정보를 수신하는 과정을 더 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 4

제 1항에 있어서,

일정 기간 이내에 상기 접근 요청된 콘텐츠가 차단된 기록이 있는 경우, 곧바로 상기 접근 요청된 콘텐츠를 차단하는 과정을 더 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 5

제 1항에 있어서,

상기 프로파일 서버로부터 정책을 수신하는 과정은 다른 사용자 기기에 의해 상기 정책이 수정된 수정 정책을 수신하는 과정을 더 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 6

제 1항에 있어서,

상기 정책에 차단 설정된 카테고리에 속하는 콘텐츠에 대한 접근 해제 요청을 수신하는 과정; 및

상기 수신된 접근 해제 요청을 상기 프로파일 서버를 통해 다른 사용자 기기로 전송하는 과정을 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 7

제 6항에 있어서,

상기 다른 사용자 기기에서 상기 접근 해제 요청이 허락 또는 거절되면, 상기 다른 사용자 기기가 상기 접근 해제 요청 허락 또는 거절에 대한 정보를 상기 프로파일 서버로 전송하는 과정을 더 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 8

제 7항에 있어서,

상기 프로파일 서버에서 상기 접근 해제 요청이 허락된 콘텐츠 및 상기 접근 해제 요청이 허락된 콘텐츠가 속하는 카테고리에 대한 정보를 저장하는 과정;

상기 프로파일 서버로부터 상기 접근 해제 요청이 허락된 콘텐츠 및 상기 접근 해제 요청이 허락된 콘텐츠가 속하는 카테고리에 대한 정보를 수신하는 과정; 및

상기 접근 해제 요청된 콘텐츠에 대한 접근을 허용하는 과정을 더 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 9

제 7항에 있어서,

일정 기간 동안 저장된 상기 접근 해제 요청이 허락된 콘텐츠 및 상기 접근 해제 요청이 허락된 콘텐츠가 속하는 카테고리에 대한 정보에 기초하여, 상기 정책을 업데이트(update)하는 과정을 더 포함하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 10

제 1항에 있어서,

상기 정책은 상기 사용자 기기가 속하는 그룹에 따라 다르게 설정되는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 방법.

청구항 11

정책을 설정하고, 설정된 정책을 전송하는 프로파일 서버; 및

상기 프로파일 서버로부터 상기 설정된 정책을 수신하고, 콘텐츠 접근 요청을 수신하고, 상기 접근 요청된 콘텐츠가 속하는 카테고리를 확인하며, 상기 확인된 카테고리가 상기 정책에 차단 설정된 카테고리와 일치하는지 결정하고, 상기 확인된 카테고리가 상기 정책에 포함된 카테고리와 일치하는 경우, 상기 접근 요청된 콘텐츠를 차단하는 제 1 사용자 기기를 포함하는 것을 특징으로 하는 콘텐츠 차단 시스템.

청구항 12

제 11항에 있어서, 상기 정책은 상기 사용자 기기 또는 상기 사용자 기기의 사용자가 속하는 지역, 문화와 상기 사용자 기기의 사용자의 연령, 성별, 직업 및 종교에 기초하여 설정되는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 시스템.

청구항 13

제 11항에 있어서,

상기 제 1 사용자 기기로부터 상기 접근 요청된 콘텐츠에 대한 정보를 수신하고, 상기 접근 요청된 콘텐츠가 속하는 카테고리에 대한 정보를 검색하여, 상기 검색된 접근 요청된 콘텐츠가 속하는 카테고리에 대한 정보를 상기 제 1 사용자 기기로 전송하는 콘텐츠 분류 서버를 더 포함하고,

상기 제 1 사용자 기기는 상기 검색된 접근 요청된 콘텐츠가 속하는 카테고리에 대한 정보에 기초하여, 상기 접근 요청된 콘텐츠가 속하는 카테고리를 확인하는 것을 특징으로 하는 콘텐츠 차단 시스템.

청구항 14

제 11항에 있어서,

상기 제 1 사용자 기기는 일정 기간 이내에 상기 접근 요청된 콘텐츠가 차단된 기록이 있는 경우, 곧바로 상기 접근 요청된 콘텐츠를 차단하는 것을 특징으로 하는 콘텐츠 차단 시스템.

청구항 15

제 11항에 있어서,

상기 제 1 사용자 기기를 관리하고, 상기 정책을 수정한 수정 정책을 설정하는 제 2 사용자 기기를 더 포함하는 것을 특징으로 하는 콘텐츠 차단 시스템.

청구항 16

제 11항에 있어서,

상기 제 1 사용자 기기로 상기 정책에 차단 설정된 카테고리에 속하는 콘텐츠에 대한 접근 해제 요청을 수신되고, 상기 수신된 접근 해제 요청을 상기 프로파일 서버를 통해 상기 제 2 사용자 기기로 전송하는 것을 특징으로 하는 콘텐츠 차단 시스템.

청구항 17

제 16항에 있어서,

상기 제 2 사용자 기기에 의해 상기 접근 해제 요청이 허락 또는 거절되면, 상기 제 2 사용자 기기가 상기 접근 해제 요청 허락 또는 거절에 대한 정보를 상기 프로파일 서버로 전송하는 것을 특징으로 하는 콘텐츠 차단 시스템.

청구항 18

제 17항에 있어서,

상기 프로파일 서버는 상기 접근 해제 요청이 허락된 콘텐츠 및 상기 접근 해제 요청이 허락된 콘텐츠가 속하는 카테고리에 대한 정보를 저장하고, 상기 제 1 사용자 기기는 상기 프로파일 서버로부터 상기 접근 해제 요청이 허락된 콘텐츠 및 상기 접근 해제 요청이 허락된 콘텐츠가 속하는 카테고리에 대한 정보를 수신하고, 상기 접근 해제 요청된 콘텐츠에 대한 접근을 허용하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 시스템.

청구항 19

제 17항에 있어서,

상기 프로파일 서버는 일정 기간 동안 저장된 상기 접근 해제 요청이 허락된 콘텐츠 및 상기 접근 해제 요청이 허락된 콘텐츠가 속하는 카테고리에 대한 정보에 기초하여, 상기 정책을 업데이트(update)하는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 시스템.

청구항 20

제 11항에 있어서,

상기 정책은 상기 제 1 사용자 기기가 속하는 그룹에 따라 다르게 설정되는 것을 특징으로 하는 사용자 기기의 콘텐츠 차단 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 유해 콘텐츠를 적응적으로 차단하기 위한 콘텐츠 차단 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 정보 통신 기술의 발전에 따라 사용자 기기가 광범위하게 보급 및 이용되고 있다. 이에 따라, 사용자는 사용자 기기를 이용하여 오픈 마켓 등을 통해 사용자는 다양한 콘텐츠를 편리하고 간이하게 다운로드하여 사용할

수 있다.

[0003] 반면, 다양한 콘텐츠가 사용자 기기로 다운로드됨에 따라 유익한 콘텐츠뿐만 아니라 유해한 콘텐츠 또한 사용자에게 제공되고 있다. 예를 들어, 청소년이 사용자 기기의 웹 브라우저 등을 통해 손쉽게 유해한 사진 및 동영상 등의 콘텐츠에 접근할 수 있으며, 의도적으로 유해한 콘텐츠에 접근하지 않더라도 유익한 콘텐츠와 함께 유해한 콘텐츠가 동시에 다운로드되어 청소년에게 노출될 수 있다.

[0004] 이러한 유해 콘텐츠를 차단하기 위해 종래에는 사용자 기기로부터 유해한 콘텐츠가 위치하는 URL(Uniform resource locator)이 입력되는 경우, 유해한 콘텐츠가 위치하는 것으로 미리 정의된 URL과 일치하는 지 판단하고, 일치되는 것으로 판단되면, 입력된 URL로의 접속을 차단하는 방식을 이용하고 있다. 또는, 마약, 해킹, 도박, 종교 등의 미리 정의된 카테고리에 해당되는 유해 콘텐츠를 일률적으로 차단하는 방식을 사용하고 있다.

발명의 내용

해결하려는 과제

[0005] 그러나 위와 같은 종래 기술은 사용자 기기 사용자의 문화적 특성 및 지역적 특성 등 콘텐츠의 유해성에 대한 다양성을 반영하지 못하는 문제가 있다. 예를 들어, 사용자가 사용하려는 콘텐츠의 카테고리가 속옷인 경우 국가에 따라 유해 여부가 달라질 수 있다. 또한, 종교의 경우에는 특정 문화를 가진 민족 및 국가에서는 유해한 콘텐츠 카테고리로 정의될 수 있는 반면, 다른 문화를 가진 민족 및 국가에서는 유익한 정보에 해당될 수도 있다. 또한, 종래 기술은 사용자와의 피드백(feedback) 없이 콘텐츠의 유해 기준을 두고 있다. 다시 말해, 콘텐츠의 유해 여부는 고정된 것이 아니라, 시간에 따라 변동될 수 있으며, 종래 기술은 이를 반영하지 못하고 있다. 이와 같이, 종래 기술은 유해 콘텐츠의 필터링에 대한 기준이 적응적이지 못하는 문제가 있다.

과제의 해결 수단

[0006] 본 발명의 일 실시예에 따른 사용자 기기의 콘텐츠 차단 방법은 프로파일 서버로부터 정책을 수신하는 과정; 콘텐츠 접근 요청을 수신하는 과정; 상기 접근 요청된 콘텐츠가 속하는 카테고리를 확인하는 과정; 상기 확인된 카테고리가 상기 정책에 차단 설정된 카테고리와 일치하는지 결정하는 과정; 및 상기 확인된 카테고리가 상기 정책에 포함된 카테고리와 일치하는 경우, 상기 접근 요청된 콘텐츠를 차단하는 과정을 포함하는 것을 특징으로 한다.

[0007] 본 발명의 일 실시예에 따른 사용자 기기의 콘텐츠 차단 시스템은 정책을 설정하고, 설정된 정책을 전송하는 프로파일 서버; 및 상기 프로파일 서버로부터 상기 설정된 정책을 수신하고, 콘텐츠 접근 요청을 수신하고, 상기 접근 요청된 콘텐츠가 속하는 카테고리를 확인하며, 상기 확인된 카테고리가 상기 정책에 차단 설정된 카테고리와 일치하는지 결정하고, 상기 확인된 카테고리가 상기 정책에 포함된 카테고리와 일치하는 경우, 상기 접근 요청된 콘텐츠를 차단하는 제 1 사용자 기기를 포함하는 것을 특징으로 한다.

발명의 효과

[0008] 이상에서 살펴본 바와 같이 본 발명의 실시예에 따른 콘텐츠 차단 방법 및 시스템은 다양한 기준에 따라 설정된 정책에 의해 유해 콘텐츠가 차단되도록 설정할 수 있고, 사용자와의 피드백을 통해 적응적으로 유해 콘텐츠 정책을 업데이트함으로써 효과적으로 유해 콘텐츠를 필터링할 수 있다.

