



**(19) 대한민국특허청(KR)**  
**(12) 등록특허공보(B1)**

(45) 공고일자 2010년01월15일  
 (11) 등록번호 10-0937020  
 (24) 등록일자 2010년01월07일

(51) Int. Cl.

G06F 11/00 (2006.01)

(21) 출원번호 10-2007-0124977  
 (22) 출원일자 2007년12월04일  
 심사청구일자 2007년12월04일  
 (65) 공개번호 10-2009-0058271  
 (43) 공개일자 2009년06월09일

(56) 선행기술조사문헌  
 KR1020080044145 A  
 KR100748246 B1\*  
 KR1020040052569 A

\*는 심사관에 의하여 인용된 문헌

(73) 특허권자

(주)모니터랩

서울특별시 구로구 구로동 197-17 에이스테크노타워1차 306호

(72) 발명자

윤영

서울 용산구 도원동 삼성아파트 201동 601호

(74) 대리인

특허법인명인

전체 청구항 수 : 총 11 항

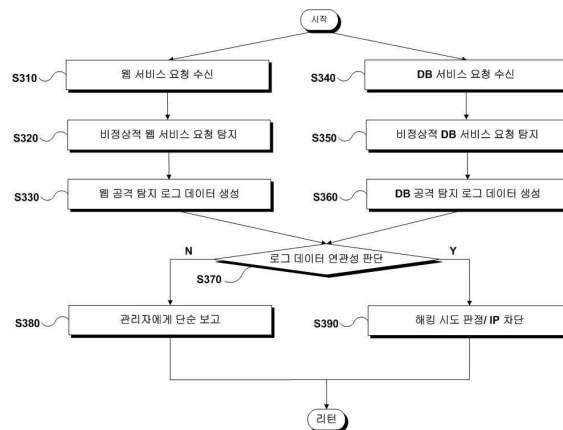
심사관 : 이옥우

**(54) 웹-데이터베이스 공격 탐지 로그 데이터 상관관계 추적에 의한 통합 보안 시스템 및 방법**

**(57) 요약**

본 발명은 웹-데이터베이스 공격 탐지 로그 데이터 상관관계 추적에 의한 통합 보안 시스템 및 방법에 관한 것이다. 본 발명에 따른 통합 보안 방법은, 비정상적 웹 서비스 요청을 탐지하는 단계, 비정상적 데이터베이스 서비스 요청을 탐지하는 단계 및, 상기 비정상적 웹 서비스 요청에 대한 웹 공격 탐지 로그 데이터와 상기 비정상적 데이터베이스 서비스 요청에 대한 데이터베이스 공격 탐지 로그 데이터에 연관성이 있는 경우 상기 웹 서비스 요청을 데이터베이스에 대한 해킹 시도로 판정하는 단계를 포함한다. 본 발명에 따르면 웹 서버 및 데이터베이스에 대한 공격을 정확하게 탐지하여 대응할 수 있다.

**대표도 - 도3**



**특허청구의 범위**

**청구항 1**

삭제

**청구항 2**

비정상적 웹 서비스 요청을 탐지하는 단계;

비정상적 데이터베이스 서비스 요청을 탐지하는 단계; 및,

상기 비정상적 웹 서비스 요청에 대한 웹 공격 탐지 로그 데이터와 상기 비정상적 데이터베이스 서비스 요청에 대한 데이터베이스 공격 탐지 로그 데이터에 연관성이 있는 경우 상기 웹 서비스 요청을 데이터베이스에 대한 해킹 시도로 판정하는 단계; 를 포함하고,

상기 웹 공격 탐지 로그 데이터는 상기 웹 서비스 요청이 전송된 사용자 단말기의 아이피(IP) 주소, 상기 웹 서비스 요청에서 추출되는 입력 파라미터 값을 포함하고,

상기 데이터베이스 공격 탐지 로그 데이터는 상기 데이터베이스 서비스 요청에서 추출되는 쿼리 값을 포함하는 것을 특징으로 하는 웹-데이터베이스 통합 보안 방법.

**청구항 3**

제 2 항에 있어서,

상기 입력 파라미터 값과 상기 쿼리 값이 동일한 경우,

상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터는 서로 연관성이 있는 것으로 판정되는 것을 특징으로 하는 웹-데이터베이스 통합 보안 방법.

**청구항 4**

제 2 항에 있어서,

상기 웹 공격 탐지 로그 데이터는 서버 응답 코드를 더 포함하고, 상기 데이터베이스 공격 탐지 로그 데이터는 DB 에러 코드를 더 포함하며,

상기 입력 파라미터 값과 상기 쿼리 값이 동일하고, 상기 서버 응답 코드와 상기 DB 에러 코드가 연관성이 있는 경우,

상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터는 서로 연관성이 있는 것으로 판정되는 것을 특징으로 하는 웹-데이터베이스 통합 보안 방법.

**청구항 5**

제 3 항 또는 제 4 항에 있어서,

상기 데이터베이스에 대한 해킹 시도로 판정된 경우 상기 아이피 주소를 통한 접속을 차단하는 단계; 를 더 포함하는 것을 특징으로 하는 웹-데이터베이스 통합 보안 방법.

**청구항 6**

제 5 항에 있어서,

상기 아이피 주소를 통한 접속을 차단하는 단계는,

상기 해킹 시도로 판정된 회수가 미리 정해진 회수 이상일 경우 수행되는 것을 특징으로 하는 웹-데이터베이스 통합 보안 방법.

**청구항 7**

제 2 항 내지 제 4 항 중 어느 한 항의 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록

매체.

