관인생략

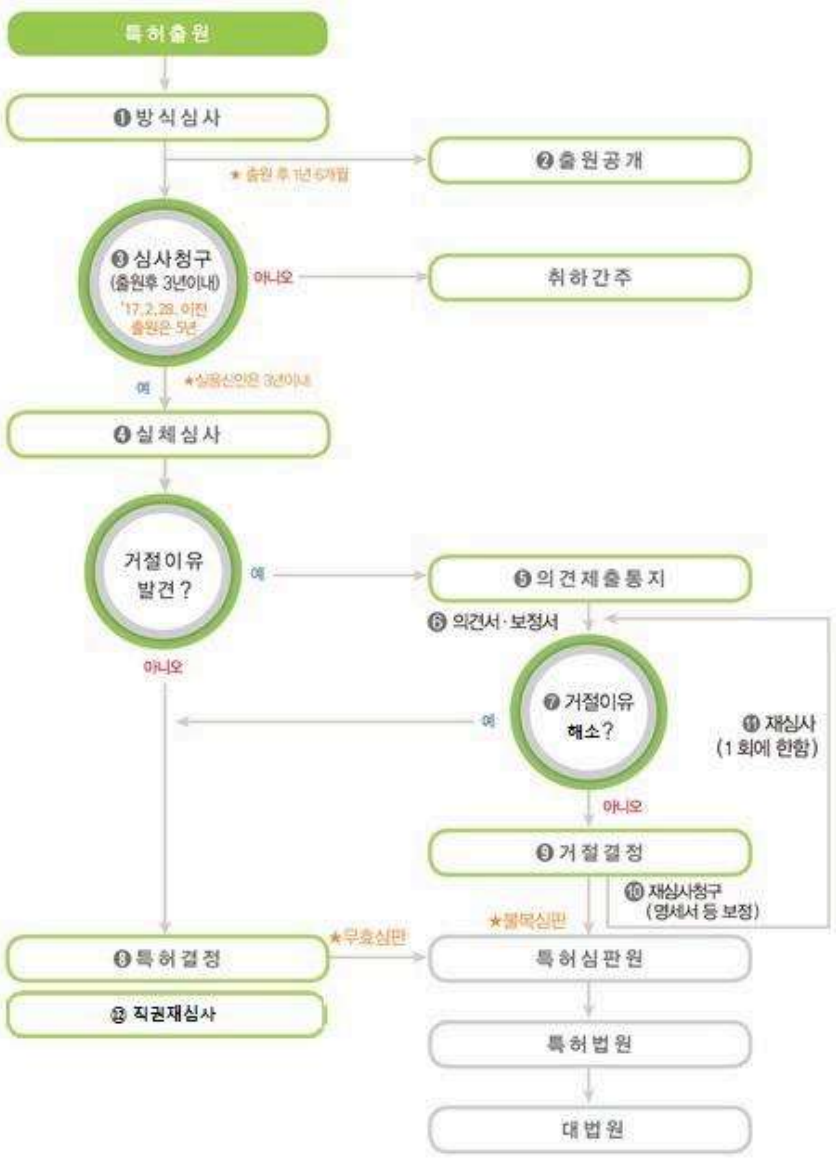
출원번호통지서

출원일자	2025.07.28
특기사항	심사청구(무) 공개신청(무) 참조번호(P2504049)
출원번호	10-2025-0102398 (접수번호 1-1-2025-0855768-11) (DAS접근코드5E07)
출원인 명칭	삼성전자주식회사(1-1998-104271-3) 외 1명
대리인 성명	권혁록(9-1998-000115-1)
발명자 성명	김재곤 남석현 류승호 홍원기 김태우
발명의 명칭	로그 데이터를 분석하여 네트워크 엔티티의 상태를 탐지하는 방법 및 장치

특 허 청 장

<< 안내 >>

1. 귀하의 출원은 위와 같이 정상적으로 접수되었으며, 이후의 심사 진행상황은 출원번호를 이용하여 특허로 홈페이지(www.patent.go.kr)에서 확인하실 수 있습니다.
2. 출원에 따른 수수료는 접수일로부터 다음날까지 동봉된 납입영수증에 성명, 납부자번호 등을 기재하여 가까운 은행 또는 우체국에 납부하여야 합니다.
※ 납부자번호 : 0131(기관코드) + 접수번호
3. 귀하의 주소, 연락처 등의 변경사항이 있을 경우, 즉시 [특허고객번호 정보변경(경정), 정정신고서]를 제출하여야 출원 이후의 각종 통지서를 정상적으로 받을 수 있습니다.
4. 기타 심사 절차(제도)에 관한 사항은 특허청 홈페이지를 참고하시거나 특허고객상담센터(☎ 1544-8080)에 문의하여 주시기 바랍니다.
※ 심사제도 안내 : https://www.kipo.go.kr-지식재산제도


특허출원
❶방식심사
★출원후 1년 6개월
❷출원공개
❸심사청구
(출원후 3년이내)
'17.2.28. 이전
출원은 5년
아니오
취하간주
예
★실용신안은 3년이내
❹실체심사
거절이유
발견?
예
❺의견제출통지
❻의견서·보정서
아니오
❼거절이유
해소?
예
⓫재심사
(1회에 한함)
아니오
❾거절결정
❿재심사청구
(명세서 등 보정)
★불복심판
★무효심판
❽특허결정
특허심판원
⓬직권재심사
특허법원
대법원

【서지사항】

【서류명】 특허출원서

【참조번호】 P2504049

【출원구분】 특허출원

【출원인】

【명칭】 삼성전자 주식회사

【특허고객번호】 1-1998-104271-3

【출원인】

【명칭】 포항공과대학교 산학협력단

【특허고객번호】 2-2004-043336-1

【대리인】

【성명】 권혁록

【대리인번호】 9-1998-000115-1

【포괄위임등록번호】 2002-060519-2

【포괄위임등록번호】 2006-056564-1

【대리인】

【성명】 이정순

【대리인번호】 9-1998-000404-2

【포괄위임등록번호】 2005-005297-6

【포괄위임등록번호】 2006-056565-9

【발명의 국문명칭】 로그 데이터를 분석하여 네트워크 엔티티의 상태를 탐지하는 방법 및 장치

【발명의 영문명칭】 METHOD AND APPARATUS TO DETECT STATUS OF NETWORK ENTITY BY ANALYZING LOG DATA

【발명자】

【성명】 김재곤

【성명의 영문표기】 KIM, Jaegon

【국적】 KR

【주민등록번호】 000000-0XXXXXX

【우편번호】 16677

【주소】 경기도 수원시 영통구 삼성로 129(매탄동)

【거주국】 KR

【발명자】

【성명】 남석현

【성명의 영문표기】 NAM, Sukhyun

【국적】 KR

【주민등록번호】 000000-0XXXXXX

【우편번호】 37673

【주소】 경상북도 포항시 남구 청암로 77(지곡동)

【거주국】 KR

【발명자】

【성명】 류승호

【성명의 영문표기】 RYU, Seungho

【국적】 KR

【주민등록번호】 000000-0XXXXXX

【우편번호】 16677

【주소】 경기도 수원시 영통구 삼성로 129(매탄동)

【거주국】 KR

【발명자】

【성명】 홍원기

【성명의 영문표기】 HONG, Wonki

【국적】 CA

【주소】 경상북도 포항시 남구 청암로 77(지곡동)

【주소의 영문표기】 77, Cheongam-ro, Nam-gu, Pohang-si, Gyeongsangbuk-do, Republic of Korea

【거주국】 KR

【발명자】

【성명】 김태우

【성명의 영문표기】 KIM, Taewoo

【국적】 US

【주소】 경기도 수원시 영통구 삼성로 129(매탄동)

【주소의 영문표기】 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, Republic of Korea

【거주국】 KR

【출원언어】 국어

【우선권 주장】

【출원국명】 KR

【출원번호】 10-2025-0073887

【출원일자】 2025.06.05

【증명서류】 미첨부

【취지】 위와 같이 특허청장에게 제출합니다.

대리인 권혁록 (서명 또는 인)

대리인 이정순 (서명 또는 인)

【수수료】

【출원료】	0	면	46,000 원
【가산출원료】	65	면	0 원
【우선권주장료】	1	건	18,000 원
【심사청구료】	0	항	0 원
【합계】	64,000원		

【발명의 설명】

【발명의 명칭】

로그 데이터를 분석하여 네트워크 엔티티의 상태를 탐지하는 방법 및 장치 {METHOD AND APPARATUS TO DETECT STATUS OF NETWORK ENTITY BY ANALYZING LOG DATA}

【기술분야】

【0001】 본 개시는 네트워크 엔티티의 상태를 탐지하는 방법과 장치에 관한 것이다. 구체적으로, 본 개시는 로그 데이터를 분석하여 네트워크 엔티티의 상태를 탐지하는 방법과 장치에 관한 것이다.

【발명의 배경이 되는 기술】

【0002】 네트워크 시스템의 규모가 커지고 구성이 복잡해짐에 따라, 패킷 손실, 지연 증가 등 다양한 형태의 네트워크 관리 문제가 증가하고 있다. 따라서, 네트워크 장비에 심각한 장애가 발생하기 전에 네트워크 장비의 이상 동작을 조기에 탐지할 필요가 있다. 또한, 네트워크 장비의 장애가 발생한 경우, 그 원인을 신속하게 파악하는 것도 중요하다.

【0003】 네트워크 장비의 동작 상태는 해당 장비가 기록하는 로그 데이터를 통하여 확인할 수 있다. 그러나, 로그 데이터는 비정형화된 텍스트 형태로 단순 이벤트만을 기록하고 있어, 자동화된 분석이 어렵다.

【0004】일반적인 자연어 처리에서는, 임베딩(embedding) 기법을 활용하여 문장의 의미를 벡터로 변환하고, 문맥 정보를 기반으로 이상 여부를 분석한다. 하지만, 로그 데이터는 이러한 문맥 구조가 부족한 단순 기록이므로, 임베딩 기법은 로그 분석에 적합하지 않다. 따라서, 로그 데이터를 적절히 분석하기 위한 방법이 필요하다.

【0005】상술한 정보는 본 개시에 대한 이해를 돕기 위한 목적으로 하는 배경 기술(related art)로 제공될 수 있다. 상술한 내용 중 어느 것도 본 개시와 관련된 종래 기술(prior art)로서 적용될 수 있는지에 대하여 어떠한 주장이나 결정이 제기되지 않는다.

