(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월23일
(11) 등록번호 10-1120777
(24) 등록일자 2012년02월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(21) 출원번호 10-2005-0033674
(22) 출원일자 2005년04월22일
심사청구일자 2010년04월15일
(65) 공개번호 10-2006-0047435
(43) 공개일자 2006년05월18일
(30) 우선권주장
10/830,632 2004년04월23일 미국(US)
(56) 선행기술조사문헌
US20040103305 A1
US20040205510 A1
US6253193 B1
KR1020020021030 A
전체 청구항 수 : 총 16 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
커터, 벤자민 브룩스
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
에반스, 브라이언 피.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
(뒷면에 계속)
(74) 대리인
제일특허법인

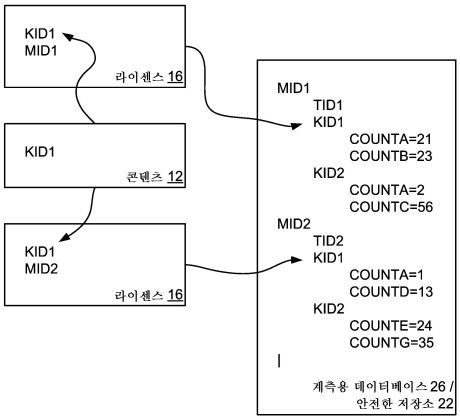
심사관 : 양종필

(54) 발명의 명칭 **콘텐츠 보호 시스템 또는 동종 시스템에서의 콘텐츠 또는동종물에 대한 액세싱 계측 방법**

(57) 요 약

계측된 데이터는 누적되어(accumulated), 계측 ID(MID)와 콘텐츠-관련 ID(KID)에 따라 클라이언트의 계측용 데이터베이스 내에서 색인된다. 클라이언트는 특정 MID를 선택하고, 선택된 MID를 갖는 계측용 데이터베이스에서 계측된 데이터를 선택하고, 선택된 계측 데이터에 근거하여 시도 메시지를 구성하고, 시도 메시지를 계측 서비스에 전송한다. 계측 서비스는 시도 메시지로부터 계측된 데이터를 획득하고, 계측된 데이터를 저장하고, 응답 메시지를 구성한다. 클라이언트는 시도 메시지에 있는 선택된 계측된 데이터에 대한 KID 리스트를 포함하는 응답 메시지를 수신하고, 리스트에 있는 각각의 KID 마다 선택된 MID와 KID를 갖는 계측용 데이터베이스로부터, 계측된 데이터를 삭제함으로써 KID 리스트를 처리한다.

대 표 도 - 도3



(72) 발명자

스트롬, 클리포드 피.

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

파크스, 마이클 제이

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

특허청구의 범위

청구항 1

클라이언트로부터의 계측된 데이터(metered data)를 누적하여 계측 서비스에 보고하는 방법 - 각각의 계측된 데이터는 상기 클라이언트의 계측용 데이터베이스(metering database) 내에서 계측 ID(MID)에 따라 색인되고 상기 계측용 데이터베이스 내에서 콘텐츠 관련 ID(KID)에 따라 이차적으로 색인됨 - 으로서, 상기 방법은 클라이언트에 의해,

특정 MID를 선택하는 단계,

상기 선택된 MID를 갖는 상기 계측용 데이터베이스 내의, 상기 계측된 데이터의 적어도 일부분을 선택하는 단계 - 상기 선택된 계측된 데이터는 KID에 따라 정렬됨 -,

상기 선택된 계측된 데이터에 근거하여 시도 메시지(challenge)를 구성하는 단계,

상기 구성된 시도 메시지를 상기 계측 서비스에 전송하는 단계 - 상기 계측 서비스는 상기 시도 메시지로부터 상기 선택된 계측된 데이터를 획득 및 저장하고 상기 시도 메시지에 근거하여 상기 클라이언트에게 되돌아갈 응답 메시지를 구성함 -,

상기 시도 메시지 내의 상기 선택된 계측된 데이터에 대한 KID 리스트를 포함하는 상기 응답 메시지를 상기 계측 서비스로부터 수신하는 단계,

상기 응답 메시지가 상기 시도 메시지에 대응함을 확인하는 단계, 및

상기 KID 리스트 내의 각각의 KID 마다, 상기 선택된 MID와 해당 KID를 갖는 상기 계측된 데이터를 상기 계측용 데이터베이스로부터 삭제함으로써, 상기 응답 메시지 내의 상기 KID 리스트를 처리하는 단계를 포함하고,

상기 시도 메시지는,

상기 MID,

상기 계측 서비스의 위치의 식별자,

상기 시도 메시지를 위해 선택된 트랜잭션 ID(TID), 및

상기 선택된 계측된 데이터를 포함하도록 구성되며,

상기 선택된 계측된 데이터는 대칭 패스 키(pass key)에 따라 암호화되어 생성된 (passkey(metereddata))를 포함하고, 상기 패스 키가 상기 계측 서비스의 공용키 (PU-M)에 따라 암호화되어 생성된 PUM(passkey)을 더 포함하고,

상기 계측 서비스는 PU-M에 대응하는 개인 키(PR-M)를 상기 시도 메시지로부터의 PUM(passkey)에 적용하여 상기 패스 키를 획득할 수 있고, 상기 획득한 패스 키를 상기 시도 메시지로부터의 (passkey(metereddata))에 적용하여 상기 선택된 계측된 데이터를 획득할 수 있으며, 그 이후에 상기 획득한 계측된 데이터를 저장할 수 있는, 보고 방법.

청구항 2

제1항에 있어서,

상기 시도 메시지를 구성하는 단계는, 상기 시도 메시지의 적어도 일부분에 대한 해쉬로부터 상기 패스 키에 근거하여 추출한 해쉬값을 더 포함하도록 상기 시도 메시지를 구성하는 단계를 더 포함하며, 이로써 상기 시도 메시지의 상기 적어도 일부분이 이후에 수정되는 경우에 상기 해쉬값은 검증에 실패할 것이며, 이로써 상기 계측 서비스는 상기 패스 키에 근거하여 상기 시도 메시지로부터의 상기 해쉬값을 검증할 수 있는, 보고 방법.

청구항 3

제1항에 있어서,

상기 시도 메시지를 구성하는 단계는, 상기 클라이언트가, 상기 시도 메시지를 상기 선택된 MID에 관한 상기 계측용 데이터베이스 내에 누적된 모든 계측된 데이터를 포함하도록 구성하지 못할 경우, 상기 시도 메시지가 세

트된 부분 데이터 플래그를 더 포함하도록 상기 시도 메시지를 구성하는 단계를 포함하는, 보고 방법.

청구항 4

제1항에 있어서,

상기 응답 메시지는 상기 시도 메시지에 기재된 MID, 상기 시도 메시지에 기재된 트랜잭션 ID(TID), 및 상기 시도 메시지에 기재된 상기 선택된 계측된 데이터의 적어도 일부분을 포함하는, 보고 방법.

청구항 5

제4항에 있어서,

상기 응답 메시지는 상기 선택된 계측된 데이터의 적어도 일부분에 대한 상기 KID 리스트를 더 포함하는, 보고 방법.

청구항 6

제4항에 있어서,

상기 응답 메시지는 상기 선택된 계측된 데이터의 적어도 일부분을 대칭 패스 키에 따라 암호화하여 생성된 (passkey(metereddata))를 더 포함하며,

상기 보고 방법은 상기 클라이언트가 상기 패스 키를 획득하여 상기 획득한 패스 키를 상기 응답 메시지로부터의 (passkey(metereddata))에 적용시켜 상기 계측된 데이터의 상기 적어도 일부분을 획득하는 단계를 더 포함하는, 보고 방법.

청구항 7

제6항에 있어서,

상기 패스 키에 근거하여 상기 응답 메시지의 적어도 일부분에 대한 해쉬로부터 추출한 해쉬값을 더 포함하는 상기 시도 메시지를 수신하는 단계를 더 포함하고, 상기 보고 방법은 상기 클라이언트가 상기 패스 키에 근거하여 상기 응답 메시지로부터의 상기 해쉬값을 검증하는 단계를 더 포함하는, 보고 방법.

청구항 8

제4항에 있어서,

상기 응답 메시지는, 상기 시도 메시지가 세트된 부분 데이터 플래그를 포함하는 경우에 상기 세트된 부분 데이터 플래그를 더 포함하며,

상기 세트된 부분 데이터 플래그는, 상기 클라이언트가 상기 시도 메시지를 상기 선택된 MID에 관한 상기 계측용 데이터베이스 내의 누적된 모든 계측된 데이터를 포함하도록 구성할 수 없었다는 것, 및 상기 클라이언트가 상기 시도 메시지의 상기 선택된 MID에 관련하여 상기 계측 서비스에 보고해야 하는 부가적인 계측된 데이터를 갖고 있다는 것을 나타내는(signifying), 보고 방법.

청구항 9

제8항에 있어서,

상기 응답 메시지가 상기 세트된 부분 데이터 플래그를 포함할 경우,

상기 선택된 MID를 갖는 상기 계측용 데이터베이스 내의 상기 부가적인 계측된 데이터의 적어도 일부분을 선택하는 단계,

상기 선택된 부가적인 계측된 데이터에 근거하여 부가적인 시도 메시지를 구성하는 단계, 및

상기 구성된 부가적인 시도 메시지를 상기 계측 서비스에 전송하는 단계를 더 포함하는, 보고 방법.

청구항 10

제4항에 있어서,

상기 응답 메시지가 상기 시도 메시지에 대응한다는 것을 확인하는 단계는, 상기 응답 메시지에 있는 TID와 MID가 상기 선택된 MID를 갖는 계측용 데이터베이스에 저장된 TID와 일치한다는 것을 확인하는 단계를 포함하는, 보고 방법.

청구항 11

제1항에 있어서,

상기 선택된 MID에 따라 상기 계측용 데이터베이스에 저장된 트랜잭션 ID(TID)를 검색하여 상기 시도 메시지가 상기 TID를 포함하도록 구성하는 단계, 상기 계측 서비스로부터 상기 TID를 더 포함한 상기 응답 메시지를 수신하는 단계, 및 상기 응답 메시지에 있는 상기 KID 리스트를 처리할 시에, 상기 MID에 대한 다음 시도 메시지의 새로운 TID를 생성하여, 상기 MID에 대한 상기 다음 시도 메시지와 관련된 검색 및 사용을 위해 상기 선택된 MID에 따라 상기 생성된 TID를 상기 계측용 데이터베이스에 저장시키는 단계를 더 포함하는, 보고 방법.

