

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0096742
(43) 공개일자 2012년08월31일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) H04L 9/32 (2006.01)
H04L 12/24 (2006.01) H04L 12/26 (2006.01)
(21) 출원번호 10-2011-0016015
(22) 출원일자 2011년02월23일
심사청구일자 2011년02월23일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
조충호
충청남도 천안시 동남구 터미널9길 59, 대림아파트 205동 1105호 (신부동)
류승완
경기도 용인시 수지구 상현로 58, 금호베스트빌 252동 1403호 (상현동)
(뒷면에 계속)
(74) 대리인
나승택, 조영현

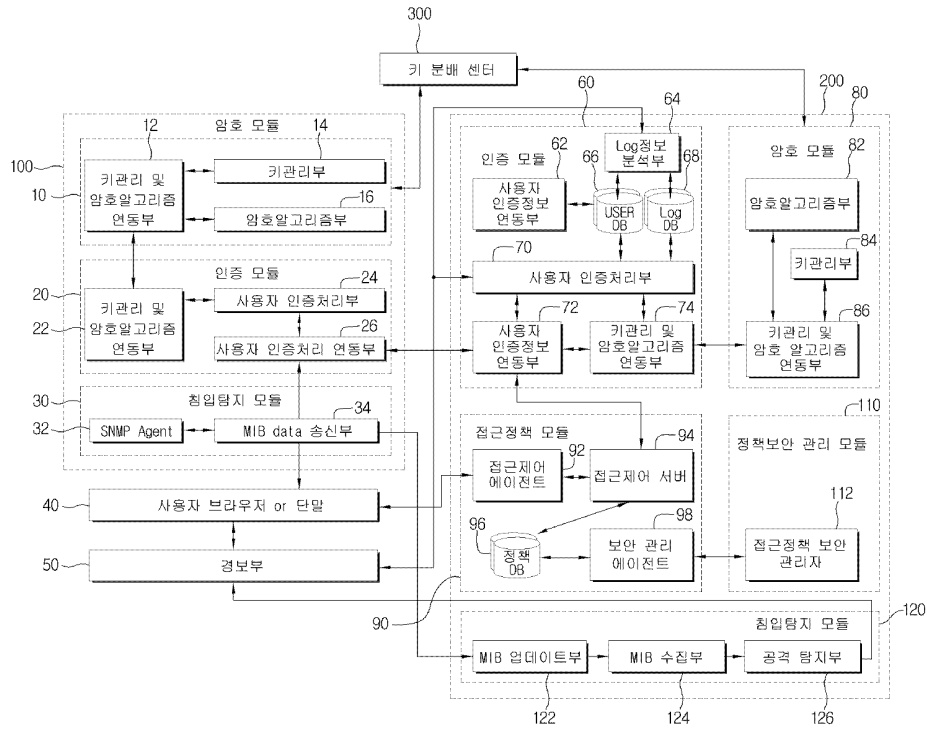
전체 청구항 수 : 총 27 항

(54) 발명의 명칭 **빌딩 에너지 통합 관제 장치 및 방법**

(57) 요약

통합 관제 센터에서 빌딩 용도별 보안정책 정의를 통해 통합적인 에너지 관리를 위한 효율적인 접근제어가 이루어지도록 한 빌딩 에너지 통합 관제 장치 및 방법을 제시한다. 제시된 빌딩 에너지 통합 관제 장치는 서버/클라이언트 구조의 빌딩 에너지 통합 관제 장치로서, 다수의 보안 레벨중에서 어느 한 보안 레벨이 설정되어 사용자에게 부여되되 다수의 빌딩 에너지 관련 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 사용자에게 부여된 접근 정책 정보를 저장하는 정책 데이터베이스, 접근 정책 정보를 생성하고, 다수의 빌딩 에너지 관련 기기들의 일부 또는 전부에 대하여 상기 사용자의 접근 허용 여부를 재설정하는 정책 보안 관리 모듈, 및 서비스 요청을 한 사용자에게 대하여 접근 정책 정보에 근거하여 서비스 접근 여부를 결정하는 접근 제어 서버를 포함한다. 빌딩 에너지 통합 관제 장치의 빌딩 용도별 보안정책 정의를 통해 센터 중심의 통합 에너지 관리를 위한 효율적인 접근제어가 이루어질 수 있다. 임의적 접근 제어 방식과 강제적 접근 제어 방식이 혼용된 보안 정책 설정 방법을 이용함으로써, 보안정책이 효율적으로 관리될 수 있는 효과가 있다.

대표도



(72) 발명자

김태섭

경기도 수원시 팔달구 팔달문로42번길 22, 동오아파트 205호 (지동)

임치현

서울특별시 중구 장충단로10길 36, 15 / 5 (광희동2가)

서시오

충청남도 연기군 조치원읍 새내17길 7, 목화아파트 808호

김이강

충청남도 연기군 조치원읍 모과나무2길 18, 501호

윤석호

서울특별시 관악구 법원단지26길 8 (신림동)

이 발명을 지원한 국가연구개발사업

과제고유번호 1003514220100110031001391810035142201001

부처명 지식경제부

연구사업명 산업원천기술개발사업

연구과제명 고효율 건물에너지 감응형 EMM(Energy Monitoring & Management) 플랫폼 기술개발

주관기관 한국전자통신연구원

연구기간 2010.04.01 ~ 2011.03.31

특허청구의 범위

청구항 1

서버/클라이언트 구조의 빌딩 에너지 통합 관제 장치에서의 빌딩 에너지 통합 관제 방법으로서,
다수의 보안 레벨중에서 어느 한 보안 레벨을 설정하여 사용자에게 부여하되, 다수의 빌딩 에너지 관련 기기들에 대한 접근 허용 여부를 서로 다르게 설정하여 상기 사용자에게 부여하는 단계; 및
상기 다수의 빌딩 에너지 관련 기기들의 일부 또는 전부에 대하여 상기 사용자의 접근 허용 여부를 재설정하는 단계;를 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 2

청구항 1에 있어서,
상기 다수의 보안 레벨은 건물 용도에 따라 분류된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 3

청구항 1에 있어서,
상기 다수의 보안 레벨의 각각은 서로 다른 인증 방식이 적용된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 4

청구항 1에 있어서,
상기 사용자에게 대한 인증을 행하는 단계를 추가로 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 5

청구항 1에 있어서,
상기 사용자로부터의 서비스 요청에 대해 상기 보안 레벨 설정 단계 및 상기 접근 허용 재설정 단계에 의하여 생성된 접근 제어 정책을 근거로 수행하는 단계를 추가로 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 6

청구항 5에 있어서,
상기 접근 제어 정책 수행 단계는,
상기 사용자로부터의 서비스 요청을 수신함에 따라 상기 접근 제어 정책을 기반으로 상기 사용자의 접근 허용 여부를 결정하는 단계; 및
상기 접근 허용으로 결정된 상기 사용자에게 대한 접근 제어 정책에 따른 내용을 수행하는 단계;를 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 7

청구항 6에 있어서,
상기 사용자의 접근 허용 여부 결정 단계는,
상기 사용자로부터의 접근 요청 메시지를 수신하는 단계;
상기 접근 요청 메시지로부터 사용자 아이디, 접근하고자 하는 대상, 및 해당 동작 정보를 추출하는 단계; 및
상기 추출된 정보를 기반으로 해당하는 모든 접근 제어 정책을 검색하여 검색 내용을 제공하는 단계;를 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 8

청구항 5에 있어서,

상기 접근 제어 정책 수행 단계는,

접근 거부 수행시 해당 접근 요청을 거부하고 상기 사용자에게 서비스 거부 메시지를 전달하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 9

청구항 5에 있어서,

상기 접근 제어 정책 수행 단계는 접근 거부 수행시 접근 요청 거부된 정보를 로그 파일에 저장하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 10

청구항 5에 있어서,

상기 접근 제어 정책 수행 단계는 접근 거부 수행시 관리자에게 경보를 전달하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 11

청구항 1에 있어서,

상기 보안 레벨 설정 단계 및 상기 접근 허용 재설정 단계에 의하여 상기 사용자에게 부여된 접근 제어 정책을 저장하는 단계를 추가로 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 12

청구항 1에 있어서,

상기 빌딩 에너지 통합 관제 장치와의 네트워크 연결에 따른 네트워크 구간별로 차별화된 인증 정책이 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 13

청구항 12에 있어서,

상기 인증 정책은 외부 단말과 상기 빌딩 에너지 통합 관제 장치의 보안 게이트웨이 간에는 아이피 인증, 강제적 접근 제어 인증, 및 사용자 아이디 및 패스워드 인증을 혼합한 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 14

청구항 12에 있어서,

상기 인증 정책은 외부 단말과 상기 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 공인인증서에 의한 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 15

청구항 12에 있어서,

상기 인증 정책은 외부 단말에서 상기 빌딩 에너지 통합 관제 장치의 서비스 이용시 아이피 인증, 강제적 접근 제어 인증, 및 사용자 아이디 및 패스워드 인증을 혼합한 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 16

청구항 12에 있어서,

상기 인증 정책은 상기 빌딩 에너지 통합 관제 장치의 관리자와 상기 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 사용자 아이디 및 패스워드 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 17

청구항 12에 있어서,

상기 인증 정책은 건물 내부의 사용자와 상기 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 사용자 아이디 및 패스워드 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 18

청구항 12에 있어서,

상기 인증 정책은 상기 빌딩 에너지 통합 관제 장치의 보안 게이트웨이에서 상기 빌딩 에너지 통합 관제 장치의 서비스 이용시 아이피 인증, 강제적 접근 제어 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 19

청구항 12에 있어서,

상기 인증 정책은 건물 내부의 사용자와 상기 빌딩 에너지 통합 관제 장치의 보안 게이트웨이 간에는 사용자 아이디 및 패스워드 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 20

청구항 12에 있어서,

상기 인증 정책은 상기 빌딩 에너지 통합 관제 장치의 관리자와 보안 게이트웨이 간에는 사용자 아이디 및 패스워드 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 21

청구항 1에 있어서,

트래픽 공격 정보를 수집하고 수집된 정보를 이용하여 공격유무 및 공격유형을 판단하는 단계를 추가로 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 방법.

청구항 22

서버/클라이언트 구조의 빌딩 에너지 통합 관제 장치로서,

다수의 보안 레벨중에서 어느 한 보안 레벨이 설정되어 사용자에게 부여되되 다수의 빌딩 에너지 관련 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 상기 사용자에게 부여된 접근 정책 정보를 저장하는 정책 데이터베이스;

상기 접근 정책 정보를 생성하고, 상기 다수의 빌딩 에너지 관련 기기들의 일부 또는 전부에 대하여 상기 사용자의 접근 허용 여부를 재설정하는 정책 보안 관리 모듈; 및

서비스 요청을 한 사용자에게 대하여 상기 접근 정책 정보에 근거하여 서비스 접근 여부를 결정하는 접근 제어 서버;를 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 장치.

청구항 23

청구항 22에 있어서,

상기 다수의 보안 레벨은 건물 용도에 따라 분류된 것을 특징으로 하는 빌딩 에너지 통합 관제 장치.

청구항 24

청구항 22에 있어서,

상기 다수의 보안 레벨의 각각은 서로 다른 인증 방식이 적용된 것을 특징으로 하는 빌딩 에너지 통합 관제 장치.

청구항 25

청구항 22에 있어서,

상기 사용자에 대한 인증을 행하는 인증 모듈을 추가로 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 장치.

청구항 26

청구항 22에 있어서,

상기 접근 제어 서버의 결정에 따라 접근 제어를 수행하여 그 결과를 로그 파일에 저장하는 접근 제어 에이전트를 추가로 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 장치.

청구항 27

청구항 22에 있어서,

트래픽 공격 정보를 수집하고 수집된 정보를 이용하여 공격유무 및 공격유형을 판단하는 침입 탐지 모듈을 추가로 포함하는 것을 특징으로 하는 빌딩 에너지 통합 관제 장치.

명세서

기술 분야

[0001] 본 발명은 빌딩 에너지 통합 관제 장치 및 방법에 관한 것으로, 보다 상세하게는 다수의 빌딩별 에너지 정보 등을 통합적으로 관제하고 사용자 접근을 제어할 수 있는 빌딩 에너지 통합 관제 장치 및 방법에 관한 것이다.

배경 기술

[0002] 빌딩 에너지 절약에 관한 분야(친환경 저에너지 건축기술)는 녹색성장위원회에서 27대 중점 녹색기술 분야로 선정될 만큼 중요한 사업이다. 빌딩 에너지 절약에 관한 분야는 단순히 빌딩내 센서 기반의 통신망을 구축하여 에너지 절감을 한다는 좁은 의미에 한정되지 않고, 콘텐츠, 통신, 방송, 정보기기 등 여러 분야가 결합되어 다양한 시너지를 창출할 수 있는 분야로 각광받고 있다.