【발명의 내용】

【과제의 해결 수단】

【0006】본 개시의 일 실시예에 따른 전자 장치에 의해 수행되는 방법은, 네트워크 엔티티로부터 로그 데이터를 획득하는 단계; 상기 획득한 로그 데이터로부터 로그 패턴과 이벤트 번호를 식별하는 단계; 상기 로그 패턴의 발생 빈도에 기초하여, 상기 로그 패턴에 대해서 정상 상태에서의 상기 로그 패턴의 희귀도를 획득하는 단계; 상기 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 상기 이벤트 번호에 대응하는 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득하는 단계; 및 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여, 상기 네트

워크 엔티티의 비정상 상태를 탐지하는 단계를 포함할 수 있다.

【0007】본 개시의 일 실시예에 따른 전자 장치는, 적어도 하나의 트랜시버(transceiver); 상기 적어도 하나의 트랜시버에 통신적으로(communicatively) 결합된(coupled to) 적어도 하나의 프로세서; 및 상기 적어도 하나의 프로세서에 통신적으로 결합되어 명령어들(instructions)을 저장하는 적어도 하나의 메모리를 포함하고, 상기 명령어들은 상기 적어도 하나의 프로세서에 의해서 개별적으로(individually) 또는 임의의 조합(any combination)으로 실행되어, 상기 전자 장치가 네트워크 엔티티로부터 로그 데이터를 획득하고, 상기 획득한 로그 데이터로부터 로그 패턴과 이벤트 번호를 식별하고, 상기 로그 패턴의 발생 빈도에 기초하여, 상기 로그 패턴에 대해서 정상 상태에서의 상기 로그 패턴의 희귀도를 획득하고, 상기 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 상기 이벤트 번호에 대응하는 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득하고, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여, 상기 네트워크 엔티티의 비정상 상태를 탐지하도록 할 수 있다.

【발명의 효과】

【0008】일 실시예에 따른 전자 장치 및 이의 동작 방법은, 네트워크 엔티티에서 발생하는 로그 데이터에 기반하여 실시간으로 네트워크 엔티티의 상태를 파악할 수 있다. 이와 더불어, 전자 장치는 정상 상태에서의 로그 데이터를 기반으로 획득한 로그 데이터의 희귀도를 고려함으로써, 더욱 효과적으로 네트워크 엔티티의

비정상 상태를 탐지할 수 있다.

【0009】 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

【도면의 간단한 설명】

【0010】 도 1은, 다양한 실시예들에 따른, 네트워크 환경(100) 내의 전자 장치(101)의 블록도이다.

도 2는, 일 실시예에 따른 전자 장치가 동작하는 시스템을 설명하기 위한 도면이다.

도 3은, 일 실시예에 따른 전자 장치가 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

도 4는, 일 실시예에 따른 전자 장치가 획득한 로그 데이터로부터 로그 패턴 및 이벤트 번호를 식별하는 흐름도를 도시한다.

도 5는, 일 실시예에 따른 전자 장치가 이벤트가 정상 상태에서 발생할 확률을 획득하는 흐름도를 도시한다.

도 6은, 일 실시예에 따른 전자 장치가 비정상 점수를 계산하여 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

도 7은, 일 실시예에 따른 전자 장치가 반복 횟수를 기반으로 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

도 8은, 일 실시예에 따른 전자 장치가 시간을 기반으로 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

도 9는, 일 실시예에 따른 전자 장치의 구성을 도시한다.

도 10은, 일 실시예에 따른 네트워크 엔티티의 구성을 도시한다.

【발명을 실시하기 위한 구체적인 내용】

【0011】 아래에서는 첨부한 도면을 참조하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 개시의 실시예를 상세히 설명한다. 그러나 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 개시를 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

【0012】 본 개시에서 사용되는 용어는, 본 개시에서 언급되는 기능을 고려하여 현재 사용되는 일반적인 용어로 기재되었으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 다양한 다른 용어를 의미할 수 있다. 따라서 본 개시에서 사용되는 용어는 용어의 명칭만으로 해석되어서는 안되며, 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 해석되어야 한다.

【0013】 또한, 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 구성 요소들은 이 용어들에 의해 한정되어서는 안 된다. 이 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로 사용된다.

【0014】명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

【0015】본 개시에서 다양한 곳에 등장하는 "일 실시예에서" 등의 어구는 반드시 모두 동일한 실시예를 가리키는 것은 아니다.

【0016】본 개시의 일 실시예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들의 일부 또는 전부는, 특정 기능들을 실행하는 다양한 개수의 하드웨어 및/또는 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 본 개시의 기능 블록들은 하나 이상의 마이크로프로세서들에 의해 구현되거나, 소정의 기능을 위한 회로 구성들에 의해 구현될 수 있다. 또한, 예를 들어, 본 개시의 기능 블록들은 다양한 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능 블록들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 개시는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. "매커니즘", "요소", "수단" 및 "구성"등과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다.

【0017】또한, 도면에 도시된 구성 요소들 간의 연결 선 또는 연결 부재들은 기능적인 연결 및/또는 물리적 또는 회로적 연결들을 예시적으로 나타낸 것일 뿐이

다. 실제 장치에서는 대체 가능하거나 추가된 다양한 기능적인 연결, 물리적인 연결, 또는 회로 연결들에 의해 구성 요소들 간의 연결이 나타내어질 수 있다.

도 1은, 다양한 실시예들에 따른, 네트워크 환경(100) 내의 전자 장치(101)의 블록도이다.

【0018】도 1을 참조하면, 네트워크 환경(100)에서 전자 장치(101)는 제 1 네트워크(198)(예: 근거리 무선 통신 네트워크)를 통하여 전자 장치(102)와 통신하거나, 또는 제 2 네트워크(199)(예: 원거리 무선 통신 네트워크)를 통하여 전자 장치(104) 또는 서버(108) 중 적어도 하나와 통신할 수 있다. 일실시예에 따르면, 전자 장치(101)는 서버(108)를 통하여 전자 장치(104)와 통신할 수 있다. 일실시예에 따르면, 전자 장치(101)는 프로세서(120), 메모리(130), 입력 모듈(150), 음향 출력 모듈(155), 디스플레이 모듈(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 연결 단자(178), 햅틱 모듈(179), 카메라 모듈(180), 전력 관리 모듈(188), 배터리(189), 통신 모듈(190), 가입자 식별 모듈(196), 또는 안테나 모듈(197)을 포함할 수 있다. 어떤 실시예에서는, 전자 장치(101)에는, 이 구성요소들 중 적어도 하나(예: 연결 단자(178))가 생략되거나, 하나 이상의 다른 구성요소가 추가될 수 있다. 어떤 실시예에서는, 이 구성요소들 중 일부들(예: 센서 모듈(176), 카메라 모듈(180), 또는 안테나 모듈(197))은 하나의 구성요소(예: 디스플레이 모듈(160))로 통합될 수 있다.

【0019】프로세서(120)는, 예를 들면, 소프트웨어(예: 프로그램(140))를 실행하여 프로세서(120)에 연결된 전자 장치(101)의 적어도 하나의 다른

구성요소(예: 하드웨어 또는 소프트웨어 구성요소)를 제어할 수 있고, 다양한 데이터 처리 또는 연산을 수행할 수 있다. 일실시예에 따르면, 데이터 처리 또는 연산의 적어도 일부로서, 프로세서(120)는 다른 구성요소(예: 센서 모듈(176) 또는 통신 모듈(190))로부터 수신된 명령 또는 데이터를 휘발성 메모리(132)에 저장하고, 휘발성 메모리(132)에 저장된 명령 또는 데이터를 처리하고, 결과 데이터를 비휘발성 메모리(134)에 저장할 수 있다. 일실시예에 따르면, 프로세서(120)는 메인 프로세서(121)(예: 중앙 처리 장치 또는 어플리케이션 프로세서) 또는 이와는 독립적으로 또는 함께 운영 가능한 보조 프로세서(123)(예: 그래픽 처리 장치, 신경망 처리 장치(NPU: neural processing unit), 이미지 시그널 프로세서, 센서 허브 프로세서, 또는 커뮤니케이션 프로세서)를 포함할 수 있다. 예를 들어, 전자 장치(101)가 메인 프로세서(121) 및 보조 프로세서(123)를 포함하는 경우, 보조 프로세서(123)는 메인 프로세서(121)보다 저전력을 사용하거나, 지정된 기능에 특화되도록 설정될 수 있다. 보조 프로세서(123)는 메인 프로세서(121)와 별개로, 또는 그 일부로서 구현될 수 있다.

【0020】 보조 프로세서(123)는, 예를 들면, 메인 프로세서(121)가 인액티브(예: 슬립) 상태에 있는 동안 메인 프로세서(121)를 대신하여, 또는 메인 프로세서(121)가 액티브(예: 어플리케이션 실행) 상태에 있는 동안 메인 프로세서(121)와 함께, 전자 장치(101)의 구성요소들 중 적어도 하나의 구성요소(예: 디스플레이 모듈(160), 센서 모듈(176), 또는 통신 모듈(190))와 관련된 기능 또는 상태들의 적어도 일부를 제어할 수 있다. 일실시예에 따르면, 보조 프로세서(123)(예: 이미지

시그널 프로세서 또는 커뮤니케이션 프로세서)는 기능적으로 관련 있는 다른 구성 요소(예: 카메라 모듈(180) 또는 통신 모듈(190))의 일부로서 구현될 수 있다. 일 실시예에 따르면, 보조 프로세서(123)(예: 신경망 처리 장치)는 인공지능 모델의 처리에 특화된 하드웨어 구조를 포함할 수 있다. 인공지능 모델은 기계 학습을 통해 생성될 수 있다. 이러한 학습은, 예를 들어, 인공지능 모델이 수행되는 전자 장치(101) 자체에서 수행될 수 있고, 별도의 서버(예: 서버(108))를 통해 수행될 수도 있다. 학습 알고리즘은, 예를 들어, 지도형 학습(supervised learning), 비지도형 학습(unsupervised learning), 준지도형 학습(semi-supervised learning) 또는 강화 학습(reinforcement learning)을 포함할 수 있으나, 전술한 예에 한정되지 않는다. 인공지능 모델은, 복수의 인공 신경망 레이어들을 포함할 수 있다. 인공 신경망은 심층 신경망(DNN: deep neural network), CNN(convolutional neural network), RNN(recurrent neural network), RBM(restricted boltzmann machine), DBN(deep belief network), BRDNN(bidirectional recurrent deep neural network), 심층 Q-네트워크(deep Q-networks) 또는 상기 중 둘 이상의 조합 중 하나일 수 있으나, 전술한 예에 한정되지 않는다. 인공지능 모델은 하드웨어 구조 이외에, 추가적으로 또는 대체적으로, 소프트웨어 구조를 포함할 수 있다.