**청구항 8**

삭제

**청구항 9**

웹 서비스 요청이 비정상적인 경우 웹 공격 탐지 로그 데이터를 생성하는 웹 보안부;

데이터베이스 서비스 요청이 비정상적인 경우 데이터베이스 공격 탐지 로그 데이터를 생성하는 데이터베이스 보안부; 및,

상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터에 연관성이 있는 경우 상기 웹 서비스 요청을 데이터베이스에 대한 해킹 시도로 판정하는 해킹 판정부; 를 포함하고,

상기 웹 공격 탐지 로그 데이터는 상기 웹 서비스 요청이 전송된 사용자 단말기의 아이피(IP) 주소, 상기 웹 서비스 요청에서 추출되는 입력 파라미터 값을 포함하고,

상기 데이터베이스 공격 탐지 로그 데이터는 상기 데이터베이스 서비스 요청에서 추출되는 쿼리 값을 포함하는 것을 특징으로 하는 웹-데이터베이스 통합 보안 시스템.

**청구항 10**

제 9 항에 있어서,

상기 입력 파라미터 값과 상기 쿼리 값이 동일한 경우,

상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터는 서로 연관성이 있는 것으로 판정되는 것을 특징으로 하는 웹-데이터베이스 통합 보안 시스템.

**청구항 11**

제 9 항에 있어서,

상기 웹 공격 탐지 로그 데이터는 서버 응답 코드를 더 포함하고, 상기 데이터베이스 공격 탐지 로그 데이터는 DB 에러 코드를 더 포함하며,

상기 입력 파라미터 값과 상기 쿼리 값이 동일하고, 상기 서버 응답 코드와 상기 DB 에러 코드가 연관성이 있는 경우,

상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터는 서로 연관성이 있는 것으로 판정되는 것을 특징으로 하는 웹-데이터베이스 통합 보안 시스템.

**청구항 12**

제 10 항 또는 제 11 항에 있어서,

상기 해킹 판정부는,

상기 데이터베이스에 대한 해킹 시도로 판정된 경우 상기 아이피 주소를 통한 접속을 차단하는 것을 특징으로 하는 웹-데이터베이스 통합 보안 시스템.

**청구항 13**

제 12 항에 있어서,

상기 해킹 판정부는,

상기 해킹 시도로 판정된 회수가 미리 정해진 회수 이상일 경우 상기 아이피 주소를 통한 사용자 단말기의 접속을 차단하는 것을 특징으로 하는 웹-데이터베이스 통합 보안 시스템.

**명세서**

**발명의 상세한 설명**

**기술 분야**

<1> 본 발명은 보안 시스템 및 보안 방법에 관한 것으로, 보다 상세하게는 웹 서버 및 데이터베이스에 대한 통합 보안을 수행할 수 있는 보안 시스템 및 방법에 관한 것이다.

**배경 기술**

<2> 최근 들어 컴퓨터 통신 기술의 발전에 따라 인터넷을 통해서 상품을 구입하거나 은행 업무를 보는 등의 전자상거래 서비스, 각종 증명서 발급 서비스 및 게임서비스 등 다양한 인터넷 서비스 제공이 폭발적으로 증가하고 있다.

<3> 그런데 인터넷을 통한 서비스의 급증만큼이나 금전적, 정치적 또는 명예욕 등의 다양한 목적을 가진 해킹 시도가 급증하고 있다. 특히 최근들어 해킹의 화두는 웹 애플리케이션의 취약성을 이용하는 것이다.

<4> 일반적으로 인터넷 서비스를 제공하기 위한 대부분의 웹 사이트는 사용자들에게 인터넷 서비스를 제공하기 위한 창구로 웹 애플리케이션을 제공하고 있으며, 웹 애플리케이션은 데이터베이스에 연동되어 있다. 사용자들이 인터넷 서비스를 이용하기 위해서 웹 브라우저에서 특정 파라미터 값을 입력하여 전송하면 웹 서버는 이를 받아들여 다시 웹 애플리케이션 서버(WAS:Web Application Server)로 전달한다. WAS는 사전에 준비된 질의문(QUERY)과 전달받은 입력 파라미터 값을 조합하여 완전한 질의문을 작성하여 데이터베이스로 전달하고 데이터베이스는 전달된 질의문에 따른 동작을 수행하고 그 결과는 입력 파라미터 값이 전달된 반대 순서로 사용자에게 전달된다.

<5> 그런데 사용자가 정상적인 값을 입력한 경우 문제가 없으나 비정상적인 값을 입력하고 입력 값에 대한 검증이 수행되지 않은 경우 WAS에서 질의문으로 조합되는 과정에서 문법에 맞지 않는 잘못된 작성된 질의문이 데이터베이스에 전달되어 구문 오류를 발생시킬 수 있으며, 더 나아가서는 부정한 의도를 가지는 공격자가 적절한 입력 값 조작으로 개발 당시 의도하지 않은 결과를 유도시킬 수 있다. 이러한 공격을 SQL 삽입 공격이라고 한다.

<6> 위에서 설명한 것과 같은 SQL 삽입 공격 외에도 다양한 형태의 데이터베이스 공격이 시도되고 있으며, 이러한 공격들로부터 데이터베이스를 보호하기 위한 데이터베이스 보안 제품이 출시되고 있다. 또한 웹 서버 자체에 대한 공격을 탐지하여 대응하기 위한 웹 서버 보안 제품도 출시되고 있으며, 일반적으로 데이터베이스 보안 제품과는 별도로 설치되어 운영되고 있다.

<7> 그런데 데이터베이스에 대한 공격이 위에서 설명한 것과 같이 WAS를 통해 이루어지는 경우 개별적인 데이터베이스 공격은 탐지하여 차단할 수 있을지라도 해당 공격을 시도한 공격자에 대한 IP를 데이터베이스 보안 시스템이 알 수 없기 때문에 공격자가 입력 파라미터를 변경해가면서 계속적으로 해킹 시도를 하는 것을 근본적으로 차단하기 어려운 문제점이 있다.