청구항 12

클라이언트로부터의 계측된 데이터를 누적하여 계측 서비스에 보고하는 방법 - 각각의 계측된 데이터는 상기 클라이언트의 계측용 데이터베이스 내에서 계측 ID(MID)에 따라 색인되고 상기 계측용 데이터베이스 내에서 콘텐츠 관련 ID(KID)에 따라 이차적으로 색인됨 - 으로서, 상기 방법은 클라이언트에 의해,

특정의 계측용 인증서를 선택하고, 상기 특정의 계측용 인증서를 검증하며, 상기 검증된 계측용 인증서로부터 상기 검증된 계측용 인증서 내에 기재되어 있는 MID를 결정하는 단계,

상기 선택된 계측용 인증서로부터 상기 결정된 MID를 갖는 상기 계측용 데이터베이스 내의 상기 계측된 데이터의 적어도 일부분을 선택하는 단계 - 상기 선택된 계측된 데이터는 KID에 따라 정렬됨 -,

상기 선택된 계측된 데이터와 상기 선택된 계측용 인증서에 근거하여 시도 메시지를 구성하는 단계,

상기 구성된 시도 메시지를 상기 계측 서비스에 전송하는 단계 - 상기 계측 서비스는 상기 시도 메시지로부터 상기 선택된 계측된 데이터를 획득 및 저장하고 상기 시도 메시지에 근거하여 상기 클라이언트에게 되돌아갈 응답 메시지를 구성함 -,

상기 시도 메시지 내의 상기 선택된 계측된 데이터에 대한 KID 리스트를 포함하는 상기 응답 메시지를 상기 계측 서비스로부터 수신하는 단계,

상기 응답 메시지가 상기 시도 메시지에 대응함을 확인하는 단계, 및

상기 KID 리스트의 각각의 KID 마다, 상기 결정된 MID와 해당 KID를 갖는 상기 계측된 데이터를 상기 계측용 데이터베이스로부터 삭제함으로써, 상기 응답 메시지 내의 KID 리스트를 처리하는 단계를 포함하고,

상기 시도 메시지는,

상기 계측용 인증서로부터의 상기 MID,

상기 계측용 인증서로부터 상기 계측 서비스의 위치의 식별자,

상기 시도 메시지를 위해 선택된 트랜잭션 ID(TID), 및

상기 선택된 계측된 데이터를 포함하도록 구성되며,

상기 선택된 계측된 데이터가 대칭 패스 키에 따라 암호화되어 생성된 (passkey(meteredata))를 포함하고, 상기 패스 키가 상기 계측용 인증서로부터의 공용키 PU-M에 따라 암호화되어 생성된 PUM(passkey)을 더 포함하고,

상기 계측 서비스는 PU-M에 대응하는 개인 키(PR-M)를 상기 시도 메시지로부터의 PUM(passkey)에 적용하여 상기 패스 키를 획득할 수 있고, 상기 획득한 패스 키를 상기 시도 메시지로부터의 (passkey(metereddata))에 적용하여 상기 선택된 계측된 데이터를 획득할 수 있으며, 그 이후에 상기 획득한 계측된 데이터를 저장할 수 있는, 보고 방법.

청구항 13

제12항에 있어서,

상기 시도 메시지를 구성하는 단계는, 상기 클라이언트가, 상기 시도 메시지를 상기 선택된 계측용 인증서로부

터 상기 결정된 MID를 갖는 상기 계측용 데이터베이스 내의 누적된 모든 계측된 데이터를 포함하도록 구성하지 못하는 경우에, 상기 시도 메시지가 세트된 부분 데이터 플래그를 더 포함하도록 구성하는 단계를 포함하는, 보고 방법.

청구항 14

제12항에 있어서,

상기 응답 메시지는 상기 시도 메시지에 기재된 MID, 상기 시도 메시지에 기재된 트랜잭션 ID(TID), 및 상기 시도 메시지에 기재된 상기 선택된 계측된 데이터의 적어도 일부분을 더 포함하는, 보고 방법.

청구항 15

제14항에 있어서,

상기 응답 메시지는, 상기 시도 메시지가 세트된 부분 데이터 플래그를 포함하는 경우에, 상기 세트된 부분 데이터 플래그를 더 포함하며,

상기 세트된 부분 데이터 플래그는, 상기 클라이언트가 상기 시도 메시지를 상기 선택된 계측용 인증서로부터 상기 결정된 MID에 관한 상기 계측용 데이터베이스 내의 누적된 모든 계측된 데이터를 포함하도록 구성할 수 없었다는 것, 및 상기 클라이언트가 상기 시도 메시지의 상기 결정된 MID에 관련하여 상기 계측 서비스에 보고해야 하는 부가적인 계측된 데이터를 갖고 있다는 것을 나타내는, 보고 방법.

청구항 16

제15항에 있어서,

상기 응답 메시지가 상기 세트된 부분 데이터 플래그를 포함할 경우,

상기 선택된 계측용 인증서로부터 상기 결정된 MID를 갖는 상기 계측용 데이터베이스 내의 상기 부가적인 계측된 데이터의 적어도 일부분을 선택하는 단계,

상기 선택된 부가적인 계측된 데이터와 상기 선택된 계측용 인증서에 근거하여 부가적인 시도 메시지를 구성하는 단계, 및

상기 구성된 부가적 시도 메시지를 상기 계측 서비스에 전송하는 단계를 더 포함하는, 보고 방법.

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0015] 본 발명은 특히 콘텐츠 보호 시스템의 맥락에서 디지털 콘텐츠 또는 동종물에 대한 액세스를 계측(metering)할

수 있는 아키텍처 및 방법에 관한 것이다. 보다 상세하게는, 본 발명은 계측된 콘텐츠의 액세스를 나타내는 데이터를 수집하고 계측 서비스로 보고하는 아키텍처 및 방법에 관한 것이다.

[0016] 알려진 바와 같이, 도 1를 참조해 보면, 콘텐츠 보호 시스템 및 강화 시스템은 디지털 오디오, 디지털 비디오, 디지털 텍스트, 디지털 데이터, 디지털 멀티미디어 등과 같은 디지털 콘텐츠(12)와 관련되는 것이 매우 바람직하며, 여기서 디지털 콘텐츠(12)는 사용자들에게 배포되는 것으로 되어 있다. 사용자가 디지털 콘텐츠를 수신하면, 개인용 컴퓨터(14)의 미디어 플레이어와 같은 적절한 렌더링(rendering) 장치, 즉 휴대용 재생 장치 또는 동종 장치를 사용하여 디지털 콘텐츠를 렌더링하거나 재생한다.

[0017] 전형적으로, 디지털 콘텐츠(12)를 배포하는 콘텐츠 소유자는, 사용자가 배포된 디지털 콘텐츠(12)를 사용하는 것에 대하여 제한을 가하길 원한다. 예를 들면, 콘텐츠 소유자는 사용자가 이러한 콘텐츠(12)를 복제하여 제 3 자에게 재배포하지 못하도록 하거나, 배포된 디지털 콘텐츠(12)가 제한된 횟수만큼, 정해진 시간 만큼, 정해진 종류의 기계에서만, 정해진 미디어 플레이어에서만, 정해진 형태의 사용자에게서만 재생되게끔 하고자 원할 수 있다.

[0018] 그러나, 디지털 콘텐츠(12)의 배포 후에, 콘텐츠 소유자가 제어하는 일은 있다손 치더라도 거의 없다. 그래서, 복제 보호 시스템(10)에 의해 임의 형태의 디지털 콘텐츠(12)의 렌더링 또는 재생에 대해 제어하도록 하게 하고, 이러한 제어 사항은 시스템내에서 디지털 콘텐츠 소유자에 의해 정의가능하고 변경가능하다. 전형적으로, 콘텐츠(12)는 어떤 적절한 배포 채널에 의해 패키지(13)의 형태로 사용자에게 배포된다. 디지털 콘텐츠 패키지(13)는 배포될 때, 대칭 암호 키/복호 키(KD),즉 KD(CONTENT)로 암호화된 디지털 콘텐츠(12) 뿐만 아니라 콘텐츠를 위한 라이센스를 어떻게 획득할 것인지 등의 콘텐츠를 식별하게 하는 다른 정보를 포함할 수 있다.

[0019] 신뢰성 기반의 복제 보호 시스템(10)은, 디지털 콘텐츠(12)가 렌더링되기 이전에 만족되야하는 규정들을 상술된 디지털 콘텐츠(12) 소유자가 명기하게큼 할 수 있다. 규정들은 요건 및/또는 다른 것들을 포함할 수 있으며, 클라이언트/컴퓨팅 장치(14)(특별한 상황이 아닌한, 이하에서 용어들은 상호변경가능함)가 콘텐츠 소유자 또는 그 대리인으로부터 획득해야하는 디지털 라이센스(16) 내에 포함될 수 있거나, 아니면 이미 콘텐츠(12)에 첨부되어 있을 수 있다. 이러한 라이센스(16) 또는 규정들은 예를 들면, 사용자의 컴퓨팅 장치 또는 다른 재생 장치에 의해 복호화될 수 있는 다른 어떤 키에 따라 암호화된 디지털 콘텐츠(12)를 복호할 수 있는 복호 키(KD)를 포함할 수 있다.

[0020] 어느 한 디지털 콘텐츠(12)의 콘텐츠 소유자는, 콘텐츠 소유자에 의해 라이센스(16) 또는 다른 것들에 명기된 규정들을 사용자가 엄수할 것으로 확신할 수 없다면, 콘텐츠(12)를 사용자에게 배포하는 원하지 않을 것이다. 그러므로, 사용자의 컴퓨팅 장치(14) 또는 다른 재생 장치에는 이런 규정들을 따르지 않는 디지털 콘텐츠(12)는 렌더링하지 않을 트러스티드 컴포넌트 또는 메커니즘(18)이 제공되는 것이 바람직하다.

[0021] 트러스티드 컴포넌트(18)는 전형적으로 평가기를 갖고 있으며, 이 평가기는 규정을 검토한 후, 이를 바탕으로 요청하는 사용자가 무엇보다도 요청한 디지털 콘텐츠(12)를 추구하는 방식으로 렌더링할 권한을 갖고 있는지를 판정한다. 이해한 바와 같이, 평가기(20)는 복제 보호 시스템(10) 내에서 규정들에 따라 디지털 콘텐츠(12)의 소유자의 요청을 실행하는 것으로 기대되며, 사용자는 트러스티드 컴포넌트(18) 및/또는 평가기(20)를 악의적으로나 그렇지 않은 다른 목적으로도 쉽게 바꿀 수 없어야 한다.

[0022] 이해한 바와 같이, 사용자가 누구인지, 사용자가 어디에 위치하는지, 사용자가 어떤 컴퓨팅 장치(14) 또는 재생 장치를 사용하는지, 어떤 렌더링 애플리케이션이 복제 보호 시스템(10)을 호출하는지, 날짜, 시간 등을 비롯한 여러가지 요인들 중 임의의 것에 기반하여, 사용자가 렌더링하는 권한을 갖고 있는지를 콘텐츠(12)를 렌더링하는 규정들에 명기할 수 있다. 부가적으로, 예를 들면 규정들은 렌더링을 예정된 재생 횟수 만큼 또는 예정된 재생 시간으로 제한할 수 있다.

[0023] 어떤 적절한 언어 및 구문에 따라 규정들을 명기할 수 있다. 예를 들면, 이 언어는 만족해야 하는 속성 및 값들을 명기할 수 있으며(예를 들면, DATE must be later than X), 명확한 스크립에 따라 함수들의 실행을 요구할 수 있다(예를 들면, IF DATA greater than X, THEN DO...).

[0024] 평가기(20)가 규정들을 만족한 것으로 판정하면, 디지털 콘텐츠(12)는 그 이후에 렌더링될 수 있다. 특히, 콘텐츠(12)를 렌더링하기 위해서, 상술한 라이센스(16)와 같은 미리 예정된 소스로부터 복호 키(KD)를 획득하여, 콘텐츠 패키지(13)로부터의 KD(CONTENT)에 적용하여 실제 콘텐츠(12)를 만들어 내며, 그 이후에 실제로 콘텐츠(12)를 렌더링한다.

[0025] 트러스티드 컴포넌트(18)는 때때로 특정 콘텐츠(12)를 렌더링하는 것과 특정 라이센스(16)의 사용에 관련된 상태 정보를 유지할 필요가 있다는 것에 유의해야 한다. 예를 들면, 특정 라이센스(16)가 재생 횟수에 대한 요건을 갖게 되는 경우가 있을 수 있으며, 트러스티드 컴포넌트(18)는 이에 따라 라이센스(16)가 해당 콘텐츠(12)를 렌더링하는데 몇 회 이용되었는지 기억하거나, 이후 몇 회 더 해당 콘텐츠(12)를 렌더링하는데 이용될 수 있는가에 대해 기억해야 한다. 따라서, 트러스티드 컴포넌트(18)는 이런 상태 정보가 보안 상태로 영속적으로 유지되는 적어도 하나의 영속적인 안전한 저장소(22)를 포함할 수 있다. 그러므로, 트러스티드 컴포넌트(18)는 이런 상태 정보를 안전한 저장소(22)에 영속적으로 저장하여, 컴퓨팅 장치(14)의 전 사용 세션에 걸쳐 그 상태 정보를 유지한다. 이런 안전한 저장소(22)는 컴퓨팅 장치(14) 상에서 트러스티드 컴포넌트(18)에 존재하는 경우가 많지만, 그 밖 다른 공간에 위치할 수 있다.