【0021】 메모리(130)는, 전자 장치(101)의 적어도 하나의 구성요소(예: 프로세서(120) 또는 센서 모듈(176))에 의해 사용되는 다양한 데이터를 저장할 수 있다. 데이터는, 예를 들어, 소프트웨어(예: 프로그램(140)) 및, 이와 관련된 명령에 대한 입력 데이터 또는 출력 데이터를 포함할 수 있다. 메모리(130)는, 휘발성

메모리(132) 또는 비휘발성 메모리(134)를 포함할 수 있다.

【0022】 프로그램(140)은 메모리(130)에 소프트웨어로서 저장될 수 있으며, 예를 들면, 운영 체제(142), 미들 웨어(144) 또는 어플리케이션(146)을 포함할 수 있다.

【0023】 입력 모듈(150)은, 전자 장치(101)의 구성요소(예: 프로세서(120))에 사용될 명령 또는 데이터를 전자 장치(101)의 외부(예: 사용자)로부터 수신할 수 있다. 입력 모듈(150)은, 예를 들면, 마이크, 마우스, 키보드, 키(예: 버튼), 또는 디지털 펜(예: 스타일러스 펜)을 포함할 수 있다.

【0024】 음향 출력 모듈(155)은 음향 신호를 전자 장치(101)의 외부로 출력할 수 있다. 음향 출력 모듈(155)은, 예를 들면, 스피커 또는 리시버를 포함할 수 있다. 스피커는 멀티미디어 재생 또는 녹음 재생과 같이 일반적인 용도로 사용될 수 있다. 리시버는 착신 전화를 수신하기 위해 사용될 수 있다. 일실시예에 따르면, 리시버는 스피커와 별개로, 또는 그 일부로서 구현될 수 있다.

【0025】 디스플레이 모듈(160)은 전자 장치(101)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 디스플레이 모듈(160)은, 예를 들면, 디스플레이, 홀로그램 장치, 또는 프로젝터 및 해당 장치를 제어하기 위한 제어 회로를 포함할 수 있다. 일실시예에 따르면, 디스플레이 모듈(160)은 터치를 감지하도록 설정된 터치 센서, 또는 상기 터치에 의해 발생되는 힘의 세기를 측정하도록 설정된 압력 센서를 포함할 수 있다.

【0026】오디오 모듈(170)은 소리를 전기 신호로 변환시키거나, 반대로 전기 신호를 소리로 변환시킬 수 있다. 일실시예에 따르면, 오디오 모듈(170)은, 입력 모듈(150)을 통해 소리를 획득하거나, 음향 출력 모듈(155), 또는 전자 장치(101)와 직접 또는 무선으로 연결된 외부 전자 장치(예: 전자 장치(102))(예: 스피커 또는 헤드폰)를 통해 소리를 출력할 수 있다.

【0027】센서 모듈(176)은 전자 장치(101)의 작동 상태(예: 전력 또는 온도), 또는 외부의 환경 상태(예: 사용자 상태)를 감지하고, 감지된 상태에 대응하는 전기 신호 또는 데이터 값을 생성할 수 있다. 일실시예에 따르면, 센서 모듈(176)은, 예를 들면, 제스처 센서, 자이로 센서, 기압 센서, 마그네틱 센서, 가속도 센서, 그립 센서, 근접 센서, 컬러 센서, IR(infrared) 센서, 생체 센서, 온도 센서, 습도 센서, 또는 조도 센서를 포함할 수 있다.

【0028】인터페이스(177)는 전자 장치(101)가 외부 전자 장치(예: 전자 장치(102))와 직접 또는 무선으로 연결되기 위해 사용될 수 있는 하나 이상의 지정된 프로토콜들을 지원할 수 있다. 일실시예에 따르면, 인터페이스(177)는, 예를 들면, HDMI(high definition multimedia interface), USB(universal serial bus) 인터페이스, SD카드 인터페이스, 또는 오디오 인터페이스를 포함할 수 있다.

【0029】연결 단자(178)는, 그를 통해서 전자 장치(101)가 외부 전자 장치(예: 전자 장치(102))와 물리적으로 연결될 수 있는 커넥터를 포함할 수 있다. 일실시예에 따르면, 연결 단자(178)는, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.

【0030】 햅틱 모듈(179)은 전기적 신호를 사용자가 촉각 또는 운동 감각을 통해서 인지할 수 있는 기계적인 자극(예: 진동 또는 움직임) 또는 전기적인 자극으로 변환할 수 있다. 일실시예에 따르면, 햅틱 모듈(179)은, 예를 들면, 모터, 압전 소자, 또는 전기 자극 장치를 포함할 수 있다.

【0031】 카메라 모듈(180)은 정지 영상 및 동영상을 촬영할 수 있다. 일실시예에 따르면, 카메라 모듈(180)은 하나 이상의 렌즈들, 이미지 센서들, 이미지 시그널 프로세서들, 또는 플래시들을 포함할 수 있다.

【0032】 전력 관리 모듈(188)은 전자 장치(101)에 공급되는 전력을 관리할 수 있다. 일실시예에 따르면, 전력 관리 모듈(188)은, 예를 들면, PMIC(power management integrated circuit)의 적어도 일부로서 구현될 수 있다.

【0033】 배터리(189)는 전자 장치(101)의 적어도 하나의 구성요소에 전력을 공급할 수 있다. 일실시예에 따르면, 배터리(189)는, 예를 들면, 재충전 불가능한 1차 전지, 재충전 가능한 2차 전지 또는 연료 전지를 포함할 수 있다.

【0034】 통신 모듈(190)은 전자 장치(101)와 외부 전자 장치(예: 전자 장치(102), 전자 장치(104), 또는 서버(108)) 간의 직접(예: 유선) 통신 채널 또는 무선 통신 채널의 수립, 및 수립된 통신 채널을 통한 통신 수행을 지원할 수 있다. 통신 모듈(190)은 프로세서(120)(예: 어플리케이션 프로세서)와 독립적으로 운영되고, 직접(예: 유선) 통신 또는 무선 통신을 지원하는 하나 이상의 커뮤니케이션 프로세서를 포함할 수 있다. 일실시예에 따르면, 통신 모듈(190)은 무선 통신 모듈

(192)(예: 셀룰러 통신 모듈, 근거리 무선 통신 모듈, 또는 GNSS(global navigation satellite system) 통신 모듈) 또는 유선 통신 모듈(194)(예: LAN(local area network) 통신 모듈, 또는 전력선 통신 모듈)을 포함할 수 있다. 이들 통신 모듈 중 해당하는 통신 모듈은 제 1 네트워크(198)(예: 블루투스, WiFi(wireless fidelity) direct 또는 IrDA(infrared data association)와 같은 근거리 통신 네트워크) 또는 제 2 네트워크(199)(예: 레거시 셀룰러 네트워크, 5G 네트워크, 차세대 통신 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN)와 같은 원거리 통신 네트워크)를 통하여 외부의 전자 장치(104)와 통신할 수 있다. 이런 여러 종류의 통신 모듈들은 하나의 구성요소(예: 단일 칩)로 통합되거나, 또는 서로 별도의 복수의 구성요소들(예: 복수 칩들)로 구현될 수 있다. 무선 통신 모듈(192)은 가입자 식별 모듈(196)에 저장된 가입자 정보(예: 국제 모바일 가입자 식별자(IMSI))를 이용하여 제 1 네트워크(198) 또는 제 2 네트워크(199)와 같은 통신 네트워크 내에서 전자 장치(101)를 확인 또는 인증할 수 있다.

【0035】무선 통신 모듈(192)은 4G 네트워크 이후의 5G 네트워크 및 차세대 통신 기술, 예를 들어, NR 접속 기술(new radio access technology)을 지원할 수 있다. NR 접속 기술은 고용량 데이터의 고속 전송(eMBB(enhanced mobile broadband)), 단말 전력 최소화와 다수 단말의 접속(mMTC(massive machine type communications)), 또는 고신뢰도와 저지연(URLLC(ultra-reliable and low-latency communications))을 지원할 수 있다. 무선 통신 모듈(192)은, 예를 들어, 높은 데이터 전송률 달성을 위해, 고주파 대역(예: mmWave 대역)을 지원할 수 있다. 무선

통신 모듈(192)은 고주파 대역에서의 성능 확보를 위한 다양한 기술들, 예를 들어, 빔포밍(beamforming), 거대 배열 다중 입출력(massive MIMO(multiple-input and multiple-output)), 전차원 다중입출력(FD-MIMO: full dimensional MIMO), 어레이 안테나(array antenna), 아날로그 빔형성(analog beam-forming), 또는 대규모 안테나(large scale antenna)와 같은 기술들을 지원할 수 있다. 무선 통신 모듈(192)은 전자 장치(101), 외부 전자 장치(예: 전자 장치(104)) 또는 네트워크 시스템(예: 제 2 네트워크(199))에 규정되는 다양한 요구사항을 지원할 수 있다. 일실시예에 따르면, 무선 통신 모듈(192)은 eMBB 실현을 위한 Peak data rate(예: 20Gbps 이상), mMTC 실현을 위한 손실 Coverage(예: 164dB 이하), 또는 URLLC 실현을 위한 U-plane latency(예: 다운링크(DL) 및 업링크(UL) 각각 0.5ms 이하, 또는 라운드 트립 1ms 이하)를 지원할 수 있다.

【0036】안테나 모듈(197)은 신호 또는 전력을 외부(예: 외부의 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 일실시예에 따르면, 안테나 모듈(197)은 서브스트레이트(예: PCB) 위에 형성된 도전체 또는 도전성 패턴으로 이루어진 방사체를 포함하는 안테나를 포함할 수 있다. 일실시예에 따르면, 안테나 모듈(197)은 복수의 안테나들(예: 어레이 안테나)을 포함할 수 있다. 이런 경우, 제 1 네트워크(198) 또는 제 2 네트워크(199)와 같은 통신 네트워크에서 사용되는 통신 방식에 적합한 적어도 하나의 안테나가, 예를 들면, 통신 모듈(190)에 의하여 상기 복수의 안테나들로부터 선택될 수 있다. 신호 또는 전력은 상기 선택된 적어도 하나의 안테나를 통하여 통신 모듈(190)과 외부의 전자 장치 간에 송신되거나 수신될

수 있다. 어떤 실시예에 따르면, 방사체 이외에 다른 부품(예: RFIC(radio frequency integrated circuit))이 추가로 안테나 모듈(197)의 일부로 형성될 수 있다.