[0003] 빌딩 에너지 관제 센터의 서비스는 다른 사업으로의 무궁한 발전 가능성을 내재함과 동시에 여러 분야의 기술들을 유기적으로 결합하여 사용하고 이중의 유/무선 네트워크와 프로토콜의 혼재로 기존의 다양한 보안 취약점을 그대로 내포하고 있다. 이러한 보안 취약성은 생명 및 자산까지 직접적인 피해를 줄 수 있어 대응책 마련이 필수적이다.

[0004] 따라서, 빌딩 에너지 관제 센터의 서비스 이용의 편리성과 안전성을 동시에 만족시키며, 기존 빌딩 관리 서비스 시스템에 용이하고 유연하게 적용할 수 있는 통합적인 보안 인프라 구축이 필요하다.

[0005] 이에 다양한 사용자의 특성이나 빌딩의 특성을 반영해서 원하는 인증 수단을 선택할 수 있으며, 모든 클라이언트 기기에 탑재될 수 있고, 효율성과 편의성을 고려한 사용자 인증 기술을 제공해야 한다. 또한, 내/외부의 불법 접근이나 침해 사고가 발생 시 능동적으로 접근 권한을 제어하고, 비록 인가된 사용자라 할지라도 불필요한 서비스로의 접근을 차단하는 실시간 접근 권한 제어 기술 개발이 절실하다.

[0006] 통상적으로, 각각의 빌딩에는 에너지 추이 및 다양한 환경요소에 대한 분석을 할 수 있는 전문가가 존재하지 않는다. 그에 따라, 각각의 빌딩에서는 해당 빌딩의 관리자가 경험 기반의 제어를 하였다. 하지만 이러한 경험 기반의 제어 반영은 통일적이지 못하고, 잘못된 제어를 할 수 있어 통합적으로 에너지를 관리해 주는 센터가 필요하다.

[0007] 그에 따라, 빌딩 에너지 통합 관제 센터의 제어 및 관제 대상은 각 건물내 존재하는 조명기기, 냉방기기, 난

방기기, 전열기기 등이 될 수 있다.

- [0008] 빌딩 에너지 통합 관제 센터에 적용되는 통신 방식으로는, 유선 통신 및 무선 통신 모두 활용될 수 있다. 최근 집중적으로 연구되고 있는 무선 통신 기술로는, RF(Radio Frequency), 블루투스(Bluetooth), 무선 LAN, 적외선을 이용하는 IrDA 등이 있다.
- [0009] 한편, 빌딩 에너지 통합 관제 센터에서는 최적화된 에너지 절감대책을 빌딩 에너지 관리자 및 사용자에게 주어야 한다. 그리고, 빌딩 에너지 관리자 및 사용자는 안전하고 신뢰성 있는 정보를 근거로 제어를 행해야 한다. 이를 위해서는, 사용자/빌딩 용도별/서비스에 따라 차등적인 접근을 통해 접근할 수 있도록 하는 접근정책 정의가 필요하다.
- [0010] 또한, 에너지 통합 관제가 이루어지는 빌딩 에너지 통합 관제 센터에서는 강력한 보안 정책에 기반하여 사용자의 다양한 에너지 관련 기기에 대한 데이터 접근이 허용되거나 제한되어야 한다.

발명의 내용

해결하려는 과제

- [0011] 그러나, 일반적으로 사용하는 사용자의 접근권한을 설정하는 보안정책 적용 방식은 각 사용자별로 접근할 수 있는 기기들 및 접근이 제한되는 기기들을 별도로 구분하여 설정하고 있다. 그에 따라, 사용자의 수가 많아지고 관리할 대상인 건물이 많아지게 되면 적용되는 보안정책이 복잡해지고 관리하기 어려운 문제점이 발생한다.
- [0012] 일반적인 보안 설정 방법 중 각각의 기기들에 대한 접근 권한을 차별화하여 설정한 레벨 적용 방식이 있다. 이러한 다양한 건물 용도에 따라 각 개별 사용자의 접근 권한을 해당되는 레벨로 설정하는 보안정책 방식은 사용자와 관리 대상 건물이 많은 환경에서 편리하게 보안정책을 적용할 수 있는 장점이 있다. 그러나, 특정 사용자에게 다른 접근 권한을 적용하기 위해서는 기본적으로 설정된 레벨 이외에 다른 레벨을 생성 및 설정하여 접근 권한을 적용해야 하는 문제점이 있다.
- [0013] 본 발명은 상기한 종래의 문제점을 해결하기 위해 제안된 것으로, 통합 관제 센터에서 빌딩 용도별 보안정책 정의를 통해 통합적인 에너지 관리를 위한 효율적인 접근제어가 이루어지도록 한 빌딩 에너지 통합 관제 장치 및 방법을 제공함에 그 목적이 있다.

과제의 해결 수단

- [0014] 상기와 같은 목적을 달성하기 위하여 본 발명의 바람직한 실시양태에 따른 빌딩 에너지 통합 관제 장치는, 서버/클라이언트 구조의 빌딩 에너지 통합 관제 장치로서, 다수의 보안 레벨중에서 어느 한 보안 레벨이 설정되어 사용자에게 부여되 다수의 빌딩 에너지 관련 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 사용자에게 부여된 접근 정책 정보를 저장하는 정책 데이터베이스; 접근 정책 정보를 생성하고, 다수의 빌딩 에너지 관련 기기들의 일부 또는 전부에 대하여 상기 사용자의 접근 허용 여부를 재설정하는 정책 보안 관리 모듈; 및 서비스 요청을 한 사용자에게 대하여 접근 정책 정보에 근거하여 서비스 접근 여부를 결정하는 접근 제어 서버;를 포함한다.
- [0015] 다수의 보안 레벨은 건물 용도에 따라 분류된다. 이 경우, 다수의 보안 레벨의 각각은 서로 다른 인증 방식이 적용된다.
- [0016] 바람직하게, 사용자에게 대한 인증을 행하는 인증 모듈을 추가로 포함한다.
- [0017] 접근 제어 서버의 결정에 따라 접근 제어를 수행하여 그 결과를 로그 파일에 저장하는 접근 제어 에이전트를 추가로 포함하여도 된다.
- [0018] 그리고, 트래픽 공격 정보를 수집하고 수집된 정보를 이용하여 공격유무 및 공격유형을 판단하는 침입 탐지 모듈을 추가로 포함하여도 된다.
- [0019] 본 발명의 바람직한 실시양태에 따른 빌딩 에너지 통합 관제 방법은, 서버/클라이언트 구조의 빌딩 에너지 통합 관제 장치에서의 빌딩 에너지 통합 관제 방법으로서, 다수의 보안 레벨중에서 어느 한 보안 레벨을 설정하

여 사용자에게 부여하되, 다수의 빌딩 에너지 관련 기기들에 대한 접근 허용 여부를 서로 다르게 설정하여 사용자에게 부여하는 단계; 및 다수의 빌딩 에너지 관련 기기들의 일부 또는 전부에 대하여 사용자의 접근 허용 여부를 재설정하는 단계;를 포함한다.

- [0020] 다수의 보안 레벨은 건물 용도에 따라 분류된다. 이 경우, 다수의 보안 레벨의 각각은 서로 다른 인증 방식이 적용된다.
- [0021] 사용자에게 대한 인증을 행하는 단계를 추가로 포함한다.
- [0022] 사용자로부터의 서비스 요청에 대해 보안 레벨 설정 단계 및 접근 허용 재설정 단계에 의하여 생성된 접근 제어 정책을 근거로 수행하는 단계를 추가로 포함한다.
- [0023] 접근 제어 정책 수행 단계는, 사용자로부터의 서비스 요청을 수신함에 따라 접근 제어 정책을 기반으로 사용자의 접근 허용 여부를 결정하는 단계; 및 접근 허용으로 결정된 사용자에게 대한 접근 제어 정책에 따른 내용을 수행하는 단계;를 포함한다.
- [0024] 사용자의 접근 허용 여부 결정 단계는, 사용자로부터의 접근 요청 메시지를 수신하는 단계; 접근 요청 메시지로부터 사용자 아이디, 접근하고자 하는 대상, 및 해당 동작 정보를 추출하는 단계; 및 추출된 정보를 기반으로 해당하는 모든 접근 제어 정책을 검색하여 검색 내용을 제공하는 단계;를 포함한다.
- [0025] 접근 제어 정책 수행 단계는, 접근 거부 수행시 해당 접근 요청을 거부하고 사용자에게 서비스 거부 메시지를 전달한다.
- [0026] 접근 제어 정책 수행 단계는 접근 거부 수행시 접근 요청 거부된 정보를 로그 파일에 저장한다.
- [0027] 접근 제어 정책 수행 단계는 접근 거부 수행시 관리자에게 정보를 전달한다.
- [0028] 보안 레벨 설정 단계 및 접근 허용 재설정 단계에 의하여 사용자에게 부여된 접근 제어 정책을 저장하는 단계를 추가로 포함한다.
- [0029] 빌딩 에너지 통합 관제 장치와의 네트워크 연결에 따른 네트워크 구간별로 차별화된 인증 정책이 규정된다. 이 경우, 인증 정책은 외부 단말과 빌딩 에너지 통합 관제 장치의 보안 게이트웨이 간에는 아이피 인증, 강제적 접근 제어 인증, 및 사용자 아이디 및 패스워드 인증을 혼합한 인증을 수행하도록 규정된다. 인증 정책은 외부 단말과 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 공인인증서에 의한 인증을 수행하도록 규정된다. 인증 정책은 외부 단말에서 빌딩 에너지 통합 관제 장치의 서비스 이용시 아이피 인증, 강제적 접근 제어 인증, 및 사용자 아이디 및 패스워드 인증을 혼합한 인증을 수행하도록 규정된다. 인증 정책은 빌딩 에너지 통합 관제 장치의 관리자과 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 사용자 아이디 및 패스워드 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된다. 인증 정책은 건물 내부의 사용자와 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 사용자 아이디 및 패스워드 인증을 수행하도록 규정된다. 인증 정책은 빌딩 에너지 통합 관제 장치의 보안 게이트웨이에서 빌딩 에너지 통합 관제 장치의 서비스 이용시 아이피 인증, 강제적 접근 제어 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된다. 인증 정책은 건물 내부의 사용자와 빌딩 에너지 통합 관제 장치의 보안 게이트웨이 간에는 사용자 아이디 및 패스워드 인증을 수행하도록 규정된다. 인증 정책은 빌딩 에너지 통합 관제 장치의 관리자와 보안 게이트웨이 간에는 사용자 아이디 및 패스워드 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된다.
- [0030] 바람직하게, 트래픽 공격 정보를 수집하고 수집된 정보를 이용하여 공격유무 및 공격유형을 판단하는 단계를 추가로 포함하여도 된다.

발명의 효과

- [0031] 이러한 구성의 본 발명에 따르면, 빌딩 에너지 통합 관제 장치의 빌딩 용도별 보안정책 정의를 통해 센터 중심의 통합 에너지 관리를 위한 효율적인 접근제어가 이루어질 수 있다.
- [0032] 본 발명에서는 임의적 접근 제어 방식과 강제적 접근 제어 방식이 혼용된 보안 정책 설정 방법을 이용함으로써, 보안정책이 효율적으로 관리될 수 있는 효과가 있다.
- [0033] 본 발명에 의하면 특정 사용자에게 특화된 보안정책이 효율적으로 수립 및 관리될 수 있는 효과가 있다.
- [0034] 본 발명에 의하면 웹포탈 또는 관리 GUI에 접속한 보안정책 관리자에 의해 보안정책을 수립할 수 있으므로,

보안정책 관리자가 외부에 존재하는 경우에도 빌딩 에너지 통합 관제 센터 내부의 기기들을 제어하는 접근 권한을 설정할 수 있는 효과가 있다.

도면의 간단한 설명

[0035]

도 1은 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 장치와 빌딩 클라이언트 및 외부 터미널간의 연결을 개략적으로 설명하는 도면이다.

도 2는 도 1에 도시된 빌딩 클라이언트와 빌딩 에너지 통합 관제 장치를 위한 보안 모델을 설명하기 위한 도면이다.

도 3은 도 1에 도시된 빌딩 클라이언트와 빌딩 에너지 통합 관제 장치의 접근 제어 구조를 설명하기 위한 도면이다.

도 4는 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 장치를 설명하기 위한 도면이다.

도 5는 도 4에 도시된 빌딩 클라이언트와 빌딩 에너지 통합 관제 장치를 위한 구간별 보안 인증 정책을 설명하기 위한 도면이다.

도 6은 도 4에 도시된 키분배 센터에서의 키분배 메커니즘을 설명하기 위한 도면이다.