<8> 한편 웹 서버 보안 시스템은 공격자 IP를 알 수 있기 때문에 부정한 공격자의 접속을 차단시킬 수는 있으나, 악의적이지 않은 웹 서비스 요청에 대해서 해킹 시도로 오탐(False Positive)하고 해당 IP 접속을 차단하는 경우 사용자 불편이 가증될 수 있다는 문제점이 있다. 또한 해당 인터넷 서비스 시스템에 대한 신뢰도가 떨어질 수도 있다.

**발명의 내용**

**해결 하고자하는 과제**

<9> 따라서 본 발명이 이루고자 하는 기술적 과제는 웹 서버 및 데이터베이스에 대한 공격을 정확하게 탐지하여 대응할 수 있는 통합 보안 시스템 및 방법을 제공하는 것이다.

**과제 해결수단**

<10> 이러한 기술적 과제를 해결하기 위한 본 발명의 한 실시예에 따른 통합 보안 방법은, 비정상적 웹 서비스 요청을 탐지하는 단계와, 비정상적 데이터베이스 서비스 요청을 탐지하는 단계 및, 상기 비정상적 웹 서비스 요청에 대한 웹 공격 탐지 로그 데이터와 상기 비정상적 데이터베이스 서비스 요청에 대한 데이터베이스 공격 탐지 로그 데이터에 연관성이 있는 경우 상기 웹 서비스 요청을 데이터베이스에 대한 해킹 시도로 판정하는 단계를 포

함한다.

- <11> 여기서, 상기 웹 공격 탐지 로그 데이터는 상기 웹 서비스 요청이 전송된 사용자 단말기의 아이피(IP) 주소, 상기 웹 서비스 요청에서 추출되는 입력 파라미터 값을 포함하고, 상기 데이터베이스 공격 탐지 로그 데이터는 상기 데이터베이스 서비스 요청에서 추출되는 쿼리 값을 포함할 수 있다.
- <12> 상기 입력 파라미터 값과 상기 쿼리 값이 동일한 경우, 상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터는 서로 연관성이 있는 것으로 판정될 수 있다.
- <13> 상기 웹 공격 탐지 로그 데이터는 서버 응답 코드를 더 포함하고, 상기 데이터베이스 공격 탐지 로그 데이터는 DB 에러 코드를 더 포함하며, 상기 입력 파라미터 값과 상기 쿼리 값이 동일하고, 상기 서버 응답 코드와 상기 DB 에러 코드가 연관성이 있는 경우, 상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터는 서로 연관성이 있는 것으로 판정될 수 있다.
- <14> 상기 데이터베이스에 대한 해킹 시도로 판정된 경우 상기 아이피 주소를 통한 접속을 차단하는 단계를 더 포함할 수 있다.
- <15> 상기 접속 차단 단계는 상기 해킹 시도로 판정된 회수가 미리 정해진 회수 이상일 경우 수행될 수 있다.
- <16> 본 발명의 다른 실시예에 따른 컴퓨터로 읽을 수 있는 매체는 상기한 방법 중 어느 하나를 컴퓨터에 실행시키기 위한 프로그램을 기록한다.
- <17> 본 발명의 또 다른 실시예에 따른 보안 시스템은, 웹 서비스 요청이 비정상적인 경우 웹 공격 탐지 로그 데이터를 생성하는 웹 보안부와, 데이터베이스 서비스 요청이 비정상적인 경우 데이터베이스 공격 탐지 로그 데이터를 생성하는 데이터베이스 보안부 및, 상기 웹 공격 탐지 로그 데이터와 상기 데이터베이스 공격 탐지 로그 데이터에 연관성이 있는 경우 상기 웹 서비스 요청을 데이터베이스에 대한 해킹 시도로 판정하는 해킹 판정부를 포함한다.
- <18> 상기 해킹 판정부는, 상기 데이터베이스에 대한 해킹 시도로 판정된 경우 상기 아이피 주소를 통한 접속을 차단할 수 있다.
- <19> 상기 해킹 판정부는, 상기 해킹 시도로 판정된 회수가 미리 정해진 회수 이상일 경우 상기 아이피 주소를 통한 사용자 단말기의 접속을 차단할 수 있다.

**효 과**

- <20> 이와 같이 본 발명에 의하면, 웹 공격과 데이터베이스 공격의 연관성을 분석하여 더욱 정확한 해킹 탐지를 할 수 있게 됨으로써 오탐을 최소화 시킬 수 있다. 웹 보안 제품과 데이터베이스 보안 제품의 통합 관리를 통해 보안 관리의 접점을 줄일 수 있다. 특히 SQL 삽입 공격, 웹 유희 공격, 알려지지 않은 공격(unknown attack), 제로 데이 공격(Zero-day attack)으로부터 데이터베이스에 대한 보안을 강화시킬 수 있다.