【0037】 다양한 실시예에 따르면, 안테나 모듈(197)은 mmWave 안테나 모듈을 형성할 수 있다. 일실시예에 따르면, mmWave 안테나 모듈은 인쇄 회로 기판, 상기 인쇄 회로 기판의 제 1 면(예: 아래 면)에 또는 그에 인접하여 배치되고 지정된 고주파 대역(예: mmWave 대역)을 지원할 수 있는 RFIC, 및 상기 인쇄 회로 기판의 제 2 면(예: 윗 면 또는 측 면)에 또는 그에 인접하여 배치되고 상기 지정된 고주파 대역의 신호를 송신 또는 수신할 수 있는 복수의 안테나들(예: 어레이 안테나)을 포함할 수 있다.

【0038】 상기 구성요소들 중 적어도 일부는 주변 기기들간 통신 방식(예: 버스, GPIO(general purpose input and output), SPI(serial peripheral interface), 또는 MIPI(mobile industry processor interface))을 통해 서로 연결되고 신호(예: 명령 또는 데이터)를 상호간에 교환할 수 있다.

【0039】 일실시예에 따르면, 명령 또는 데이터는 제 2 네트워크(199)에 연결된 서버(108)를 통해서 전자 장치(101)와 외부의 전자 장치(104)간에 송신 또는 수신될 수 있다. 외부의 전자 장치(102, 또는 104) 각각은 전자 장치(101)와 동일한 또는 다른 종류의 장치일 수 있다. 일실시예에 따르면, 전자 장치(101)에서 실행되는 동작들의 전부 또는 일부는 외부의 전자 장치들(102, 104, 또는 108) 중 하나 이상의 외부의 전자 장치들에서 실행될 수 있다. 예를 들면, 전자 장치(101)가

어떤 기능이나 서비스를 자동으로, 또는 사용자 또는 다른 장치로부터의 요청에 반응하여 수행해야 할 경우에, 전자 장치(101)는 기능 또는 서비스를 자체적으로 실행시키는 대신에 또는 추가적으로, 하나 이상의 외부의 전자 장치들에게 그 기능 또는 그 서비스의 적어도 일부를 수행하라고 요청할 수 있다. 상기 요청을 수신한 하나 이상의 외부의 전자 장치들은 요청된 기능 또는 서비스의 적어도 일부, 또는 상기 요청과 관련된 추가 기능 또는 서비스를 실행하고, 그 실행의 결과를 전자 장치(101)로 전달할 수 있다. 전자 장치(101)는 상기 결과를, 그대로 또는 추가적으로 처리하여, 상기 요청에 대한 응답의 적어도 일부로서 제공할 수 있다. 이를 위하여, 예를 들면, 클라우드 컴퓨팅, 분산 컴퓨팅, 모바일 에지 컴퓨팅(MEC: mobile edge computing), 또는 클라이언트-서버 컴퓨팅 기술이 이용될 수 있다. 전자 장치(101)는, 예를 들어, 분산 컴퓨팅 또는 모바일 에지 컴퓨팅을 이용하여 초저지연 서비스를 제공할 수 있다. 다른 실시예에 있어서, 외부의 전자 장치(104)는 IoT(internet of things) 기기를 포함할 수 있다. 서버(108)는 기계 학습 및/또는 신경망을 이용한 지능형 서버일 수 있다. 일실시예에 따르면, 외부의 전자 장치(104) 또는 서버(108)는 제 2 네트워크(199) 내에 포함될 수 있다. 전자 장치(101)는 5G 통신 기술 및 IoT 관련 기술을 기반으로 지능형 서비스(예: 스마트 홈, 스마트 시티, 스마트 카, 또는 헬스 케어)에 적용될 수 있다.

【0040】 도 2는, 일 실시예에 따른 전자 장치가 동작하는 시스템을 설명하기 위한 도면이다.

【0041】일 실시예에 따르면, 복수의 네트워크(210a, 210b, ..., 210n)는 센서나 IoT 기기가 연결된 수집용 네트워크 또는 데이터 처리 및 분석을 담당하는 서버가 위치한 내부 업무망일 수 있다. 다만, 이는 일 예에 불과하고, 복수의 네트워크(210a, 210b, ..., 210n)는 다양한 목적, 형태, 기능을 갖는 네트워크를 포함할 수 있다.

【0042】복수의 네트워크(210a, 210b, ..., 210n)는 네트워크 엔티티(220)와 연결되어 있을 수 있다. 이때, 복수의 네트워크(210a, 210b, ..., 210n)는 네트워크 엔티티(220)와 통신을 통해 데이터를 주고받을 수 있다. 예를 들어, 복수의 네트워크(210)는 네트워크 엔티티(220)와 제어 명령, 설정 변경 요청 또는 접속과 인증 절차를 위한 데이터를 송수신 할 수 있다.

【0043】일 실시예에 따르면, 네트워크 엔티티(220)는 복수의 네트워크(210a, 210b, ..., 210n) 및 전자 장치(230)와 연결되어 있을 수 있다. 네트워크 엔티티(220)는 적어도 하나의 네트워크 스위치, 라우터, 서버 또는 방화벽을 포함할 수 있다. 스위치 또는 라우터와 같은 전송 장비는 복수의 네트워크 간의 데이터 흐름을 중계하고 최적의 경로로 데이터 패킷을 전달할 수 있다. 서버는 복수의 네트워크로부터 수집한 정보를 저장하고 처리할 수 있다. 방화벽은 보안 기능을 수행하여 외부의 위협으로부터 복수의 네트워크를 보호할 수 있다. 네트워크 엔티티(220)는 복수의 네트워크(210)와 통신을 통해 제어 명령, 설정 변경 요청 또는 접속과 인증 절차를 위한 데이터를 송수신할 수 있다. 다만, 이에 한정되지 않고, 네트워크 엔티티(220)는 다양한 종류의 디바이스를 포함할 수 있다.

【0044】일 실시예에 따르면, 네트워크 엔티티(220)는 네트워크 엔티티에서 발생한 이벤트나 동작 이력을 로그 형태로 기록할 수 있다. 또한, 네트워크 엔티티(220)는 전자 장치(230)에게 로그 데이터를 전송할 수 있다.

【0045】일 실시예에 따르면, 전자 장치(230)는 네트워크 엔티티(220)와 연결되어 있을 수 있다. 예를 들어, 전자 장치(230)는 네트워크 엔티티(220)의 비정상 상태를 탐지하는 컨트롤러를 포함할 수 있다. 전자 장치(230)는 네트워크 엔티티(220)로부터 로그 데이터를 수신할 수 있다. 또한, 전자 장치(230)는 수신한 로그 데이터를 분석하여 네트워크 엔티티(220)의 상태를 탐지할 수 있다. 다만, 이에 한정되지 않고, 전자 장치(230)는 다양한 종류의 디바이스를 포함할 수 있다.

【0046】도 3은, 일 실시예에 따른 전자 장치가 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

【0047】일 실시예에 따르면, 동작 310에서, 전자 장치는 네트워크 엔티티로부터 로그 데이터를 획득할 수 있다. 네트워크 엔티티는 네트워크 엔티티에서 발생한 이벤트나 동작 이력을 로그 형태로 기록할 수 있다. 이 경우에, 네트워크 엔티티는 적어도 하나의 네트워크 스위치, 서버, 라우터 또는 방화벽을 포함할 수 있다.

【0048】일 실시예에 따르면, 전자 장치는 네트워크 엔티티가 기록한 로그 데이터를 획득하기 위해 다양한 방법을 사용할 수 있다. 예를 들어, 전자 장치는 Syslog 프로토콜을 이용하여 네트워크 엔티티로부터 로그 데이터를 수신할 수

있다. Syslog 프로토콜은 표준화된 로그 전송 방식으로, 네트워크 엔티티에서 이벤트가 발생했을 때 실시간으로 네트워크 엔티티가 로그 메시지를 전자 장치에게 전송하면, 전자 장치는 로그 메시지를 수신하여 저장하고 분석할 수 있다. 예를 들어, 네트워크 스위치에서 포트의 연결이 끊어졌을 경우 해당 이벤트를 Syslog 메시지로 전자 장치에게 전송하고, 전자 장치는 이를 수신하여 장애 상황을 인지할 수 있다.

【0049】 또한, 전자 장치는 SNMP(simple network management protocol)를 이용하여 네트워크 엔티티로부터 로그 데이터를 수신할 수도 있다. 전자 장치는 주기적으로 네트워크 엔티티에 로그 또는 상태 정보를 수신하기 위한 요청을 보낼 수 있다. 예를 들어, 전자 장치는 방화벽의 트래픽 상황이나 자원 사용 현황을 실시간으로 수신하기 위한 요청을 보낼 수 있다. 전자 장치는 SNMP를 활용하여 다양한 로그 정보를 구조화된 형태로 획득할 수 있다.

【0050】 나아가, 전자 장치는 네트워크 엔티티에 설치된 에이전트를 이용하여 네트워크 엔티티로부터 로그 데이터를 획득할 수도 있다. 예를 들어, 리눅스 서버에 설치된 로그 수집 에이전트를 통해 전자 장치는 시스템 로그 파일을 실시간으로 모니터링할 수 있다.

【0051】 일 실시예에 따르면, 동작 320에서, 전자 장치는 네트워크 엔티티로부터 획득한 로그 데이터로부터 로그 패턴 및 이벤트 번호를 식별할 수 있다.