[0026] 복제 보호 시스템(10)에서, 콘텐츠(12)는 콘텐츠(12)를 암호화하고, 일련의 규정들과 콘텐츠(12)를 결합시킴으로써, 사용자들이 사용할 수 있도록 패키징 되므로, 콘텐츠(12)는 규정들에 따라서만 렌더링될 수 있다. 규정들에 따라서만 렌더링될 수 있기 때문에, 규정들을 준수할 때만 재생될 수 콘텐츠(12)는 이후에도 자유롭게 배포될 수 있다. 전형적으로, 콘텐츠(12)는 상술한 복호 키(KD)와 같은 대칭 키에 따라 암호화되어 KD(CONTENT)가 생성되므로, KD(CONTENT)는 복호 키(KD)에 따라 복호되어 콘텐츠(12)가 생성된다. 이어서, 복호 키(KD)는 콘텐츠(12)에 대응하는 라이센스(16) 내에 포함된다. 빈번히, 복호 키(KD)는 콘텐츠(12)를 렌더링하는 컴퓨팅 장치(14)의 공용키(PU-C)와 같은 공용키에 따라서 암호화됨으로써, PU-C(KD)가 생성된다. 그러나, 다른 공용키들이 이용될 수 있는데, 예를 들면 사용자 공용키로서 사용자가 구성원으로 속해있는 그룹의 공용키 등이 이용 가능하다는 것에 주목할 필요가 있다.

[0027] 사용자가 배포된 디지털 콘텐츠(12)를 어떻게 처리하는가를 제한시키는 것 이외에도, 콘텐츠 소유자 등은 사용자, 컴퓨팅 장치, 또는 동종 장치들에 의한 콘텐츠(12)의 사용을 계측하기를 원할 수 있다. 예를 들면, 콘텐츠 소유자는 사용자에게 사용 요금을 부과한 근거, 미징수한 사용 요금 근거 등에 대해 콘텐츠(12)가 몇 회 렌더링 되었는지 알기를 원할 수 있다. 이에 상응하여, 콘텐츠 소유자는 옵션이 가능하다는 가정 아래 콘텐츠가 몇 회 복제되었는지, 또 다른 옵션이 가능하다는 가정 아래 콘텐츠가 다른 콘텐츠(12)와 몇 회 통합되었는지, 콘텐츠가 렌더링된 시간 및 콘텐츠가 렌더링된 일시 등을 알고자 할 수 있다. 요약하면, 콘텐츠 소유자 등은 콘텐츠의 사용을 실제로 계측하거나 그렇지 않으면 계수하거나 누적시키는 방식으로 계측하기를 원할 수 있다. 그러므로, 컴퓨팅 장치(14) 상에 있는 트러스티드 컴포넌트(18)는 이러한 계측 기능을 수행하며, 이로부터 획득한 계측된 데이터를 안전한 저장소(22)에 저장하는데 이용될 수 있다.

[0028] 일반적으로, 계측이란 하나의 콘텐츠(12)에 관련된 양을 계수하거나 누적시키는 것을 의미할 수 있으며, 여기서 그것은 콘텐츠 사용자 등의 요청에 따라 측정되는 양을 나타낸다. 상기에 설명한 대로, 계측은 콘텐츠(12)가 렌더링되거나, 복제되거나, 전송되거나 하는 액세스 횟수, 콘텐츠(12)가 렌더링되는 시간 등에 전형적으로 기반한다. 물론, 다른 형태의 계측이 존재할 수 있고, 아래에 설명된 본 발명과 관련되어 이용될 수 있다.

[0029] 인식할 수 있는 바와 같이, 계측은 피드백, 금전적 가치 등을 비롯한 다른 여러 이유로 인해 유용하다. 한 예로서, 콘텐츠(12) 사용에 대한 통계치는 콘텐츠 소유자에게 콘텐츠(12)가 인기가 있는지, 유용한지, 잘 평가받고 있는지, 즐겨 이용되는지 등을 알려주는 지표로서 중요할 수 있다. 다른 예로서, 하나의 콘텐츠(12) 사용에 대한 통계치는 한 콘텐츠(12)의 저자에게 보상해 주는 것에 이용될 수 있으며, 여기서 저자는 많은 저자들 중 한명이다. 또 다른 예로서, 한 콘텐츠(12)의 사용에 대한 통계치는 콘텐츠 소유자에게 돌아가게 될 금전적 가치를 계산하는데 이용될 수 있다. 특히 후자의 경우에는, 음악 악보와 같은 콘텐츠(12)는 사용시마다 라이센스를 체결하거나, 일시불로 체결하거나, 복합방식으로 라이센스를 체결한다. 그러므로, 콘텐츠 소유자에게 지급되는 콘텐츠(12) 사용에 따른 라이센스 요금은 라이센스 유형에 의거하여 다양하며, 특히 라이센스 요금을 종량제 방식으로 부과할 것인지, 사용시마다 부과할 것인지 등 매우 다양하다.

[0030] 또한, 상세화된 계측이 아직 실행되고 있지 않으므로, 이와 같이 상세한 계측을 실행하는 능력을 제공하면, 지금까지는 불가능했던 향후의 비즈니스 모델들을 창조해낼 가능성이 크다. 예를 들면, 주로 광고/콘텐츠(12)를 보여주는 비용이 현재 일반적으로 고정되어 있지만, 본 발명에 의해 계측되어 실시된다면, 이후에는 광고/콘텐츠(12)의 사용 요금이 렌더링의 횟수에 의거하여 결정되게 된다. 다른 예를 들면, 텔레비전 프로그램(콘텐츠(12))은 현재 극소 통계 조사에 기반한 평가치을 갖는 평가 서비스(rating service)를 통해 측정된 최소한 부분적으로 시장 점유율에 의거하여 평가 받고 있지만, 본 발명에 의하면, 이런 평가는 프로그램/콘텐츠(12)의 시청자/사용자들을 계측하여 측정한 매우 자세한 측정에 기반하여 얻어질 수 있다.

[0031] 컴퓨팅 장치(14) 상에서 콘텐츠(12)의 액세스와 사용도는 비교적 간단한 방식으로 계측될 수 있는 반면에, (1)

무엇을 계측할 것인지 정의하기, (2) 계측으로부터 추출된 데이터를 컴퓨팅 장치(14) 상에 어떤 방법으로 저장할 것인지 정의하기, (3) 여러 대의 컴퓨팅 장치들 각각으로부터 계측된 데이터를 수집하는 계측 서비스 정의하기, 또는 (4) 어떻게 계측된 데이터를 계측 서비스에 보고 할지를 정의하기에 대해, 어떤 아키텍처 또는 방법도 존재하지 않았음에 주목할 필요가 있다.

[0032] 따라서, 데이터 계측을 효과적으로 수행하고, 계측된 데이터를 계측 서비스에 보고하는 아키텍쳐 및 방법이 존재할 필요가 있다. 특히, 무엇을 계측할 것인지 정의하고, 계측으로부터 추출된 데이터를 컴퓨팅 장치(14) 상에 어떤 방법으로 저장할 것인지 정의하고, 여러 대의 컴퓨팅 장치들 각각으로부터 계측된 데이터를 수집하는 계측 서비스에 대해 정의하고, 어떻게 이런 계측된 데이터를 계측 서비스에 보고 할지를 정의하는 아키텍터 및 방법이 필요하다.

발명이 이루고자 하는 기술적 과제

[0033] 상술한 요건은 누적시킨 계측된 데이터를 클라이언트로부터 계측 서비스에 보고하는 방법을 제공할 본 발명에 의해서 적어도 부분적으로 만족된다. 각각의 계측된 데이터는 계측 ID(MID)에 따라 클라이언트의 계측용 데이터베이스 내부에서 일차적으로 색인되고, 콘텐츠-관련 ID(KID)에 따라 계측용 데이터베이스 내부에서 이차적으로 색인된다.

[0034] 본 방법에서, 클라이언트는 특정 MID를 선택하고, 선택된 MID를 가진 계측용 데이터베이스에서 계측된 데이터의 적어도 일부분을 선택하고, 여기서 선택된 계측된 데이터는 KID에 따라 정렬되어 있다. 그 이후에 클라이언트는 선택된 계측된 데이터에 기반하여 시도 메시지를 구성하고, 구성된 시도 메시지를 계측 서비스에 전송한다. 계측 서비스는 시도 메시지로부터 계측된 데이터를 획득하고, 계측된 데이터를 저장한 후, 시도 메시지에 기반하여 클라이언트에게 되돌아갈 응답 메시지를 구성한다.

[0035] 클라이언트는 선택된 계측된 데이터의 KID 리스트를 포함하는 응답 메시지를 계측 서비스로부터 수신하고, 시도 메시지에 대응하는 응답 메시지임을 확인한다. 그 이후에, 클라이언트는 리스트에 있는 각각의 KID를 마다 선택된 MID 와 KID를 가진 계측용 데이터베이스로부터 계측된 데이터를 제거함으로써 응답 메시지의 KID 리스트를 처리 한다.

발명의 구성 및 작용

[0036] [컴퓨터 환경]

[0037] 도 1과 다음의 설명은 본 발명 및/또는 그 일부분이 구현될 수 있는 적당한 컴퓨팅 환경을 일반적으로 설명한다. 비록 필요 조건은 아니지만, 본 발명은 클라이언트 워크스테이션 또는 서버와 같은 컴퓨터에 의해 실행되는 프로그램 모듈과 같은, 컴퓨터-실행가능 명령어들의 일반적인 관점에서 설명될 수 있다. 일반적으로, 프로그램 모듈은 특정 작업을 수행하거나 특정 추상화 데이터 타입들을 구현하는 루틴들, 프로그램들, 객체들, 컴포넌트들, 데이터 구조들을 포함한다. 또한, 본 발명 및/또는 그 일부분은 휴대형 장치, 멀티프로세서 시스템들, 마이크로프로세서 또는 프로그램가능한 가전 제품, 네트워크 PC들, 미니컴퓨터들, 메인프레임 컴퓨터들 등을 포함하여 다른 컴퓨터 시스템에서 구현될 수 있는 것에 주목할 필요가 있다. 또한, 본 발명은 통신 네트워크를 통하여 링크 연결된 원격 처리 장치들에 의해 작업들이 수행되는 분산 컴퓨터 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈들은 지역 저장 장치들, 및 원격 저장 장치들에 위치될 수 있다.

[0038] 도 2에 도시된 바와 같이, 예시된 범용 컴퓨팅 시스템은 프로세싱 유닛(121), 시스템 메모리(122), 및 시스템 메모리를 포함하는 다양한 시스템 컴포넌트들을 프로세싱 유닛(121)에 연결시키는 시스템 버스(123)를 포함하는 통상의 개인용 컴퓨터(120) 등을 포함한다. 시스템 버스(123)는 메모리 버스 또는 메모리 컨트로러, 주변장치 버스, 및 다양한 버스 아키텍처 중 임의의 것을 사용하는 지역 버스를 포함한 여러 형태의 버스 구조가 될 수 있다. 시스템 메모리는 롬(ROM:124)과 램(RAM:125)을 포함한다. 시동 시와 같은 개인용 컴퓨터(120) 내의 엘리먼트 사이의 정보 전송을 돕기 위한 기본 루틴을 포함하는 바이오스(126:BIOS)는 롬(124)에 저장되어 있다.

[0039] 개인용 컴퓨터(120)는 하드디스크(도시 안됨)로부터 읽고 쓰기 위한 하드디스크 드라이브(127), 가반형 자기디스크(129)로부터 읽고 쓰기 위한 자기디스크 드라이브(128), CD-ROM 또는 다른 광 매체와 같은 가반형 광디스크(131)로부터 읽고 쓰기 위한 광디스크 드라이브(130)를 추가로 포함한다. 하드디스크 드라이브(127), 자기디스크 드라이브(128), 및 광디스크 드라이브(130)는 각각 하드디스크 드라이브 인터페이스(132), 자기디스크 드라이브 인터페이스(133), 및 광디스크 인터페이스(134)를 통해 시스템 버스(123)에 연결되어 있다. 드라이브들과 이와 관련된 컴퓨터 판독가능한 매체들은 개인용 컴퓨터(120)를 위한 컴퓨터 판독가능 명령어들, 데이터

구조들, 프로그램 모듈들, 및 다른 데이터들을 저장할 수 있는 비휘발성 저장 공간을 제공한다.