도면의 간단한 설명

[0009] 도 1은 본 발명의 일 실시예에 따른 콘텐츠 차단 시스템을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른 콘텐츠 차단 시스템의 흐름도이다.

도 3은 본 발명의 다른 실시예에 따른 콘텐츠 차단 시스템을 나타내는 도면이다.

도 4는 본 발명의 다른 실시예에 따른 콘텐츠 차단 시스템의 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 제 1 사용자 기기를 나타내는 블록 도면이다.

도 6은 본 발명의 일 실시예에 따른 프로파일 서버를 나타내는 블록 도면이다.

도 7은 본 발명의 일 실시예에 따른 제 2 사용자 기기를 나타내는 블록 도면이다.

8은 본 발명의 일 실시예에 따른 제 1 사용자 기기의 콘텐츠 차단 방법을 나타내는 흐름도이다.

9는 본 발명의 다른 실시예에 따른 제 1 사용자 기기의 콘텐츠 차단 방법을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0010] 본 발명의 실시예를 설명하기에 앞서, '제 1 사용자 기기'는 '제 2 사용자 기기(또는 관리자 기기)'의 관리하에 콘텐츠 접근이 제어되는 전자장치로 정의될 수 있다.

[0011] '제 2 사용자 기기'는 '제 1 사용자 기기'의 콘텐츠 접근을 제어하고, 적어도 하나의 '제 1 사용자 기기'를 그룹 별로 관리하기 위한 전자장치로 정의될 수 있으며, 관리자 기기로 혼용하여 설명한다.

[0012] '정책(policy)'은 적어도 하나의 콘텐츠가 속하는 카테고리에 대하여 차단 여부를 설정한 기준으로 정의될 수 있다.

[0013] 여기서 본 발명의 일 실시예에 따른 제 1 사용자 기기 및 제 2 사용자 기기(또는 관리자 기기)는 컴퓨팅 리소스를 가지는 장치로서 예를 들어, 스마트 폰 태블릿 PC, 디지털 카메라, 컴퓨터 모니터, PDA(Personal Digital Assistant), 전자수첩, 데스트탑 PC, PMP(Portable Multimedia Player), 미디어 플레이어(Media Player)(예를 들어, MP3 플레이어), 음향기기, 손목시계, 게임용 단말기 등을 포함할 수 있다.

[0014] 이하, 첨부된 도면들을 참조하여 다양한 실시예들을 상세히 설명한다. 이때, 첨부된 도면들에서 동일한 구성 요소는 가능한 동일한 부호로 나타내고 있음에 유의해야 한다. 또한 본 발명의 요지를 흐리게 할 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략할 것이다. 하기의 설명에서는 본 발명의 다양한 실시 예들에 따른 동작을 이해하는데 필요한 부분만이 설명되며, 그 이외 부분의 설명은 본 발명의 요지를 흩트리지 않도록 생략될 것이라는 것을 유의하여야 한다.

[0015] 도 1은 본 발명의 일 실시예에 따른 콘텐츠 차단 시스템을 나타내는 도면이다.

[0016] 도 1을 참조하면, 콘텐츠 차단 시스템(10)은 제 1 사용자 기기(100), 콘텐츠 분류 서버(110) 및 프로파일 서버(120)등을 포함할 수 있다.

[0017] 제 1 사용자 기기(100)는 사용자로부터 콘텐츠 접근(또는 접속) 요청 입력을 수신하고, 접근 요청되는 콘텐츠가 속하는 카테고리가 기본(default) 정책에 포함되는지 여부에 따라 접근 요청되는 콘텐츠를 차단하거나 허용할 수 있다. 보다 상세히 설명하면, 제 1 사용자 기기(100)는 접근 요청되는 콘텐츠가 속하는 카테고리를 확인하기 위하여, 콘텐츠 분류 서버(110)에 콘텐츠에 대한 정보를 전송할 수 있다. 제 1 사용자 기기(100)는 콘텐츠 분류 서버(110)로부터 콘텐츠가 속하는 카테고리를 확인하여, 콘텐츠가 속하는 카테고리가 정책에 포함된 카테고리와 일치하는지 확인할 수 있다. 제 1 사용자 기기(100)는 접근 요청되는 콘텐츠가 속하는 카테고리가 정책에 포함된 카테고리와 일치하는 것으로 확인되면, 접근 요청되는 콘텐츠를 차단할 수 있다. 반면, 제 1 사용자가 기기는 접근 요청되는 콘텐츠가 속하는 카테고리가 정책에 포함된 카테고리와 일치하지 않는 것으로 확인되면, 접근 요청되는 콘텐츠의 접근을 허용할 수 있다. 예를 들어, 사용자가 콘텐츠 접근을 위하여 특정 URL(Uniform Resource Locator)을 입력하는 경우, 제 1 사용자 기기(100)는 특정 URL에 대한 정보를 콘텐츠 분류 서버(110)로 전송할 수 있다. 제 1 사용자 기기(100)는 콘텐츠 분류 서버(110)로부터 특정 URL이 속하는 카테고리(예를 들어, 범죄 사이트 카테고리) 정보를 수신하고, 수신된 카테고리가 정책에 포함된 카테고리와 일치하는지 확인할 수 있다. 제 1 사용자 기기(100)는 카테고리가 정책에 포함된 카테고리와 일치하는 것으로 확인하면 특정 URL로의 접속을 차단할 수 있다. 반면, 제 1 사용자 기기(100)는 카테고리가 정책에 포함된 카테고리와 일치하지 않는 것으로 확인되면 특정 URL의 접속을 허용할 수 있다.

[0018] 또한, 제 1 사용자 기기(100)는 접근 요청되는 콘텐츠가 일정 기간 동안 차단된 기록이 있는 경우, 별도로 접근 요청되는 콘텐츠가 속하는 카테고리를 확인하지 않고 곧바로 접근 요청되는 콘텐츠를 차단할 수 있다. 예를 들어, 특정 URL에 대하여 차단한 기록이 있는 경우, 제 1 사용자 기기(100)는 사용자로부터 다시 특정 URL로의 접속이 요청되면 콘텐츠 분류 서버(110)를 통해 특정 URL이 속하는 카테고리를 확인하는 절차 없이, 특정 URL로의 접속을 차단할 수 있다. 이를 통해, 유해 콘텐츠를 신속하게 차단할 수 있다.

[0019] 콘텐츠 분류 서버(110)는 제 1 사용자 기기(100)로부터 콘텐츠에 대한 정보가 수신되면, 콘텐츠가 속하는 카테고리를 확인할 수 있다. 보다 상세히 설명하면, 콘텐츠 분류 서버(110)는 콘텐츠가 속하는 카테고리를 확인하기 위하여 컨텐츠 분류 데이터베이스(DB)를 검색할 수 있다. 예를 들어, 컨텐츠 분류 서버는 제 1 사용자 기기

(100)로부터 "www.XXX.com"에 대한 카테고리 확인 요청이 수신되면, 컨텐츠 분류 데이터베이스를 통해 "www.XXX.com"이 속하는 카테고리(예를 들어, 포털 사이트, 특정 종교 사이트, 도박 사이트 등)를 검색할 수 있다. 콘텐츠 분류 서버(110)는 검색을 통해 "www.XXX.com"이 속하는 카테고리를 확인하고, 확인된 카테고리 정보를 제 1 사용자 기기(100)로 전송할 수 있다.

[0020] 프로파일 서버(120)는 기본(default) 정책을 설정하고, 설정된 기본 정책을 제 1 사용자 기기(100)로 전송할 수 있다. 여기서 기본 정책은 설명의 편의상 제 2 사용자 기기(또는 관리자 기기)로부터 수정되지 않은 정책으로 정의하며, 제 2 사용자 기기에 의해 기본 정책이 수정되는 경우 수정 정책으로 정의한다. 본 발명의 일 실시예에 따른 프로파일 서버(120)는 다양한 특성을 반영하여 기본 정책을 설정할 수 있다. 보다 상세히 설명하면, 프로파일 서버(120)는 지역적 범위 예를 들어, 국가, 시, 도 등의 행정적 구역을 비롯하여 특정 문화적 특성을 반영한 문화적 지역 범위뿐만 아니라 제 1 사용자 기기(100) 사용자 및 제 2 사용자 기기 사용자의 연령, 성별, 직업 및 종교 등과 같은 세부적인 특성을 반영하여 기본 정책을 설정할 수 있다. 예를 들어, 프로파일 서버(120)는 제 1 사용자 기기(100)의 사용자가 속하는 문화적 환경에 따라 특정 종교(예를 들어, 이슬람교)를 기본 정책에 포함할지 결정할 수 있으며, 제 1 사용자 기기(100) 사용자의 연령(예를 들어, 미성년자)에 따라 술, 담배 카테고리 등을 기본 정책에 포함할지를 결정할 수 있다. 그리고, 프로파일 서버(120)는 기본 정책을 제 1 사용자 기기(100)로 전송할 수 있다. 제 1 사용자 기기(100)로 전송되는 기본 정책은 카테고리 별로 차단 여부가 표시된 리스트 형태로 제공될 수 있다.

[0021] 도 2는 본 발명의 일 실시예에 따른 콘텐츠 차단 시스템의 흐름도이다.

[0022] 도 2를 참조하면, 과정 201에서 프로파일 서버(120)는 제 1 사용자 기기(100)로 기본(default) 정책을 전송할 수 있다. 기본 정책은 카테고리 별로 차단 여부가 표시된 리스트 형태로 제공될 수 있다.

[0023] 한편, 도 2에서 도시되지는 않았지만, 과정 201 전에 제 1 사용자 기기(100)의 사용자는 본 발명의 실시예에 따른 콘텐츠 차단 서비스에 가입 또는 등록하기 위하여 제 1 사용자 기기(100)에 대한 정보, 제 1 사용자 기기(100) 사용자 정보 예를 들어, 사용자의 거주 지역, 연령 등을 프로파일 서버(120)에 전송할 수 있다.

[0024] 과정 203에서 제 1 사용자 기기(100)는 콘텐츠에 접근하기 위한 입력을 수신할 수 있다. 예를 들어, 제 1 사용자 기기(100)의 사용자는 특정 콘텐츠에 접근하기 위하여 애플리케이션, 인터넷 브라우저 등을 실행하고, 콘텐츠가 위치하는 파일 경로 또는 URL을 입력할 수 있다.