도 7은 도 4에 도시된 빌딩 에너지 통합 관제 장치의 인증 모듈에서의 사용자 인증 메커니즘을 설명하기 위한 도면이다.

도 8은 도 4에 도시된 빌딩 에너지 통합 관제 장치의 접근 정책 모듈에서의 접근 제어를 설명하는 흐름도이다.

도 9는 도 8의 접근 제어 결정 단계의 세부 흐름도이다.

도 10은 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 방법을 설명하기 위한 플로우차트이다.

도 11은 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 방법의 설명중에서 보안정책 관리자의 단말기와 보안서버 간에 송수신되는 데이터와 동작을 설명하기 위한 플로우차트이다.

발명을 실시하기 위한 구체적인 내용

[0036]

이하, 첨부된 도면을 참조하여 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 장치 및 방법에 대하여 설명하면 다음과 같다. 본 발명의 상세한 설명에 앞서, 이하에서 설명되는 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니된다. 따라서, 본 명세서에 기재된 실시예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일실시예에 불과할 뿐이고 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형예들이 있을 수 있음을 이해하여야 한다.

[0037]

본 발명의 명세서에서, 빌딩 에너지 통합 관제 장치는 하나의 통합 서버를 구축하여 각 빌딩의 에너지 사용량 추이, 자동제어 운전 상태 및 환경요소들을 모니터링하고, 이를 기반으로 다수 빌딩의 에너지 소비 데이터를 수집/분석 처리하여, 각 빌딩 에너지 낭비요소를 찾아내어 최적화된 에너지 절감대책을 빌딩 에너지 관리자 및 사용자에게 제공할 수 있는 장치를 말한다. 그에 따라, 본 발명의 명세서의 빌딩 에너지 통합 관제 장치는 기존 빌딩별 새로운 제품으로 신재생 에너지, 고효율 전자 제품을 통합하고 외부 전력망과 효율적으로 연계하기 위한 HEMS(Home Energy Management System)나 BEMS(Building Energy Management System), 스마트 미터(Smart Meter) 등의 시스템과는 다른 것으로 이해하면 된다.

[0038]

물론, 빌딩 에너지 통합 관제 장치는 빌딩 에너지 통합 관제 센터로 칭할 수 있다. 본 발명의 명세서에 기재된 보안 정책 또는 접근 제어 정책은 보안 방식(또는 룰) 또는 접근 제어 방식(또는 룰)으로 칭하여도 된다.

[0039]

도 1은 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 장치와 빌딩 클라이언트 및 외부 터미널간의 연결을 개략적으로 설명하는 도면이다.

[0040]

다수의 용도로 구분되어지는 빌딩 클라이언트(100)와 서버 역할을 하는 빌딩 에너지 통합 관제 장치(200)는 네트워크(400)(인터넷)와 게이트웨이(420)를 통해 연결된다. 외부 사용자는 네트워크(400) 및 게이트웨이(420)를 통해 원하는 정보 및 서비스 등을 요구하고 수신한다. 외부 터미널(410)은 외부에서 접근하여 빌딩

에너지 통합 관제 장치(200)에서 제공되는 정보를 기반으로 제어된다. 게이트웨이(420)는 방화벽, VPN(Virtual Private Network), IDS(Intrusion Detection System), IPS(Intrusion Prevention System) 등의 보안 처리 유닛을 갖는다.

[0041] 여기서, 빌딩 에너지 통합 관제 장치(200)는 각 빌딩의 에너지 사용량 추이, 자동제어 운전 상태 및 환경요소들을 모니터링한다. 빌딩 에너지 통합 관제 장치(200)는 모니터링된 정보를 기반으로 다수의 빌딩의 에너지 소비 데이터를 수집/분석 처리한다. 빌딩 에너지 통합 관제 장치(200)는 분석 처리된 결과를 근거로 각 빌딩의 에너지 낭비요소를 찾아내어 최적화된 에너지 절감대책을 빌딩 에너지 관리자 및 사용자에게 제공한다. 이를 위해, 빌딩 에너지 통합 관제 장치(200)는 인증, 접근 제어, 침입 탐지 등의 기능을 포함한다.

[0042] 인증 기능이라 함은 임의의 정보에 접근할 수 있는 주체의 능력이나 주체의 자격을 검증하는 것을 의미한다. 인증 기능은 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방지해 준다. 사용자 인증에는 허가(Authentication), 책임 추적성(Accountability)이 있다. 허가는 시스템이 사용자, 프로그램 또는 프로세스에게 허가한 권한을 말하는 것이다. 책임 추적성이란 멀티유저, 멀티태스킹이 지원되는 네트워크 환경에서는 누가, 언제, 어떠한 행동을 하였는지 기록하여 필요시 그 행위자를 추적 가능하도록 한다. 책임 추적성은 책임 소재를 명확하게 해야 할 필요성이 생기게 되었기 때문에, 시스템의 보호 관점에서도 비인가자 또는 인가된 사용자에게 대하여 경각심을 불러 일으켜 컴퓨터의 부정사용을 줄이는 효과를 거둘 수 있어 반드시 보장되어야 할 보안의 중요 요소 중의 하나라 할 수 있다.

[0043] 접근 제어(또는 액세스 제어) 기능이라 함은 누군가가 무언가를 사용하는 것을 허가하거나 거부하는 기능을 말한다. 접근 제어 기능은 파일이나 디렉토리 서비스 개체 등에 대한 서비스 사용자의 권한을 결정하여 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방지해 준다.

[0044] 침입 탐지 기능은 유해 트래픽을 탐지하고 차단하는 것을 의미한다. 인터넷의 발달은 사용자에게 네트워크를 통한 다양하고 빠른 서비스를 제공받을 수 있는 환경을 제공하였다. 이와 같이 네트워크 기반 서비스에 대한 의존도가 증가하면서 유해 트래픽 탐지 및 차단은 안전한 서비스 제공을 위해 필수 불가결한 요건이 되었다. 대표적인 유해 트래픽인 트래픽 폭주 공격이 발생하면 컴퓨터는 물론 네트워크까지 마비시켜 업무에 엄청난 영향을 미치고 막대한 피해를 주게 된다. 일반적인 공격탐지 방법인 패킷 수집을 통한 트래픽 폭주 공격 탐지는 상세한 분석이 가능하지만 고가의 고성능 분석시스템이 요구되고 설치 및 운영의 확장성이 부족한 단점을 가지고 있다. 따라서, 본 발명의 빌딩 에너지 통합 관제 장치에서의 침입 탐지 기능은 시스템 및 네트워크 리소스의 사용이 적고, 계층과 프로토콜 기준으로 표준화된 네트워크 성능 관리 데이터를 제공 받을 수 있는 효과적인 탐지가 가능한 SNMP(Simple Network Management Protocol) 기반 침입 탐지 기능으로 정의할 수 있다.

[0045] 한편, 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 장치는 전자서명 기능, 암호화 기능, 데이터 위/변조 방지 기능 등을 추가로 갖추는 것으로 하여도 무방하다.

[0046] 도 2는 도 1에 도시된 빌딩 클라이언트와 빌딩 에너지 통합 관제 장치를 위한 보안 모델을 설명하기 위한 도면이다.

[0047] 레거시 빌딩 디바이스는 보통은 통신 인터페이스가 없다. 그러나, B형 빌딩 디바이스에 연결된 전용 경로가 있어서 레거시 빌딩 디바이스는 B형 빌딩 디바이스를 통해 빌딩 네트워크에 접근할 수 있다. 몇몇 빌딩 디바이스는 A형 빌딩 디바이스와 C형 빌딩 디바이스의 기능이 결합되어있다. 이 모델에는 8개의 개체들(① 원격 사용자, ② 원격 터미널, ③ 응용 서버, ④ 빌딩 게이트웨이, ⑤ 보안 응용 서버, ⑥ 빌딩 사용자, ⑦ 센터 관리자, ⑧ 빌딩 디바이스)이 있다.

[0048] 여기서, 바람직하게 빌딩 디바이스 타입으로는 3개의 카테고리(A형 빌딩 디바이스, B형 빌딩 디바이스, C형 빌딩 디바이스)로 그룹되어질 수 있다. 빌딩 디바이스는 다른 디바이스를 제어하거나 또는 다른 디바이스에 의해 제어되는 PDA, PC, TV/VCR와 같은 개체(또는 빌딩 응용)이며, 빌딩 사용자에게 서비스를 제공한다. A형 빌딩 디바이스는 프레젠테이션 페이지(presentation page)와 고급 디스플레이(rich display)를 통해 B형 빌딩 디바이스 또는 C형 빌딩 디바이스를 제어하는 원격 제어기(리모컨), PC 또는 PDA 등이다. B형 빌딩 디바이스는 빌딩 네트워크에서 통신 인터페이스가 없는 C형 빌딩 디바이스를 연결하는 브리지이다. 보안 카메라, A/V 디바이스 등과 같은 C형 빌딩 디바이스는 오직 몇몇 빌딩 디바이스의 잔여 서비스 종류만을 제공한다. 만약, B형 빌딩 디바이스 또는 C형 빌딩 디바이스의 보안 소유자라면, A형 또는 C형 빌딩 디바이스는 보안 콘솔이라 불려진다.

- [0049] 그리고, 보안 모델에는 13개의 관계가 있다. 즉, 원격 사용자와 원격 터미널, 원격 터미널과 빌딩 게이트웨이, 원격 터미널과 보안 응용 서버, 원격 터미널과 빌딩 디바이스, 응용 서버와 빌딩 게이트웨이, 응용 서버와 보안 응용 서버, 응용 서버와 빌딩 디바이스, 빌딩 게이트웨이와 빌딩 디바이스, 보안 응용 서버와 빌딩 디바이스, 빌딩 디바이스와 빌딩 사용자, 빌딩 디바이스와 다른 빌딩 디바이스, 빌딩 게이트웨이와 보안 응용 서버, 및 빌딩 관리자와 빌딩 게이트웨이의 관계가 있다.
- [0050] 도 3은 도 1에 도시된 빌딩 클라이언트와 빌딩 에너지 통합 관제 장치의 접근 제어 구조를 설명하기 위한 도면이다.
- [0051] 빌딩 클라이언트(100)와 빌딩 에너지 통합 관제 장치(200)의 접근 제어 시나리오는 아래와 같이 크게 4가지 형태로 구분된다.
- [0052] 1. 빌딩내 클라이언트를 이용한 빌딩 에너지 통합 관제 서비스 이용
- [0053] (가) 빌딩 클라이언트(100) 내부 → 외부 서비스(컨텐츠 사업자)로의 접근(도 3에서 "①")
- [0054] (나) 빌딩 클라이언트(100) 내부 → 빌딩 에너지 통합 관제 장치(200) 내 서비스 접근(도 3에서 "②")
- [0055] 2. 빌딩외 클라이언트를 이용한 빌딩 에너지 통합 관제 서비스 이용
- [0056] (가) 빌딩 클라이언트(100) 외부 → 빌딩 클라이언트(100)내 빌딩 기기접근/제어(도 3에서 "③")
- [0057] 3. 빌딩 에너지 통합 관제 장치(센터)내 클라이언트를 이용한 빌딩 에너지 통합 관제 서비스 이용
- [0058] (가) 빌딩 에너지 통합 관제 장치(200)내 → 외부 서비스(컨텐츠 사업자)로의 접근(도 3에서 "④")
- [0059] (나) 빌딩 에너지 통합 관제 장치(200)내 → 빌딩 기기접근/제어(도 3에서 "⑤")
- [0060] 4. 센터외 클라이언트를 이용한 빌딩 에너지 통합 관제 서비스 이용
- [0061] (가) 빌딩 에너지 통합 관제 장치(200)외 → 빌딩 에너지 통합 관제 장치(200)내 서비스 접근(도 3에서 "⑥")
- [0062] 도 4는 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 장치를 설명하기 위한 도면으로서, 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 장치의 통합 보안 플랫폼 구조이다.
- [0063] 도 4에 도시된 빌딩 클라이언트(100)와 빌딩 에너지 통합 관제 장치(200)는 키분배 센터(300)와 사용자 브라우저 또는 단말(40) 및 경보부(50)를 통해 연결된다.
- [0064] 사용자 브라우저 또는 단말(40)은 인증을 수행하는 부분과 접근 제어 정책에 따라 접근가능한 서비스들을 보여주기 위한 유니트에 해당한다.
- [0065] 경보부(50)는 크게는 시스템 전체적인 경보(Alert) 역할을 하고, 작게는 침입 탐지 부분의 감지 여부에 따라 사용자에게 알려주는 역할을 한다.
- [0066] 빌딩 클라이언트(100)는 암호 모듈(10), 인증 모듈(20), 및 침입 탐지 모듈(30)을 포함한다.
- [0067] 암호 모듈(10)은 키관리부(14)와 암호알고리즘부(16)와의 연동을 통해 암호화 과정에 필요로 하는 키관리 및 관리되는 키를 기반으로 대칭키/비대칭키 기반의 암호알고리즘 연동을 수행하는 키 관리 및 암호알고리즘 연동부(12), 암호화 과정에 필요로 하는 키를 관리하는 키관리부(14), 및 관리되는 키를 대상으로 대칭키/비대칭키 기반의 암호화를 위한 알고리즘들을 관리하는 암호알고리즘부(16)를 포함한다.
- [0068] 인증 모듈(20)은 키관리 UNIT과 암호알고리즘 UNIT의 연동을 통해 인증 과정에서 필요로 하는 키관리 및 관리되는 키를 기반으로 대칭키/비대칭키 기반의 암호알고리즘 연동을 수행하는 키관리 및 암호알고리즘 연동부(22), 통합 에너지 관제 센터의 서비스를 받기 위해 사용자의 인증 성공 여부를 결정하고, 결정된 결과에 따라 접근을 제한하는 사용자 인증 처리부(24), 및 사용자 인증처리를 위해 빌딩 에너지 통합 관제 장치(200)의

사용자 인증 처리 연동부(72)와 연동하여 암호화 프로토콜을 통해 양방향 사용자 인증을 수행하는 사용자 인증 처리 연동부(26)를 포함한다.