[0040] 비록 여기에 예시된 환경이 하드디스크, 가반형 자기디스크(129), 및 가반형 광디스크(131)를 이용할지라도, 컴퓨터에 의해 액세스가능한 데이터를 저장할 수 있는 다른 유형의 컴퓨터 판독가능한 매체들도 예시된 운영 환경에서 사용될 수 있다. 다른 형태의 매체들은 자기 카세트, 플래시 메모리, 디지털 비디오 디스크, 베르누이(Bernoulli) 카트리지, 램, 롬 등의 매체들이 될 수 있다.

[0041] 운영 체제(135), 하나 이상의 애플리케이션 프로그램(136), 다른 프로그램 모듈(137), 및 프로그램 데이터(138)를 포함한 많은 프로그램 모듈들이 하드디스크, 자기디스크(129), 광디스크(131), 롬(124), 또는 램(125) 상에 저장될 수 있다. 사용자는 명령어들과 정보를 키보드(140)과 마우스(142)와 같은 입력 장치들을 통해 개인용 컴퓨터(120)에 입력할 수 있다. 다른 입력 장치들(도시 안됨)로서는 마이크로폰, 조이스틱, 게임 패드, 위성 디스크, 스캐너 등이 포함될 수 있다. 입력 장치들은 시스템 버스에 접속되어 있는 직렬 포트 인터페이스(146)를 통하여 프로세싱 유닛(121)에 주로 연결되나, 병렬 포트, 게임 포트, 또는 USB와 같은 다른 인터페이스들을 통해서도 연결될 수 있다. 모니터(147) 또는 다른 형태의 표시 장치들은 비디오 어댑터(148)와 같은 인터페이스를 통해 시스템 버스(123)에 연결되어 있다. 모니터(147)와는 별도로, 개인용 컴퓨터는 전형적으로 스피커나 프린터와 같은 다른 주변 출력 장치들(도시 안됨)을 포함한다. 또한, 도 2에 예시된 시스템은 호스트 어댑터(155), SCSI 버스(156), 및 SCSI 버스(156)에 연결된 외부 저장 장치(162)를 포함한다.

[0042] 개인용 컴퓨터(120)는 원격 컴퓨터(149)와 같은 하나 이상의 원격 컴퓨터에 논리적으로 연결된 네트워크 환경에서도 동작할 수 있다. 원격 컴퓨터(149)는 다른 개인용 컴퓨터, 서버, 라우터, 네트워크 PC, 대등(peer) 장치 또는 일반적인 다른 네트워크 노드일 수 있으며, 도 2에는 오직 하나의 저장 장치로 메모리(150)가 도시되었을지라도 전형적으로 개인용 컴퓨터(120)에 관련되어 위에서 엘리먼트 전부 또는 대부분을 포함한다. 도 2에 도시된 논리적인 연결은 근거리 통신망(LAN:151)과 광역 통신망(WAN:152)을 포함한다. 이런 네트워킹 환경은 사무실, 기업 컴퓨터 네트워크, 인트라넷, 및 인터넷에서 흔히 존재한다.

[0043] 개인용 컴퓨터(120)가 근거리 통신망 환경에서 사용될 때, 네트워크 인터페이스(153) 또는 어댑터를 통하여 근거리 통신망(151)에 접속된다. 개인용 컴퓨터(120)가 광역 통신망 환경에서 사용될 때, 인터넷과 같은 광역 통신망(152)을 통해 통신 링크를 설정하기 위한 모뎀(154) 및 다른 수단들을 전형적으로 포함한다. 내부 또는 외부의 모뎀(154)은 직렬 포트 인터페이스(146)를 통해 시스템 버스(123)에 연결된다. 네트워크 환경에서, 개인용 컴퓨터(120) 또는 그 일부분에 관련하여 설명한 프로그램 모듈들은 원격 메모리 저장 장치에 저장될 수 있다. 도시한 네트워크 연결들을 예로서 제시하였으며, 컴퓨터들 사이에 통신 링크을 설정하기 위한 다른 수단들도 이용가능 하다.

[0044] [콘텐츠(12)에 대한 액세싱 계측]

[0045] 본 발명에서, 콘텐츠 보호 시스템(10)에 따른 컴퓨팅 장치(14) 상에서의 콘텐츠(12) 액세싱은 무엇을 계측할 것인가 정의하기, 계측으로부터 추출된 데이터를 컴퓨팅 장치 또는 그 밖의 어느 곳에 어떤 방법으로 저장할지 정의하기에 따라 계측된다. 이렇게 계측된 데이터는 여러 컴퓨팅 장치들(14) 각각으로부터 계측된 데이터를 수집하는 계측 서비스(24)(도 1)에 주기적으로 보고하며, 특히 일련의 프로시저에 따라 계측서비스(28)에 보고된다.

[0046] 엄밀히 말해서, 콘텐츠 보호란 콘텐츠 소유자 및 제공자의 요건에 맞지 않는 방식으로는 디지털 콘텐츠(12)를 사용할 수 없도록 하는 콘텐츠(12)의 모든 방법들과 기술 범위를 의미하는 것에 주목할 필요가 있다. 그 방법들에는 특히 복제 보호(CP:Copy Protection), 링크 보호(LP:Link Protection), 조건부 액세스(CA:Conditional Access), 권한 관리(RM:Rights Management), 및 디지털 권한 관리(DRM:Digital Rights Management)가 포함된다. 임의 콘텐츠 보호 시스템(10)의 기본은 보호된 콘텐츠(12)의 사용을 위한 암시적 및 명시적 규정들을 확실하게 준수하는 트러스티드 애플리케이션만이 비보호된 형태로 액세스를 시도할 수 있다는 것이다. 전형적으로, 콘텐츠(12)는 암호화함으로써, 오직 트러스티드 당사자만이 콘텐츠를 복호화할 수 있는 방식으로 보호된다.

[0047] 엄격한 의미에서, 복제 보호는 저장 장치 상에 상주하는 콘텐츠(12)에 적용되는 반면에, 링크 보호는 애플리케이션들과 장치들 사이에서 전송 매체 통해 콘텐츠를 전송할 때에 적용된다. 조건부 액세스는, 프리미엄 프로그램들, 채널들 또는 영화들을 전송 중에 암호화하는, 좀더 정교한 형태의 링크 보호라고 여겨질 수 있다. 콘텐츠(12)를 접속하기 위해, 오직 사용 요금을 지불한 가입자에게만 콘텐츠를 복호화할 키가 제공된다.

[0048] 디지털 권한 관리는 특정 콘텐츠(12)의 사용 허가에 관련된 규정들이 명확하고, 콘텐츠(12) 자체에 속하거나 관련되는 확장가능한 아키텍처이다. 디지털 권한 관리 메커니즘은 각각의 콘텐츠에 또는 그 콘텐츠의 하위 컴포넌트까지의 수준으로 보다 강력한 제어 기능과 융통성을 제공하면서도, 다른 방법들 보다 더욱 다양하고 강력한 규정들을 지원할 수 있다. 디지털 권한 관리 시스템의 한 실시예는 1999년 4월 12일 출원된 미국특허출원 09/290,363과 1999년 3월 27일 가출원된 60/126,614에 개시되어 있으며, 이들 문헌의 전체는 참조 문헌으로서 본원에 포함되는 것으로 한다.

[0049] 권한 관리는 콘텐츠(12)가 기관 또는 그 기관 부속 기관 내에서만 액세스되도록 보호되는 디지털 권한 관리 유형을 갖는다. 권한 관리의 한 예로서 2002년 7월 29일 출원된 미국특허출원 10/185,527, 10/185,278, 및 10/185,511에 개시되어 있으며, 이들 문헌의 전체는 참조 문헌으로서 본원에 포함되는 것으로 한다.

[0050] [무엇을 계측할 것인가 정의하기]

[0051] 본 발명의 한 실시예로서, 컴퓨팅 장치 상에서의 계측은 해당 콘텐츠(12)를 렌더링하기 위해 라이센스(16)를 이용하는 과정중에, 컴퓨팅 장치(14) 상의 트러스티드 컴포넌트(18)의 감시와 제어하에 실행된다. 이 실시예에서, 확장성 생성 언어(XML:eXtensible Markup Language) 기반의 라이센스(16) 등에서 이용될 수 있는 계측 탭을 라이센스(16)가 포함하면, 콘텐츠(12)의 액세싱, 콘텐츠(12) 사용 정도, 콘텐츠(12)의 렌더링을 계측할 수 있다. 그러므로, 라이센스(16) 내의 계측 탭의 존재에 의거하여 계측 실행여부가 결정될지라도, 실제 계측은 콘텐츠(12)에 관련되어 실행된다는 것에 주목해야 한다.

[0052] 예를 들면, 라이센스(16) 중 다음 일부분이 계측 ID(MID) 태그를 포함하므로, 대응하는 콘텐츠(12)는 콘텐츠(12)를 렌더링하는 과정에서 트러스티드 컴포넌트(18)에 의해 계측될 수 있다.

[0053]
```
<LICENSE version = "2.0.0.0">
```

[0054]
```
        ...
```

[0055]
```
        <LICENSORINFO>
```

[0056]
```
                ...
```

[0057]
```
                <DATA>
```

[0058]
```
                        ...
```

[0059]
```
                        <KID>FgA3Mep5 + UiW5yB2CuevGg==</KID>
```

[0060]
```
                        <MID>UiW5yBMep2CuevGg5 + FgA3==</MID>
```

[0061]
```
                        ...
```

[0062]
```
                </DATA>
```

[0063]
```
                ...
```

[0064]
```
        </LICENSORINFO>
```

[0065]
```
        ...
```

[0066]
```
</LICENSE>
```

[0067] MID 태그(이후, MID로 표기)와 관련된 데이터는 Base64 인코딩된 16바이트 식별자(Base64 endcoded 16-byte identification)일 수 있다. 이후에 설명될 본 발명의 한 실시예에서, MID는 라이센스(16)와 관련하여 수집된 계측된 데이터의 수신자를 식별함에 주목해야 한다. 또한 KID 태그는 라이센스(16)가 포함된 콘텐츠(12)임을 식별하고, 최소한 일부 경우에는 KID 태그(이후, KID로 표기)와 관련있는 데이터는 콘텐츠(12)를 복호화하기 위한 콘텐츠 키(KD)를 추출해낼 수 있는 값을 나타낼 수 있다는 것에 주목할 필요가 있다.

[0068] 본 발명의 정신과 범주 내에서, 트러스티드 컴포넌트(18)는 콘텐츠(12)의 사용에 관련하여 특정 타입의 계측된 데이터를 수집할 수 있다. 본 발명의 한 실시예에서, 트러스티드 컴포넌트(18)는 안전한 저장소(22)에 렌더링

권한(재생, 복제, 전송, 편집, 등)에 관련된 각각의 계수를 유지하고, 콘텐츠(12)를 액세스할 때마다 각각의 권한에 대한 계수 값을 증가시킨다. 사용자 또는 이외의 사람들이 계측된 데이터를 부정 사용하지 않도록, 안전한 저장소(22)를 사용하여 계측된 데이터를 저장한다는 것에 주목할 필요가 있다. 그렇지 않다면, 예를 들어 사용시마다 요금을 지불하는 사용자가 계측된 데이터를 인가된 것보다 더 적게 사용한 것으로 바꿀 수도 있다.