[0025] 과정 203에서 사용자로부터 콘텐츠로 접근하기 위한 입력이 수신되면, 과정 205에서 제 1 사용자 기기(100)는 콘텐츠의 카테고리를 확인하기 위하여 콘텐츠 분류 서버(110)로 콘텐츠 정보를 전송할 수 있다. 또는, 본 발명의 일 실시예에서 제 1 사용자 기기(100)는 접근 요청되는 콘텐츠가 일정 기간 내에 차단된 기록이 있는지 확인할 수 있다. 확인 결과 접근 요청되는 콘텐츠가 일정 기간 내에 차단된 기록이 있는 것으로 확인된 경우, 별도로 접근 요청되는 콘텐츠가 속하는 카테고리를 확인하지 않고 곧바로 접근 요청되는 콘텐츠를 차단할 수 있다. 반면, 접근 요청되는 콘텐츠가 일정 기간 내에 차단된 기록이 없는 것으로 확인되면 제 1 사용자 기기(100)는 콘텐츠 분류 서버(110)로 접근 요청된 콘텐츠 정보를 전송할 수 있다.

[0026] 과정 207에서 콘텐츠 분류 서버(110)는 제 1 사용자 기기(100)로부터 수신된 콘텐츠 정보에 기초하여, 접근 요청된 콘텐츠가 속하는 카테고리를 확인하고, 이를 제 1 사용자 기기(100)로 전송할 수 있다. 보다 상세히 설명하면, 콘텐츠 분류 서버(110)는 콘텐츠가 속하는 카테고리를 확인하기 위하여 콘텐츠 분류 데이터베이스(DB)를 검색할 수 있다. 콘텐츠 분류 서버(110)는 검색을 통해 접근 요청된 콘텐츠가 속하는 카테고리를 확인하고, 확인된 카테고리를 제 1 사용자 기기(100)로 전송할 수 있다.

[0027] 과정 209에서 제 1 사용자 기기(100)는 콘텐츠 분류 서버(110)로부터 접근 요청된 콘텐츠가 속하는 카테고리 정보를 수신하여, 접근 요청된 콘텐츠의 차단 여부를 결정할 수 있다. 보다 상세히 설명하면, 제 1 사용자 기기(100)는 접근 요청된 콘텐츠가 속하는 카테고리가 기본 정책 내에 차단 설정된 카테고리와 일치하는지 여부로 접근 요청된 콘텐츠의 차단 여부를 결정할 수 있다.

[0028] 과정 211에서 제 1 사용자 기기(100)는 접근 요청된 콘텐츠를 차단 또는 접근을 허용할 수 있다. 보다 상세히 설명하면, 접근 요청된 콘텐츠가 속하는 카테고리가 기본 정책 내에 차단 설정된 카테고리와 일치하는 경우 접근 요청된 콘텐츠를 차단할 수 있다. 예를 들어, 접근 요청된 콘텐츠가 위치하는 URL이 마약 카테고리에 속하는 것으로 확인되고, 기본 정책에 마약 카테고리가 차단 설정된 경우, 제 1 사용자 기기(100)는 접근 요청된 콘텐츠를 차단할 수 있다. 다른 예를 들면, 접근 요청되는 콘텐츠가 위치하는 경로가 회사 비밀 카테고리에 속하는 것으로 확인되고, 기본 정책에 회사 비밀 카테고리가 차단 설정되어 있는 경우, 제 1 사용자 기기(100)는 접근

요청된 콘텐츠를 차단할 수 있다. 다만, 이는 예시에 불과하다. 다시 말하면, 제 1 사용자 기기(100) 마다 프로파일 서버(120)로부터 제공되는 기본 정책이 달라질 수 있으므로, 제 1 사용자 기기(100)에 의한 콘텐츠의 차단 여부도 달라질 수 있다. 예를 들어, 제 1 사용자 기기(100)의 사용자가 의사 등과 같이 환자 진료를 위해 마약이 필요한 사람인 경우, 프로파일 서버(120)로부터 제공되는 기본 정책에 마약 카테고리가 접근 허용으로 설정될 수 있다. 이에 따라, 제 1 사용자 기기(100)를 통해 접근 요청된 콘텐츠가 위치하는 URL이 마약 카테고리에 속하더라도 제 1 사용자 기기(100)는 콘텐츠 접근을 허용할 수 있다. 반면, 제 1 사용자 기기(100)는 접근 요청된 콘텐츠가 속하는 카테고리가 기본 정책 내에 차단 설정된 카테고리와 일치하지 않는 경우 접근 요청된 콘텐츠의 접근을 허용할 수 있다.

[0029] 도 3은 본 발명의 다른 실시예에 따른 콘텐츠 차단 시스템을 나타내는 도면이다.

[0030] 도 3을 참조하면, 콘텐츠 차단 시스템(10)은 제 1 사용자 기기(100), 콘텐츠 분류 제공 서버, 프로파일 서버(120) 및 제 2 사용자 기기(130)(또는 관리자 기기) 등을 포함할 수 있다.

[0031] 제 1 사용자 기기(100)는 사용자로부터 콘텐츠 접근 요청 입력을 수신하고, 접근 요청되는 콘텐츠가 속하는 카테고리가 수정 정책에 포함되는지 여부에 따라 접근 요청되는 콘텐츠를 차단하거나 허용할 수 있다. 여기서 수정 정책은 프로파일 서버(120)에서 설정된 기본 정책이 제 2 사용자 기기(130)에 의해 수정된 정책으로 정의될 수 있다. 그리고, 제 1 사용자 기기(100)는 콘텐츠 분류 서버(110)로부터 콘텐츠가 속하는 카테고리를 확인하여, 콘텐츠가 속하는 카테고리가 수정 정책에 포함되는지 결정할 수 있다. 제 1 사용자 기기(100)는 접근 요청되는 콘텐츠가 속하는 카테고리가 수정 정책에 포함된 카테고리와 일치하는 것으로 확인되면, 접근 요청되는 콘텐츠를 차단할 수 있다. 반면, 제 1 사용자가 기기는 접근 요청되는 콘텐츠가 속하는 카테고리가 정책에 포함된 카테고리와 일치하지 않는 것으로 확인되면, 접근 요청되는 콘텐츠의 접근을 허용할 수 있다. 또한, 제 1 사용자 기기(100)는 접근 요청되는 콘텐츠가 일정 기간 동안 차단된 기록이 있는 경우, 별도로 접근 요청되는 콘텐츠가 속하는 카테고리를 확인하지 않고 곧바로 접근 요청되는 콘텐츠를 차단할 수 있다.

[0032] 본 발명의 일 실시예에 따른 제 1 사용자 기기(100)는 수정 정책에 차단 설정되어 있는 카테고리에 속하는 콘텐츠에 대한 차단 설정 해제를 요청함으로써, 콘텐츠에 접근할 수 있다. 보다 상세히 설명하면, 제 1 사용자 기기(100)의 사용자는 기본 정책 또는 수정 정책에 차단 설정된 카테고리에 해당하는 콘텐츠 또는 일정 기간 이내에 차단된 기록이 있는 콘텐츠에 접근을 원하는 경우가 있다. 이러한 경우 제 1 사용자 기기(100)는 프로파일 서버(120)를 통해 제 2 사용자 기기(130)(또는 관리자 기기)에 해당 콘텐츠에 대한 차단 설정 해제를 요청할 수 있다. 그리고, 제 2 사용자 기기(130)로부터 차단 설정된 콘텐츠에 대한 차단 해제가 허락되고, 프로파일 서버(120)로부터 기본 정책을 수정한 정책이나 수정 정책을 수정한 재수정 정책을 수신하거나 또는 차단 설정 해제 요청된 콘텐츠 및 콘텐츠가 속하는 카테고리에 대한 해제 정보가 수신되면, 제 1 사용자 기기(100)는 차단 설정되었던 콘텐츠에 대한 차단을 해제하고, 콘텐츠로의 접근을 허용할 수 있다. 반면, 제 2 사용자 기기(130)로부터 차단 설정된 콘텐츠에 대한 차단 해제가 거절된 경우에는 제 1 사용자 기기(100)는 차단 설정된 콘텐츠에 대한 차단 설정을 유지할 수 있다.

[0033] 한편, 차단 설정된 콘텐츠에 대하여 일정 기간 이내에 차단된 기록이 있는 경우, 제 1 사용자 기기(100)로부터의 차단 해제 요청은 자동적으로 수행될 수 있다. 다시 말하면, 제 1 사용자 기기(100)가 콘텐츠 접근 입력을 수신한 후, 일정 기간 이내에 차단된 기록이 있어 접근 요청된 콘텐츠를 차단하는 경우, 제 1 사용자 기기(100)는 자동적으로 프로파일 서버(120)를 통해 제 2 사용자 기기(130)로 차단 해제 요청을 전송할 수 있다.

[0034] 콘텐츠 분류 서버(110)는 제 1 사용자 기기(100)로부터 콘텐츠에 대한 정보가 수신되면, 콘텐츠가 속하는 카테고리를 확인할 수 있다. 보다 상세히 설명하면, 콘텐츠 분류 서버(110)는 콘텐츠가 속하는 카테고리를 확인하기 위하여 콘텐츠 분류 데이터베이스(DB)를 검색할 수 있다. 콘텐츠 분류 서버(110)는 검색을 통해 접근 요청된 콘텐츠가 속하는 카테고리를 확인하고, 확인된 카테고리를 제 1 사용자 기기(100)로 전송할 수 있다.

[0035] 프로파일 서버(120)는 기본(default) 정책을 설정하고, 설정된 기본 정책을 제 2 사용자 기기(130)로 전송할 수 있다. 그리고, 프로파일 서버(120)는 제 2 사용자 기기(130)로부터 기본 정책이 수정된 수정 정책을 수신하여, 제 1 사용자 기기(100)로 전송할 수 있다. 본 발명의 일 실시예에 따른 프로파일 서버(120)는 기본 정책 또는 수정 정책에 차단 설정된 카테고리 또는 차단 해제를 요청한 특정 콘텐츠에 대하여 제 2 사용자 기기(130)에 의하여 차단 해제가 허락된 경우, 차단 해제가 허락된 카테고리 또는 차단 해제가 허락된 콘텐츠에 대한 정보를 화이트 리스트(white list)에 저장할 수 있다. 그리고, 프로파일 서버(120)는 차단 해제가 허락된 카테고리 또는 차단 해제가 허락된 콘텐츠에 대한 접근이 허용되도록 제 1 사용자 기기(100)로 전송하였던 기본 정책을 수정하거나 수정 정책을 재수정하여 제 1 사용자 기기(100)로 전송할 수 있다. 또는, 실시예에 따라, 프로파일 서

버(120)는 차단 설정 해제 요청된 콘텐츠 및 콘텐츠가 속하는 카테고리에 대한 해제 정보를 제 1 사용자 기기(100)로 전송할 수도 있다.