**발명의 실시를 위한 구체적인 내용**

- <21> 그러면 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다.
- <22> 도 1은 본 발명의 일 실시예에 따른 보안 시스템을 설명하기 위해 제공되는 도면이다.
- <23> 도 1을 참조하면, 본 발명의 실시예에 따른 보안 시스템(100)은 웹 보안부(110), 데이터베이스 보안부(120:이하 'DB 보안부'라 함) 및 해킹 판정부(130)를 포함할 수 있다. 보안 시스템(100)은 통신망을 통해 복수의 사용자 단말기(10), 웹 서버(20), 웹 애플리케이션 서버(30:이하 'WAS 서버'라 함) 및 데이터베이스 서버(40:이하 'DB 서버'라 함)와 연결되어 각종 정보를 주고 받을 수 있으며, 웹 서버(20)와 DB 서버(40)에 대한 공격을 탐지하고 그에 따른 대응 조치를 수행할 수 있다. 여기서 통신망은 구내 정보 통신망(local area network:LAN), 도시권 통신망(metropolitan area network:MAN), 광역 통신망(wide area network:WAN), 인터넷 등을 가리지 않고, 통신 방식도 유선, 무선을 가리지 않으며 어떠한 통신 방식이라도 상관없다.
- <24> 사용자 단말기(10)는 웹 서비스를 이용하기 위해 사용자가 이용하는 통신 단말장치로서, 데스크톱 컴퓨터뿐만 아니라 노트북 컴퓨터, 워크스테이션, 팜톱(palmtop) 컴퓨터, 개인 휴대 정보 단말기(personal digital assistant:PDA), 웹 패드 등과 같은 메모리 수단을 구비하고 마이크로 프로세서를 탑재하여 연산 능력을 갖춘

통신 단말기로 이루어질 수 있다. 사용자 단말기(10)는 웹 서버(20)에 웹 서비스 요청 메시지를 TCP/IP 기반의 HTTP 메시지 형태로 전송할 수 있으며, 그에 따른 응답 데이터를 제공받아 사용자에게 제공할 수 있다. 사용자는 사용자 단말기(10)의 웹 브라우저 상에서 특정 입력 파라미터 값을 입력하고 웹 요청 메시지에 포함시켜 웹 서버(20)로 전달할 수 있다. 예컨대, 사용자는 웹 브라우저의 주소창(URL 입력창)에서 URL 뒤에 '?'를 붙이고 그 뒤에 입력 파라미터 이름과 입력 파라미터에 대한 값을 입력하면, 소정의 입력 파라미터 값이 포함된 웹 요청 메시지를 GET 방식으로 웹 서버(20)에 전송할 수 있다. 물론 사용자는 웹 페이지의 HTTP 폼에 입력 파라미터 값을 입력하여 POST 방식으로 웹 요청 메시지를 전송할 수도 있다.

- <25> 웹 서버(20)는 사용자 단말기(10)로부터 전송되는 웹 서비스 요청에 따른 응답 데이터를 사용자 단말기(10)에 제공한다. 웹 서버(20)는 웹 서비스 요청에 WAS 서버(30)로 전달해야 할 특정 파라미터 값이 포함되어 있으면 이를 WAS 서버(30)에 전달하여 그에 대응하는 응답 데이터를 제공받고 이를 사용자 단말기(10)에 제공할 수도 있다.
- <26> WAS 서버(30)는 사전에 준비된 질의문(QUERY)과 전달받은 입력 파라미터 값을 조합하여 완전한 SQL 질의문을 작성하여 DB 서버(40)로 데이터베이스 서비스 요청을 전달하고, 그에 따른 데이터베이스 응답 데이터를 제공받아 다시 웹 서버(20)로 전달할 수 있다.
- <27> DB 서버(40)는 WAS 서버(30)로부터 전달된 SQL 질의문에 따른 작업(예컨대, 데이터 삽입, 갱신, 삭제, 검색 등)을 수행하고 그 처리 결과를 웹 서버(20)에 데이터베이스 응답 데이터로 제공할 수 있다.
- <28> 그러면 도 2를 참고하여 본 발명의 일 실시예에 따른 보안 시스템에 대해 보다 자세히 설명한다.
- <29> 도 2는 도 1의 보안 시스템을 보다 자세히 나타낸 블록도이다.
- <30> 도 2를 참고하면, 웹 보안부(110)는 사용자 단말기로부터 전송되는 웹 서비스 요청을 수신하여 정상적인지 또는 비정상적인지 여부를 판단하고, 비정상적인 웹 서비스 요청이 탐지된 경우 이에 대한 탐지 로그 데이터(이하, '웹 공격 탐지 로그 데이터'라 함)를 생성한다.
- <31> 보다 자세하게는 웹 보안부(110)는 웹 공격 시그너처 DB(111), 웹 서비스 프로파일 DB(113), 웹 요청 검증 모듈(115) 및 웹 공격 탐지 로그 DB(117)를 포함할 수 있다.
- <32> 웹 공격 시그너처 DB(111)는 이미 알려진 웹 서비스 공격의 시그너처(signature)를 저장할 수 있다.
- <33> 웹 서비스 프로파일 DB(113)는 사용자의 접근이 허용되는 서비스에 대한 URL 패턴을 저장할 수 있다.
- <34> 웹 요청 검증 모듈(115)은 웹 공격 시그너처 DB(111)와 웹 서비스 프로파일 DB(113)를 이용하여 네가티브 및 포지티브 방식을 혼용하여 웹 서비스 요청에 대한 정상 또는 비정상 여부를 탐지할 수 있다. 실시예에 따라서 웹 요청 검증 모듈(115)은 네가티브 또는 포지티브 방식 중 어느 하나에 의해 웹 서비스 요청의 정상 여부를 탐지할 수 있으며, 기타 다른 방식에 의해 비정상적 웹 서비스 요청을 탐지할 수도 있다. 웹 요청 검증 모듈(115)은 비정상적 웹 서비스 요청이 탐지된 경우 그에 대한 웹 공격 탐지 로그 데이터를 생성하여 웹 공격 탐지 로그 DB(117)에 저장할 수 있다.
- <35> 웹 공격 탐지 로그 데이터는 아래 표 1과 같이 시퀀스 번호, 클라이언트 IP 주소, 타겟(Target) URL, 서버 응답 코드, 입력 파라미터 값들이 포함될 수 있다.