[0069] 본 발명의 또 다른 실시예에서, MID 태그는 이것과 함께 권한 사항을 계수하고 있는(도시 안됨) 데이터를 포함할 수도 있고, 측정해야할 콘텐츠(12)의 다른 사용도 측면 및 측정 방법(도시 안됨)에 대한 데이터를 포함할 수 있다. 그러므로, 암시된 바와 같이 트러스티드 컴포넌트는, 콘텐츠(12)가 렌더링된 시간 만큼, 랜터링이 시작된 횟수 만큼, 렌더링이 종료된 횟수 만큼, 또는 렌더링 동안의 키보드 타이핑 정도 혹은 마우스 움직임 정도 등의 계측을 수행할 수 있고, 계측된 데이터를 안전한 저장소(22)에 적절하게 저장한다.

[0070] [계측으로부터 추출된 데이터를 저장하기]

[0071] 도 3에서 도시된 바와 같이, 트러스티드 컴포넌트(18)는 콘텐츠(12)를 렌더링(즉, 액세스)하기 위해서 해당 라이센스(16)의 이용에 관련하여 콘텐츠(12)에 관련된 계측된 데이터를 수집하고, 수집된 계측된 데이터를 안전한 저장소(22)에 적절하게 저장하는 것이 바람직하다. 또한 부가적으로 트러스티드 컴포넌트(18)는 렌더링하기 위해 라이센스(16) 사용에 관련된 데이터를 수집할 수도 있고, 안전한 저장소(22)에 수집된 데이터를 라이센스 데이터로서 저장할 수 있다(도시 안됨).

[0072] 본 발명의 한 실시예에서, 도 3에 도시된 바와 같이 트러스티드 컴포넌트(18)는 계측을 촉발시켜 계측 데이터를 생성하는 라이센스(16)의 MID에 따라 또한 라이센스(16)에 설정되어 있는 대로 해당 계측된 콘텐츠(12)의 MID와 KID에 따라 계측된 데이터를 안전한 저장소(22)의 계측용 데이터베이스(26)에 저장한다. MID는 특히, 트러스티드 컴포넌트(18)는 계측된 데이터를 안전한 저장소(22)의 계측용 데이터베이스(26)에 저장할 때, 일차적인 색인 값으로는 MID를 이차적인 색인 값으로는 KID를 사용한다. 그러므로, 특정 MID 와 KID를 갖는 라이센스(16)를 사용하여 특정 KID를 갖는 콘텐츠(12)를 렌더링할 경우, 트러스티드 컴포넌트(18)는 사용도를 반영하기 위해 안전한 저장소(22)의 데이터베이스(26)에 있는 해당 MID와 KID 색인값을 업데이트한다. 예를 들면, 콘텐츠를 재생 두번(PLAYed twice) 및 복제 한번(COPYed once) 하였다면, 트러스티드 컴포넌트(18)는 안정한 저장소(22)의 데이터베이스(26)에 존재하는 해당 MID와 KID 색인값을 찾아서, 재생(PLAY) 계수 값을 두번 증가시키고, 복제(COPY) 계수 값을 한번 증가시킬 수 있다.

[0073] 여러 라이센스(16)들이 각각 동일한 콘텐츠(12)를 렌더링할 때, 동일한 MID 혹은 다른 MID를 가질 수 있는 것에 주목해야 한다. 그러므로, 만약 두개의 라이센스(16)가 각각 동일한 MID를 갖고 콘텐츠(12)를 한번 재생하는 것에 사용된다면, MID와 KID 색인값에 해당하는 재생 계수를 두번 재생하였으므로 두번 증가시킨다. 따라서, 만약 두개의 라이센스(16)가 다른 MID(MID1과 MID2)를 갖고 콘텐츠(12)를 한번 재생하는 것에 사용된다면, MID1과 KID 색인값에 해당하는 재생 계수를 한번 재생에 대해 한번만 증가시키고, MID2와 KID 색인값에 해당하는 재생 계수도 한번 재생에 대해 한번만 증가시킬 것이다.

[0074] [계측 서비스]

[0075] 인식할 수 있는 바와 같이, 트러스티드 컴포넌트(18)에 의해 안전한 저장소(22)의 계측용 데이터베이스(26)에 누적된 계측된 데이터는 중심 계측 서비스(24)에 주기적으로 전달되며, 이로써 계측서비스(24)는 다수의 컴퓨팅 장치들로부터 계측된 데이터를 수신하고 적절하게 처리할 수 있다. 본 발명의 정신과 범주 내에서, 적절한 처리를 한다. 예를 들면, 콘텐츠(12)의 저자가 사용량에 근거하여 특허권 사용료를 징수하려고 한다면, 계측 서비스(24)는 콘텐츠(12)에 관련하여 정해진 기간동안 총 사용 횟수를 통합하여, 그 횟수를 저자나 특허권 지불 개체에게 보고할 수 있다. 또는, 계측 서비스는 처리를 수행하는 다른 서비스가 검색할 수 있도록 단순히 계측된 데이터를 수신하고 저장할 수 있거나, 저장된 계측된 데이터를 다른 서비스에게 주기적으로 전달할 수 있다.

[0076] 어느 서비스가 계측된 데이터를 실제로 처리하는 것에는 관계없이, 각각의 계측된 데이터가 MID와 KID 색인값에 따라 계측용 데이터베이스(26)에 저장되므로, 이런 데이터는 MID와 KID 색인값을 갖고 계측 서비스(24)에 전달될 수 있으며, 또한 이런 MID와 KID 색인값에 따라 처리될 수 있다. 따라서, 전달된 계측된 데이터의 처리는 MID와 KID 색인값에 따라 실행될 수 있다. 그러므로, 콘텐츠(12)의 총 사용량이 임의의 값에 도달하면 콘텐츠(12) 소유자가 정액 요금을 징수하는 경우, 총 사용량은 계측 서비스(24)를 통해 콘텐츠(12)에 대응하는 계측된

데이터와 관련된 KID 색인값에 근거하여 얻어질 수 있다.

[0077] 본 발명의 한 실시예로서, 다양한 계측 서비스들(28)은 전달된 보고된 계측된 데이터를 수신하도록 예를 들어 설명할 수 있고, 각각의 계측된 데이터는 각각의 계측된 데이터와 관련된 MID에 근거하여 특정 계측 서비스(24)에 전달된다. 인식할 수 있는 바와 같이, 각각의 계측 서비스(24)는 하나 이상의 MID와 관련이 있을 수 있으므로, 하나 또는 그 이상의 MID와 관련될 수 있고, 이런 하나 또는 그 이상의 MID와 관련된 계측된 데이터를 수신할 수 있다.

[0078] 계측 서비스(24)와 MID의 관계는 계측용 인증서(30)를 발행하는 콘텐츠 관리기관에 의해 설정되는데, 계측용 인증서는 URL(웹주소), 공용키 PU-M, 서명과 같은 해당 계측 서비스(24)의 식별자, 즉 MID를 포함하고 있다. 그러므로, 해당 계측 서비스(25)에 관련된 특정 MID를 가진 계측된 데이터를 보고하는, 각각의 컴퓨팅 장치(14) 상의 트러스티드 컴포넌트(18)가, 계측 서비스(24)를 갖는 특정 MID를 식별하려고 한다면, 각각에 대응하는 계측용 인증서(30)를 소유해야 한다. 전형적으로, 트러스티드 컴포넌트(18)가 초기화될 때나 정기적으로 업데이트 될 때, 트러스티드 컴포넌트는 하나 이상의 계측용 인증서(30)를 제공받을 수 있다.

[0079] [계측된 데이터를 계측 서비스에 보고하기]

[0080] 컴퓨팅 장치(14)(이하, 클라이언트(14)로 표기)는 계측용 데이터베이스(26)에 계측된 데이터를 일정 시간 누적시켜 저장하였다가, 계측된 데이터를 하나 또는 그 이상의 계측 서비스(28)에 주기적으로 보고할 수 있다. 본 발명의 정신과 범주 내에서, 보고 주기는 적절하게 정해질 수 있다. 예를 들면, 하루마다, 일주일마다, 격주마다, 월마다 보고될 수 있다. 또한, 보고 주기는 계측용 데이터베이스(26)가 일정 크기에 도달하거나 일정량의 계측된 데이터를 갖는 경우에 근거하여 정해질 수 있다.

[0081] 계측된 데이터를 보고할 때, 클라이언트(14)는 계측용 데이터베이스(26)에 있는 누적시킨 모든 계측된 데이터를 보고하거나, 계측용 데이터베이스(26)에 있는 누적시킨 계측된 데이터의 일부분만을 보고할 수 있다. 특히, 본 발명의 한 실시예에서, 클라이언트(14)는 계측용 인증서(30) 각각에 근거하여 계측용 데이터베이스(26)에 있는 누적시킨 계측된 데이터를 보고한다. 그러므로, 만약 클라이언트(14)가 계측용 데이터베이스(26)에 있는 소정의 계측된 데이터에 대응하는 계측용 인증서(30)를 소유하고 있지 않다면, 이런 소정의 계측된 데이터는 보고되지 않는다.

[0082] 어쨌든, 도 4를 참조해 보면, 본 발명의 한 실시예에서, 클라이언트(14)는 계측용 인증서(30) 각각에 근거하여 계측용 데이터베이스(26)에 있는 누적시킨 계측된 데이터를 다음의 과정에 따라 보고한다. 처음에, 클라이언트(14)는 특정 계측용 인증서(30)를 선택하고 서명에 근거하여 이를 검증하며(단계 401), 검증된 계측용 인증서(30)로부터 이미 설정된 MID 결정한다(단계 403). 그 다음에, 클라이언트(14)는 이런 MID에 근거하여, 이와 관련된 MID를 갖는 계측용 데이터베이스(26) 내에 있는 계측된 데이터 중 적어도 일부분을 선택하고, 소정의 포맷으로 복제한다(단계 405).

[0083] 계측용 데이터베이스에 있는 모든 계측된 데이터는 일차적으로 관련 MID에 근거하여 색인되어 있으므로, 특정 MID와 관련된 계측된 데이터는 최소한 논리적인 의미에서 함께 위치되고, 따라서 특정 MID와 관련된 계측된 데이터를 선택하는 것은 상대적으로 쉬운 작업일 것임을 주목할 필요가 있다. 또한 계측용 데이터베이스에 있는 계측된 데이터는 이차적으로 관련 KID에 근거하여 색인되어 있으므로, 선택된 계측된 데이터는 이미 관련 KID에 따라 정렬되어 있다. 그러므로, 선택된 계측된 데이터는 KID에 따라 정렬된 리스트, 계수 리스트 등과 같은 것이어야 하며, 예를 들면 다음과 같은 XML 포맷을 갖는다.

[0084] <KID0>

[0085] <COUNT1>a</COUNT1>

[0086] <COUNT2>b</COUNT2>

[0087] <COUNT3>c</COUNT3>

[0088] </KID0>

[0089] <KID1>

[0090] <COUNT4>d</COUNT4>

[0091] <COUNT5>e/<COUNT5>

[0092] </KID1>

[0093] <KID2>

[0094] <COUNT6>f</COUNT6>

[0095] </KID2>

[0096] 계측된 데이터는 이미 클라이언트(14)의 계측된 데이터베이스(26)에 XML 포맷으로 존재할 수 있으며, 이 경우 시도 메시지에도 말그대로 동일하게 복제될 수 있다.

[0097] 본 발명의 한 실시예에서, 정형화된 선택된 계측된 데이터를 가진 클라이언트(14)는 정형화된 계측된 데이터와 계측용 인증서(30)에 의거하여 시도 메시지를 구성한다(단계 407). 예를 들어 시도 메시지는, 계측용 인증서(30)로부터의 MID, 계측용 인증서(30)로부터 해당 계측 서비스(24)에 관한 URL 이나 다른 식별자, 시도 메시지용으로 선택된 트랜잭션 ID(TID), 정형화된 계측된 데이터를 포함한다. 정형화된 계측된 데이터가 다른 개체에게 보여지지 않도록, 시도 메시지내의 정형화된 계측된 데이터는 대칭 패스 키에 따라 암호화되어 passkey(metereddata)를 생성하며, 패스 키는 그 자체가 계측용 인증서(30)로부터의 PU-M에 따라 시도 메시지에서 암호화되어 PU-M(passkey)를 생성한다. 이런 패스 키는 본 발명의 정신과 범주 내에서 임의의 적절한 다른 키가 될 수 있다. 예를 들면, 패스 키는 클라이언트(14)에 의해서 단방향 재현 가능한 방식으로 MID로부터 부분적으로 추출되어 진다.