[0036] 프로파일 서버(120)는 일정 기간 화이트 리스트에 저장된 차단 해제가 허락된 콘텐츠 정보 또는 차단 해제가 허락된 콘텐츠가 속하는 카테고리에 대한 정보에 기초하여, 기본 정책을 업데이트할 수 있다. 보다 상세히 설명하면, 기본 정책에 유해 사이트로 지정되어 차단 설정된 카테고리라도 일정 기간 동안 제 2 사용자 기기(130)에 의해 차단 해제가 허락된 횟수가 임계 횟수 이거나, 다른 카테고리와 비교하여 차단 해제가 허락된 횟수가 평균값 이상인 경우, 프로파일 서버(120)는 차단 설정된 카테고리에 대한 차단 설정을 해제하도록 기본 정책을 변경할 수 있다. 또한, 일 실시예에서 프로파일 서버(120)는 차단 해제가 허락된 콘텐츠가 속하는 카테고리에 대한 차단 설정을 유지하고, 차단 해제가 허락된 콘텐츠를 별도의 카테고리로 추가하는 설정을 할 수도 있다. 예를 들어, 차단 해제가 요청된 콘텐츠가 위치하는 URL "www.yyy.com"이 마약 카테고리에 속하고, "www.yyy.com"에 대하여 차단 해제가 허락된 경우, 프로파일 서버(120)는 기본 정책 내에서 마약 카테고리에 대한 차단 설정을 유지하고, "www.yyy.com" 을 별도의 카테고리로 추가할 수도 있다.

[0037] 또한, 프로파일 서버(120)는 제 2 사용자 기기(130)에 의해 기본 정책의 적어도 하나의 차단 설정된 카테고리에 대한 차단 설정을 차단 해제 설정으로 변경하는 수정 정책을 수신한 경우에도 차단 해제 설정으로 변경되는 카테고리에 대한 정보를 화이트 리스트에 저장할 수 있다. 그리고, 프로파일 서버(120)는 차단 해제가 허락된 콘텐츠에 대한 경우와 마찬가지로, 일정 기간 누적된 통계에 기초하여 프로파일 서버(120)는 차단 설정된 카테고리에 대한 차단 설정을 해제하도록 기본 정책을 변경할 수 있다.

[0038] 그리고, 프로파일 서버(120)는 차단 설정되지 않은 카테고리에 대하여 제 2 사용자 기기(130)로부터 차단 설정으로 변경하는 수정 정책을 수신한 경우, 차단 설정으로 변경되는 콘텐츠에 대한 정보를 블랙 리스트(black list)에 저장할 수 있다. 프로파일 서버(120)는 일정 기간 제 2 사용자 기기(130)에 의해 차단 설정으로 변경된 횟수가 임계 횟수이거나, 다른 카테고리와 비교하여 차단 설정으로 변경된 횟수가 평균값 이상인 경우, 프로파일 서버(120)는 카테고리에 대하여 차단을 설정하도록 기본 정책을 변경할 수 있다. 이와 같이, 프로파일 서버(120)는 일정 기간 동안 제 1 사용자 기기(100) 또는 제 2 사용자 기기(130)에 기초하여, 기본 정책 또는 수정 정책에 차단 설정이 변경된 경우 이를 반영하여 기본 정책을 업데이트할 수 있다. 이를 통해, 프로파일 서버(120)는 시간의 흐름에 따른 유해 사이트에 대한 기준 변경에 적응적으로 대처할 수 있다. 그리고, 프로파일 서버(120)는 제 2 사용자 기기(130)에 의해 제 1 사용자 기기(100)를 그룹 별로 관리하는 경우, 그룹 별로 분류된 기본 정책을 저장할 수 있다.

[0039] 제 2 사용자 기기(130)는 제 1 사용자 기기(100)를 관리하기 위하여 프로파일 서버(120)로부터 기본 정책이 수신되면, 수신된 기본 정책을 수정한 수정 정책을 설정할 수 있다. 보다 상세히 설명하면, 제 2 사용자 기기(130)는 프로파일 서버(120)로부터 기본 정책이 수신되면, 기본 정책을 모니터링하여 기본 정책에 대하여 차단 설정된 카테고리를 변경하여 수정 정책을 설정할 수 있다. 예를 들어, 제 2 사용자 기기(130)는 카테고리에 대한 차단 설정이 리스트로 형태로 제공되는 기본 정책을 출력하고, 출력된 리스트 상에서 차단 설정을 변경할 수 있다. 즉, 속옷 카테고리에 대하여 리스트 상에 차단 설정되어 있는 경우, 차단 설정을 해제할 수 있으며, 종교 카테고리에 대하여 차단이 설정되지 않은 경우 차단 설정으로 변경할 수 있다.

[0040] 또한, 제 2 사용자 기기(130)는 제 1 사용자 기기(100)로부터 프로파일 서버(120)를 통해 차단 해제 요청이 수신되면, 이를 모니터링하고, 차단 해제가 요청되는 콘텐츠 또는 콘텐츠가 속하는 카테고리에 대하여 차단 해제를 허락하거나 거절할 수 있다.

[0041] 본 발명의 일 실시예에 따른 제 2 사용자 기기(130)는 적어도 하나의 제 1 사용자 기기(100)를 관리하기 위하여, 그룹 별로 제 1 사용자 기기(100)를 분류하여 관리할 수 있다. 보다 상세히 설명하면, 제 2 사용자 기기(130)는 적어도 하나의 제 1 사용자 기기(100)를 가정, 회사, 특정 모임 등 다양한 그룹으로 분류하고, 분류된 그룹 별로 관리할 수 있다. 예를 들어, 제 2 사용자 기기(130)는 적어도 하나의 제 1 사용자 기기(100)를 가정 그룹으로 분류하고, 가정 그룹에 적응적으로 기본 정책을 수정할 수 있다. 또한, 제 2 사용자 기기(130)는 다른 적어도 하나의 제 1 사용자 기기(100)를 회사 그룹으로 분류하고, 회사 그룹에 적응적으로 기본 정책을 수정한 수정 정책을 설정할 수 있다. 예를 들어, 적어도 하나의 제 1 사용자 기기(100)가 회사 그룹으로 분류되면, 회사 그룹에 대하여 특정 동영상이 속하는 카테고리를 차단 설정하는 수정 정책을 설정할 수 있다.

[0042] 도 4는 본 발명의 다른 실시예에 따른 콘텐츠 차단 시스템의 흐름도이다.

[0043] 도 4를 참조하면, 과정 401에서 프로파일 서버(120)는 기본 정책을 제 2 사용자 기기(130)로 전송할 수 있다.

그리고, 과정 403에서 제 2 사용자 기기(130)는 기본 정책을 수정하여 수정 정책을 설정하고, 수정 정책을 프로파일 서버(120)로 전송할 수 있다. 프로파일 서버(120)는 제 2 사용자 기기(130)로부터 수정 정책이 수정되면, 기본 정책으로부터 차단 설정이 변경된 카테고리 정보를 저장하고, 과정 405에서 수정 정책을 제 1 사용자 기기(100)로 전송할 수 있다. 다만, 과정 401 및 403은 생략될 수 있다. 이러한 경우, 과정 405에서 프로파일 서버(120)는 기본 정책을 제 1 사용자 기기(100)로 전송할 수 있다.

[0044] 과정 407에서 제 1 사용자 기기(100)는 차단 설정된 콘텐츠에 대한 해제를 요청할 수 있다. 보다 상세히 설명하면, 제 1 사용자 기기(100)는 프로파일 서버(120)로 차단 설정된 콘텐츠에 대한 해제를 요청하기 위한 정보를 전송할 수 있다. 그리고, 프로파일 서버(120)로 차단 설정된 콘텐츠에 대한 해제 요청은 사용자가 제 1 사용자 기기(100)로 해제 요청을 입력한 경우뿐만 아니라, 제 1 사용자 기기(100)에 의해 자동적으로 수행될 수도 있다. 다시 말하면, 제 1 사용자 기기(100)는 접근 요청된 콘텐츠가 속하는 카테고리에 대한 정보를 콘텐츠 분류 서버(110)로 전송하고, 확인된 카테고리가 수정 정책에 차단 설정된 카테고리인 경우, 접근 요청된 콘텐츠를 차단할 수 있다. 또는 일정 기간 이내에 차단된 기록이 있는 콘텐츠에 대하여 다시 접근 요청되면 제 1 사용자 기기(100)는 접근 요청된 콘텐츠를 차단할 수 있다. 이와 같이, 제 1 사용자 기기(100)에서 접근 요청이 차단된 경우, 제 1 사용자 기기(100)는 프로파일 서버(120)로 차단 설정된 콘텐츠에 대한 차단 해제 요청 정보를 전송할 수 있다. 과정 409에서 프로파일 서버(120)는 제 1 사용자 기기(100)로부터 수신된 차단 해제 요청 정보를 제 2 사용자 기기(130)로 전송할 수 있다.

[0045] 과정 411에서 제 2 사용자 기기(130)는 차단 요청된 콘텐츠 또는 차단 요청된 콘텐츠가 속하는 카테고리에 대하여 차단 여부를 결정할 수 있다. 과정 411에서 제 2 사용자 기기(130)에 의해 차단 설정된 콘텐츠 또는 차단 요청된 콘텐츠가 속하는 카테고리에 대한 차단 해제를 허락하는 경우 과정 413에서 제 2 사용자 기기(130)는 차단 설정된 콘텐츠 또는 차단 요청된 콘텐츠가 속하는 카테고리에 대한 차단 해제에 대한 정보를 프로파일 서버(120)로 전송할 수 있다.

[0046] 과정 415에서 프로파일 서버(120)는 제 2 사용자 기기(130)로부터 수신된 차단 설정된 콘텐츠 또는 차단 요청된 콘텐츠가 속하는 카테고리에 대한 차단 해제에 대한 정보를 화이트 리스트로 저장할 수 있다. 프로파일 서버(120)는 화이트 리스트에 일정 기간 동안 저장된 차단 설정된 콘텐츠 또는 차단 요청된 콘텐츠가 속하는 카테고리에 차단 해제 정보 예를 들어, 차단 해제가 허락된 콘텐츠 및 차단 해제가 허락된 콘텐츠의 차단 해제 허락 횟수, 차단 해제가 허락된 콘텐츠가 속하는 카테고리 및 차단 해제가 허락된 콘텐츠가 속하는 카테고리에 대한 차단 해제 허락 횟수에 기초하여, 기본 정책 또는 수정 정책을 업데이트할 수 있다. 과정 417에서는 프로파일 서버(120)는 수정 정책을 재수정한 재수정 정책 또는 과정 401 및 과정 403이 생략되어 프로파일 서버(120)로부터 제 1 사용자 기기(100)로 기본 정책이 전송되었던 경우 기본 정책이 수정된 수정 정책을 제 1 사용자 기기(100)로 전송할 수 있다. 이에 따라, 제 1 사용자 기기(100)는 차단 설정되었던 콘텐츠 또는 콘텐츠가 속하는 카테고리에 대한 접근을 허용할 수 있다.