[0069] 침입 탐지 모듈(30)은 빌딩 에너지 통합 관제 장치(200)의 침입 탐지 모듈(120)에 해당 침입탐지에 사용하는 MIB(Management Information Base) 정보에 대한 데이터를 송신하는 SNMP 에이전트(32), 및 실제 UDP 통신 프로토콜을 사용하여 빌딩 에너지 통합 관제 장치(200)의 침입 탐지 모듈(120)에게로 MIB 정보를 송신하는 MIB 데이터 송신부(34)를 포함한다.

[0070] 빌딩 에너지 통합 관제 장치(200)는 인증 모듈(60), 암호 모듈(80), 접근 정책 모듈(90), 정책 보안 관리 모듈(110), 및 침입 탐지 모듈(120)을 포함한다.

[0071] 인증 모듈(60)은 사용자 인증처리 및 접근 제어를 위해 필요한 사용자 정보를 관리하는 사용자 인증 정보 연동부(62), 인증 수행과 접근 제어 수행시 발생하는 보안 이벤트를 관리하여 추후 상황인지 기반의 역할을 수행할 수 있도록 하는 로그(Log)를 분석하는 로그 정보 분석 처리부(64), 인증 및 접근 제어 수행에 있어서 사용자들의 정보(예컨대, 아이디(ID), 패스워드 등)를 저장하고 있는 사용자 데이터베이스(66), 인증 및 접근 제어 수행에 따라 발생하는 모든 로그(Log) 정보를 저장하는 로그 데이터베이스(68), 해당 빌딩 에너지 통합 관제 장치의 서비스를 받기 위해 사용자의 인증 성공 여부를 결정하고 결정된 결과에 따라 접근을 제한하는 사용자 인증 처리부(70), 사용자 인증 처리를 위해 빌딩 클라이언트(100)의 사용자 인증 처리 연동부(26)와 연동하여 암호화 프로토콜을 통해 양방향 사용자 인증을 수행하는 사용자 인증 처리 연동부(72), 및 암호 모듈(80)의 암호알고리즘부(82) 및 키관리부(84)와의 연동을 통해 인증 과정에서 필요로 하는 키관리 및 관리되는 키를 기반으로 대칭키/비대칭키 기반의 암호알고리즘 연동을 수행하는 키 관리 및 암호알고리즘 연동부(74)를 포함한다.

[0072] 암호 모듈(80)은 관리되는 키를 대상으로 대칭키/비대칭키 기반의 암호화를 위한 알고리즘들을 관리하는 암호알고리즘부(82), 암호화 과정에서 필요로 하는 키를 관리하는 키관리부(84), 및 암호알고리즘부(82)와 키관리부(84)와의 연동을 통해 암호화 과정에서 필요로 하는 키관리 및 관리되는 키를 기반으로 대칭키/비대칭키 기반의 암호알고리즘 연동을 수행하는 키 관리 및 암호알고리즘 연동부(86)를 포함한다.

[0073] 접근 정책 모듈(90)은 접근 제어 서버(94)로부터 서비스 접근 가능여부를 부여받아 실제로 사용자 브라우저 또는 단말(40)을 통해 상이한 서비스를 제공하는 접근 제어 에이전트(92), 접근 정책 보안 관리자(112)로부터 생성된 접근 제어 정책(보안 정책이라고도 할 수 있음)에 따라 서비스 접근 여부를 결정하는 접근 제어 서버(94), 접근 제어 정책 관련 정보(예컨대, 사용자 및/또는 건물 용도에 따른 보안 레벨, 사용자에게 따른 네트워크 구간 별 및 서비스 별로의 인증 정책 등)를 가지고 있는 정책 데이터베이스(96), 및 접근 정책 보안 관리자(112)와의 연동을 통해 해당 접근 제어 정책을 정책 데이터베이스(96)에 저장하는 보안 관리 에이전트(98)를 포함한다.

[0074] 정책 보안 관리 모듈(110)은 접근 정책 보안 관리자(112)가 DAC 기법 및 MAC 기법을 사용하여 생성한 접근 제어 정책을 관리한다.

[0075] DAC(Discretionary Access Control) 기법은 임의적 접근 제어 기법으로서, 주체(Subject) 또는 그것이 속해 있는 그룹의 신원(Identity)에 근거하여 객체(Object)에 대한 접근을 제한하는 방법이다. 즉, DAC 기법은 허가된 사용자(Subject)와 허가권을 변경할 수 있는 정보(Object)에 대한 관계를 설정한다. 그리하여 정보의 소유자(Owner)가 특정 사용자에게 특정 권한의 부여를 결정한다. DAC 기법에 의한 접근 제어 정책은 접근통제행렬 모델로 표현되는 것들로 행(row) 중심적 표현형태를 갖는 캐패빌리티 리스트(Capability List)와 프로파일(Profile) 및 패스워드(Password) 등이 있다. 또한, 열(column) 중심적 표현을 갖는 정책으로는 보호 비트(Protection Bits) 및 ACL(Access Control Lists)이 있다. DAC 기법에 의한 접근 제어 정책은 모든 사용자와 정보에 대하여 단일화되어 있지 않으며, 하나의 사용자 정보단위로 이루어진다. 예를 들어, 유닉스(Unix)시스템내의 정보 소유자는 소유자 임의의 결정으로 특정 사용자 또는 사용자 그룹에게만 접근권한을 부여할 수 있다. 또한, 정보에 대한 접근권한을 부여받은 사용자가 그 정보를 복사해올 경우 원래 정보에 부여된 접근권한은 복사된 객체로 전파되지 않으며 하나의 주체 및 객체 단위로 접근제한 설정되기 때문에 새로 발생하는 주체 및 객체 관계의 생성에는 영향을 주지 않는다. DAC 속성상 접근은 주체의 ID에 전적으로 근거를 두고 있어서 DAC 기법에 의한 접근 제어 정책은 데이터의 의미에 대한 아무런 지식도 갖고 있지 않으며 이에 근거하여 접근 허가를 결정하지 않는다.

- [0076] MAC(Mandatory Access Control) 기법은 강제적 접근 제어 기법으로서, 비밀성(Sensitivity)을 갖는 객체(Object)에 대하여 주체(Subject)가 갖는 권한(Authorization)에 근거하여 객체에 대한 접근을 제어하는 방법이다. MAC 기법은 객체의 주인이 아닌 접근통제의 관리자(Administrator)만이 정보자원의 분류를 설정, 변경하고 이외의 접근권한 부여는 정책에 의해 엄격히 제한한다. 그에 따라, MAC 기법은 DAC 기법보다 대체로 안전하다고 할 수 있다. 또한, MAC 기법은 객체의 소유자에 의하여 변경할 수 없는, 한 주체와 한 객체간의 접근통제 관계를 정의함으로써 DAC 기법에 의한 접근 제어 정책보다는 정보의 비밀성을 요구하는 곳에 사용되며 다른 주체(Subject)에 의한 접근통제정책이 부과되는 것을 원천적으로 제한해 놓았다. 모든 객체(Object)는 정보의 비밀성(Sensitivity)에 근거하여 보안레벨(security label)이 주어지며 허가된 사용자만이 접근할 수 있도록 엄격히 관리된다.
- [0077] 침입 탐지 모듈(120)은 빌딩 클라이언트(100)의 MIB 데이터 송신부(34)를 통해 주기적인 MIB 정보에 대한 업데이트를 수행하는 MIB 업데이트부(122), MIB 업데이트부(122)를 통해 업데이트된 정보 중 침입탐지 부분에 필요한 정보만을 수집/보관하는 MIB 수집부(124), 및 수집된 MIB 데이터와 탐지 알고리즘을 통해 공격을 탐지하는 공격 탐지부(126)를 포함한다.
- [0078] 키분배 센터(300)는 빌딩 클라이언트(100)와 빌딩 에너지 통합 관제 장치(200)에서 사용되는 대칭키/비대칭키의 키를 분배한다.
- [0079] 도 4에서, 빌딩 에너지 통합 관제 장치(200)는 보안 정책 서버(도시 생략) 및 보안 서버(도시 생략)로 나눌 수 있다. 이 경우, 도 4의 정책 보안 관리 모듈(110)이 보안 정책 서버(도시 생략)에 내장되고, 정책 보안 관리 모듈(110)을 제외한 모든 모듈(60, 80, 90, 120)은 보안 서버(도시 생략)에 내장되는 것으로 이해하면 된다.
- [0080] 상술한 바와 같은 시스템에서, 인증 요청이 빌딩 클라이언트(100)를 통해 사용자 브라우저 또는 단말(40)에서 발생하면 요청을 받은 빌딩 에너지 통합 관제 장치(200)의 인증 모듈(60)로 넘어간다. 인증 모듈(60)내의 사용자 인증 처리부(70)를 사용자 정보를 확인 후 서비스를 이용하게 된다. 빌딩 클라이언트(100)와 빌딩 에너지 통합 관제 장치(200)에 포함된 각각의 키 관리 및 암호알고리즘 연동부(12, 22; 74, 86)에서 데이터의 암호화를 수행하여 안전하게 송/수신한다.
- [0081] 한편, 접근 제어 서버(94)에 서비스 요청이 발생하면, 접근 정책 보안 관리자(112)에 의해서 설정된 접근 제어 정책과 환경 정보(예컨대, 사용자 정보(사용자 ID, 패스워드), 건물 용도, 제어 상태(예컨대, 빌딩 에너지 관련 기기의 온/오프 상태 등))를 기반으로 접근 허용 여부를 결정해서 접근 제어를 수행하는 접근 제어 에이전트(92)에게로 넘겨준다. 접근 제어 에이전트(92)는 접근 제어 정책이 정한 과정을 수행하며 로그 파일에 저장한다. 여기서, 빌딩 에너지 관련 기기라 함은 빌딩에 설치된 각종의 전열 기기 등을 의미한다.
- [0082] 그리고, 침입 탐지의 경우 빌딩 에너지 통합 관제 장치(200)에서 MIB 정보를 MIB 수집부(124)를 이용하여 수집한 후, 공격 탐지부(126)를 통해 수집된 정보를 이용하여 공격유무와 공격유형을 판단한다.
- [0083] 도 5는 도 4에 도시된 빌딩 클라이언트와 빌딩 에너지 통합 관제 장치를 위한 구간별 보안 인증 정책을 설명하기 위한 도면이다.
- [0084] 빌딩 에너지 통합 관제 장치를 위한 접근 제어 기술은 빌딩 에너지 통합 관제 장치와 빌딩 클라이언트 내외부의 불법 접근을 차단할 뿐만 아니라, 비록 정당한 사용자라 할지라도 불필요한 서비스 접근을 허용하지 않기 위한 실시간 제어 기술이다. 빌딩 에너지 통합 관제 장치는 다양한 건물의 특성(유형/용도)을 가진 사용자를 대상으로 하며, 빌딩 에너지 통합 관제 장치내의 등급별 관리자를 대상으로 한다. 그에 따라, 설정된 정책을 일률적으로 적용하는 것은 비효율적이며 서비스의 남용과 잘못된 사용을 초래할 수 있다. 또한, 사용자 ID 및 해당 비밀 정보가 외부로 누출되었을 경우 빌딩 에너지 통합 관제 장치와 빌딩 클라이언트에 심각한 타격을 줄 수 있다.
- [0085] 따라서, 본 발명에서는 실시간 접근 제어 기능을 통해서 빌딩 에너지 통합 관제 장치의 보안성을 강화하여, 빌딩 에너지 통합 관제 장치와 빌딩 클라이언트 내외부의 불법 접근이나 불필요한 시스템 자원 사용을 제한한다.
- [0086] 본 발명에서는 빌딩 에너지 통합 관제 장치의 안전성을 확보하기 위해 규정된 사용자 인증 보안 정책을 실질

적으로 준수하기 위하여 네트워크 구간 별, 서비스 별로 차별화된 인증 정책을 규정하였다. 또한 이를 준수하기 위한 별도의 사용자 인증 기술을 채택하였다. 사용자 인증 보안 정책이란 정보 시스템에 접속하는 사용자가 정당한 사용자인지 판단하기 위해 필요한 보안 요소 규정한 일련의 규칙을 말한다.