[0098] TID는 Base 64 코딩된 16 바이트 식별자일 수 있으며, 시도 메시지가 성공적으로 송수신 될 때마다 램덤하게 생성되고, 이후에 자세히 설명되어 있듯이 소정의 계측된 데이터가 계측용 데이터베이스(26)으로부터 삭제된다. 이후에 더욱 상세히 설명되어 있듯이, 클라이언트(14)는 MID를 위한 이전 시도 메시지 처리를 성공적으로 수행하자 마자, 현재 시도 메시지에 관한 MID를 위한 TID를 이미 생성하고, 이런 생성된 TID를 계측용 데이터베이스(26)에 현재 시도 메시지의 MID에 따라 저장하는데 MID를 위한 현재 시도 메시지와 연계되어 검색되고 사용되기 위해서이다.

[0099] 어떤 상황 하에서, 클라이언트(14)는 정형화된 계측된 데이터를 모두를 포함하는 시도 메시지를 구성하지 못할 수 있다. 예를 들면, 만약 클라이언트(14)가 상대적으로 제한된 메모리를 가진 단순한 장치라면, 시도 메시지의 크기가 클라이언트(14)의 가용 버퍼 공간 크기에 의해 제한될 수 있다. 실제로 클라이언트(14)가 정형화된 계측된 데이터를 모두 포함하는 시도 메시지를 구성하지 못한다면, 시도 메시지는 세트된 부분 데이터 플래그를 포함할 수 있다. 이후에 더욱 자세히 설명하자면, 시도 메시지를 수신하는 계측 서비스(24)는 수신된 시도 메시지가 정형화된 계측된 데이터 모두를 포함할 것인지에 대한 특정한 고려를 하거나 하지 않을수 있지만, 이 시도 메시지에 응답할 계측 서비스(24)는 세트된 데이터 플래그를 포함하여 클라이언트(14)가 부가적인 정형화된 계측된 데이터를 갖는 다른 시도 메시지를 전송할 것을 상기시킬 것이다.

[0100] 상기에 기술된 바와 같이, 시도 메시지 내의 정형화된 계측된 데이터는 다른 개체들에게 보여지는 것을 막기 위해서, 패스 키에 의해 암호화된다. 다시 말하면, 시도 메시지 또는 적어도 일부분은 패스 키에 의해 해싱 처리되어 해쉬값을 갖고, 그 해쉬값은 다른 개체에 의해 수정되었는지 검출하기 위해 시도 메시지에 포함되어 있다. 인식할 수 있는 바와 같이, 시도 메시지 또는 적어도 일부분이 해쉬값이 추출된 이후에 고의적이든 고의적이 아니든 수정된다면, 해쉬값은 검증에 실패할 것이다.

[0101] 상술한 바와 같이 정형화된 계측된 데이터를 갖는 시도 메시지의 실례는 다음과 같이 구성된다:

[0102] <METERDATA type="challenge">

[0103] <DATA>

[0104] <MID>UiW5yBMep2CuevGg5+FgA3==</MID>

[0105] <TID>Mep2CuevGgUiW5yB5+FgA3==</TID>

[0106] <PASSWORD>encrypted, base64 password</PASSWORD>

[0107] <RECORDS>

[0108] <KID value="KID1">

[0109] <ACTION value="Play">5</ACTION>

[0110] </KID>

[0111] <KID value="KID2">

[0112] <ACTION value="Play">71</ACTION>

[0113] <ACTION value="Burn">2</ACTION>

[0114] </KID>

[0115] ...

[0116] </RECORDS>

[0117] <PARTIALDATA>set</PARTIALDATA>

[0118] </DATA>

[0119] <HASH>

[0120] <HASHALGORITHM type="HMAC" />

[0121] <VALUE>

[0122] Base64-encoded hash

[0123] </VALUE>

[0124] </HASH>

[0125] </METERDATA>

[0126] 시도 메시지는 METERDATA 태그의 타입 속성이 'challenge'로 설정되는 것으로서 식별된다.

[0127] 클라이언트(14)에 의해 구성된 시도 메시지를 네트워크 연결과 같은 적절한 연결을 통해 계측 서비스(24)에 전송한다(단계 409). 이런 네트워크 연결은 본 발명의 정신과 범주 내에서 다른 것으로 대체 가능하다. 한 가지 시나리오를 예를 들면, 이런 연결은 인터넷과 같은 네트워크를 통해 HTTP 같은 상호 수용가능한 프로토콜을 사용하여 클라이언트/컴퓨팅 장치(14)가 계측 서비스(24)와 직접 대화하는 것이 될 수 있다. 또 다른 시나리오의 경우, 클라이언트(14)와 계측 서비스(24)가 바로 연결되는 경우, 이런 연결은 USB-1394와 같은 직접 연결 기술을 의미할 수 있다.

[0128] 시도 메시지가 수신되면, 계측 서비스(24)는 패스 키를 얻기 위해 PR-M을 수신된 시도 메시지에 있는 PU-M(passkey)에 적용하고(단계 411), 얻어진 패스 키에 근거하여 수신된 시도 메시지로부터의 해쉬값을 검증한다(단계 413). 만약 어떤 이유로 인해 해쉬값이 검증되지 않을 경우, 계측 서비스(24)는 동일 MID를 위한 시도 메시지를 재차 보내줄 것을 클라이언트(14)에게 요청하거나 시도 메시지를 단순하게 무시할 수 있는데, 무시하는 경우 클라이언트(14)는 두번의 이전 보고 주기로부터 MID를 위한 계측된 데이터를 누적시켜서, 다음 보고 주기가 만료될 때 시도 메시지를 전송하여 계측된 데이터를 효과적으로 보고하게 된다.

[0129] 해쉬값이 검증될 경우, 계측 서비스(24)는 passkey 를 수신된 시도 메시지의 passkey(metereddata)에 적용하여 계측된 데이터를 얻어낼 수 있고(단계 415), 그 이후에 얻어진 계측된 데이터를 적절한 방식으로 저장할 수 있다. 본 발명의 정신과 범주 내에서, 얻어진 계측된 데이터를 적절한 방식으로 저장할 수 있다(단계 417). 특정한 저장소의 위치 및 저장 방법은 저장된 계측된 데이터를 검색하고 이용하는 다른 서비스(32)(도 1)와 일차적으로 관련된다.

[0130] 트랜잭션을 완수하기 위해, 계측 서비스는 시도 메시지에 근거하여 클라이언트(14)에게 되돌아갈 응답 메시지를

구성한다(단계 419). 보여지는 바와 같이, 응답 메시지에 근거하여, 클라이언트(14)는 시도 메시지의 근간이 되는 선택된 계측된 데이터를 클라이언트(14)의 계측용 데이터베이스(26)에서 삭제한다.

[0131] 어쨰든 본 발명의 한 실시예에서, 사실 시도 메시지의 콘텐츠는 대응하는 응답 메시지의 콘텐츠와 유사하고, 사실 시도 메시지의 일부분을 포함할 수 있다. 그러므로, 예를 들어 응답 메시지는 시도 메시지로부터 MID와 TID를 포함하거나, 정형화된 계측된 데이터의 적어도 일부분을 포함할 수 있다. 응답 메시지를 통해 계측 서비스(24)가 원하는 것은, 클라이언트(14)에게 어떤 KID들을 갖는 계측된 데이터가 처리되었다는 사실을 알려주는 것이며, 응답 메시지가 실제 처리된 계측된 데이터를 포함할 필요는 없다. 따라서, 처리된 계측된 데이터에 관한 KID 리스트가 정형화된 계측된 데이터 중 일부분에 포함되어 응답 메지지가 구성된다.

[0132] 이전에 말했듯이, 리스트가 중요도가 낮아 암호화를 필요로 하지 않을지라도, 응답 메시지에 있는 KID 리스트가 다른 개체에게 공개되는 것을 막기 위해, 시도 메시지에서 얻어낸 패스 키 또는 다른 키에 따라 리스트를 암호화할 수 있다. 만약 클라이언트(14)가 동일한 패스키를 MID 또는 다른 소스로부터 추출할 수 있는 경우에, 시도 메시지에서 패스 키를 얻어낼 수 있으므로, 패스 키를 암호화된 형태로 응답 메시지에 삽입할 필요가 없다.

[0133] 상기에 설명한 바와 같이, 만약 클라이언트(14)가 모든 정형화된 계측된 데이터를 포함하는 시도 메시지를 구성할 수 없다면, 부분 데이터 플래그를 포함하여 구성할 수 있다. 이런 경우에, 응답 메시지가 부분 데이터 플래그 만을 포함하므로, 계측 서비스(24)는 클라이언트(14)에게 정형화된 계측된 데이터를 가진 다른 시도 메시지를 보내줄 것을 상기시킨다. 결과적으로, 응답 메시지 또는 적어도 일부분은 패스 키에 따라 해싱되어 해싱값을 출력하고, 해싱 값은 다른 개체가 임의 수정하는 것을 검출해 낼 수 있도록 응답 메시지에 포함된다. 해쉬값이 추출된 이후에 고의적이든 아니든 응답 메시지 또는 그 일부분이 수정된다면, 해쉬값 검증은 실패한다.

[0134] 응답 메시지의 한 실시예는 다음과 구성된다.

[0135] <METERDATA type="response">

[0136] <DATA>

[0137] <MID>UiW5yBMep2CuevGg5+FgA3==</MID>

[0138] <TID>Mep2CuevGgUiW5yB5+FgA3==</TID>

[0139] <COMMAND>RESET</COMMAND>

[0140] <RECORDS>

[0141] <KID value="KID1" />

[0142] <KID value="KID2" />

[0143] ...

[0144] </RECORDS>

[0145] <PARTIALDATA>set</PARTIALDATA>

[0146] </DATA>

[0147] <HASH>

[0148] <HASHALGORITHM type="HMAC" />

[0149] <VALUE>

[0150] Base64-encoded hash

[0151] </VALUE>

[0152] </HASH>

[0153] </METERDATA>

[0154] 응답 메시지는 METERDATA 태그에서 타입 속성이 'response' 로 설정됨으로서 식별된다. 응답 메시지는 RESET 명령을 포함하고, 이후에 보여지는 바와 같이 클라이언트(14)가 선택된 계측된 데이터를 계측용 데이터베이스(26)에서 삭제할 권한을 필수적으로 부여한다.

[0155] 계측 서비스(24)에 의해 구성된 응답 메시지를 그들 사이의 연결을 통해 클라이언트(14)에게 전송한다(단계 421). 응답 메시지를 수신하면, 클라이언트(14)는 패스 키 재추출 또는 저장되어 있는 패스 키 복제본을 검색함으로써 패스 키를 얻어내고, 얻어진 패스 키에 근거하여 수신된 응답 메시지의 해쉬값을 검증한다(단계 423). 만약 해쉬값이 검증되지 않을 경우, 클라이언트(14)는 동일 시도 메시지에 대한 응답 메시지를 재차 보내줄 것을 계측 서비스(24)에게 요청하거나 응답 메시지를 단순하게 무시할 수 있는데, 무시하는 경우는 클라이언트(14)가 두번의 보고 주기 동안 MID를 위한 계측된 데이터를 누적시켜서 다음 보고 주기가 만료될 때 시도 메시지를 전송하여 계측된 데이터를 효과적으로 보고하기 때문에 가능하다.