[0047] 한편, 과정 411에서 제 2 사용자 기기(130)에 의해 차단 설정된 콘텐츠 또는 차단 요청된 콘텐츠가 속하는 카테고리에 대한 차단 해제를 거절하는 경우, 과정 419에서 제 2 사용자 기기(130)는 차단 해제를 거절하는 정보를 프로파일 서버(120)로 전송할 수 있다. 과정 421에서 프로파일 서버(120)는 차단 설정된 콘텐츠 및 차단 설정된 콘텐츠가 속하는 카테고리에 대한 차단 설정을 유지한다는 정보를 제 1 사용자 기기(100)로 전송할 수 있다. 이에 따라, 제 1 사용자 기기(100)는 차단 해제 요청된 콘텐츠에 대한 차단을 유지할 수 있다. 그리고, 제 1 사용자 기기(100)는 차단 해제 요청된 콘텐츠에 대한 차단 해제가 거절되었음을 알리는 정보를 출력할 수 있다.

[0048] 도 5는 본 발명의 일 실시예에 따른 제 1 사용자 기기를 나타내는 블록 도면이다. 여기서, 501은 제 1 사용자 기기를 나타내는 블록 도면을 나타내고, 503은 제 1 사용자 기기의 제어부(560)를 나타내는 도면이다.

[0049] 도 5를 참조하면, 제 1 사용자 기기는 무선 통신부(510), 터치 스크린(520), 입력부(530), 오디오 처리부(540), 저장부(550) 및 제어부(560) 등을 포함할 수 있다.

[0050] 무선 통신부(510)는 제 1 사용자 기기가 통신 기능을 지원하는 전자 장치인 경우 추가될 수 있는 구성으로서, 제 1 사용자 기기가 통신 기능을 지원하지 않는 경우 생략될 수도 있다. 무선 통신부(510)는 제어부(560)의 제어 하에 지원 가능한 네트워크(이동통신 네트워크 등)와 설정된 방식의 통신 채널을 형성하여 음성 통신, 영상 통신 등의 무선 통신과 단문 메시지 서비스(SMS, Short Message Service), 멀티미디어 메시지 서비스(MMS, Multimedia Messaging Service), 인터넷(internet) 등의 메시지 서비스 기반의 데이터 통신과 관련된 신호를 송수신할 수 있다. 또한, 무선 통신부(510)는 송신되는 신호의 주파수를 상승변환 및 증폭하고, 수신되는 신호의 주파수를 저잡음 증폭 및 하강 변환하는 송수신기를 포함할 수 있다. 무선 통신부(510)는 제어부(560) 제어

하에 메시지 서비스를 위한 데이터 통신 채널을 형성하여 메시지 서비스 기반의 데이터 송수신을 처리할 수 있다. 여기서 통신 채널은 CDMA(Code Division Multiple Access), TDMA(Time Division Multiple Access), OFDMA(Orthogonal Frequency-Division Multiple Access) 등의 이동통신채널과 유선 인터넷 네트워크, 무선 인터넷 네트워크 등과 같은 방식의 인터넷 통신 채널을 포함할 수 있다.

[0051] 본 발명의 일 실시예에서 무선 통신부(510)는 접근 요청된 콘텐츠가 속하는 카테고리를 확인하기 위하여 접근 요청된 콘텐츠에 대한 정보를 콘텐츠 분류 서버로 전송할 수 있다. 그리고, 무선 통신부(510)는 콘텐츠 분류 서버로부터 접근 요청된 콘텐츠가 속하는 카테고리에 대한 정보를 수신할 수 있다. 무선 통신부(510)는 접근 요청된 콘텐츠가 속하는 카테고리가 기본 정책 또는 수정 정책에 차단 설정되지 않은 카테고리에 해당되는 경우, 콘텐츠로 접근할 수 있도록 콘텐츠가 위치하는 파일 경로 및 URL로 접속하기 위한 정보를 송신할 수 있다. 그리고, 무선 통신부(510)는 프로파일 서버로 차단 설정된 콘텐츠에 대하여 해제 요청 정보를 전송하고, 프로파일 서버로부터 기본 정책, 수정 정책을 비롯하여 해제 요청 허락 정보 및 차단 설정 유지 정보를 수신할 수 있다.

[0052] 터치 스크린(520)은 제 1 사용자 기기 운용에 필요한 다양한 화면을 제공할 수 있다. 예를 들어, 터치 스크린(520)은 제 1 사용자 기기 운용에 필요한 대기 화면, 메뉴 화면 및 애플리케이션 실행 화면 등을 지원할 수 있다. 이러한 터치 스크린(520)은 터치 패널(521) 및 표시 패널(523)을 포함할 수 있다. 터치 패널(521)은 표시 패널(523) 위에 위치하는 애드 온 타입(add-on type)이나 표시 패널(523) 내에 삽입되는 인 셀 타입(in-cell type)으로 구현될 수 있다.

[0053] 터치 패널(521)은 화면에 대한 사용자의 터치 제스처에 응답하여 터치 이벤트를 발생하고, 터치 이벤트를 AD(Analog to Digital) 변환하여 제어부(560)로 전달할 수 있다.

[0054] 표시 패널(523)은 제어부(560)의 제어 하에 데이터를 화면에 표시할 수 있다. 예를 들어, 제어부(560)가 데이터를 처리(예를 들어, 디코딩(decoding))하여 버퍼에 저장하면 표시 패널(523)은 버퍼에 저장된 데이터를 아날로그 신호로 변환하여 화면에 표시할 수 있다. 표시 패널(523)은 제어부(560) 제어 하에 휴대형 전자장치의 이용에 따른 다양한 화면 예를 들어, 잠금 화면, 홈(home) 화면, 애플리케이션 실행 화면, 메뉴 화면, 키패드 화면, 메시지 작성 화면 및 인터넷 화면 등을 표시할 수 있다.

[0055] 이와 같은 표시 패널(523)은 액정 표시 장치(Liquid Crystal Display; LCD), AMOLED(Active Matrix Organic Light Emitted Diode), PMOLED(Passive Matrix Organic Light Emitted Diode), 플랙서블 디스플레이(Flexible display) 또는 투명 디스플레이로 구성될 수 있다.

[0056] 입력부(530)는 제 1 사용자 기기 운용에 필요한 다양한 입력 신호를 생성하는 구성이다. 이러한 입력부(530)는 제 1 사용자 기기의 호환 가능 여부에 따라 키보드나 키패드, 키버튼 등의 다양한 입력 수단을 포함할 수 있다. 또한 입력부(530)는 터치스크린에 출력되는 터치 맵 형태로 구성될 수도 있다.

[0057] 오디오 처리부(540)는 제 1 사용자 기기의 운용과정에서 설정된 다양한 오디오 데이터 및 저장부(550)에 저장된 오디오 파일 재생에 따른 오디오 데이터, 외부로부터 수신되는 오디오 데이터 등을 출력할 수 있다. 본 발명의 일 실시예에서, 오디오 처리부(540)는 접근 요청한 콘텐츠에 대하여 차단되거나 차단 해제 요청이 거절되는 경우 이에 해당하는 알림음 또는 효과음을 출력할 수 있다.

[0058] 저장부(550)는 제어부(560)의 보조 기억 장치(secondary memory unit)로써, 디스크, 램(RAM) 및 플래쉬 메모리를 포함할 수 있다. 저장부(550)는 제어부(560) 제어 하에 제 1 사용자 기기에서 생성되거나 무선 통신부(510) 또는 외부 인터페이스부(미도시)를 통해 외부 장치 예를 들어, 서버, 데스크 탑 PC 등으로부터 수신한 데이터를 저장할 수 있다. 또한, 저장부(550)는 다양한 데이터 예를 들어, 동영상 데이터, 게임 데이터, 음악 데이터, 영화 데이터, 지도 데이터 등을 저장할 수 있다. 본 발명의 일 실시예에서 저장부(550)는 프로파일 서버로부터 수신되는 기본 정책 및 수정 정책을 저장할 수 있다. 또한 저장부(550)는 일정 기간 이내 차단된 콘텐츠를 기록하기 위하여 캐시(cache)를 포함할 수 있다.

[0059] 제어부(560)는 제 1 사용자 기기의 전반적인 동작 및 제 1 사용자 기기의 내부 구성들 간의 신호 흐름을 제어하고, 데이터를 처리하는 기능을 수행할 수 있다. 예를 들어, 제어부(560)는 중앙 처리 장치(Central Processing Unit; CPU), 애플리케이션 프로세서(Application Processor; AP) 등으로 구성될 수 있다. 또한, 제어부(560)는 싱글 코어 프로세어(single core processor) 또는 멀티 코어 프로세서(multi-core processor)로 구성될 수 있다.

[0060] 503을 참조하면, 본 발명의 일 실시예에 따른 제어부(560)는 필터링 모듈(561) 및 판단 모듈(563) 등을 포함할

수 있다. 필터링 모듈(561)은 접근 요청된 콘텐츠가 속하는 카테고리가 기본 정책 또는 수정 정책에 차단 설정된 카테고리인 경우, 접근 요청된 콘텐츠를 차단할 수 있다. 또한, 필터링 모듈(561)은 일정 기간 이내에 차단된 기록이 있는 콘텐츠에 대하여 접근이 요청된 경우에는 접근 요청된 콘텐츠가 속하는 카테고리를 확인하지 않고 곧바로 차단할 수 있다. 도 503에서 필터링 모듈(561)은 제어부(560)에 포함된 것으로 도시하였으나, 별도의 모듈로서 구성될 수도 있다. 이러한 필터링 모듈(561)은 필터링 모듈(561)을 통과하는 패킷에 포함되어 있는 헤더 파일 및 실제 데이터 내용에 기초하여, 접근 요청된 콘텐츠가 위치하는 파일 경로 또는 URL로의 접속을 차단할 수 있다.

[0061] 판단 모듈(563)은 접근 요청된 콘텐츠가 속하는 카테고리가 기본 정책 또는 수정 정책에 차단 설정된 카테고리와 일치하는지 판단할 수 있다. 보다 상세히 설명하면, 사용자로부터 입력부(530) 등을 통해 콘텐츠에 접근하기 위한 입력이 수신되면 필터링 모듈(561)은 이에 대한 정보를 판단 모듈(563)로 전달하고, 판단 모듈(563)은 접근 요청한 콘텐츠가 속하는 카테고리를 확인하기 위하여 콘텐츠 분류 서버로 수신된 입력 정보를 전송하도록 제어할 수 있다. 판단 모듈(563)은 콘텐츠 분류 서버로부터 접근 요청된 콘텐츠가 속하는 카테고리 및 기본 정책 또는 수정 정책을 비교하여, 일치 여부를 확인할 수 있다. 판단 모듈(563)은 접근 요청된 콘텐츠가 속하는 카테고리가 기본 정책 또는 수정 정책과 일치하는 것으로 확인되면, 접근 요청된 콘텐츠를 차단하기 위한 정보를 필터링 모듈(561)로 전달할 수 있다. 그리고, 판단 모듈(563)은 접근 요청된 콘텐츠에 대한 차단 해제 요청이 있는 경우, 차단 해제 요청 정보를 프로파일 서버로 전송하도록 결정할 수 있다. 또한, 판단 모듈(563)은 프로파일 서버로부터 차단 해제 요청된 콘텐츠에 대하여 차단 해제 허락에 대한 정보를 수신하는 경우, 콘텐츠 접근을 허용하기 위한 정보를 필터링 모듈(561)로 전달할 수 있다. 반면, 판단 모듈(563)은 프로파일 서버로부터 차단 해제 요청 거절에 대한 정보를 수신한 경우, 차단 해제 요청된 콘텐츠를 차단하기 위한 정보를 필터링 모듈(561)로 전달할 수 있다.