[0087] 도 5에서는 보안 취약성과 보안 요구사항들을 고려하여 빌딩 에너지 통합 관제 장치에서 제공하는 네트워크 구간 별, 서비스 별 보안 인증 정책을 설명한다.

[0088] 도 5를 보면, 외부 사용자와 외부 단말 간에는 사용자 아이디 및 패스워드에 의한 인증을 수행하도록 규정된다. 외부 단말과 보안 게이트웨이(또는 보안 서버) 간에는 아이피(IP) 인증, 강제적 접근 제어(MAC) 인증, 및 사용자 아이디 및 패스워드 인증을 혼합한 인증을 수행하도록 규정된다. 외부 단말과 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 공인인증서에 의한 인증(PKI)을 수행하도록 규정된다. 외부 단말에서 빌딩 에너지 통합 관제 장치의 서비스 이용시 아이피 인증, 강제적 접근 제어 인증, 및 사용자 아이디 및 패스워드 인증을 혼합한 인증을 수행하도록 규정된다. 빌딩 에너지 통합 관제 장치의 관리자와 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 사용자 아이디 및 패스워드 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된다. 건물 내부의 사용자와 빌딩 에너지 통합 관제 장치의 보안 정책 서버 간에는 사용자 아이디 및 패스워드 인증을 수행하도록 규정된다. 보안 게이트웨이(또는 보안 서버)에서 빌딩 에너지 통합 관제 장치의 서비스 이용시 아이피 인증, 강제적 접근 제어 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된다. 건물 내부의 사용자와 보안 게이트웨이(또는 보안 서버) 간에는 사용자 아이디 및 패스워드 인증을 수행하도록 규정된다. 빌딩 에너지 통합 관제 장치의 관리자와 보안 게이트웨이(또는 보안 서버) 간에는 사용자 아이디 및 패스워드 인증, 및 건물내 자체 인증서 인증을 혼합한 인증을 수행하도록 규정된다.

[0089] 도 5에 도시된 바와 같이, 빌딩 외부인 빌딩 클라이언트에서 빌딩 에너지 통합 관제 장치의 보안을 통한 서비스를 이용할 경우와 빌딩 에너지 통합 관제 장치에서의 센터 관리자 혹은 내부 사용자의 관제 서버(즉, 빌딩 에너지 통합 관제 장치)내 서비스를 이용할 경우, 관제 서버 플랫폼이 사용자 인증을 수행하여야 한다. 이때, 인증방법은 아이디(ID)/패스워드(PASSWORD)와 인증서를 기반으로 사용자 인증을 한다. 사용자 인증이 이루어지면 관제 서버 플랫폼에 의해 서비스 인증이 이루어진다. 서비스 인증은 관제 서버 플랫폼인 보안 정책 관리자에 의해 제공되는 접근제어 서비스를 받아 이루어진다. 관제 서버 플랫폼에서 제공되는 접근 제어 기능은 개체의 정당한 접근을 결정하고 시행하기 위해 인증된 개체에 관한 정보 혹은 개체의 특성을 사용한다. 만약, 개체가 인가되지 않은 자원을 사용하기 위한 시도를 하거나 인가된 자원이지만 적절하지 못한 접근 권한을 가지고 사용하기 위한 시도를 한다면, 접근 제어 기능은 요구를 거부하고 추가로 경보 발생하기 위해 사건을 보고하고 보안 감사 흔적에 기록한다. 접근 제어 기능은 다음 항목(예컨대, 패스워드, 소유물, 개체의 인가 증거와 같은 인증 정보; 특징, 소유물, 특징에 의해 정의되는 개체 혹은 자원으로 접근하기 위한 정당한 증거; 권한 인증서; 주로 보안 정책에 따라 접근 허가 또는 거부하기 위해 사용되는 개체와 연관된 보안 레벨; 접근 시도 경로; 접근을 시도한 물리적인 위치 등)의 사용에 기초하고 있다.

[0090] 도 6은 도 4에 도시된 키분배 센터에서의 키분배 메커니즘을 설명하기 위한 도면이다.

[0091] 효율적인 키 분배를 위해, 빌딩 클라이언트(100), 게이트웨이(420), 빌딩 에너지 통합 관제 장치(200), 키분배 센터(Key Distribution Center)(300)를 필요로 한다. 키 분배 시나리오에서 빌딩 클라이언트(100), 게이트웨이(420), 빌딩 에너지 통합 관제 장치(200)는 각각 자신의 개인키 $KR_x(x=c, ap, s)$ 를 가지고 있고, 키분배 센터(300)는 KR_x 를 미리 갖고 있다고 가정한다. 키 분배는 다음과 같은 과정을 거친다.

[0092] ① 사용자가 키 분배 요청을 하면, 빌딩 클라이언트(100)에서는 ID_c 와 Nonce 값인 $N1$ 을 이용하여 $EKR_c(ID_c, N1)$ 을 생성하여 게이트웨이(420)에게로 전송한다. ID_c 는 빌딩 클라이언트(100)의 정보이다. 여기서, $EKR_c(ID_c, N1)$ 는 비대칭 암호화 알고리즘인 RSA를 이용하여 암호화하며, 이때 개인키 KR_c 를 사용한다.

[0093] ② $EKR_c(ID_c, N1)$ 를 전송받은 게이트웨이(420)는 Nonce값 $N2$ 를 생성하고 $N2$, $EKR_c(ID_c, N1)$ 를 개인키 KR_{ap} 로 암호화하여 키분배 센터(300)에게로 전송한다.

[0094] ③ $EKR_{ap}(N2, EKR_c(ID_c, N1))$ 를 전송받은 키분배 센터(300)는 공개키인 KU_{ap} , KU_c 를 이용하여 복호화할 수 있으며, 빌딩 클라이언트(100)의 ID_c , $N1$, AP/GW 에서의 $N2$ 값을 얻어 $EKU_s(KU_c, KU_s, KU_{ap}, ID_c, N1, N2)$ 을 생성하여 빌딩 에너지 통합 관제 장치(200)의 인증 서버(즉, 인증 모듈)로 전송한다. 빌딩 에너지 통합 관제 장치(200)의 인증 서버에서는 개인키 KR_s 를 사용하여 $EKU_s(KU_c, KU_s, KU_{ap}, ID_c, N1, N2)$ 을 복호화하여 KU_c , KU_s , KU_{ap} 를 얻는다.

- [0095] ④ 빌딩 에너지 통합 관제 장치(200)의 인증 서버에서는 간단한 함수를 이용하여 $f(N1)$ 과 $f(N2)$ 의 값인 $N1+1$ 과 $N2+1$ 값을 생성하여 $EKUap(EKUc(KUs, KUc, N1+1), IDc, KUap, KUs, N2+1)$ 를 게이트웨이(420)에게로 전송한다.
- [0096] ⑤ $EKUap(EKUc(KUs, KUc, N1+1), IDc, KUap, KUs, N2+1)$ 을 전송받은 게이트웨이(420)는 자신의 공개키 $KUap$ 를 사용하여 복호화시켜 $EKUc(KUs, KUc, N1+1), IDc, KUap, KUs, N2+1$ 를 얻는다. 여기서, 얻은 $f2+1$ 은 이전에 키 분배 센터(300)로 전송했던 $N2$ 에 $f(N2)$ 을 적용시켜 얻어진 결과와 비교하여 올바른 패킷인지 확인할 수 있다. $KUs, KUap$ 등 AP에서 필요한 정보는 빌딩 클라이언트(100)로 전송되고 빌딩 클라이언트(100)에서는 개인키 KRc 를 이용하여 복호화 후 위의 게이트웨이(420)에서와 같은 방법으로 $N1$ 을 확인, KUs, KUc 를 획득하게 되면 키 분배는 완료된다.
- [0097] 도 7은 도 4에 도시된 빌딩 에너지 통합 관제 장치의 인증 모듈에서의 사용자 인증 메커니즘을 설명하기 위한 도면으로서, 키분배 센터(300)를 이용하여 키분배가 이루어진 상태에서 각 사용자를 인증하는 과정을 설명한다.
- [0098] ① 빌딩 클라이언트(100)는 보유하고 있는 아이디(IDc)와 시간을 가지고 생성한 랜덤값 $R1$ 을 RSA암호화 방식을 통해 홈게이트웨이 공개키(KUs)로 암호화 후 파일(`code.txt`)로 저장하고, 게이트웨이(420)에게로 그 파일을 전송한다.
- [0099] ② 게이트웨이(420)는 빌딩 클라이언트(100)에서 받은 파일을 바로 빌딩 에너지 통합 관제 장치(200)의 인증 서버로 전송한다.
- [0100] ③ 빌딩 에너지 통합 관제 장치(200)의 인증서버는 자신의 개인키(KRs)로 파일을 복호화하여 IDc 와 $R1$ 값을 획득한 후 미리 등록된 사용자 ID와 복호화된 사용자 ID($IDc2$)를 비교하여 일치하면 획득한 $R1$ 값을 일정하게 변환시키는 함수($f()$)를 통하여 새로운 값($f(R1)$)과 또 다른 랜덤 값($R2$), $f(R2)$ 를 생성한다. 이후에 빌딩 에너지 통합 관제 장치(200)의 인증서버는 시간에 따라 다르게 생성되는 랜덤값을 통하여 인증번호를 만들고 사용자 ID, 인증번호, 게이트웨이의 공개키, $R2$ 값을 RSA암호화한다(`code2.txt` 생성). 그리고 나서, 빌딩 에너지 통합 관제 장치(200)의 인증서버는 게이트웨이(420)의 공개키($KUap$)로 빌딩 클라이언트(100)의 공개키(KUc)와 `code2.txt`, $f(R2)$ 값을 암호화 한 후 결과 파일(`code3.txt`)을 게이트웨이(420)에게로 전송한다.
- [0101] ④ 게이트웨이(420)는 `code3.txt`를 자신의 개인키($KRap$)로 복호화하여 얻은 $f(R2)$ 값을 다시 자신의 공개키로 암호화해서 세션키($Kap-s$)를 만들고, 랜덤 값 $R3$ 를 생성하여 Gateway ID($IDap$), `code2.txt` 내용, $R3$ 를 빌딩 클라이언트(100)의 공개키 KUc 로 암호화 한다. 게이트웨이(420)는 이렇게 만들어진 `code4.txt`를 빌딩 클라이언트(100)에게로 보낸다.
- [0102] ⑤ 빌딩 클라이언트(100)는 게이트웨이(420)로부터 받은 `code4.txt`를 빌딩 클라이언트(100)의 개인키 KRc 로 복호화 한 후, 빌딩 클라이언트(100)에 미리 저장된 Gateway ID와 복호화해서 얻은 $IDap$ ($IDap2$)를 비교하여 게이트웨이(420)를 확인한다. 또한, 빌딩 클라이언트(100)는 빌딩 클라이언트(100)에 미리 저장된 사용자 ID(IDc)와 빌딩 에너지 통합 관제 장치(200)의 인증서버(즉, 인증 모듈)로부터의 사용자 ID($IDc2$)를 비교하여 빌딩 클라이언트(100)가 빌딩 에너지 통합 관제 장치(200)의 인증서버에 전송했던 ID가 되돌아 왔는지 확인한다. 그리고, 빌딩 클라이언트(100)는 $f()$ 함수를 통하여 $R1$ 값을 변경하여 빌딩 에너지 통합 관제 장치(200)의 인증서버로부터 전송된 $f(R1)$ 값과 비교하여 일치하는지 확인하여 빌딩 에너지 통합 관제 장치(200)의 인증서버를 확인한다. 이렇게 확인 절차를 수행 후 빌딩 클라이언트(100)는 $f()$ 함수를 통해 빌딩 에너지 통합 관제 장치(200)의 인증서버에서 받은 $R3$ 를 변경시켜 만든 값 $f(R3)$ 을 생성한다. 그 후 빌딩 클라이언트(100)는 빌딩 에너지 통합 관제 장치(200)의 인증서버에서 받은 게이트웨이(420)의 공개키($KUap$)로 사용자 ID와 랜덤 값 $R4$, $f(R3)$ 를 RSA암호화하여 생성된 `code6.txt` 파일을 게이트웨이(420)에게로 전송한다.
- [0103] ⑥ 게이트웨이(420)는 빌딩 클라이언트(100)로부터 `code6.txt` 파일을 받아 자신의 개인키($KRap$)로 복호화한다. 그 후 게이트웨이(420)는 이전에 생성한 $R3$ 값을 $f()$ 함수로 변경시키고, 빌딩 클라이언트(100)로부터 얻은 $f(R3)$ 값과 AP에서 생성한 $f(R3)$ 값을 확인하여 빌딩 클라이언트를 확인한다. 또한, 게이트웨이(420)는 빌딩 클라이언트(100)로부터 얻은 사용자 ID와 게이트웨이에 등록된 사용자 ID를 통하여 한번 더 빌딩 클라이언트를 확인한다. 게이트웨이(420)는 이렇게 빌딩 클라이언트를 확인 후 빌딩 클라이언트(100)에서 받은 $R4$ 를 $f()$ 함수를 통해 변경시켜 그 값($f(R4)$)을 자신(즉, 게이트웨이)의 ID와 함께 빌딩 클라이언트(100)의 공개키(KUc)를 통해 RSA암호화 방식으로 암호화하여 생성된 `code7.txt` 파일을 빌딩 클라이언트(100)에게

로 전송한다.