**표 1**

시퀀스 번호
클라이언트 IP 주소
Target URL
서버 응답 코드
입력 파라미터 값 1
입력 파라미터 값 2
...
입력 파라미터 값 n

<36>

- <37> 여기서, 시퀀스 번호는 웹 공격 탐지 로그 데이터에 붙는 일련 번호이다. 클라이언트 IP 주소는 해당 웹 서비스 요청이 전송된 사용자 단말기의 IP 주소이다. 타겟 URL은 해당 웹 서비스 요청에 포함된 URL이다.
- <38> 서버 응답 코드는 해당 웹 서비스 요청에 대해 웹 서버로부터 반환되는 응답 코드이다. 일반적으로 DB 서버(40)가 해킹 공격에 의해 에러가 발생하면 DB 에러 코드가 발생하고 그 처리 결과가 WAS 서버(30)를 통해 WEB 서버(20)로 전달되는데 이때 웹 서버에서 이 DB 에러 코드를 처리할 때 두가지 방식으로 처리하게 된다. 하나는 DB 에러 코드를 그대로 서버 응답 코드로서 웹 응답 데이터에 포함시켜 반환하는 것이고, 다른 하나는 내부 서버(즉 미들웨어단에 해당하는 WAS 서버, DB 서버)에 있는 소프트웨어들의 오류 발생을 의미하는 에러 코드 값 '500'을 서버 응답 코드로 반환할 수 있다. 따라서 웹 공격 탐지 로그 데이터에는 서버 응답 코드로 '500' 또는 'DB 에러 코드 값'이 포함될 수 있다.
- <39> 입력 파라미터 값은 GET 방식으로 전송되는 웹 서비스 요청의 경우 URL 정보의 '?' 뒤에 있는 파라미터 값이 될 수 있으며, 또한 POST 방식으로 전송되는 경우 HTTP 메시지 본체(body) 부분에 포함되어 있는 HTTP 폼 입력값이 될 수 있다. 특히 본 발명에 따른 일 실시예의 경우 웹 요청 데이터에 포함된 입력 파라미터 값들 중에서 WAS 서버(30)에서 SQL 질의문을 완성하는데 사용되는 값만을 추출하여 웹 공격 탐지 로그 데이터에 포함시킬 수 있다. 예를 들어 단순 인덱스 값, SQL 바인드 변수 값, 폼 명 등에 해당하는 것들은 SQL 쿼리문을 완성할 때 그 값이 사용되지 않거나 변경될 수 있기 때문에 뒤에서 해킹 여부 판정을 위한 비교 값으로 사용하기 곤란하다. 따라서 해당 값들은 웹 공격 탐지 로그 데이터에 포함시키지 않으며 DB 공격 탐지 로그 데이터에도 포함시키지 않는 것이 바람직하다.
- <40> 다음과 같은 비정상적인 웹 서비스 요청이 탐지된 경우 각 URL 의 ? 뒤에 있는 문자열 중 볼드체로 표시되어 있는 입력 파라미터 값이 추출되어 웹 공격 탐지 로그 데이터에 포함될 수 있다.
- <41> 1) `http://target.com/forum/login.jsp?userid=admin&passwd=test`
- <42> 2) `http://target.com/forum/login.jsp?userid=' or '1'='1`
- <43> 3) `http://target.com/cafe/cafe_make_index.php?sp=categorySearch&sel=bd_contents&sch_cname='`
- <44> 4) `http://target.com/forum/bbs/view?idx=581&t_search='검색%'`
- <45> 5) `http://www.xxx.com/forun/bbs/download.jsp?idx=581'union select 1, tname,'3',444,'444' fromsys.tab where tname not in ('AOTMSRNES','AOTORGTBL','A4TCPADLG','BANK_THEME_DATA') - -`
- <46> 한편 본 실시예에서는 웹 보안부(110)에서 웹 공격 탐지 로그 데이터를 생성하는 것으로 설명하였으나 이에 한정되는 것은 아니며, 웹 보안부(110)에서 비정상적 웹 서비스 요청이 탐지된 경우 당 웹 서비스 요청에 대한 정보를 해킹 관정부(130)로 전달하면 해킹 관정부(130)가 데이터베이스 공격 탐지 로그 데이터와 비교하기 위한 정보만을 추출하여 웹 공격 탐지 로그 데이터를 생성할 수도 있다.
- <47> 다음으로 DB 보안부(120)는 WAS 서버(30)로부터 전송되는 데이터베이스 서비스 요청을 수신하여 정상적인지 또는 비정상적인지 여부를 판단하고, 비정상적인 데이터베이스 서비스 요청이 탐지된 경우 이에 대한 탐지 로그 데이터(이하, 'DB 공격 탐지 로그 데이터'라 함)를 생성한다.
- <48> 보다 자세하게는 DB 보안부(120)는 DB 공격 시그니처 DB(121), DB 서비스 프로파일 DB(123), DB 요청 검증 모듈(125) 및 DB 공격 탐지 로그 DB(127)를 포함할 수 있다.
- <49> DB 공격 시그니처 DB(121)는 이미 알려진 데이터베이스 공격의 시그니처(signature)를 저장한다.
- <50> DB 서비스 프로파일 DB(123)는 데이터베이스 접속이 허용되는 쿼리 패턴에 대한 정보가 저장될 수 있다.
- <51> DB 요청 검증 모듈(125)은 DB 공격 시그니처 DB(121)와 DB 서비스 프로파일 DB(123)를 이용하여 네가티브 및 포지티브 방식을 혼용하여 DB 서비스 요청에 대한 정상 또는 비정상 여부를 탐지할 수 있다. 실시예에 따라서는 DB 요청 검증 모듈(125)은 네가티브 방식 또는 포지티브 방식 중 어느 하나만으로 DB 서비스 요청이 정상적인지 또는 비정상적인지 탐지할 수 있다. DB 요청 검증 모듈(125)은 비정상적 DB 서비스 요청이 탐지된 경우 그에 대한 DB 공격 탐지 로그 데이터를 생성하여 DB 공격 탐지 로그 DB(127)에 저장한다.
- <52> 웹 공격 탐지 로그 데이터는 아래 표 2와 같이 시퀀스 번호, WAS 서버 IP 주소, DB 사용자 ID, DB 에러 코드, 쿼리 값들이 포함될 수 있다.