[0062] 도 6은 본 발명의 일 실시예에 따른 프로파일 서버를 나타내는 블록 도면이다. 도 6에서는 프로파일 서버(120) 및 프로파일 데이터베이스(620)(database)를 별도로 도시하였지만, 프로파일 데이터베이스(620)가 프로파일 서버(120) 내에 통합되어 구성될 수도 있다. 도 6을 참조하면, 프로파일 서버(120)는 제어 모듈(121) 및 통계 모듈(123) 등을 포함할 수 있다.

[0063] 제어 모듈(121)은 프로파일 서버(120)의 전반적인 동작 및 프로파일 서버(120)의 내부 구성들 간의 신호 흐름을 제어하고, 데이터를 처리하는 기능을 수행할 수 있다. 본 발명의 일 실시예에서 제어 모듈(121)은 기본 정책을 설정 및 관리할 수 있다. 보다 상세히 설명하면 제어 모듈(121)은 다양한 특성을 반영하여 기본 정책을 설정할 수 있다. 보다 상세히 설명하면, 프로파일 서버(120)는 지역적 범위 예를 들어, 국가, 시, 도 등의 행정적 구역을 비롯하여 특정 문화적 특성을 반영한 문화적 지역 범위뿐만 아니라 제 1 사용자 기기 사용자 및 제 2 사용자 기기 사용자의 연령, 성별, 직업 및 종교 등과 같은 세부적인 특성을 반영하여 기본 정책을 설정할 수 있다.

[0064] 그리고, 제어 모듈(121)은 그룹 별로 기본 정책을 설정할 수 있다. 보다 상세히 설명하면 제어 모듈(121)은 제 2 사용자 기기에 의해 적어도 하나의 제 1 사용자 기기가 그룹 별로 관리되는 경우, 그룹 별로 분류하여 기본 정책을 설정하도록 제어할 수 있다. 또한, 제어 모듈(121)은 제 1 사용자 기기 및 제 2 사용자 기기 간의 정보 흐름을 제어할 수 있다. 예를 들어, 제어 모듈(121)은 프로파일 서버(120)의 통신부를 통해 제 1 사용자 기기로 기본 정책을 전송하고, 제 1 사용자 기기로부터 차단 해제 요청 정보를 수신하여 제 2 사용자 기기로 전송하도록 제어할 수 있다. 또한, 제어 모듈(121)은 제 2 사용자 기기로 기본 정책을 전송하고, 수정 정책을 수신할 수 있다. 이러한 기본 정책 및 수정 정책은 프로파일 데이터베이스(620)의 정책 데이터베이스(621)에 저장될 수 있다.

[0065] 통계 모듈(123)은 기본 정책을 업데이트할 수 있다. 보다 상세히 설명하면, 통계 모듈(123)은 일정 기간 화이트 리스트(623)(white list) 또는 블랙 리스트(625)(black list) 등에 기초하여, 기본 정책을 업데이트할 수 있다. 여기서, 화이트 리스트(623)는 제 2 사용자 기기로부터 차단 해제가 허락된 콘텐츠 또는 콘텐츠가 속하는 카테고리에 대한 정보, 그리고 제 2 사용자 기기로부터 수신된 수정 정책에 따라 차단 설정이 허용되는 것으로 설정이 변경된 카테고리에 대한 정보 등을 저장할 수 있다. 그리고, 블랙 리스트(625)는 제 2 사용자 기기로부터 수정 정책에 따라 접근이 허용되는 것으로 설정된 카테고리가 차단되는 것으로 설정이 변경된 카테고리에 대한 정보 및 제 2 사용자 기기로부터 별도로 차단 설정이 요청된 카테고리에 대한 정보 등을 저장할 수 있다. 통계 모듈(123)은 일정 기간 동안 차단 설정이 변경된 특정 카테고리에 대하여 차단 설정이 변경 횟수를 다른 카테고리들과 비교함으로써 기본 정책에 이를 반영하고, 기본 정책을 업데이트할 수 있다.

[0066] 도 7은 본 발명의 일 실시예에 따른 제 2 사용자 기기를 나타내는 블록 도면이다.

[0067] 도 7을 참조하면, 제 2 사용자 기기는 무선 통신부(710), 터치 스크린(720), 입력부(730), 오디오 처리부(740), 저장부(750) 및 제어부(760) 등을 포함할 수 있다. 제 2 사용자 기기의 제 1 사용자 기기와 중복되는 기능은 생략한다.

[0068] 무선 통신부(710)는 제어부(760) 제어 하에 프로파일 서버로부터 기본 정책을 수신하고, 수정 정책을 전송할 수 있다. 그리고, 터치 스크린(720)은 터치 패널(721) 및 표시 패널(723)을 포함할 수 있다. 본 발명의 일 실시예에 따른 터치 스크린(720)은 제어부(760) 제어 하에 기본 정책을 수정하기 위하여, 차단 설정 또는 접근 허용 설정된 카테고리가 리스트 형태의 기본 정책을 표시할 수 있다. 예를 들어, 터치 스크린(720)은 적어도 하나의 콘텐츠 카테고리 정보 및 카테고리 정보에 대하여 차단 설정 여부를 체크하기 위한 박스 등을 표시할 수 있다. 또한, 터치 스크린(720)은 제어부(760) 제어 하에 그룹 별로 기본 정책을 표시할 수 있다. 이를 통해 제 2 사용자 기기 사용자는 적어도 하나의 제 1 사용자 기기를 관리할 수 있다. 또한, 입력부(730)는 터치 스크린(720)과 별도로 또는 통합하여 제 2 사용자 기기 사용자로부터의 입력을 수신할 수 있다. 예를 들어, 제 1 사용자 기기로부터 프로파일 서버를 통해 차단 설정된 콘텐츠에 대한 차단 해제가 요청되면, 사용자는 차단 해제 요청에 대한 허락 또는 거절을 위한 정보를 입력부(730)를 통해 입력할 수 있다.

[0069] 저장부(750)는 제어부(760)의 보조 기억 장치(secondary memory unit)로써, 디스크, 램(RAM) 및 플래쉬 메모리를 포함할 수 있다. 저장부(750)는 제어부(760) 제어 하에 제 2 사용자 기기에서 생성되거나 무선 통신부(710) 또는 외부 인터페이스부(미도시)를 통해 외부 장치 예를 들어, 서버, 데스크 탑 PC 등으로부터 수신한 데이터를 저장할 수 있다.

[0070] 제어부(760)는 제 2 사용자 기기의 전반적인 동작 및 제 2 사용자 기기의 내부 구성들 간의 신호 흐름을 제어하고, 데이터를 처리하는 기능을 수행할 수 있다. 예를 들어, 제어부(760)는 중앙 처리 장치(Central Processing Unit; CPU), 애플리케이션 프로세서(Application Processor; AP) 등으로 구성될 수 있다. 또한, 제어부(760)는 싱글 코어 프로세어(single core processor) 또는 멀티 코어 프로세서(multi-core processor)로 구성될 수 있다.

[0071] 도 8은 본 발명의 일 실시예에 따른 제 1 사용자 기기(100)의 콘텐츠 차단 방법을 나타내는 흐름도이다.

[0072] 도 8을 참조하면, 과정 801에서 제 1 사용자 기기(100)의 제어부(560)는 프로파일 서버(120)로부터 기본 정책을 수신할 수 있다. 기본 정책은 카테고리 별로 차단 여부가 표시된 리스트 형태로 제공될 수 있다. 도 8에서 도시하지는 않았지만, 과정 801 전에 제 1 사용자 기기(100)의 사용자는 본 발명의 실시예에 따른 콘텐츠 차단 서비스에 가입 또는 등록하기 위하여 제 1 사용자 기기(100)에 대한 정보, 제 1 사용자 기기(100)의 사용자 정보 예를 들어, 사용자의 거주 지역, 연령 등을 프로파일 서버(120)로 전송할 수 있다.

[0073] 과정 803에서 제어부(560)는 콘텐츠로 접근하기 위한 입력을 수신할 수 있다. 예를 들어, 제 1 사용자 기기(100)의 사용자는 특정 콘텐츠로 접근하기 위하여 애플리케이션, 인터넷 브라우저 등을 실행하고 콘텐츠가 위치하는 파일 경로 또는 URL 등을 입력할 수 있다.

[0074] 과정 805에서 제어부(560)는 접근 요청되는 콘텐츠가 일정 기간 이내에 차단된 기록이 있는지 확인할 수 있다. 예를 들어, 일정 기간 이내에 접근하려는 콘텐츠가 위치하는 특정 파일 경로 또는 URL로 다시 접근을 시도하는 경우, 제어부(560)는 별도로 접근 요청된 콘텐츠에 대한 카테고리 확인 및 기본 정책을 통한 비교 과정을 수행하지 않고, 곧바로 접근 요청된 콘텐츠를 차단할 수 있다. 여기서, 일정 기간 이내에 차단된 기록은 캐시(cache) 등에 저장될 수 있다. 그리고, 과정 805에서 확인 결과 접근 요청되는 콘텐츠가 일정 기간 이내에 차단된 기록이 있는 것으로 확인된 경우, 과정 811에서 별도로 접근 요청되는 콘텐츠가 속하는 카테고리를 확인하지 않고 곧바로 접근 요청되는 콘텐츠를 차단할 수 있다.

[0075] 반면, 과정 805에서 확인 결과, 요청되는 콘텐츠가 일정 기간 이내에 차단된 기록이 없는 것으로 확인된 경우, 콘텐츠에 대한 차단 여부에 대한 판단을 유보하고, 과정 807에서 제어부(560)는 콘텐츠가 속하는 카테고리를 확인할 수 있다. 보다 상세히 설명하면, 제어부(560)는 접근 요청된 콘텐츠가 속하는 카테고리를 확인하기 위하여 접근 요청된 콘텐츠 정보를 콘텐츠 분류 서버(110)로 전송할 수 있다. 그리고, 콘텐츠 분류 서버(110)로부터 접근 요청된 콘텐츠가 속하는 카테고리에 대한 정보를 수신하고, 이에 기초하여 제어부(560)는 접근 요청된 콘텐츠가 속하는 카테고리를 확인할 수 있다.

[0076] 과정 809에서 제어부(560)는 콘텐츠가 속하는 카테고리를 기본 정책과 비교하여, 콘텐츠가 속하는 카테고리가 기본 정책에 차단 설정된 카테고리인지 확인할 수 있다.