【0052】일 실시예에 따르면, 전자 장치는 로그 데이터를 전처리 하여 로그 패턴을 식별할 수 있다. 보다 구체적으로, 전자 장치는 로그 데이터에서 대소문자를 통일하고, 숫자, 날짜, 파일의 경로, 지역명, 인터페이스명 및 기호를 토큰으로 대체하거나 제거하여 로그 패턴을 식별할 수 있다. 예를 들어, 로그 데이터에 숫자가 있는 경우에, 전자 장치는 숫자를 [number] 토큰으로 대체할 수 있다. 또한, 로그 데이터에 날짜가 있는 경우에, 전자 장치는 날짜를 [date] 토큰으로 대체할 수 있다. 로그 데이터에 지역명이 있는 경우에, 전자 장치는 지역명을 [loc] 토큰으로 대체할 수도 있다. 또한, 파일 경로는 대부분 '/'로 시작하기 때문에, 로그 데이터에 '/'로 시작하는 단어가 있는 경우에, 전자 장치는 '/'로 시작하는 단어를 [path] 토큰으로 대체할 수 있다. 또다른 예로, 'interface'의 다음에 등장하는 단어는 인터페이스의 이름을 의미하므로, 로그 데이터에 'interface'가 있는 경우에, 'interface'의 다음에 등장하는 단어를 [interface] 토큰으로 대체할 수 있다.

【0053】전자 장치는 토큰으로 대체되지 않은 모든 기호를 제거할 수도 있다. 예를 들어, 전자 장치는 'Interface HundGi0/3, changed state to FREQ_LOCK'이라는 로그 데이터로부터 'HundGi0/3'를 삭제하고, 'interface [interface] changed state to freq lock'라는 로그 패턴을 식별할 수 있다.

【0054】일 실시예에 따르면, 같은 형태의 로그 패턴을 갖는 로그 데이터는 같은 이벤트로 분류될 수 있다. 이때, 이벤트별로 매겨진 번호를 이벤트 번호로 정의할 수 있다. 예를 들어, ‘Login Success [user: admin] [source: 192.168.204.151] at 05:02:41'이라는 로그 데이터는 'login success user admin

source [UNK] at [UNK]'라는 로그 패턴으로 식별되고, 이는 최종적으로 'event 5'라는 이벤트 번호로 식별될 수 있다.

【0055】일 실시예에 따르면, 동작 330에서, 전자 장치는 로그 패턴의 발생 빈도에 기초하여 식별한 로그 패턴에 대해서 정상 상태에서의 로그 패턴의 희귀도를 획득할 수 있다. 전자 장치는 로그 패턴의 정상 상태에서의 희귀도를 Log-TF-IDF(Log-term frequency-inverse document frequency)를 사용하여 획득할 수 있으며, 로그 패턴이 정상 상태에서 희귀할수록 로그 패턴의 희귀도의 값이 크게 나타날 수 있다.

【0056】일 실시예에 따르면, TF-IDF는 자연어의 희귀도를 의미하고, TF와 IDF로 구성될 수 있다. TF(term frequency)는, 문서 내에서 특정한 단어가 등장하는 빈도를 의미하고, 문서에서 특정 단어가 등장한 횟수를 문서의 전체 단어의 개수로 나누어 획득될 수 있다. IDF(inverse document frequency)는, 전체 문서에서 특정 단어가 등장하는 문서가 등장하는 빈도를 의미하고, 전체 문서의 개수를 특정 단어가 등장하는 문서의 개수로 나눈 값에 로그(logarithm)를 취하여 획득할 수 있다. 특정 단어가 문서에서 자주 나타날수록 단어의 희귀도는 낮아지는 것이므로, IDF의 값은 작아질 수 있다. TF-IDF는 TF 값과 IDF 값을 곱하여 획득될 수 있다.

【0057】일 실시예에 따르면, Log-TF-IDF는, 자연어로 구성된 문서에서 특정 단어의 중요도를 계산하는데 사용되는 TF-IDF(term frequency-inverse document frequency)를, 로그 데이터를 분석하는데 적합하게 변형한 개념일 수 있다. Log-TF-IDF는, Log-TF 값과 Log- IDF 값을 곱하여 획득될 수 있다.

【0058】일 실시예에 따르면, Log-TF(Log-term frequency)는 전체 로그 데이터 중 특정한 로그 패턴이 등장한 빈도를 의미할 수 있다. Log-TF는 하기 수식 1에 의해 획득될 수 있다. 정상 데이터에서의 특정 로그 패턴의 수가 적다는 것은 특정 로그 패턴이 희귀하다는 것을 의미하므로, Log-TF의 값은 커질 수 있다. 특정 로그 패턴이 전체 로그 데이터에서 등장하지 않을 수 있기 때문에, 분모가 0이 되는 것을 방지하기 위해 정상 데이터에서의 특정 로그 패턴의 수에 1을 더한 값이 분모가 될 수 있다. 이와 더불어, 정상 데이터의 전체 로그 데이터 수가 상대적으로 많기 때문에, Log-IDF와 scale을 맞추기 위해 로그(logarithm)를 취한 값이 Log-TF 값이 될 수 있다.

【0059】 $$Log-TF=\log\left(\frac{\text{정상 로그 데이터의 전체 로그 데이터의 수}}{\text{정상 로그 데이터에서의 특정 로그 패턴의 수}+1}\right)$$

【0060】<수식 1>

【0061】일 실시예에 따르면, Log-IDF는 특정 로그 패턴이 발생한 날짜의 빈도를 의미할 수 있다. Log-IDF는 하기 수식 2에 의해 획득될 수 있다. 정상 로그 데이터에서 특정 로그 패턴이 발생한 날짜가 적다는 것은 특정 로그 패턴이 희귀하다는 것을 의미하므로, Log-IDF의 값은 커질 수 있다. 특정 로그 패턴이 정상 로그 데이터에서 발생하지 않을 수 있기 때문에, 분모가 0이 되는 것을 방지하기 위해 정상 로그 데이터에서 특정 로그 패턴이 발생한 날짜의 수에 1을 더한 값이 분모가 될 수 있다. 이 경우에, 분모가 분자와 같아지거나 분자보다 커질 수도 있기 때문에, 정상 로그 데이터의 전체 날짜의 수에 2를 더한 값이 분자가 될 수 있다.

【0062】

$$Log-IDF=\frac{\text{정상 로그 데이터의 전체 날짜의 수}+2}{\text{정상 로그 데이터에서 특정 로그 패턴이 발생한 날짜의 수}+1}$$

【0063】<수식 2>

【0064】일 실시예에 따르면, Log-TF-IDF는 하기 수식 3과 같이 Log-TF 및 Log-IDF를 곱한 값에 로그(logarithm)를 취하여 획득될 수 있다. 이 경우에, Log-TF-IDF의 값이 상대적으로 커지는 것을 방지하기 위해 로그(logarithm)를 취할 수 있다.

【0065】$Log-TF-IDF=\log\left(Log-TF\times Log-IDF\right)$

【0066】<수식 3>

【0067】일 실시예에 따르면, 동작 340에서, 전자 장치는 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률 및 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득할 수 있다. 전자 장치가 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률을 획득하는 동작은 도 5에서 자세히 설명한다.

【0068】일 실시예에 따르면, 전자 장치는 특정 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안 발생한 횟수에 1을 더한 값에 로그(logarithm)를 취하여 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득할 수 있다. Logarithm의 진수가 0이 되는 것을 방지하기 위하여, 특정 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안 발생한 횟수에 1을 더한 값이 진수가 될

수 있다. 전자 장치가 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득함으로써, 네트워크 엔티티의 인터페이스(interface)나 포트(port)가 up과 down을 비정상적으로 반복하는 Flapping 현상을 탐지할 수 있다.

【0069】일 실시예에 따르면, 동작 350에서, 전자 장치는 획득한 로그 패턴의 희귀도, 이벤트가 정상 상태에서 발생할 확률 및 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 네트워크 엔티티의 비정상 상태를 탐지할 수 있다. 전자 장치는 로그 패턴의 희귀도, 이벤트가 정상 상태에서 발생할 확률 및 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 로그 패턴의 비정상 점수(abnormal score)를 계산할 수 있다. 예를 들어, 비정상 점수는 로그 패턴의 희귀도, 이벤트가 정상 상태에서 발생할 확률 및 이벤트가 기 설정된 시간 동안에 발생한 빈도의 곱으로 계산될 수 있다. 전자 장치는 비정상 점수가 임계 값(threshold)을 연속하여 넘은 횟수 또는 비정상 점수가 임계 값을 넘은 후 다시 임계 값을 넘은 시간에 기반하여 네트워크 엔티티의 비정상 상태를 탐지할 수 있다. 예를 들어, 전자 장치는 비정상 점수가 임계 값을 연속하여 넘은 횟수가 기 설정된 횟수 이상이면 네트워크 엔티티가 비정상이라고 판단할 수 있다. 또다른 예를 들어, 전자 장치는 비정상 점수가 임계 값을 넘은 후 기 설정된 시간 내에 다시 비정상 점수가 임계 값을 넘은 경우에 네트워크 엔티티가 비정상 상태라고 판단할 수 있다. 전자 장치가 네트워크 엔티티의 비정상 상태를 탐지하는 자세한 과정은 도 7, 도 8 및 도 9에서 더 설명한다.

【0070】일 실시예에 따르면, 전자 장치는 네트워크 엔티티에서 발생하는 로그 데이터에 기반하여 실시간으로 네트워크 엔티티의 상태를 파악할 수 있다. 이와 더불어, 정상 상태에서의 로그 데이터를 기반으로 획득한 로그 데이터의 희귀도를 고려함으로써, 더욱 효과적으로 네트워크 엔티티의 비정상 상태를 탐지할 수 있다.

【0071】도 4는, 일 실시예에 따른 전자 장치가 획득한 로그 데이터로부터 로그 패턴 및 이벤트 번호를 식별하는 흐름도를 도시한다.

【0072】일 실시예에 따르면, 동작 410에서, 전자 장치가 네트워크 엔티티로부터 로그 데이터를 획득할 수 있다. 동작 410은 도 3의 동작 310에 대응될 수 있다. 전자 장치는 네트워크 엔티티가 기록한 로그 데이터를 획득하기 위해 Syslog 프로토콜, SNMP, 로그 수집 에이전트 등 다양한 방법을 사용할 수 있다.