표 2

시퀀스 번호
WAS 서버 IP 주소
DB 사용자 ID
DB 에러 코드
WHERE/LIKE 쿼리값 1
WHERE/LIKE 쿼리값 2
...
WHERE/LIKE 쿼리값 n

- <53>
- <54> 여기서, 시퀀스 번호는 DB 공격 탐지 로그 데이터에 붙는 일련 번호이다. WAS 서버 IP 주소는 DB 서비스 요청이 전달된 WAS 서버(30)의 IP 주소이다. DB 사용자 ID는 DB 서비스 요청을 전달한 사용자 계정으로서, 여기서는 DB 서버(40) 접속을 위해 WAS 서버(30)에 할당해놓은 ID가 될 수 있다.
- <55> DB 에러 코드는 DB 서버(40)에서 에러 발생 시 반환하는 코드 값이다. 예컨대, DB 서버에 에러가 발생하면 ODBC Driver(0x80040e14) 코드가 출력될 수 있다(MS SQL 에러 코드 예임). Oracle 에러 코드 예로는 ORA-00911(Invalid character), ORA-00933(SQL command not properly ended) 등이 있다.
- <56> WHERE/LIKE 쿼리 값은 DB 서비스 요청 질의문에 포함되어 있는 쿼리 값으로 쿼리문은 WHERE/LIKE 절 구문 뒷단의 문자열(쿼리값)이 추출되어 DB 공격 탐지 로그 데이터에 포함될 수 있다.
- <57> 다음과 같은 비정상적인 데이터베이스 서비스 요청이 탐지된 경우 각 쿼리문의 WHERE/LIKE 절 구문 뒤에 있는 문자열 중 볼드체로 표시되어 있는 쿼리 값이 추출되어 웹 공격 탐지 로그 데이터에 포함될 수 있다.
- <58> 1) Select count(\*) from tab\_bbs where userid='admin' and passwd='test'
- <59> 2) Select count(\*) from tab\_bbs where userid='or'1'='1 and passwd=''
- <60> 3) SELECT \* FROM cafe\_t WHERE state<>'F' AND cname LIKE '%%'
- <61> 4) Select idx, title, contents,writer, daytime from tab\_bbs where title like = '검색%' and writer = ''order by idx DESC
- <62> 5) Select \* from tab\_bbs where idx='581' union select 1, tname,'3',444,'444' fromsys.tab where tname not in ('AOTMSRNES', 'AOTORGTBL', 'A4TCPADLG', 'BANK\_THEME\_DATA')-- order by idx DESC
- <63> 한편 본 실시예에서는 DB 보안부(120)에서 DB 공격 탐지 로그 데이터를 생성하는 것으로 설명하였으나 이에 한정되는 것은 아니며, DB 보안부(120)에서 비정상적 DB 서비스 요청이 탐지된 경우 해당 DB 서비스 요청에 대한 정보를 해킹 관정부(130)로 전달하면 해킹 관정부(130)가 추후 웹 공격 탐지 로그 데이터와 비교하기 위한 정보만을 추출하여 DB 공격 탐지 로그 데이터를 생성할 수도 있다.
- <64> 다음으로 해킹 관정부(130)는 웹 공격 탐지 로그 데이터와 DB 공격 탐지 로그 데이터를 비교하여 연관성을 분석하고, 양 로그 데이터가 연관성이 있는 경우 명백한 해킹 시도로 판정한다. 양 로그 데이터의 연관성 판단은 문자열 식별(Diff)을 통해 이루어질 수 있다. 보다 자세하게는 해킹 관정부(130)는 양 로그 데이터에 포함되어 있는 입력 파라미터 값과 쿼리 값을 비교하여 동일한 경우 양 로그 데이터가 연관성이 있는 것으로 판단하고 DB 서버(40)에 대한 해킹 시도로 판정할 수 있다.
- <65> 다만 오탐(False Positive)을 보다 최소화하기 위해서 해킹 관정부(130)는 입력 파라미터 값과 쿼리 값이 동일할 뿐만 아니라 서버 응답 코드와 DB 에러 코드에 연관성이 있는 경우에 최종적으로 양 로그 데이터가 동일한 것으로 판정하도록 구현될 수도 있다. 여기서 서버 응답 코드와 DB 에러 코드의 연관성 판단은 다음과 같이 이루어질 수 있다. 양 코드 값이 동일한 경우 또는 서버 응답 코드가 '500'인 경우 해킹 관정부(130)는 서버 응답 코드와 DB 에러 코드가 연관성이 있는 것으로 판단할 수 있다.