- [0104] ⑦ 빌딩 클라이언트(100)는 code7.txt를 개인키(KRc)로 복호화하여 게이트웨이(420)의 ID와 f(R4)값을 비교하여 게이트웨이를 확인한다. 그 후, 빌딩 클라이언트(100)는 f(R1) 값을 자신의 공개키(KUc)로 암호화하여 세션키(Kc-s)를 생성한다. 빌딩 클라이언트(100)는 세션키 생성후 이전에 code4.txt 파일을 복호화해서 얻은 인증번호(AN)을 통하여 빌딩 클라이언트(100)에 저장된 패스워드 테이블(PWTB)에서 값을 추출한다. 그 후 빌딩 클라이언트(100)는 추출된 PW와 이전에 빌딩 에너지 통합 관제 장치(200)의 인증서로부터 받은 R2 값을 함께 MD5로 암호화하고, 그 값과 세션키(Kc-s), 사용자 ID를 빌딩 에너지 통합 관제 장치(200)의 인증서부의 공개키(KUs)로 RSA암호화 방식으로 암호화한다. 이와 같이 하여 생성된 code9.txt 파일을 빌딩 클라이언트(100)는 게이트웨이(420)에게로 전송한다.
- [0105] ⑧ 게이트웨이(420)는 code9.txt의 내용과 세션키(Kap-s)를 빌딩 에너지 통합 관제 장치(200)의 인증서부의 공개키(KUs)로 암호화하여 생성된 code10.txt 파일을 빌딩 에너지 통합 관제 장치(200)의 인증서부로 보낸다.
- [0106] ⑨ 빌딩 에너지 통합 관제 장치(200)의 인증서부는 code10.txt과 code9.txt를 개인키(KRs)로 복호화하여 사용자의 ID를 확인한다. 또한, 빌딩 에너지 통합 관제 장치(200)의 인증서부는 저장되어 있는 KUc, KUap로 R1, R2를 암호화하여 세션키를 생성한 후에 빌딩 클라이언트(100)로부터 받은 세션키들을 비교하여 빌딩 클라이언트(100)와 게이트웨이(420)를 확인한다. 마지막으로, 빌딩 에너지 통합 관제 장치(200)의 인증서부는 이전에 생성한 인증번호(AN)을 바탕으로 자신의 PWTB에서 패스워드(PW)를 추출한다. 빌딩 에너지 통합 관제 장치(200)의 인증서부는 추출한 PW와 R2값을 함께 MD5한 결과를 빌딩 클라이언트(100)로부터의 값과 비교해서 일치하면 인증 메시지를 빌딩 클라이언트(100)의 공개키(KUc)를 통하여 암호화 한 후 생성된 code11.txt를 게이트웨이(420)에게로 전송한다.
- [0107] ⑩ 게이트웨이(420)는 code11.txt 파일을 빌딩 클라이언트(100)에게로 전송한다. 빌딩 클라이언트(100)는 code11.txt를 KRs로 복호화하여 인증메시지를 출력한다.
- [0108] 도 8은 도 4에 도시된 빌딩 에너지 통합 관제 장치의 접근 정책 모듈에서의 접근 제어를 설명하는 흐름도이고, 도 9는 도 8의 접근 제어 결정 단계의 세부 흐름도이다.
- [0109] 접근 정책 모듈(90)은 서비스 요청이 발생하면, 접근 정책 보안 관리자(112)에 의해 설정된 접근 제어 정책과 환경 정보를 기반으로 접근 허용 여부를 결정하고, 그에 따른 접근 제어 수행을 실시하며 로그 파일에 저장한다. 바람직하게, 접근 제어 결과에 대한 수행 정책을 보면 다음과 같다. 예를 들어, 접근이 허용된 경우에는 빌딩 에너지 통합 관제 서비스 제어, 해당 서비스 제공, 정책에 따라 관리자에게 통보를 행한다. 반대로, 접근이 거부된 경우에는 사용자에게 서비스 거부 메시지 전달하고, 이를 로그 파일에 기록하며, 관리자에게 경보를 전달한다.
- [0110] 도 8의 접근 제어 결정 단계를 세부적으로 구분해보면, 도 9에서와 같이 빌딩내/외 사용자로부터의 접근 요청을 수신하는 접근 수신 단계, 요청에 해당하는 모든 접근 제어 정책을 검색하는 정책 검색 단계, 및 이를 기반으로 접근 허용 여부를 결정하는 접근 허용 결정 단계로 나눌 수 있다. 접근 수신 단계의 경우 접근 요청을 받으면 접근 요청 메시지로부터 사용자 ID, 접근하고자 하는 대상, 및 해당 동작 정보(또는 대상물 등급 정보)를 추출한다. 추출된 정보를 기반으로 정책 검색 단계에서는 해당하는 모든 접근 제어 정책을 검색하고, 접근 허용 결정 단계에서는 그 검색된 결과를 기초로 접근 허용 여부를 결정한다.
- [0111] 도 8의 접근 제어 수행 단계는 접근 제어 결과를 수행하며, 단순히 접근 허용/거부 여부를 처리하기 보다는 요청한 서비스를 제공하는 기능까지 포함한다. 가장 단순한 접근 제어 수행으로서는 접근 거부 수행으로서, 해당 접근 요청을 거부하고 그 결과를 사용자에게 리턴하며, 로그 파일에 기록하면 된다. 접근을 허용할 경우에는 접근 서비스에 따라서 다양한 서비스를 지원해야 한다.
- [0112] 빌딩 에너지 통합 관제와 관련된 일련의 동작이 별도의 로그 파일에 저장되어야 할 필요가 있다고 판단되면 수행 결과를 로그 파일에 저장해야 한다. 필요성 판단은 빌딩 에너지 통합 관제 장치(200)의 보안 관리자(112)에 의해서 설정된 보안 정책에 기반한다. 접근 제어 수행 결과와 서비스 관련 정보는 추후 발생할 접근 제어에 영향을 미칠 수 있다. 예를 들어, 일정 기간 동안 특정 서비스 사용의 시간을 제한하는 정책을 수행하기 위해서는 서비스 사용 시간을 계산해서 유지할 필요가 있기 때문이다.

- [0113] 이어, 본 발명의 실시예에 따른 빌딩 에너지 통합 관제의 동작에 대해 도 10의 플로우차트를 참조하여 설명하면 다음과 같다. 사용자 인증 및 침입 탐지 등에 대해서는 상기에서 충분히 설명하였으므로, 이하에서는 통합적인 에너지 관리를 위한 효율적인 접근제어가 이루어지도록 하기 위해 빌딩 용도별 보안 정책(즉, 접근 제어 정책)을 설정하는 동작에 대해서만 설명한다.
- [0114] 우선, 접근 정책 보안 관리자(112)는 자신의 단말기를 통해 보안 레벨을 설정하고자 하는 특정 사용자 또는 특정 빌딩의 용도가 존재하는지를 확인한다(S10).
- [0115] 만약, 특정 사용자 또는 특정 빌딩의 용도가 존재하지 않으면 접근 정책 보안 관리자(112)는 자신의 단말기를 조작하여 특정 사용자 및 특정 빌딩의 용도를 생성한다(S12). 그에 따라 생성된 특정 사용자 및 특정 빌딩의 용도의 정보는 정책 보안 관리 모듈(110)에 의해 접근 정책 모듈(90)내의 보안 관리 에이전트(98)를 통해 정책 데이터베이스(96)에 등록된다(S14). 이와 같이 하면 특정 사용자 또는 특정 빌딩의 용도가 존재하게 된다.
- [0116] 그리고 나서, 접근 정책 보안 관리자(112)는 특정 사용자 및/또는 특정 빌딩의 용도를 선택한다(S16).
- [0117] 이후, 접근 정책 보안 관리자(112)는 해당 특정 사용자 및/또는 특정 빌딩의 용도에 대하여 적용할 보안 레벨이 존재하는지를 확인한다(S18).
- [0118] 만약, 적용할 보안 레벨이 존재하지 않으면 접근 정책 보안 관리자(112)는 보안 레벨을 생성한다(S20). 그에 따라 생성된 보안 레벨 정보는 정책 보안 관리 모듈(110)에 의해 접근 정책 모듈(90)내의 보안 관리 에이전트(98)를 통해 정책 데이터베이스(96)에 등록된다(S22). 여기서, 정책 데이터베이스(96)에 등록되는 빌딩 용도의 중요도에 따른 보안 레벨의 분류 예를 다음의 표 1에 나타낸다.

표 1

[0119]

분류(정책)	분류(인증)	분류(빌딩)
C등급 보안 레벨(L)	ID/PW	단독주택, 근린생활시설, 동물 및 식물 관리시설, 분노 및 쓰레기처리시설, 묘지관련시설
B등급 보안 레벨(M)	인증서 기반	공동주택, 운동시설, 숙박시설, 위락시설, 자동차관련시설, 관광휴게시설
A등급 보안 레벨(H)	ID/PW + 인증서 기반 (통합 인증)	문화 및 집회 시설, 판매 및 영업시설, 의료시설, 교육 및 복지시설, 업무시설, 공장, 창고시설, 위험물 저장 및 처리시설, 공공용 시설

- [0120] 그리고 나서, 접근 정책 보안 관리자(112)는 보안 레벨을 선택한다(S24). 이와 같이 하면 특정 사용자에게 대해 다수의 빌딩 에너지 관련 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 있는 다수의 보안 레벨중 특정 보안 레벨이 설정되는 강제적 접근 설정이 이루어진다.
- [0121] 이후, 특정 사용자에게 대하여 다수의 빌딩 에너지 관련 기기들 전부 또는 일부에 대한 임의적 접근 설정이 이루어진다(S26). 임의적 접근 설정은 필요한 경우에 행해지는 것으로 이해하면 된다.
- [0122] 그 임의적 접근 설정에 의한 설정 사항은 정책 보안 관리 모듈(110)에 의해 접근 정책 모듈(90)내의 보안 관리 에이전트(98)를 통해 정책 데이터베이스(96)에 등록된다(S28).
- [0123] 도 11은 본 발명의 실시예에 따른 빌딩 에너지 통합 관제 방법의 설명중에서 보안정책 관리자의 단말기와 빌딩 에너지 통합 관제 장치의 보안서버 간에 송수신되는 데이터와 동작을 설명하기 위한 플로우차트이다.

[0124] 접근 정책 보안 관리자(112)는 자신의 단말기를 통해 사용자별 보안 정책에 관한 정보를 요청하는 메시지를 빌딩 에너지 통합 관제 장치(200)의 보안서버에게로 전송한다(S100).

[0125] 그에 따라, 빌딩 에너지 통합 관제 장치(200)의 보안서버는 해당하는 보안 정책을 접근 정책 보안 관리자(112)의 단말기에게로 전송한다(S102).

[0126] 접근 정책 보안 관리자(112)는 수신된 사용자별 보안 정책에 관한 정보를 이용하여 특정 사용자에게 대한 보안 정책을 설정한다(S104). 여기서, 보안 정책의 설정이라 하면 수정 및 삭제를 포함함과 더불어 특정 사용자에게 대한 보안 정책을 새롭게 생성하는 것을 포함한다.

[0127] 이어, 접근 정책 보안 관리자(112)는 설정한 보안 정책을 자신의 단말기를 통해 빌딩 에너지 통합 관제 장치(200)의 보안서버에게로 전송한다(S106).

[0128] 빌딩 에너지 통합 관제 장치(200)의 보안서버는 수신한 보안 정책을 적용시킨다(S108). 즉, 빌딩 에너지 통합 관제 장치(200)의 보안서버는 수신한 보안 정책을 정책 데이터베이스(96)에 업데이트시킨다.