【0073】일 실시예에 따르면, 동작 420에서, 전자 장치는 네트워크 엔티티로부터 획득한 로그 데이터를 전처리(pre-process)하여 로그 패턴을 식별할 수 있다. 전처리 과정에서, 전자 장치는 로그 데이터의 대소문자를 통일하고, 숫자, 날짜, 파일의 경로, 지역명, 인터페이스명 및 기호를 토큰으로 대체하거나 제거할 수 있다. 예를 들어, 로그 데이터에 숫자가 있는 경우에, 전자 장치는 숫자를 [number] 토큰으로 대체할 수 있다. 로그 데이터에 날짜가 있는 경우에, 전자 장치는 날짜를 [date] 토큰으로 대체할 수 있다. 로그 데이터에 지역명이 있는 경우에, 전자 장치는 지역명을 [loc] 토큰으로 대체할 수도 있다. 또한, 파일 경로는 대부분 '/'로 시작하기 때문에, 로그 데이터에 '/'로 시작하는 단어가 있는 경우에, 전자 장치는 '/'로 시작하는 단어를 [path] 토큰으로 대체할 수 있다. 또다른 예로,

'interface'의 다음에 등장하는 단어는 인터페이스의 이름을 의미하므로, 로그 데이터에 'interface'가 있는 경우에, 'interface'의 다음에 등장하는 단어를 [interface] 토큰으로 대체할 수 있다.

【0074】전자 장치는 토큰으로 대체되지 않은 모든 기호를 제거할 수도 있다. 예를 들어, 전자 장치는 'Interface HundGi0/3, changed state to FREQ_LOCK'이라는 로그 데이터로부터 대소문자를 통일하고, 'HundGi0/3'를 제거하고 기호를 삭제하는 전처리 과정을 통해 'interface [interface] changed state to freq lock'라는 로그 패턴을 식별할 수 있다.

【0075】일 실시예에 따르면, 동작 430에서, 전자 장치는 패턴 분석 과정을 통해, 식별된 로그 패턴을 분석하여 같은 패턴의 로그 패턴들을 분류할 수 있다. 로그 패턴을 분류하기에 앞서, 전자 장치는 정상 상태의 로그 데이터를 학습하여, 임계치 이상의 횟수로 등장하는 단어에 대해 단어 목록을 생성할 수 있다. 전자 장치는 단어 목록에 기반하여 단어 목록에 포함되지 않는 단어를 [UNK] 토큰으로 대체함으로써, 일시적으로 생성되는 단어들을 [UNK] 토큰으로 대체할 수 있다. 예를 들어, 'interface'라는 단어는 로그 데이터에서 3회 이상 등장하여 단어 목록에 포함되므로 토큰으로 대체되지 않을 수 있지만, 동적으로 할당되는 IP 주소와 같은 단어는 로그 데이터에서 1회만 등장할 수 있고, 단어 목록에 포함되지 않으므로 [UNK] 토큰으로 대체될 수 있다.

【0076】일 실시예에 따르면, 전자 장치는 단어 목록에 포함되지 않은 단어를 [UNK] 토큰으로 대체한 후에, 유사한 형태의 로그 패턴끼리 같은 이벤트로 분류

할 수 있다. 예를 들어, 'Login Success [user: admin] [source: 192.168.204.156] at 20:06:47'이라는 로그 데이터와 'Login Success [user: admin] [source: 192.168.204.151] at 05:02:41'이라는 로그 데이터는 서로 IP 주소와 시간이 다르지만, 'login success user admin source [UNK] at [UNK]'라는 같은 로그 패턴으로 식별되므로, 같은 이벤트로 분류될 수 있다.

【0077】일 실시예에 따르면, 동작 440에서, 전자 장치는 분류된 로그 패턴을 이벤트 번호로 식별할 수 있다. 전자 장치는 유사한 형태의 로그 패턴을 같은 이벤트로 분류한 후, 최종적으로 이벤트 번호로 식별할 수 있다. 예를 들어, 'login success user admin source [UNK] at [UNK]'와 유사한 로그 패턴을 갖는 로그 데이터는 최종적으로 'event 5'로, 'interface [interface] changed state to freq lock'와 유사한 로그 패턴을 갖는 로그 데이터는 최종적으로 'event 9'로 식별될 수 있다.

【0078】도 5는, 일 실시예에 따른 전자 장치가 이벤트가 정상 상태에서 발생할 확률을 획득하는 흐름도를 도시한다.

【0079】일 실시예에 따르면, 전자 장치는 최근에 발생한 이벤트 번호의 흐름(510)을 트랜스포머 모델(520)에 입력하여, 이벤트가 정상 상태에서 발생할 확률(530)을 획득할 수 있다.

【0080】일 실시예에 따르면, 최근에 발생한 이벤트 번호의 흐름(510)은, 네트워크 엔티티의 비정상 상태를 탐지하는 시점으로부터 가장 최근에 발생한 기 설정된 개수의 이벤트 번호의 흐름일 수 있다. 또한, 최근에 발생한 이벤트 번호의

흐름은, 전자 장치가 획득한 로그 데이터를 전처리(pre-processing), 패턴 분석(pattern analysis) 및 이벤트 분류(event classification) 과정을 통해 이벤트 번호를 식별함으로써 획득될 수 있다.

【0081】 일 실시예에 따르면, 트랜스포머 모델(520)은 정상 상태에서의 이벤트 번호의 흐름을 포함하는 데이터셋(dataset)을 이용하여 사전에 학습된 기계 학습(machine learning) 알고리즘일 수 있다. 트랜스포머 모델(520)은 최근에 발생한 이벤트 번호의 흐름(510)을 입력으로 받아, 이벤트가 정상 상태에서 발생할 확률(530)을 출력할 수 있다.

【0082】 일 실시예에 따르면, 트랜스포머 모델(520)은 최근에 발생한 이벤트 번호의 흐름(510)의 시퀀스(sequence) 전체를 동시에 입력으로 받아서 병렬로 처리할 수 있다. 시퀀스 전체를 동시에 입력받고 처리하기 때문에, 데이터의 손실을 막고 더 빨리 학습될 수 있다. 먼저, 트랜스포머 모델(520)은 원-핫 인코딩(one-hot encoding)을 통해, 입력된 최근 발생한 이벤트 번호의 흐름(510)을 임베딩 벡터(embedding vector)(522)로 변환할 수 있다. 이 경우에, 원-핫 인코딩은 n번 째까지의 숫자를 벡터로 변환할 때, 해당 숫자에만 1을 채우고, 나머지에는 0을 채운 길이가 n인 벡터를 만드는 방법일 수 있다. 또한, 임베딩 벡터(522)의 차원은 입력된 이벤트 번호의 흐름(510)에 포함된 이벤트 번호의 개수와 같을 수 있다. 예를 들어, 트랜스포머 모델(520)에 [0, 2, 1]이라는 이벤트 번호의 흐름이 입력된 경우, [[1, 0, 0], [0, 0, 1], [0, 1, 0]]이라는 임베딩 벡터로 변환될 수 있다.

【0083】일 실시예에 따르면, 변환된 임베딩 벡터(522)는 임베딩 벡터(522)의 차원의 수와 같은 개수의 층을 가지는 트랜스포머 인코더(transformer encoder)(524)에 입력될 수 있다. 트랜스포머 인코더(524)의 마지막 층(524n)이 하나의 벡터(526)를 반환할 수 있다.

【0084】일 실시예에 따르면, 트랜스포머 인코더가 반환한 벡터(526)를 FC(fully connected) layer 및 softmax layer(528)에 입력하면 이벤트 번호 별로 이벤트가 정상 상태에서 발생할 확률(530)이 출력될 수 있다. 이 경우에, FC layer는 트랜스포머 인코더가 반환한 벡터(526)를 이벤트 번호 별 점수(score)로 변환할 수 있다. 또한, softmax layer는 이벤트 번호 별 점수를 이벤트 번호 별로 0과 1 사이의 확률로 변환하여 출력할 수 있다. 예를 들어, 이벤트 번호가 2개만 존재한다고 가정하면, FC layer는 트랜스포머 인코더가 반환한 벡터를 [2.1, -0.3]이라는 점수로 변환할 수 있고, 이를 softmax layer가 [0.89, 0.11]이라는 벡터로 변환하여 출력할 수 있다. 이는 정상 상태에서 이벤트 번호가 1인 이벤트가 발생할 확률이 89%, 이벤트 번호가 2인 이벤트가 발생할 확률이 11%라는 것을 의미할 수 있다.

【0085】일 실시예에 따르면, 이벤트가 정상 상태에서 발생할 확률(530)은, 이벤트가 정상 상태에서 발생할 확률을 획득하는 시점의 다음에 이벤트가 정상 상태에서 발생할 확률을 식별한 이벤트 번호 별로 포함하는 벡터일 수 있다. 예를 들어, 이벤트가 정상 상태에서 발생할 확률(530)이 [0.89, 0.11]이라는 것은, 이벤트가 정상 상태에서 발생할 확률을 획득하는 시점의 다음에 이벤트 번호가 1인 이벤트가 발생할 확률이 89%, 이벤트 번호가 2인 이벤트가 발생할 확률이 11%라는 것을

의미할 수 있다.

【0086】 도 6은, 일 실시예에 따른 전자 장치가 비정상 점수를 계산하여 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

【0087】 일 실시예에 따르면, 동작 610에서, 전자 장치는 로그 패턴의 희귀도, 이벤트가 정상 상태에서 발생할 확률 및 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 로그 패턴의 비정상 점수(abnormal score)를 계산할 수 있다. 예를 들어, 수식 4와 같이, 로그 패턴의 비정상 점수는 로그 패턴의 희귀도, 이벤트가 정상 상태에서 발생할 확률 및 이벤트가 기 설정된 시간 동안에 발생한 빈도의 곱으로 계산될 수 있다. 이 경우에, 이벤트가 정상 상태에서 발생할 확률이 낮을수록 네트워크 엔티티가 비정상 상태일 확률이 높다는 의미이므로, 1에서 이벤트가 정상 상태에서 발생할 확률을 뺀 값을 곱하여 비정상 점수가 계산될 수 있다.

【0088】 $$Abnormal\ score = Log - TF - IDF \times (1 - Log - Prob) \times Log - Freq$$

【0089】 <수식 4>

【0090】 일 실시예에 따르면, 로그 패턴의 비정상 점수는 입력된 로그 패턴이 얼마나 비정상적인지를 나타내는 수치로서, 로그 패턴이 정상 상태에서 얼마나 희귀한지, 이벤트의 흐름이 정상 상태에서는 얼마나 자주 일어나는지, 이벤트가 최근 얼마나 자주 반복되었는지를 모두 고려하여 결정된 값일 수 있다.

【0091】 일 실시예에 따르면, 동작 620에서, 전자 장치는 계산된 로그 패턴의 비정상 점수를 기반으로, 네트워크 엔티티의 비정상 상태를 탐지할 수 있다. 예

를 들어, 네트워크 엔티티는 적어도 하나의 네트워크 스위치, 라우터, 서버 또는 방화벽을 포함할 수 있다.