[0077] 과정 809에서 콘텐츠가 속하는 카테고리가 기본 정책에 차단 설정된 카테고리로 확인된 경우, 과정 811에서 제어부(560)는 접근 요청된 콘텐츠를 차단 즉, 접근 요청된 콘텐츠가 위치하는 파일 경로 또는 URL로의 접근을 차단할 수 있다. 예를 들어, 접근 요청된 콘텐츠가 위치하는 URL이 마약 카테고리에 속하는 것으로 확인되고, 기본 정책에 마약 카테고리가 차단 설정된 경우, 제어부(560)는 접근 요청된 콘텐츠가 위치하는 URL로의 접근을 차단할 수 있다.

[0078] 반면, 과정 809에서 콘텐츠가 속하는 카테고리가 기본 정책에 차단 설정되지 않은 카테고리로 확인된 경우, 과정 813에서 제어부(560)는 접근 요청된 카테고리에 대한 접근을 허용할 수 있다.

[0079] 도 9는 본 발명의 다른 실시예에 따른 제 1 사용자 기기(100)의 콘텐츠 차단 방법을 나타내는 흐름도이다.

[0080] 도 9를 참조하면, 과정 901에서 제 1 사용자 기기(100)의 제어부(560)는 기본 정책 또는 수정 정책을 수신할 수 있다. 보다 상세히 설명하면, 제어부(560)는 프로파일 서버(120)로부터 기본 정책을 수신하거나, 제 2 사용자 기기(130)에 의해 기본 정책이 수정된 수정 정책을 프로파일 서버(120)로부터 수신할 수 있다.

[0081] 과정 903에서 제어부(560)는 기본 정책 또는 수정 정책에 차단 설정된 카테고리에 속하는 콘텐츠에 대한 차단 해제 요청을 수신할 수 있다. 그리고, 과정 905에서 제어부(560)는 수신된 차단 해제 요청을 프로파일 서버(120)를 통해 제 2 사용자 기기(130)로 전송할 수 있다. 도 9에서 도시하지는 않았지만, 제어부(560)는 차단 해제 요청된 콘텐츠가 차단 설정된 카테고리에 속하는 것으로 확인되거나, 일정 기간 내에 차단된 기록이 있는 것을 확인한 후, 해제 요청된 콘텐츠에 대한 정보를 프로파일 서버(120)를 통해 제 2 사용자 기기(130)로 전송할 수 있다.

[0082] 과정 907에서 제 2 사용자 기기(130)에 의해 프로파일 서버(120)로부터 차단 해제 요청된 콘텐츠에 대한 차단 해제 요청이 허락된 경우, 과정 909에서 제어부(560)는 차단 설정된 콘텐츠 또는 차단 설정된 콘텐츠가 속하는 카테고리에 대한 차단 설정이 해제된 기본 정책이 수정된 수정 정책 또는 수정 정책이 재수정된 재수정 정책을 수신할 수 있다. 이에 따라, 과정 911에서 제어부(560)는 차단 설정된 되었던 콘텐츠에 대한 차단을 해제하고, 접근을 허용하도록 제어할 수 있다.

[0083] 반면, 과정 907에서 제 2 사용자 기기(130)에 의해 프로파일 서버(120)로부터 차단 해제 요청된 콘텐츠에 대한 차단 해제 요청이 거절된 경우, 과정 913에서 제어부(560)는 프로파일 서버(120)로부터 차단 해제 요청된 콘텐츠에 대한 거절 정보를 수신할 수 있다. 이에 따라, 과정 915에서 제어부(560)는 차단 해제 요청된 콘텐츠에 대한 차단 설정을 유지하거나, 접근이 요청된 경우 차단할 수 있다.

[0084] 이상에서 살펴본 바와 같이 본 발명의 실시예에 따른 콘텐츠 차단 방법 및 시스템은 다양한 기준에 따라 설정된 정책에 의해 유해 콘텐츠가 차단되도록 설정할 수 있고, 사용자와의 피드백을 통해 적응적으로 유해 콘텐츠 정책을 업데이트함으로써 효과적으로 유해 콘텐츠를 필터링할 수 있다.

[0085] 그리고 본 명세서와 도면에 개시된 실시 예들은 본 발명의 내용을 쉽게 설명하고, 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 따라서 본 발명의 범위는 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상을 바탕으로 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

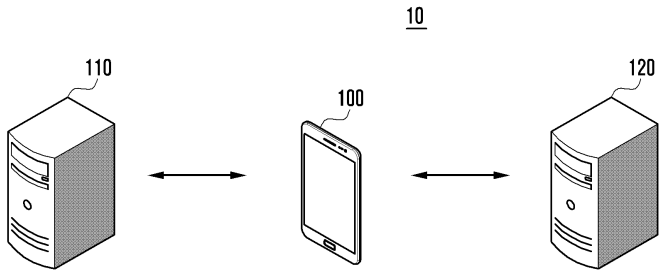
[0086] 10 : 콘텐츠 차단 시스템 100 : 제 1 사용자 기기

110 : 콘텐츠 분류 서버 120 : 프로파일 서버

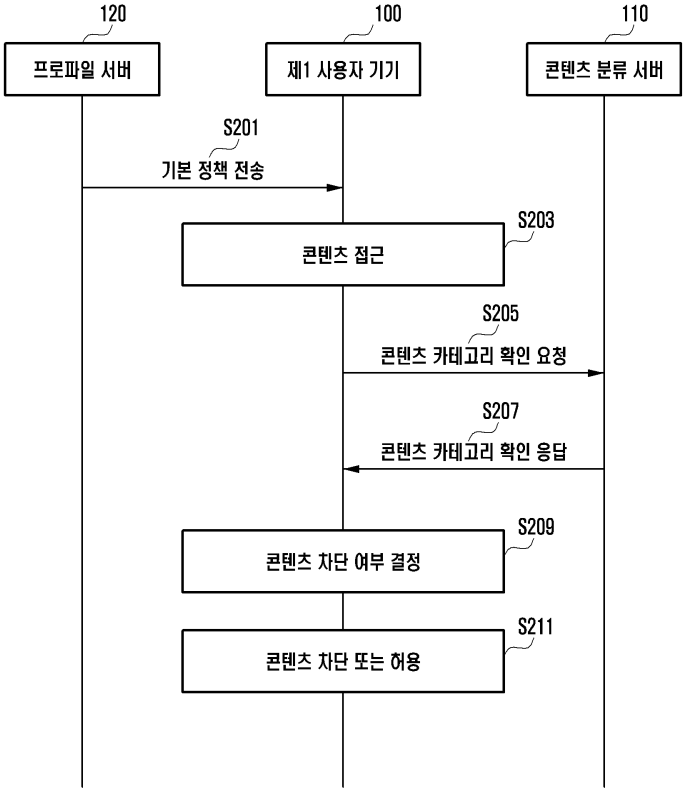
130 : 제 2 사용자 기기

도면

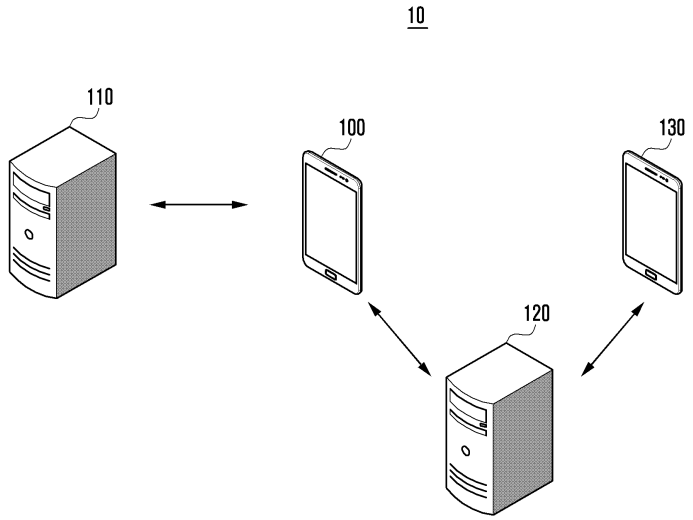
도면1


10
110
100
120

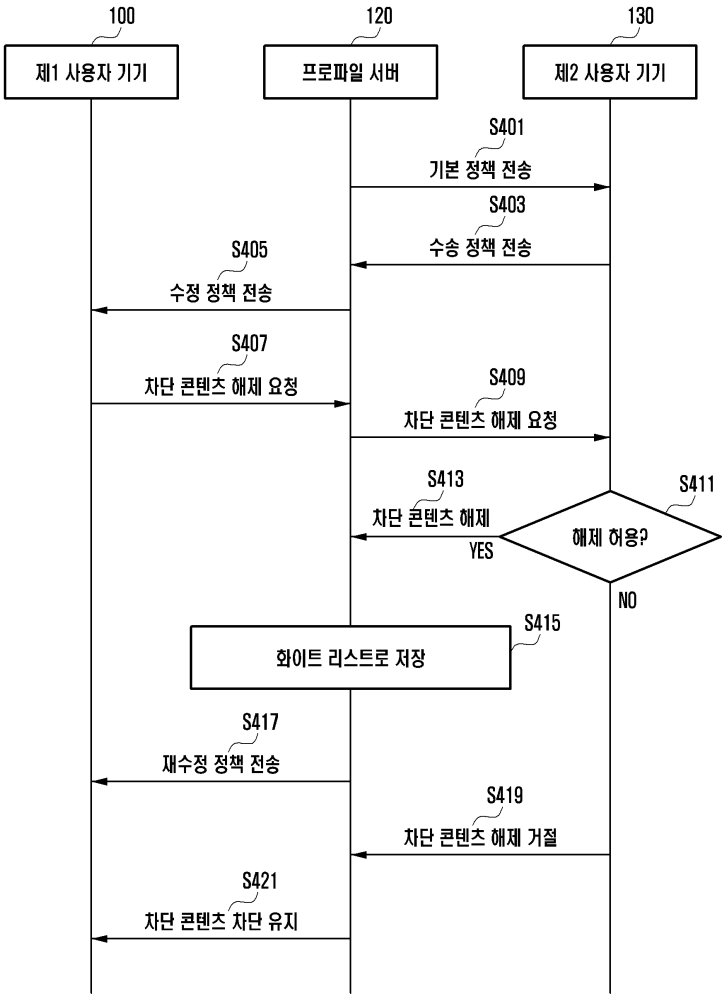
도면2


120
프로파일 서버
100
제1 사용자 기기
110
콘텐츠 분류 서버
S201
기본 정책 전송
S203
콘텐츠 접근
S205
콘텐츠 카테고리 확인 요청
S207
콘텐츠 카테고리 확인 응답
S209
콘텐츠 차단 여부 결정
S211
콘텐츠 차단 또는 허용