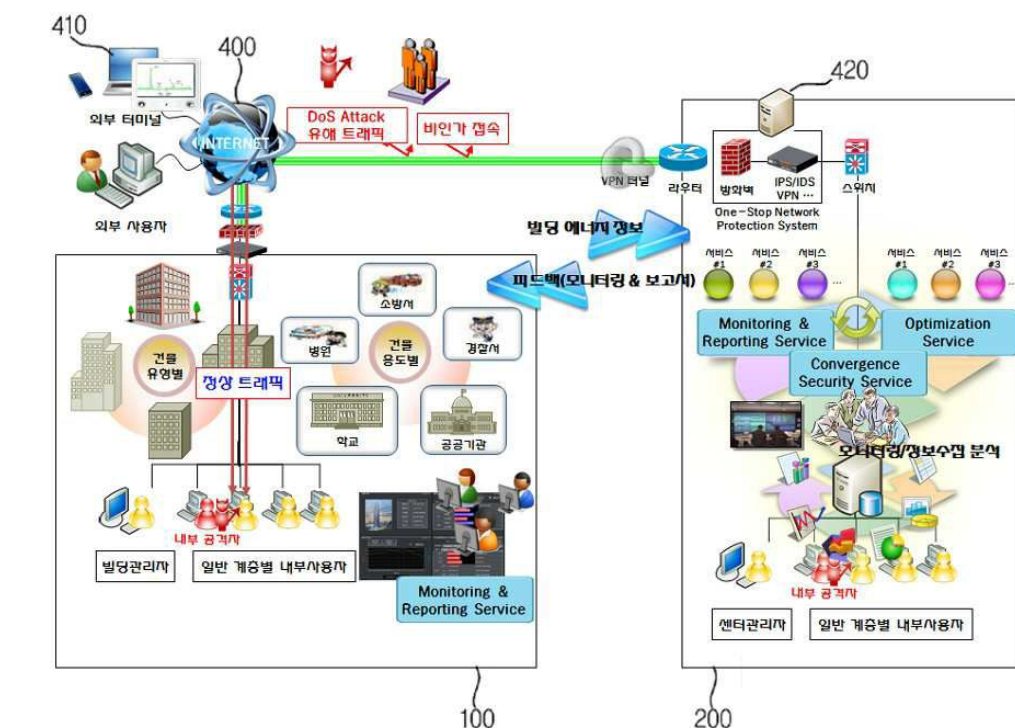
[0129] 한편, 본 발명은 상술한 실시예로만 한정되는 것이 아니라 본 발명의 요지를 벗어나지 않는 범위내에서 수정 및 변형하여 실시할 수 있고, 그러한 수정 및 변형이 가해진 기술사상 역시 이하의 특허청구범위에 속하는 것으로 보아야 한다.

부호의 설명

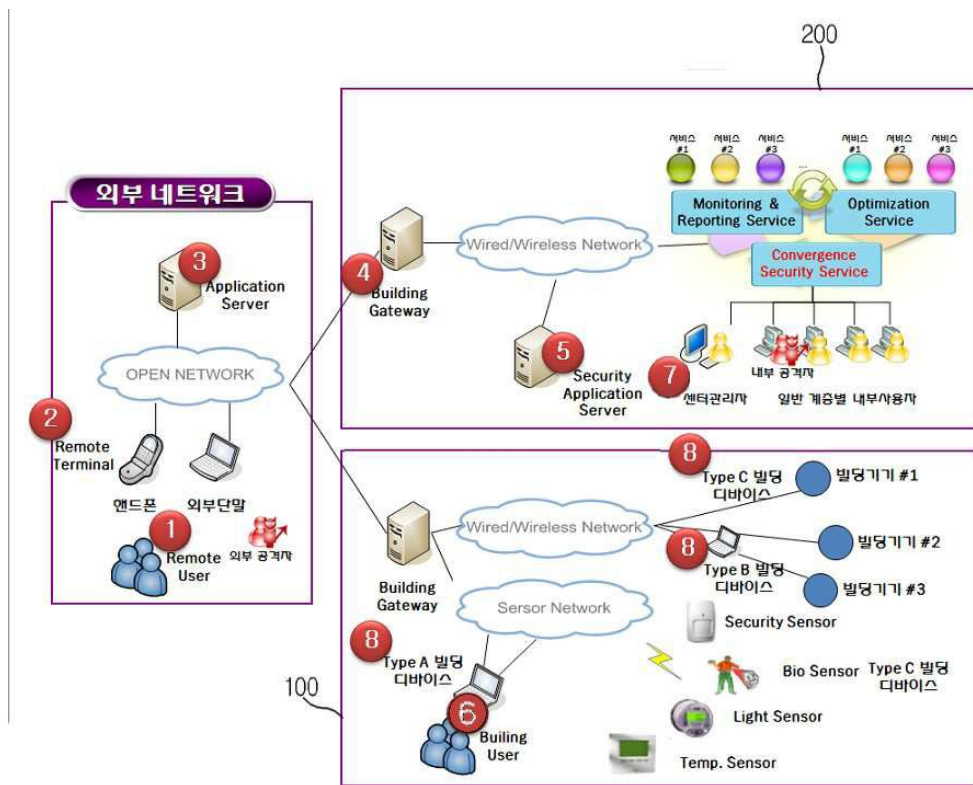
[0130]	10, 80 : 암호 모듈	20, 60 : 인증 모듈
	30, 120 : 침입 탐지 모듈	40 : 사용자 브라우저 또는 단말
	50 : 경보부	90 : 접근 정책 모듈
	100 : 빌딩 클라이언트	110 : 정책 보안 관리 모듈
	200 : 빌딩 에너지 통합 관제 장치	300 : 키분배 센터