【0092】 도 7은, 일 실시예에 따른 전자 장치가 반복 횟수를 기반으로 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

【0093】 일 실시예에 따르면, 도 7은 도 6의 동작 620을 구체적으로 설명하는 흐름도일 수 있다.

【0094】 일 실시예에 따르면, 동작 710에서, 전자 장치는 비정상 점수가 임계 값(threshold)을 넘었는지 확인할 수 있다. 전자 장치가 비정상 점수가 임계 값을 넘었다고 판단하는 경우, 전자 장치는 동작 720을 수행할 수 있다. 전자 장치가 비정상 점수가 임계 값을 넘지 않았다고 판단하는 경우, 전자 장치는 지속적으로 비정상 점수가 임계 값을 넘었는지 확인할 수 있다.

【0095】 일 실시예에 따르면, 동작 720에서, 전자 장치는 비정상 점수가 연속하여 임계 값을 넘은 횟수가 기 설정된 횟수 이상인지 확인할 수 있다. 전자 장치가 비정상 점수가 연속하여 임계 값을 넘은 횟수가 기 설정된 횟수 이상이라고 판단하는 경우, 전자 장치는 동작 730을 수행할 수 있다. 전자 장치가 비정상 점수가 연속하여 임계 값을 넘은 횟수가 기 설정된 횟수 이상이 아니라고 판단하는 경우, 전자 장치는 계속하여 동작 710을 수행할 수 있다.

【0096】 일 실시예에 따르면, 동작 730에서, 전자 장치는 네트워크 엔티티가 비정상 상태라고 탐지할 수 있다. 일 실시예에 따르면, 네트워크 엔티티는 적어도

하나의 네트워크 스위치, 라우터, 서버 또는 방화벽을 포함할 수 있다.

【0097】 도 8은, 일 실시예에 따른 전자 장치가 시간을 기반으로 네트워크 엔티티의 비정상 상태를 탐지하는 흐름도를 도시한다.

【0098】 일 실시예에 따르면, 도 8은 도 6의 동작 620을 구체적으로 설명하는 흐름도일 수 있다.

【0099】 일 실시예에 따르면, 동작 810에서, 전자 장치는 비정상 점수가 임계 값(threshold)을 넘었는지 확인할 수 있다. 전자 장치가 비정상 점수가 임계 값을 넘었다고 판단하는 경우, 전자 장치는 동작 820을 수행할 수 있다. 전자 장치가 비정상 점수가 임계 값을 넘지 않았다고 판단하는 경우, 전자 장치는 지속적으로 비정상 점수가 임계 값을 넘었는지 확인할 수 있다.

【0100】 일 실시예에 따르면, 동작 820에서, 전자 장치는 비정상 점수가 임계 값을 넘은 후 기 설정된 시간 이내에 다시 비정상 점수가 임계 값을 넘었는지 확인할 수 있다. 전자 장치가 비정상 점수가 임계 값을 넘은 후 기 설정된 시간 이내에 다시 비정상 점수가 임계 값을 넘었다고 판단하는 경우, 전자 장치는 동작 830을 수행할 수 있다. 전자 장치가 비정상 점수가 임계 값을 넘은 후 기 설정된 시간 이내에 다시 비정상 점수가 임계 값을 넘지 않았다고 판단하는 경우, 전자 장치는 계속하여 동작 810을 수행할 수 있다.

【0101】 일 실시예에 따르면, 동작 830에서, 전자 장치는 네트워크 엔티티가 비정상 상태라고 탐지할 수 있다. 일 실시예에 따르면, 네트워크 엔티티는 적어도

하나의 네트워크 스위치, 라우터, 서버 또는 방화벽을 포함할 수 있다.

【0102】도 9는, 일 실시예에 따른 전자 장치의 구성을 도시한다.

【0103】도 9를 참조하면, 전자 장치(900)는 적어도 하나의 트랜시버(901)(이하, 트랜시버), 적어도 하나의 프로세서(902)(이하, 프로세서) 및 적어도 하나의 메모리(903)(이하, 메모리)를 포함할 수 있다. 본 개시의 실시예에 해당하는 방법들 중 적어도 하나 또는 그 결합에 따라, 전자 장치(900)의 트랜시버(901), 프로세서(902) 및 메모리(903)가 동작할 수 있다. 다만, 전자 장치(900)의 구성 요소는 도 9에 도시된 구성 요소의 예시에 한정되는 것은 아니다. 다른 실시예에서는, 전자 장치(900)는 전술한 구성 요소들에 추가적인 구성 요소를 더 포함하거나 일부 구성 요소가 생략될 수도 있다. 또한, 일부 실시예에서는 트랜시버(901), 프로세서(902) 또는 메모리(903)의 임의의 조합(any combination)이 하나의 구성요소(component) 형태로 집적될 수도 있다. 일 실시예에 따르면, 전자 장치(900)는 도 2의 전자 장치(230)와 대응될 수 있다.

【0104】트랜시버(901)는 전자 장치(900)가 네트워크의 노드 또는 엔티티와 통신을 수행할 수 있도록 하는 기본적인 통신 회로(communication circuit), 통신 회로망(communication circuitry) 또는 통신 인터페이스(communication interface)일 수 있다. 일례로, 트랜시버(901)는 전자 장치(900)가 네트워크 노드 또는 엔티티와 통신을 통해 데이터를 송수신할 수 있도록 하거나, 다른 전자 장치와 통신을 통해 데이터를 송수신할 수 있도록 할 수 있다.

【0105】프로세서(902)는 본 개시의 실시예에 따라 전자 장치(900)의 전반적

인 동작을 제어할 수 있다. 프로세서(902)는 하나 이상의 IC (integrated circuit (또는 circuitry)) 칩으로 구현될 수 있고, 다양한 데이터 처리들을 실행할 수 있다. 프로세서(902)는 적어도 하나의 전기적 회로를 포함할 수 있고, 메모리(903) 내에 저장된 인스트럭션들(또는 프로그램, 코드, 데이터 등)을 개별적(individually)으로 또는 집합적(collectively) 또는 어떠한 조합(in any combination)으로도 실행할 수 있다. 또한, 프로세서(902)는 단일 코어 프로세서 또는 다중 코어 프로세서를 포함할 수 있으며, 특정 구현 방식에서는 복수 개의 프로세싱 회로를 포함하는 프로세서 집합체로 구성될 수도 있다.

【0106】프로세서(902)는 트랜시버(901)와 전기적으로(electrically) 또는 작동적으로(operatively) 또는 통신 가능하도록(communicatively) 연결(coupled)되어, 트랜시버(901)를 제어할 수 있다.

【0107】프로세서(902)는 적어도 하나의 프로세서(processor)(또는, 프로세싱 회로(processing circuitry))를 포함할 수 있으며, 적어도 하나의 프로세서는, 이하의 동작들을 개별적(individually)으로 또는 집합적(collectively) 또는 임의의 조합(in any combination)으로도 수행할 수 있다. 예를 들어, 프로세서(902)는 통신 동작을 제어하는 CP(communication processor) 및 상위 계층(예를 들어 어플리케이션(application) 계층)의 실행을 제어하는 AP(application processor)를 포함할 수 있다. 특정 실시예에서, 프로세서(902)의 적어도 일 부분이 하나의 칩에 포함되고, 프로세서(902)의 다른 일 부분이 별도의 다른 칩에 포함될 수 있다. 또는, 적어도 하나의 프로세서는 다른 구성 요소 예를 들어, 트랜시버(901), 메모리

(903) 내에 포함될 수도 있다.

【0108】 프로세서(902)는 본 개시의 실시예들에 따른 방법들 중 적어도 하나 또는 그 결합을 실행하기 위한 전자 장치의 동작을 수행하거나 또는 야기(cause)하거나 또는 제어할 수 있다. 예를 들어, 프로세서(902)는 네트워크 엔티티로부터 수신한 데이터를 처리할 수 있다. 이를 위해, 프로세서(902)는 메모리(903)에 저장된 컴퓨터 프로그램, 코드, 또는 인스트럭션들을 실행함으로써 다양한 동작들을 수행하도록 전자 장치(900)의 다른 구성요소들을 제어할 수 있다.

【0109】 메모리(903)는 정보를 임시적으로 또는 영구적으로 저장할 수 있는 하드웨어 저장 장치이며, 하나 이상의 저장 매체들을 포함할 수 있다. 예를 들어, 메모리(903)는 하나 이상의 저장 매체들을 포함하는 메모리 집합체를 포함할 수 있다. 예를 들면, 상기 하나 이상의 저장 매체들은, 하드 드라이브, 플래시 메모리, ROM(read-only memory)과 같은 영구 메모리(permanent memory), RAM(random access memory)과 같은 반영구 메모리(semipermanent memory), 캐시 메모리, 또는 이들의 어떤 조합을 포함할 수 있다.

【0110】 메모리(903)는 프로세서(902)와 전기적으로(electrically) 또는 작동적으로(operatively) 또는 통신 가능하도록(communicatively) 연결(coupled)될 수 있으며, 프로세서(902)에 의해 액세스될 수 있다.

【0111】 메모리(903)에는 프로세서(902)에 의해 실행될 수 있는 컴퓨터 프로그램, 코드, 또는 인스트럭션 등이 저장될 수 있다. 일 실시예에 따라, 프로세서(902)에 의해 실행될 수 있는 컴퓨터 프로그램, 코드, 또는 인스트럭션은 하나의

메모리 디바이스에 저장되거나 또는 분리되어 둘 이상의 메모리 디바이스에 분산되어 저장될 수도 있다. 프로세서(902)는 메모리(903)에 저장된 인스트럭션을 실행함으로써, 본 개시의 실시예에 따른 다양한 기능을 수행할 수 있다.

【0112】본 개시의 일 실시예에 따르면, 전자 장치(900)의 동작은, 메모리(903)에 저장된 인스트럭션들(또는 컴퓨터 프로그램 또는 코드)의 실행에 기반하여 본 개시의 특징들을 개별적(individually)으로 또는 집합적(collectively) 또는 임의의 조합(in any combination)으로 수행되도록 구성된 적어도 하나의 프로세서(또는 프로세싱 회로), 명령어를 실행하도록 구성되지 않은 처리 회로(processing circuitry)에 기반하여, 및/또는 명령어를 실행하도록 구성되지 않은 처리 회로의 구성 요소(component of a processing circuitry)들에 기반하여 수행되도록 야기될 수 있다.