- <66> 한편 해킹 판정부(130)는 양 로그 데이터의 연관성 분석을 통해 사용자 단말기(10)로부터 전송된 웹 서비스 요청이 DB 서버(40)에 대한 해킹 시도를 목적으로 한 것이 확인되면 웹 공격 탐지 로그 데이터에서 해당 웹 서비스 요청을 전송한 사용자 단말기(10)의 IP 주소를 확인하고 웹 보안부(110)에 해당 사용자 단말기(10)와의 접속을 차단하도록 지시할 수 있다.
- <67> 다만 오탐(False Positive)을 보다 최소화하기 위해서 해킹 판정부(130)는 해킹 시도로 판정된 회수가 미리 정해진 기준 이상인 경우, 예컨대 연관성 있는 것으로 판정된 웹 공격 탐지 로그 데이터와 DB 공격 탐지 로그 데이터가 해당 사용자 IP에 대해서 소정 개수 이상 찾아진 경우에만 해당 IP로 접속한 사용자 단말기(10)를 차단시키도록 구현할 수도 있다.
- <68> 그러면 도 3을 참고하여 본 발명의 일 실시예에 따른 보안 시스템의 동작을 상세하게 설명한다.
- <69> 도 3은 본 발명의 일 실시예에 따른 보안 시스템의 동작을 설명하기 위해 제공되는 흐름도이다.
- <70> 도 1 내지 도 3을 참고하면, 먼저 사용자 단말기(10)에서 웹 서버(20)로 전송되는 웹 서비스 요청은 웹 보안부(110)에 수신된다(S310).
- <71> 웹 보안부(110)는 사용자 단말기(10)로부터 웹 서버(20)로 전송되는 웹 서비스 요청을 감시하여 비정상적 웹 서비스 요청을 탐지한다(S320). 웹 보안부(110)는 비정상적 웹 서비스 요청이 탐지된 경우 웹 공격 탐지 로그 데이터를 생성한다(S330). 실시예에 따라서는 웹 보안부(110)는 비정상적인 것으로 탐지된 웹 서비스 요청에 대한 정보를 가공없이 로그 파일로 저장하고, 해킹 판정부(130)가 로그 파일에서 추후 데이터베이스 공격 탐지 로그 데이터와 연관성을 비교하기 위해 필요한 정보만을 추출하여 웹 공격 탐지 로그 데이터를 생성할 수도 있다.
- <72> 한편 WAS 서버(30)는 사용자 단말기(10)로부터 웹 서버(20)로 전송된 웹 서비스 요청에 포함되어 있는 입력 파라미터 값을 미리 준비된 질의문과 조합하여 완성된 SQL 질의문을 생성하여 DB 서버(40)로 전송한다.
- <73> DB 서버(40)로 전송되는 DB 서비스 요청은 DB 보안부(120)에 수신된다(S340).
- <74> DB 보안부(120)는 DB 서버(40)로 전달되는 DB 서비스 요청을 감시하여 비정상적 DB 서비스 요청을 탐지한다(S350). DB 보안부(120)는 비정상적 DB 서비스 요청이 탐지된 경우 DB 공격 탐지 로그 데이터를 생성한다(S360). 실시예에 따라서는 DB 보안부(120)는 비정상적인 것으로 탐지된 DB 서비스 요청에 대한 정보를 가공없이 로그 파일로 저장하고, 해킹 판정부(130)가 로그 파일에서 추후 웹 공격 탐지 로그 데이터와 연관성을 비교하기 위해 필요한 정보만을 추출하여 DB 공격 탐지 로그 데이터를 생성할 수도 있다.
- <75> 해킹 판정부(130)는 웹 공격 탐지 로그 데이터와 DB 공격 탐지 로그 데이터를 비교하여 연관성이 있는 지 판단한다(S370). 보다 자세하게는 양 로그 데이터의 입력 파라미터 값과 쿼리 값이 동일하면 양 로그 데이터가 연관성이 있는 것으로 판단할 수 있다. 보다 엄격하게 연관성을 판단하기 위해서는 앞에서 살펴본 입력 파라미터 값과 쿼리 값이 동일할 뿐만 아니라 양 로그 데이터에 포함되어 있는 서버 응답 코드와 DB 에러 코드에도 연관성이 있는 경우에 양 로그 데이터가 연관성이 있는 것으로 최종 판단하도록 구현할 수도 있다.
- <76> 비교 결과 양 로그 데이터에 연관성이 없는 경우(S370-N), 해킹 판정부(130)는 비정상적 웹 서비스 요청 또는 DB 서비스 요청이 탐지된 것을 관리자에게 단순 보고하고(S380), 별도의 조치를 취하지 않을 수 있다.
- <77> 한편 비교 결과 양 로그 데이터에 연관성이 있는 경우(S370-Y), 해킹 판정부(130)는 SQL 삽입 공격과 같은 데이터베이스에 대한 명백한 해킹 시도로 판정하고 해당 공격을 시도한 사용자 단말기(10)의 IP 주소를 파악하여 차단한다(S390). 다만 오탐의 가능성을 보다 최소화하기 위해서 연관성이 있는 해킹 시도로 판정된 회수가 미리 정해진 기준 이상인 경우, 즉 연관성 있는 로그 데이터가 해당 IP에 대해서 소정 회수 이상 검출된 경우에만 해당 IP 주소로 접속한 사용자 단말기(10)를 차단하도록 구현할 수도 있다.
- <78> 본 발명의 실시예는 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터로 읽을 수 있는 매체를 포함한다. 이 매체는 지금까지 설명한 통합 보안 방법을 실행시키기 위한 프로그램을 기록한다. 이 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 이러한 매체의 예에는 하드디스크, 플로피디스크 및 자기 테이프와 같은 자기 매체, CD 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 자기-광 매체, 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 구성된 하드웨어 장치 등이 있다. 또는 이러한 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에

의해서 실행될 수 있는 고급 언어 코드를 포함한다.