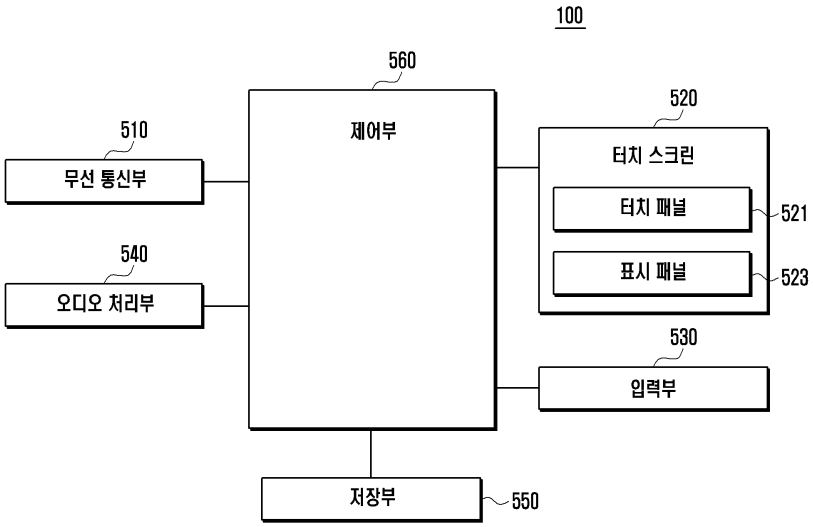
도면3


10
110
100
130
120

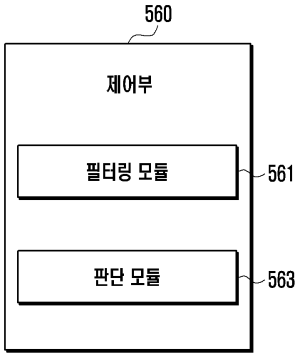
도면4


100
120
130
제1 사용자 기기
프로파일 서버
제2 사용자 기기
S401
기본 정책 전송
S403
수송 정책 전송
S405
수정 정책 전송
S407
차단 콘텐츠 해제 요청
S409
차단 콘텐츠 해제 요청
S411
해제 허용?
YES
NO
S413
차단 콘텐츠 해제
S415
화이트 리스트로 저장
S417
재수정 정책 전송
S419
차단 콘텐츠 해제 거절
S421
차단 콘텐츠 차단 유지

도면5

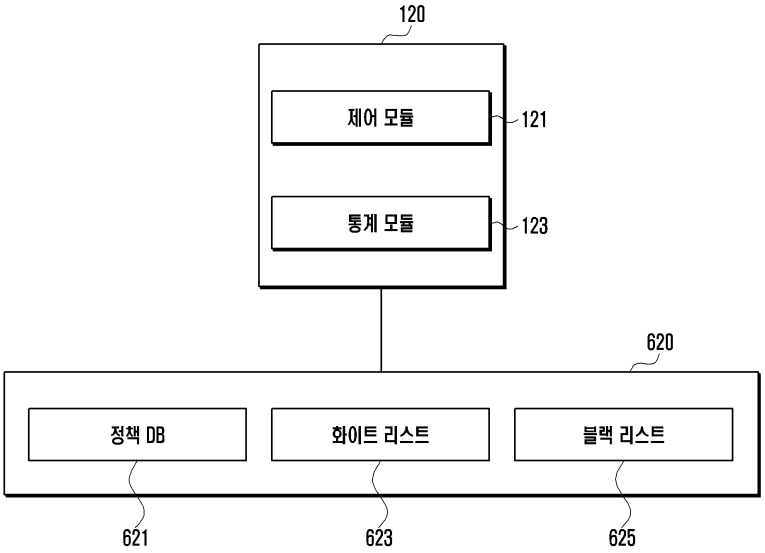

100
560
제어부
510
무선 통신부
540
오디오 처리부
520
터치 스크린
터치 패널
521
표시 패널
523
530
입력부
저장부
550

(501)

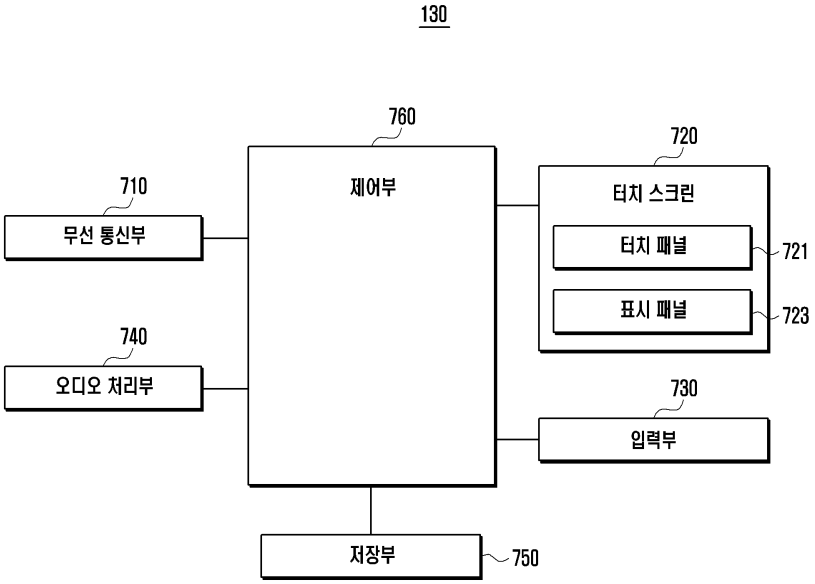

560
제어부
필터링 모듈
561
판단 모듈
563

(503)

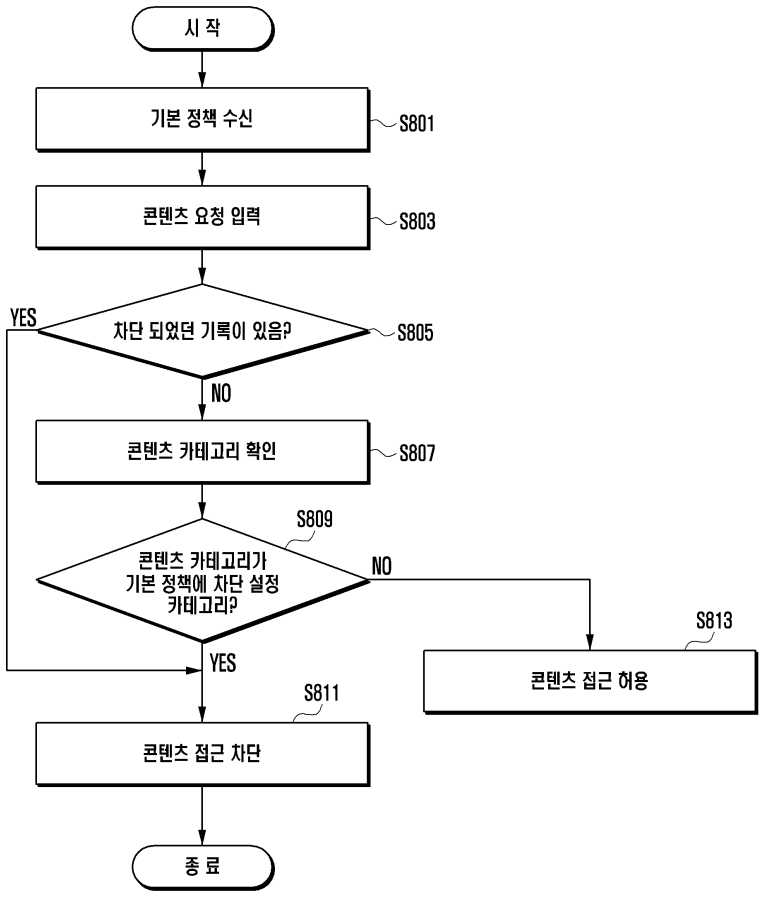
도면6


120
제어 모듈
121
통계 모듈
123
620
정책 DB
화이트 리스트
블랙 리스트
621
623
625

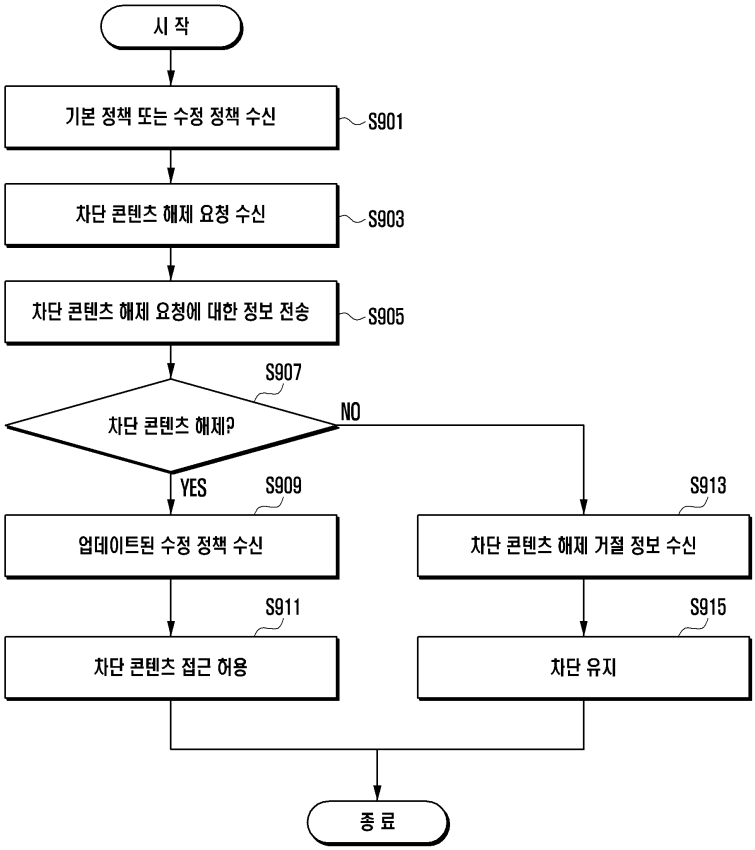
도면7


130
760
제어부
710
무선 통신부
740
오디오 처리부
720
터치 스크린
터치 패널
721
표시 패널
723
730
입력부
저장부
750

도면8


시 작
기본 정책 수신
S801
콘텐츠 요청 입력
S803
YES
차단 되었던 기록이 있음?
S805
NO
콘텐츠 카테고리 확인
S807
S809
콘텐츠 카테고리가
기본 정책에 차단 설정
카테고리?
NO
S813
콘텐츠 접근 허용
YES
S811
콘텐츠 접근 차단
종 료

도면9


시 작
기본 정책 또는 수정 정책 수신
S901
차단 콘텐츠 해제 요청 수신
S903
차단 콘텐츠 해제 요청에 대한 정보 전송
S905
S907
차단 콘텐츠 해제?
NO
YES
S909
업데이트된 수정 정책 수신
S911
차단 콘텐츠 접근 허용
S913
차단 콘텐츠 해제 거절 정보 수신
S915
차단 유지
종 료