[0156] 해쉬값이 검증될 경우, 클라이언트(14)는 응답 메시지에 있는 TID와 MID가 계측된 데이터베이스(26)에서 동일한 MID와 TID를 갖고 매칭된다는 것을 확인하게 된다(단계 425). 그 다음에, 클라이언트(14)는 필요하다면 KID 리스트를 획득하기 위해 패스 키를 응답 메시지에 있는 암호화된 KID 리스트에 적용하고, 리스트 내의 각각의 KID에 따라 선택된 MID와 KID 색인 값을 갖는 계측용 데이터베이스(26)로부터 계측된 데이터를 삭제함으로써 KID 리스트를 처리한다(단계 427). 그러므로, 계측된 데이터가 성공적으로 보고되면, 계측된 데이터는 계측용 데이터베이스(26)로부터 삭제되어 새로운 계측된 데이터가 다음 보고 주기 동안 누적될 수 있도록 한다.

[0157] 계측된 데이터를 삭제하는 것은 본 발명의 정신과 영역아래서 다른 적절한 방식으로 수행될 수 있다. 예를 들면, MID와 KID 색인 값과 이와 관련된 모든 데이터가 삭제될 수도 있고, 또는 MID와 KID 색인값은 제외하고 이와 관련된 데이터만을 삭제할 수도 있다.

[0158] 상기에 기술된 바와 같이, 모든 응답 메시지 리스트에 있는 KID들을 성공적으로 처리하자 마자, 클라이언트(14)는 MID를 위한 다음 시도 메시지에 대한 TID를 생성하고, MID를 위한 다음 시도 메시지와 관련된 검색 및 사용을 위해 현재 시도 메시지의 MID를 따라 생성된 TID를 계측용 데이터베이스(26)에 저장한다(단계 429). TID를 선행 생성하기 위해서, MID가 계측용 데이터베이스(26)에 최초로 보고될 때에 각각의 MID를 위한 TID 초기값이 생성되는 것이 바람직하다.

[0159] 시도 메시지에 있는 TID를 이용하여 응답 메시지를 발생시키면 클라이언트(14)에 의해 보고되는 누적시킨 계측된 데이터가 계측 서비스(24)에 여러 차례 계수 되는 것을 막을 수 있다. 특히, 만약 어떤 이유로 첫번째 보고 주기동안 계측된 데이터를 갖는 첫번째 시도 메시지가 계측 서비스(24)에 도달하여 저장되었으나 클라이언트(14)가 이로부터 응답 메시지를 수신하지 못했다면, 클라이언트는 MID를 위한 새로운 TID를 생성하지도 않고 첫번째 보고 주기에 대한 계측된 데이터를 삭제하지도 않을 것이다. 이런 경우에, 새로운 TID를 생성하지 않는 결과로 첫번째 보고 주기와 다음 보고 주기 동안 계측된 데이터를 갖는 MID를 위한 다음 시도 메시지가 계측 서비스(24)에 도달되고 저장될 것이다. 그러나, 다음 시도 메시지가 첫번째 시도 메시지와 동일한 TID를 갖게 되므로, 계측 서비스(24)는 첫번째 보고 주기에서 저장한 것처럼 첫번째 보고 주기와 다음 보고 주기 모두로부터 계측된 데이터를 첫번째 보고 주기로부터 계측된 데이터로서 저장하지 않아야 한다. 이렇게 저장한다면 첫번째 보고 주기 동안 계측된 데이터를 두번 계수하는 것이 된다. 대신에, 계측 서비스(24)는 다음 시도 메시지가 설정될 때, 첫번째 보고 주기 동안 계측된 데이터를, 첫번째 보고 주기와 다음 보고 주기 모두 동안 계측된 데이터로서 중복 저장해야 한다. 결과적으로, 첫번째 보고 주기 동안 계측된 데이터가 사실 두번 계수되지 않는다. 물론, 계측 서비스(24)가 다음 시도 메시지가 첫번째 시도 메시지의 TID와 동일한 TID를 갖는 다는 것을 인식하지 못한다면, 계측 서비스(24)는 TID들과 관련 계측된 데이터의 데이터베이스를 유지해야 한다.

[0160] 최종적으로, 시도 메시지의 MID를 위한 새로운 TID를 생성하는 클라이언트(14)는 응답 메시지가 부분 데이터 플래그를 포함할지를 결정한다(단계 431). 만약 그렇다면, 클라이언트(14)는 시도 메시지의 MID에 따라 계측 서비스(24)에 보고되어야 하는 부가적인 계측된 데이터를 갖게되고, 단계 405에서 단계 431에 보여진 대로 부가적인 계측된 데이터를 보고하기 위해 하나 이상의 부가적인 시도 메시지를 구성하고 전송한다. 부가적인 시도 메시지를 즉시 전송하지 않더라도, 다음 보고 주기가 만료될 때까지는 지체함 없이 신속하게 전송해야 한다.

[0161] 지금까지 클라이언트(14)가 계측 서비스(24)에게 식별된다고 가정하였다. 사실, 사생활 보호 측면에서 클라이언트(14)의 식별자를 계측 서비스로부터 분리 유지하는 것이 필요하고 권장할 만하다. 그러나, 예를 들어 만약 클라이언트(14)의 사용자가 계측된 데이터에 근거하여 사용 요금을 지불하기로 합의하였기 때문에, 클라이언트(14)가 계측된 데이터를 계측 서비스(24)에 적어도 부분적으로 보고해야 한다면, 사용자에게 계측된 사용량에 근거해서 적절하게 요금이 부과되었다는 것을 확인하기 위해서 클라이언트(14)가 계측 서비스에서 실제로 식별

가능해야 한다. 전형적으로, 이것은 시도 메시지에 클라이언트(14), 사용자들을 식별할 수 있는 디지털 인증서를 포함함으로써 구현되고, 디지털 인증서는 반드시 검증될 수 있는 공용키(PU-U), 및 서명을 포함한다. 그러므로, 시도 메시지가 패스 키에 근거하여 시도 메시지에 해쉬값을 포함하는 것보다, PR-U과 디지털 인증서로부터 PU-U에 근거하여 검증될 수 있는 서명을 대신 포함하는 것이 바람직하다. 유사한 방식으로, 응답 메시지가 패스 키에 근거한 해쉬값을 포함하는 것보다, 계측용 인증서(30)에 관련된 개인 키 PR-M과 계측용 인증서(30)로부터 해당 PU-M에 근거하여 검증될 수 있는 서명을 대신 포함하는 것이 바람직하다.

[0162] [결론]

[0163] 본 발명은 클라이언트(14) 및 계측 서비스(24)가 적절한 트러스티드 컴포넌트(18) 상에 존재하는 어떤 적절한 클라이언트(14) 및 적절한 계측 서비스(24)에서 실행될 수 있다. 본 발명은 클라이언트(14)에서 콘텐츠(14)를 사용 하거나 액세스 한 것을 계측하고, 계측 서비스(24) 또는 다른 서비스(32)에 의해 어떤 목적으로 사용되든지에 관계없이 계측된 데이터가 계측 서비스(24)에 적절하게 보고되는 것을 의미한다.

[0164] 본 발명에 관련된 프로세스들을 실행하기 위한 필수적인 프로그래밍은 관련 프로그래밍 분야에서 분명하고 명확해야 한다. 따라서, 프로그래밍은 여기에 첨부되지는 않았다. 그러므로, 특정 프로그래밍이 본 발명의 정신과 범주 내에서 효과적으로 실행될 수 있다.

[0165] 기술한대로, 본 발명은 계측된 데이터를 생성하고, 클라이언트(14)로부터 계측된 데이터를 계측 서비스(24)에 보고하는 새롭고 유용한 아키텍처 및 방법을 포함한다. 아키텍처 및 방법은 무엇을 계측할 것인지를 정의하기, 계측으로부터 추출된 데이터를 컴퓨팅 장치(14)에 어떤 방법으로 저장할 것인지를 정의하기, 각각의 여러가지 컴퓨팅 장치(14)로부터 계측된 데이터를 수집하는 계측 서비스(24) 정의하기, 어떻게 계측된 데이터를 계측 서비스(24)에 보고할 것인지 정의하기에 관한 것이다.

[0166] 상기에 기술된 실시예는 본 발명의 창의적인 의도에서 벗어남없이 변경이 가능하다. 그러므로, 일반적으로 본 발명은 예시된 특정 실시예에만 국한되지 않고, 청구항에 정의된 대로 본 발명의 정신과 범주 내에서 수정이 가능한 것으로 널리 이해되고 있다.

발명의 효과

[0167] 본 발명은 계측된 데이터를 생성하고, 클라이언트로부터 계측된 데이터를 계측 서비스에 보고하는 새롭고 유용한 아키텍처 및 방법을 제공한다.

도면의 간단한 설명

[0001] 도 1은 계측용 데이터베이스와 그곳으로부터 계측된 데이터를 수신하는 계측 서비스를 가진 클라이언트를 포함하는 예시된 신뢰성 기반의 시스템의 강화된 아키텍처를 도시한 블럭도

[0002] 도 2는 본 발명의 양상 및/또는 그 일부분이 통합될 수 있는 범용 컴퓨터 시스템을 도시한 블럭도

[0003] 도 3은 본 발명의 한 실시예에 따라 도 1의 계측용 데이터베이스에 있는 계측된 데이터, 디지털 콘텐츠, 콘텐츠에 결합된 하나 이상의 디지털 라이센스 사이의 관계를 도시한 블럭도

[0004] 도 4는 본 발명의 한 실시예에 따라 계측된 데이터를 클라이언트로부터 계측 서비스에 보고할 때, 도 1의 클라이언트와 계측 서비스에 의해 수행되는 중요 단계들을 도시한 흐름도