<79> 이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

**도면의 간단한 설명**

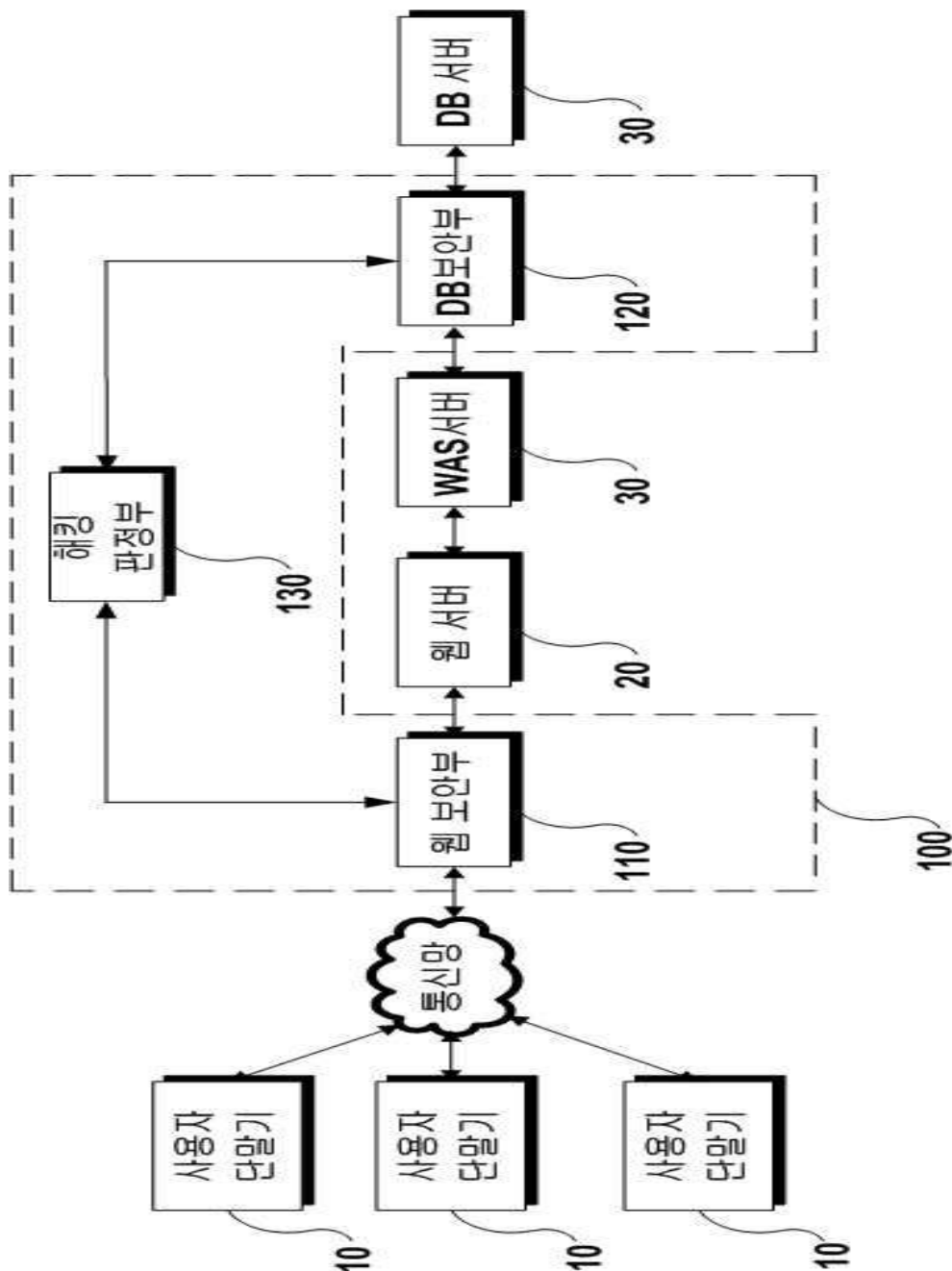
<80> 도 1은 본 발명의 일 실시예에 따른 보안 시스템을 설명하기 위해 제공되는 도면이다.

<81> 도 2는 도 1의 보안 시스템을 보다 자세히 나타낸 블록도이다.

<82> 도 3은 본 발명의 일 실시예에 따른 보안 시스템의 동작을 설명하기 위해 제공되는 흐름도이다.

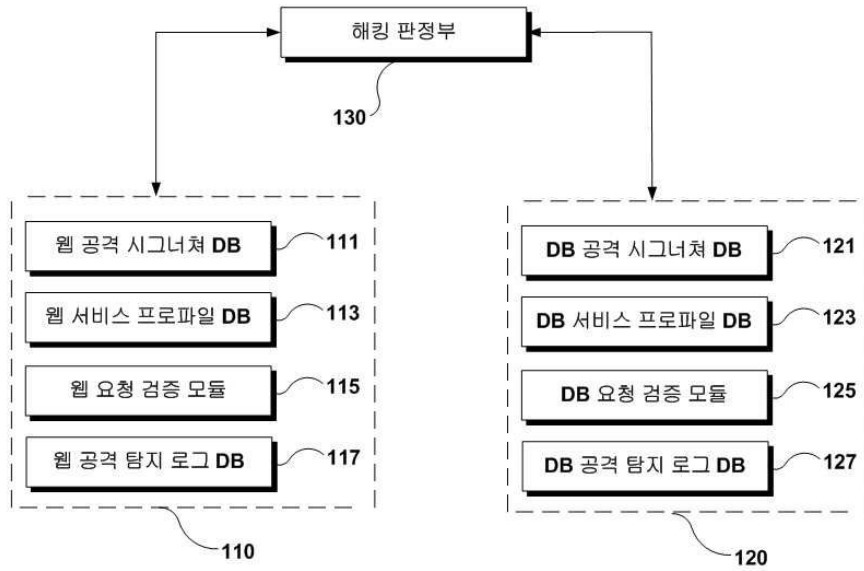
**도면**

**도면1**



도면2

100



도면3