도면

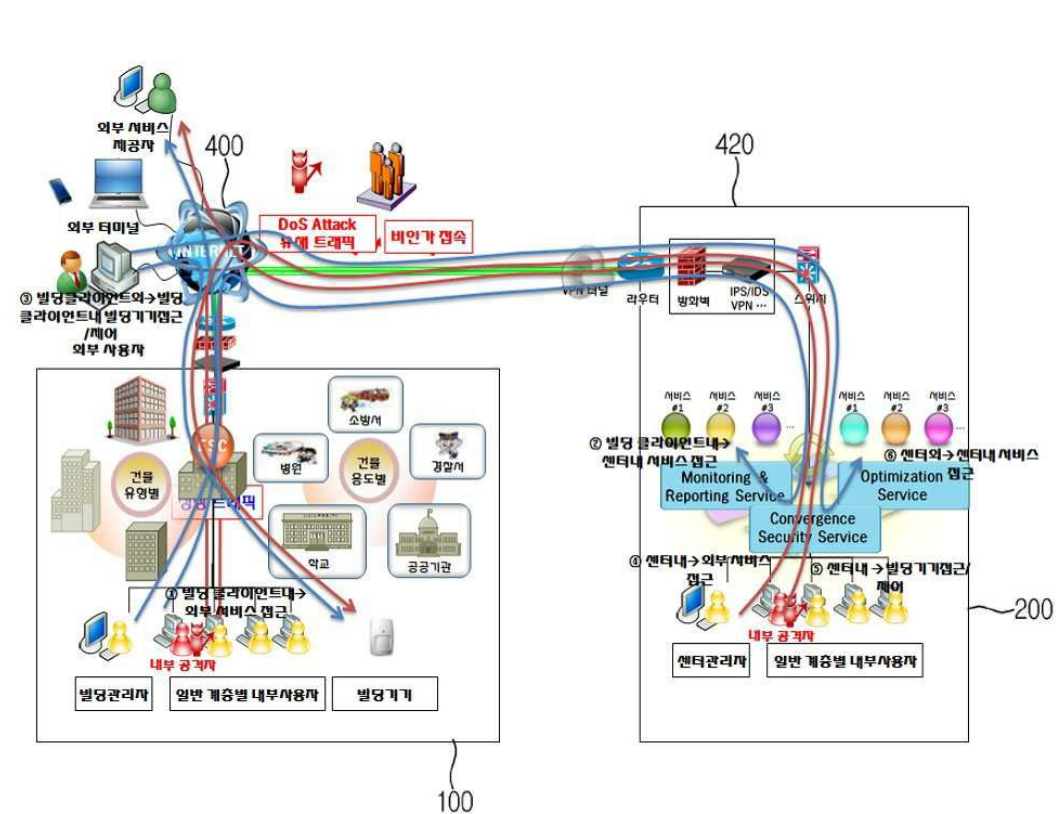
도면1



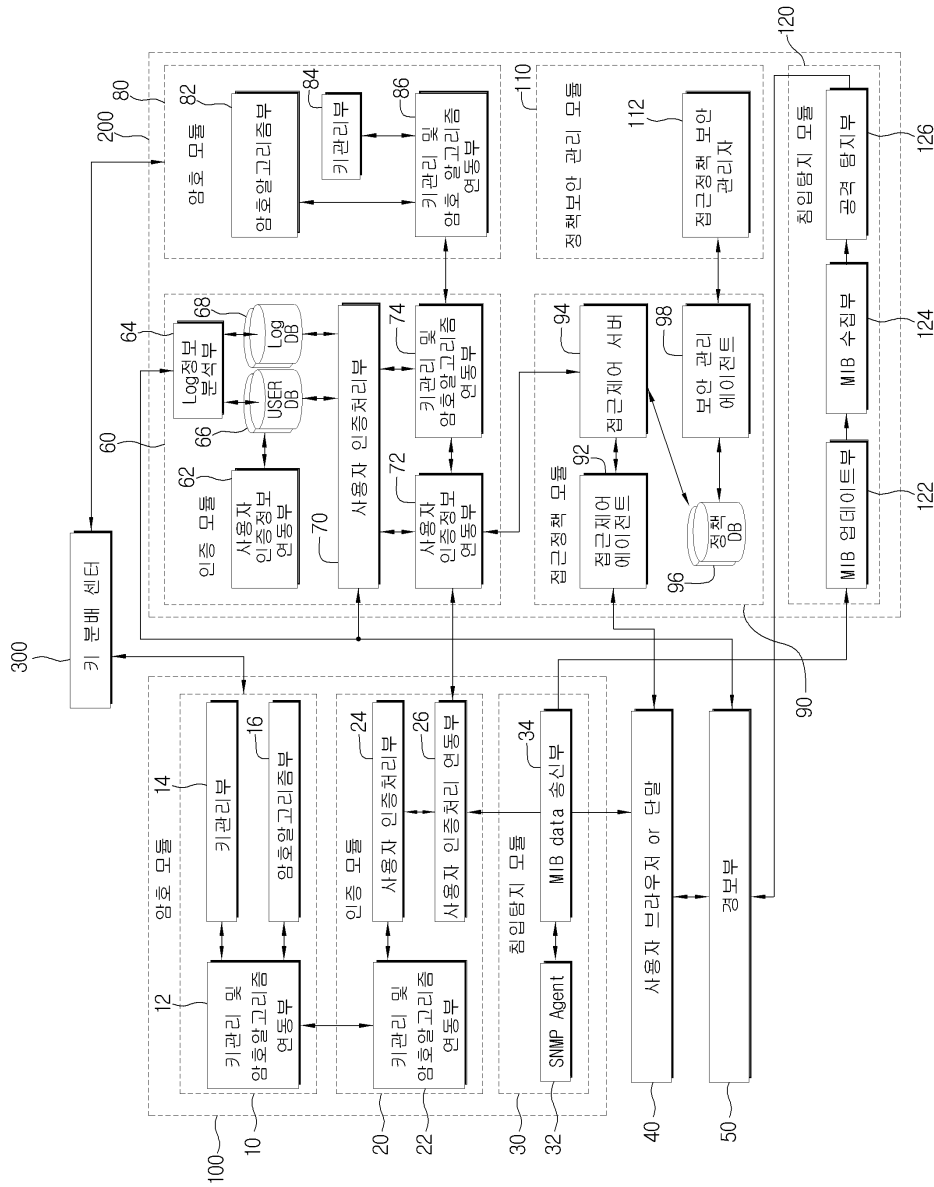
도면2



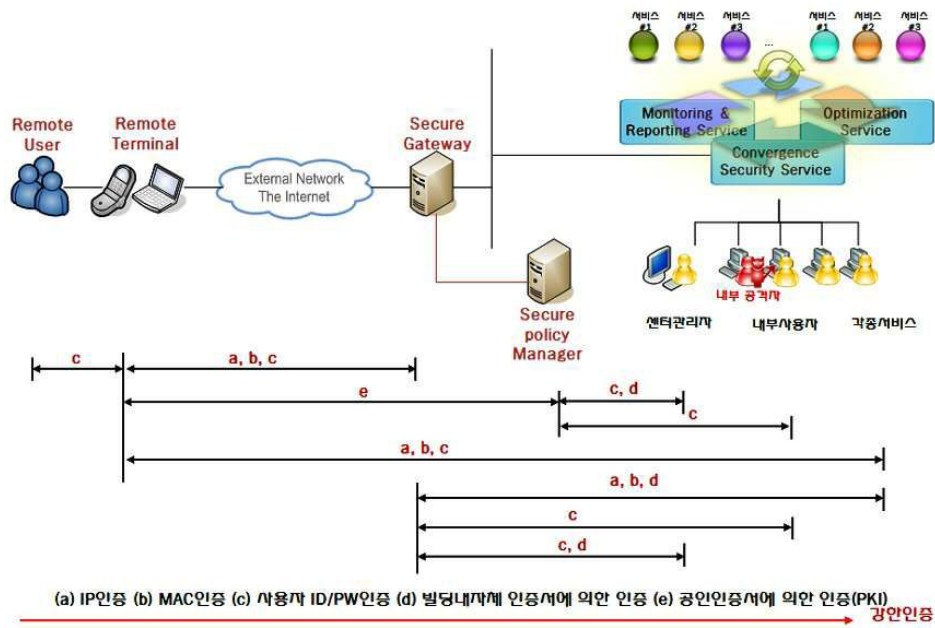
도면3



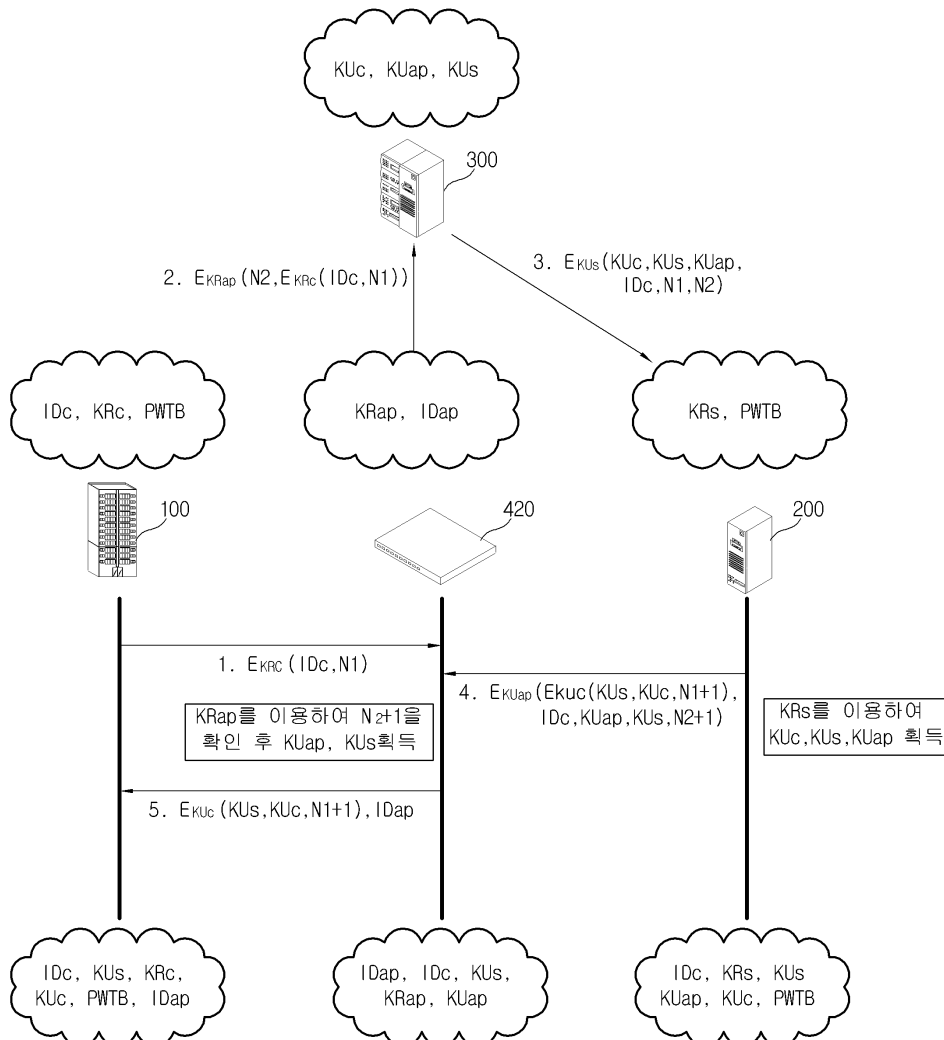
도면4



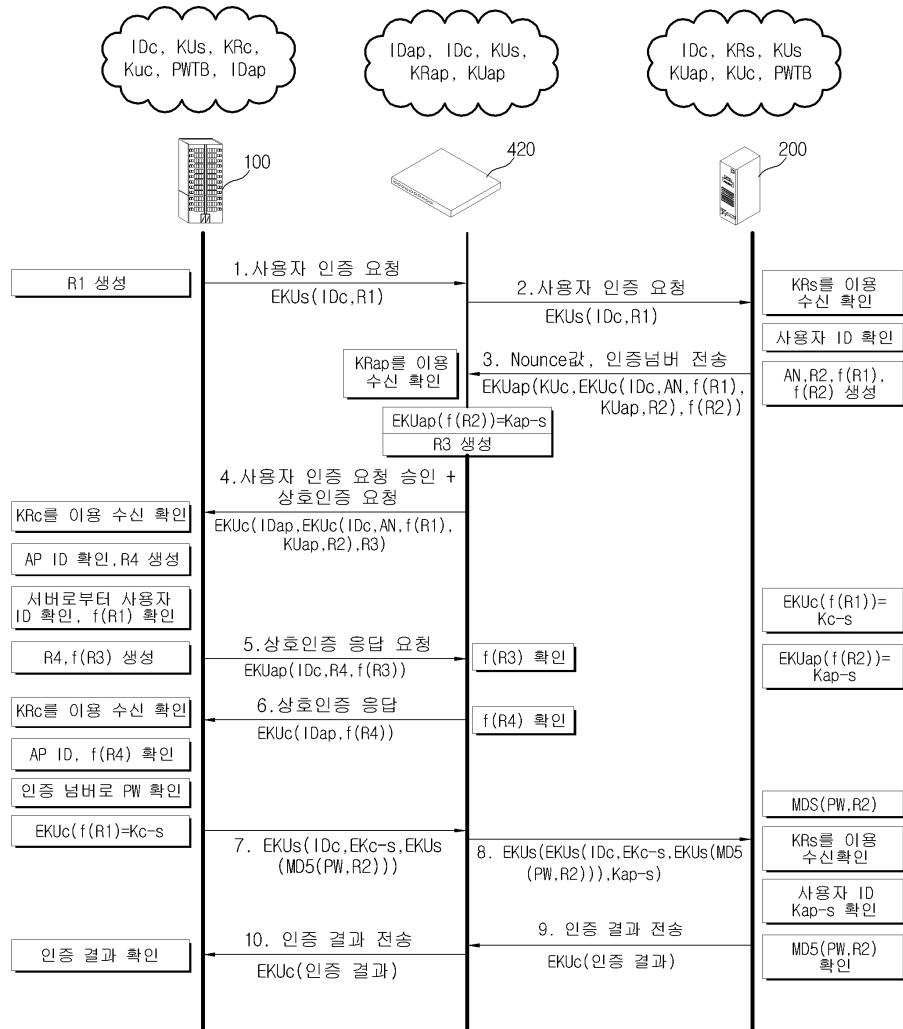
도면5



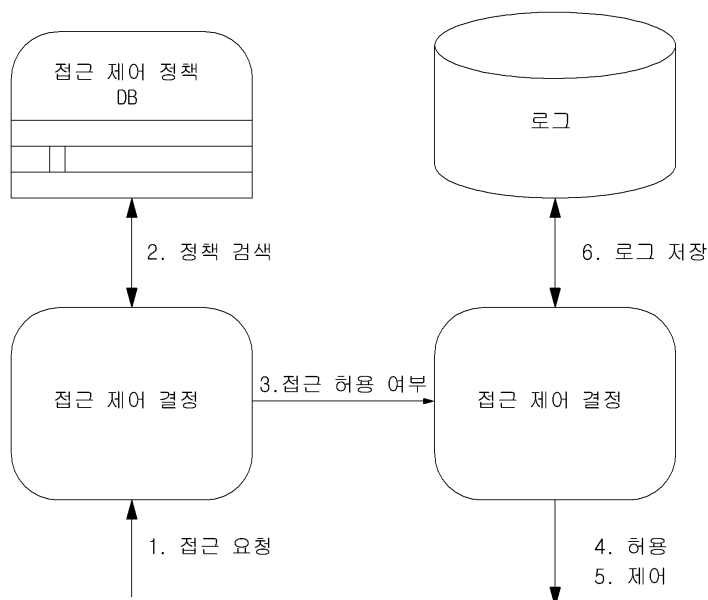
도면6



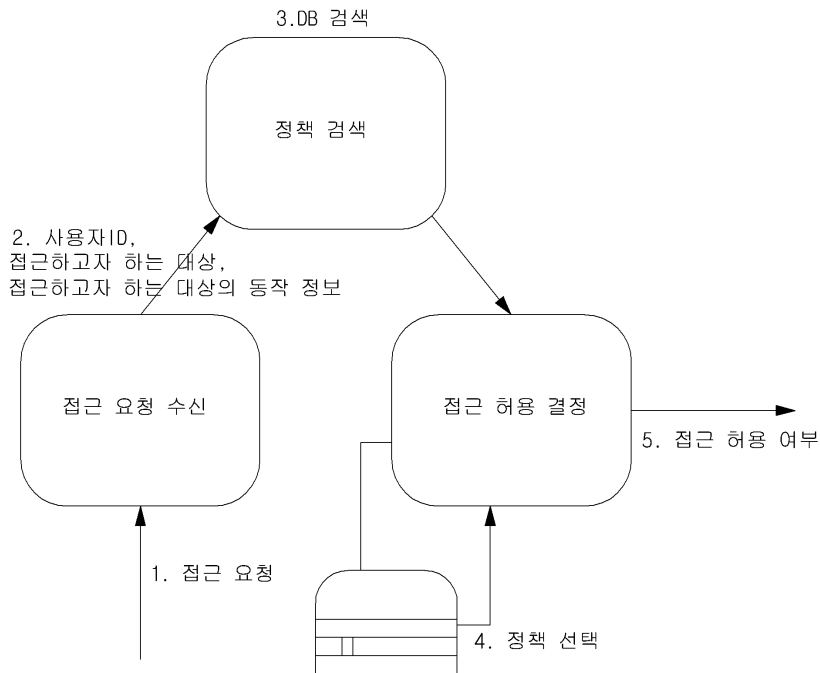
도면7



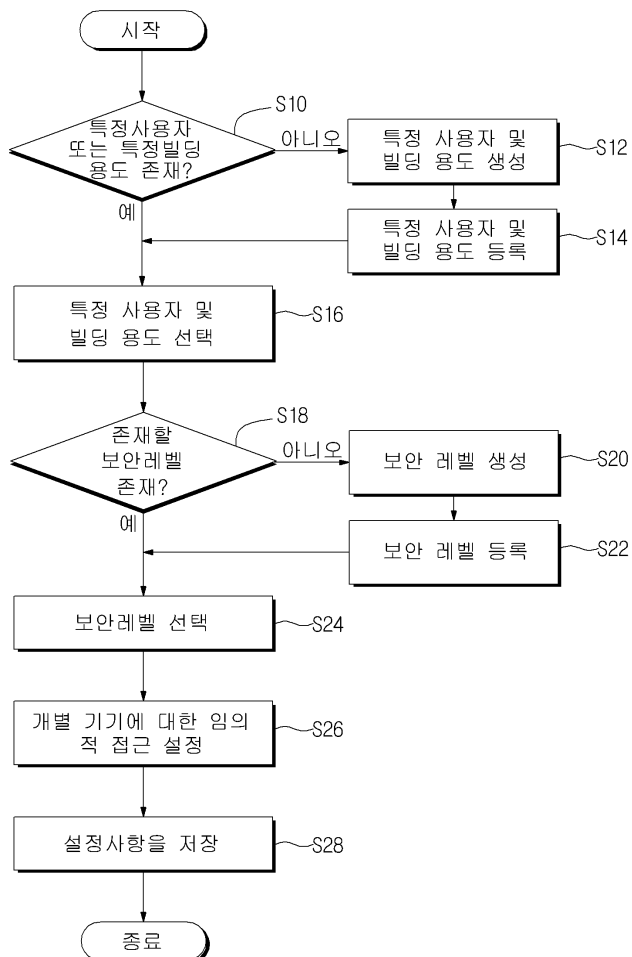
도면8



도면9



도면10



도면11