[0005] <도면의 주요 부분에 대한 부호의 설명>

[0006] 10 : 콘텐츠 보호 시스템

[0007] 13 : 콘텐츠 패키지

[0008] 14 : 클라이언트/컴퓨팅 장치

[0009] 16 : 라이센스

[0010] 18 : 트러스티드 컴포넌트

[0011] 20 : 평가기

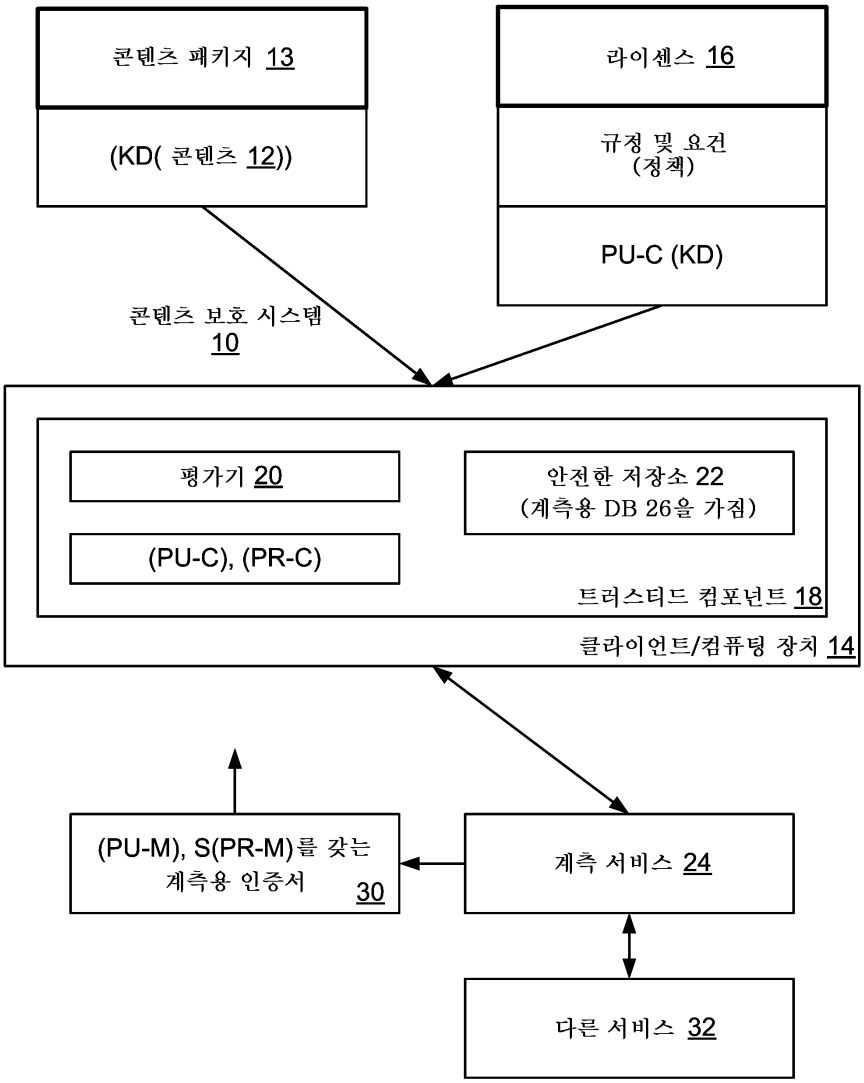
[0012] 22 : 안전한 저장소

[0013] 24 : 계측 서비스

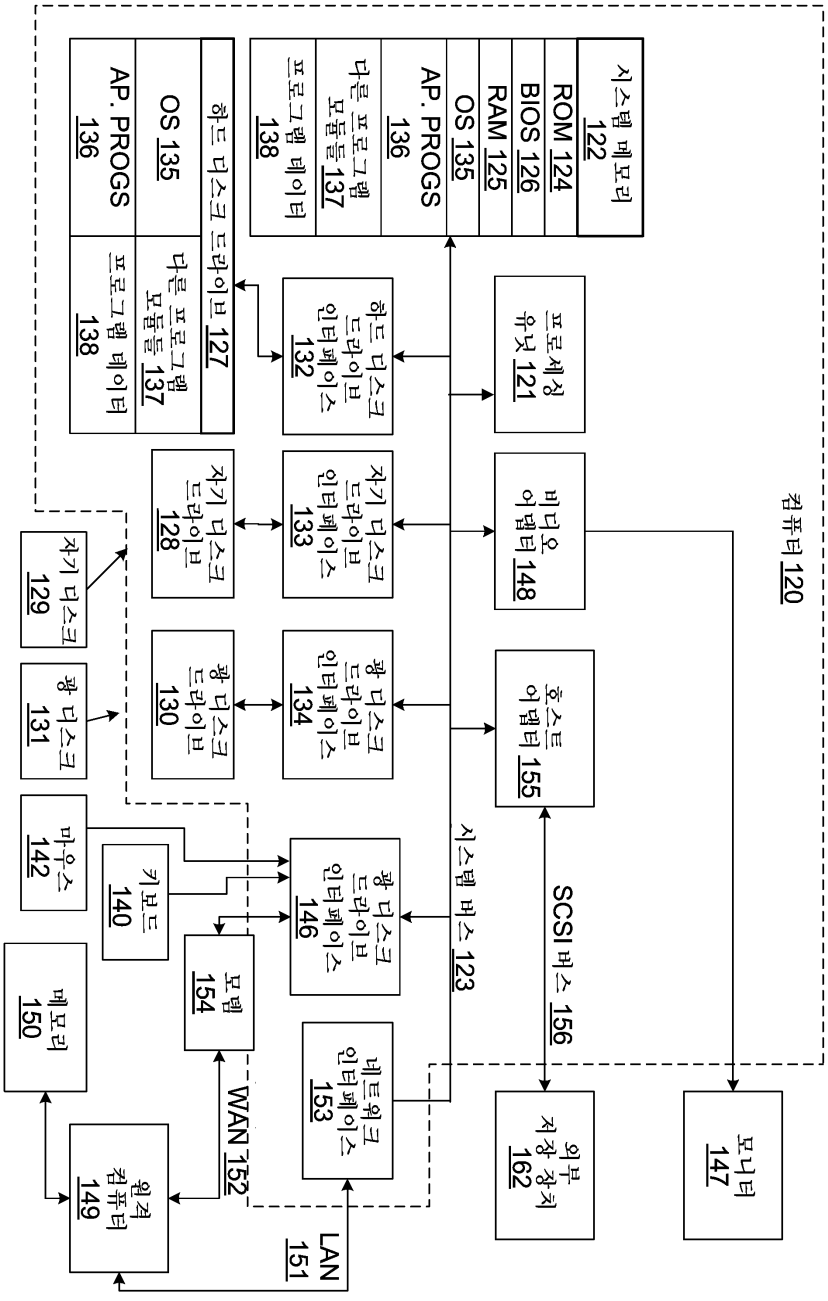
[0014] 30 : 계측용 인증서

도면

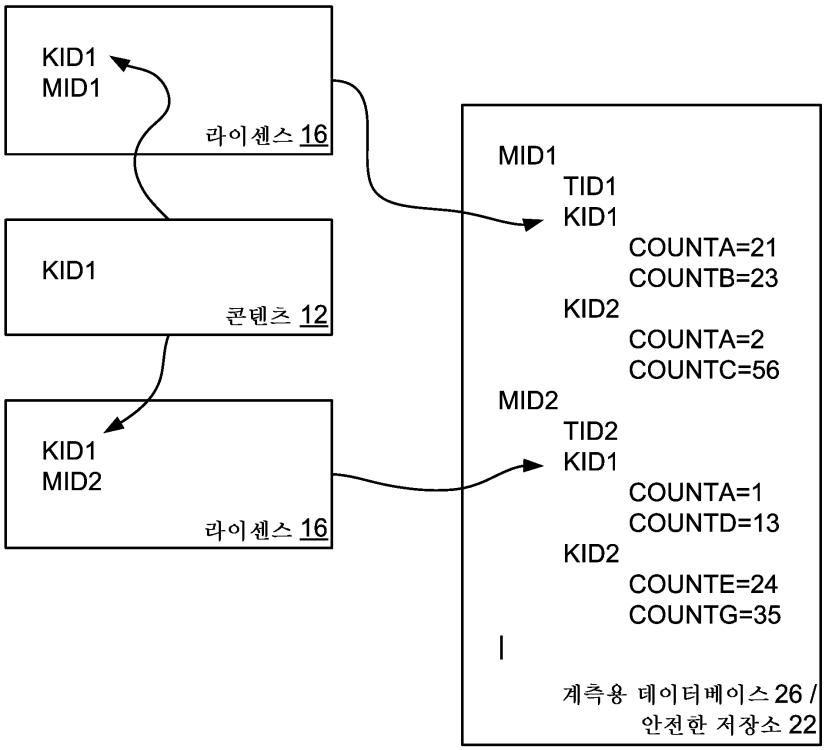
도면1



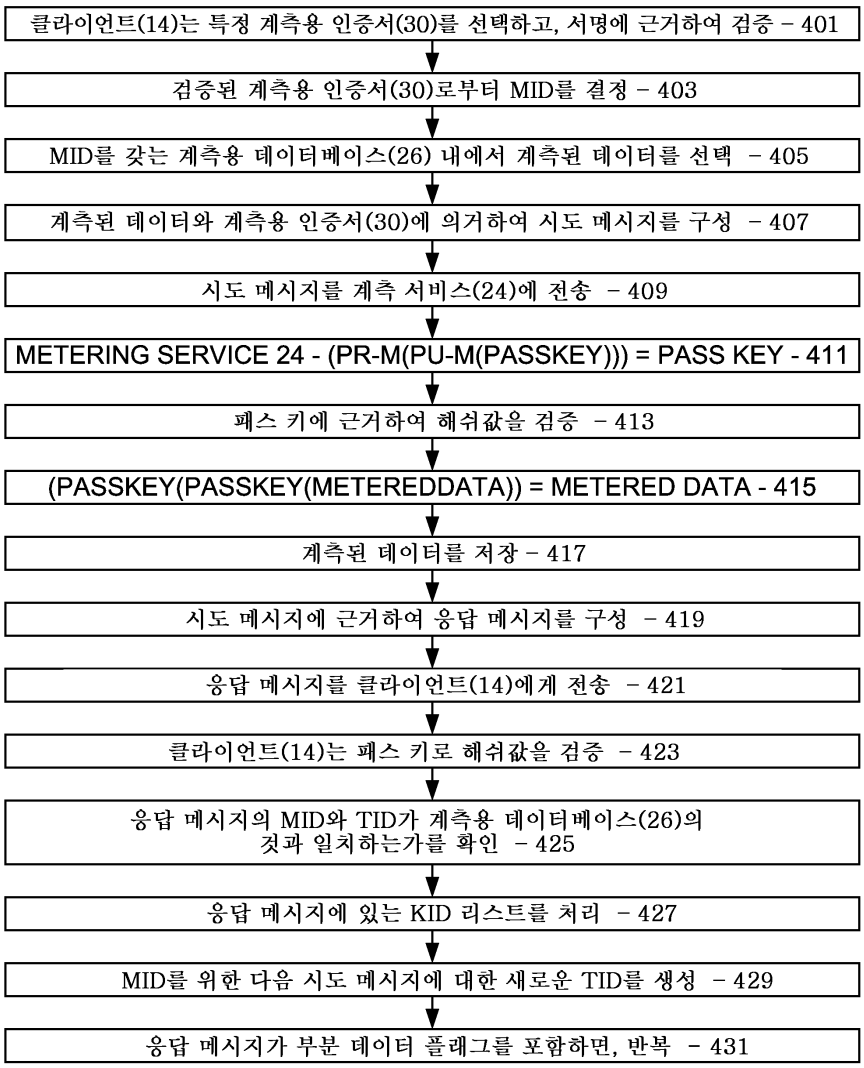
도면2


컴퓨터 120
시스템 메모리 122
ROM 124
BIOS 126
RAM 125
OS 135
AP. PROGS 136
다른 프로그램 모듈들 137
프로그램 데이터 138
하드 디스크 드라이브 127
OS 135
AP. PROGS 136
다른 프로그램 모듈들 137
프로그램 데이터 138
프로세싱 유닛 121
비디오 어댑터 148
호스트 어댑터 155
하드 디스크 드라이브 인터페이스 132
자기 디스크 드라이브 인터페이스 133
광 디스크 드라이브 인터페이스 134
자기 디스크 드라이브 128
광 디스크 드라이브 130
자기 디스크 129
광 디스크 131
마우스 142
키보드 140
광 디스크 드라이브 인터페이스 146
시스템 버스 123
SCSI 버스 156
모뎀 154
네트워크 인터페이스 153
메모리 150
WAN 152
LAN 151
원격 컴퓨터 149
외부 저장 장치 162
모니터 147

도면3


KID1
MID1
라이센스 16
KID1
콘텐츠 12
KID1
MID2
라이센스 16
MID1
TID1
KID1
COUNTA=21
COUNTB=23
KID2
COUNTA=2
COUNTC=56
MID2
TID2
KID1
COUNTA=1
COUNTD=13
KID2
COUNTE=24
COUNTG=35
계측용 데이터베이스 26 /
안전한 저장소 22

도면4


클라이언트(14)는 특정 계측용 인증서(30)를 선택하고, 서명에 근거하여 검증 - 401
검증된 계측용 인증서(30)로부터 MID를 결정 - 403
MID를 갖는 계측용 데이터베이스(26) 내에서 계측된 데이터를 선택 - 405
계측된 데이터와 계측용 인증서(30)에 의거하여 시도 메시지를 구성 - 407
시도 메시지를 계측 서비스(24)에 전송 - 409
METERING SERVICE 24 - (PR-M(PU-M(PASSKEY))) = PASS KEY - 411
패스 키에 근거하여 해쉬값을 검증 - 413
(PASSKEY(PASSKEY(METEREDDATA)) = METERED DATA - 415
계측된 데이터를 저장 - 417
시도 메시지에 근거하여 응답 메시지를 구성 - 419
응답 메시지를 클라이언트(14)에게 전송 - 421
클라이언트(14)는 패스 키로 해쉬값을 검증 - 423
응답 메시지의 MID와 TID가 계측용 데이터베이스(26)의 것과 일치하는가를 확인 - 425
응답 메시지에 있는 KID 리스트를 처리 - 427
MID를 위한 다음 시도 메시지에 대한 새로운 TID를 생성 - 429
응답 메시지가 부분 데이터 플래그를 포함하면, 반복 - 431