【0113】도 10은, 일 실시예에 따른 네트워크 엔티티의 구성을 도시한다.

【0114】도 10를 참조하면, 네트워크 엔티티(1000)는 적어도 하나의 트랜시버(1001)(이하, 트랜시버), 적어도 하나의 프로세서(1002)(이하, 프로세서) 및 적어도 하나의 메모리(1003)(이하, 메모리)를 포함할 수 있다. 일 실시예에 따르면, 네트워크 엔티티(1000)는 도 2의 네트워크 엔티티(220)와 대응될 수 있다.

【0115】본 개시의 실시예에 해당하는 방법들 중 적어도 하나 또는 그 결합에 따라, 네트워크 엔티티(1000)의 트랜시버(1001), 프로세서(1002) 및 메모리(1003)가 동작할 수 있다. 다만, 네트워크 엔티티(1000)의 구성 요소는 도 10에 도시된 구성 요소의 예시에 한정되는 것은 아니다. 다른 실시예에서는, 네트워크 엔

티티(1000)는 전술한 구성 요소들에 추가적인 구성 요소를 더 포함하거나 일부 구성 요소가 생략될 수도 있다. 또한, 일 실시예에서는, 트랜시버(1001), 프로세서(1002) 또는 메모리(1003)가 하나의 구성요소(component) 형태로 구현될 수 있다.

【0116】트랜시버(1001)는 네트워크 엔티티(1000)가 전자 장치와 통신을 수행할 수 있도록 하는 기본적인 통신 회로(communication circuit), 통신 회로망(communication circuitry) 또는 통신 인터페이스(communication interface) 일 수 있다. 일례로, 트랜시버(1001)는 네트워크 엔티티(1000)가 전자 장치와 통신을 통해 데이터를 송수신할 수 있도록 하거나, 다른 네트워크 엔티티와 통신을 통해 데이터를 송수신할 수 있도록 할 수 있다.

【0117】프로세서(1002)는 본 개시의 실시예에 따라 네트워크 엔티티(1000)의 전반적인 동작을 제어할 수 있다. 프로세서(1002)는 일 실시예에서는 하나 이상의 IC(integrated circuit 또는 circuitry) 칩으로 구현될 수 있고, 다양한 데이터 처리들을 실행할 수 있다. 프로세서(1002)는 적어도 하나의 전기적 회로를 포함할 수 있고, 메모리(1003) 내에 저장된 인스트럭션들(또는 프로그램, 코드, 데이터 등)을 개별적(individually)으로 또는 집합적(collectively)으로 또는 어떠한 조합(in any combination)으로도 실행할 수 있다. 또한, 프로세서(1002)는 단일 코어 프로세서 또는 다중 코어 프로세서를 포함할 수 있으며, 특정 구현 방식에서는 복수 개의 프로세싱 회로를 포함하는 프로세서 집합체로 구성될 수도 있다. 또한, 프로세서(1002)는 다른 일 실시예에 따라 네트워크 기능(1000)이 인스턴스 형태로 구현되는 경우에는, 반드시 물리적 하드웨어로 구성되지 않을 수도 있음에 유의해야

한다.

【0118】일 실시예에 따라, 프로세서(1002)는 네트워크 인터페이스(1001)와 전기적으로(electrically) 또는 작동적으로(operatively) 또는 통신 가능하도록(communicatively) 연결(coupled)되어, 네트워크 인터페이스(1001)를 제어할 수 있다.

【0119】프로세서(1002)는 적어도 하나의 프로세서(processor)(또는, 프로세서 회로(processor circuitry))를 포함할 수 있으며, 적어도 하나의 프로세서는, 이하의 동작들을 개별적(individually)으로 또는 집합적(collectively)으로 또는 어떠한 조합(in any combination)으로도 수행할 수 있다. 특정 실시예에서, 프로세서(1002)의 적어도 일 부분이 하나의 칩에 포함되고, 프로세서(1002)의 다른 일 부분이 별도의 다른 칩에 포함될 수 있다. 또는, 적어도 하나의 프로세서는 다른 구성 요소 예를 들어, 네트워크 인터페이스(1001), 메모리(1003) 내에 포함될 수도 있다.

【0120】 프로세서(1002)는 본 개시의 실시예들에 따른 방법들 중 적어도 하나 또는 그 결합을 수행하기 위한 네트워크 엔티티(1000)의 동작을 수행하거나 또는 제어할 수 있다. 예를 들어, 프로세서(1002)는 다양한 프로토콜들(예를 들어, NAS 프로토콜)을 이용하여 단말, 기지국, 또는 다른 코어 네트워크 엔티티들과 무선 또는 유선 통신을 통해 제어 평면 메시지 또는 사용자 평면 메시지를 교환하도록 하는 네트워크 엔티티(1000)의 동작을 제어할 수 있다. 이를 위해, 프로세서(1002)는 메모리(1003) 내에 저장된 컴퓨터 프로그램, 코드, 또는 인스트럭션들을

실행함으로써 다양한 동작들을 수행하도록 네트워크 엔티티(1000)의 다른 구성요소들을 제어할 수 있다.

【0121】 메모리(1003)는 정보를 임시적으로 또는 영구적으로 저장할 수 있는 하드웨어 저장 장치이며, 하나 이상의 저장 매체들을 포함할 수 있다. 예를 들어, 메모리(1003)는 하나 이상의 저장 매체들을 포함하는 메모리 집합체를 포함할 수 있다. 예를 들면, 상기 하나 이상의 저장 매체들은, 하드 드라이브, 플래시 메모리, ROM(read-only memory)과 같은 영구 메모리(permanent memory), RAM(random access memory)과 같은 반영구 메모리(semipermanent memory), 캐시 메모리, 또는 이들의 어떤 조합을 포함할 수 있다.

【0122】 일 실시예에 따라 메모리(1003)는 프로세서(1002)와 전기적으로(electrically) 또는 작동적으로(operatively) 또는 통신 가능하도록(communicatively) 연결(coupled)될 수 있으며, 프로세서(1002)에 의해 액세스될 수 있다.

【0123】 메모리(1003)에는 프로세서(1002)에 의해 실행될 수 있는 컴퓨터 프로그램, 코드, 또는 인스트럭션 등이 저장될 수 있다. 일 실시예에 따라, 프로세서(1002)에 의해 실행될 수 있는 컴퓨터 프로그램, 코드, 또는 인스트럭션은 하나의 메모리에 저장되거나 또는 분리되어 둘 이상의 메모리에 분산되어 저장될 수도 있다. 프로세서(1002)는 메모리(1003)에 저장된 인스트럭션을 실행함으로써, 본 개시의 실시예에 따른 다양한 기능을 수행할 수 있다.

【0124】 본 개시의 일 실시예에 따르면, 네트워크 엔티티(1000)의 동작은,

메모리(1003)에 저장된 인스트럭션들(또는 컴퓨터 프로그램 또는 코드)의 실행에 기반하여 본 개시의 특징들을 개별적(individually)으로 또는 집합적(collectively) 또는 임의의 조합(in any combination)으로 수행되도록 구성된 적어도 하나의 프로세서(또는 프로세싱 회로), 명령어를 실행하도록 구성되지 않은 처리 회로(processing circuitry)에 기반하여, 및/또는 명령어를 실행하도록 구성되지 않은 처리 회로의 구성 요소(component of a processing circuitry)들에 기반하여 수행되도록 야기될 수 있다.

【0125】본 개시의 일 실시예에 따르면, 네트워크 엔티티(1000)는 적어도 하나의 네트워크 스위치, 라우터, 서버 또는 방화벽을 포함할 수 있다.

【0126】본 개시의 다양한 실시예에 따르면, 전자 장치에 의해 로그 데이터를 분석하는 방법이 제공될 수 있다. 전자 장치에 의해 로그 데이터를 분석하는 방법은 네트워크 엔티티로부터 상기 로그 데이터를 획득하는 단계; 상기 획득한 로그 데이터로부터 로그 패턴과 이벤트 번호를 식별하는 단계; 상기 로그 패턴의 발생 빈도에 기초하여, 상기 로그 패턴에 대해서 정상 상태에서의 상기 로그 패턴의 희귀도를 획득하는 단계; 상기 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 상기 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득하는 단계; 및 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여, 상기 네트워크 엔티티의 비정상 상태를 탐지하는 단계를 포함할 수 있다.

【0127】일 실시예에 따르면, 상기 획득한 로그 데이터로부터 상기 로그 패턴을 식별하는 단계는, 상기 로그 데이터의 일부를 제거하거나 다른 단어로 대체하는 전처리(pre-processing) 단계 및 상기 로그 데이터 중 같은 형태의 로그 데이터를 상기 로그 패턴으로 압축하는 패턴 분석(pattern analysis) 단계를 포함하고, 상기 획득한 로그 데이터로부터 상기 이벤트 번호를 식별하는 단계는, 상기 로그 패턴 중 유사한 로그 패턴들을 같은 이벤트로 분류하여 상기 이벤트 번호로 대응시키는 과정을 포함하는 이벤트 분류(event classification) 단계를 포함할 수 있다.

【0128】일 실시예에 따르면, 상기 로그 패턴의 희귀도는, 상기 획득한 로그 데이터의 개수, 상기 획득한 로그 데이터에서의 상기 로그 패턴의 개수, 상기 획득한 로그 데이터가 발생한 날짜 수 및 상기 획득한 로그 데이터에서의 상기 로그 패턴이 발생한 날짜 수를 이용하여 결정될 수 있다.

【0129】일 실시예에 따르면, 상기 이벤트가 정상 상태에서 발생할 확률은, 최근에 발생한 이벤트 번호의 흐름을 포함하는 데이터를, 정상 상태에서의 이벤트 번호의 흐름 데이터셋을 학습시킨 트랜스포머 모델에 입력하여 획득될 수 있다.

【0130】일 실시예에 따르면, 상기 비정상 상태는, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 계산된 로그 패턴의 비정상 점수(Abnormal score)를 기반으로 탐지될 수 있다.

【0131】일 실시예에 따르면, 상기 비정상 점수는, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도의 곱으로 결정될 수 있다.

【0132】일 실시예에 따르면, 상기 비정상 점수가 연속하여 임계값(threshold)을 넘은 횟수가 기 설정된 횟수 이상이면, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지될 수 있다.

【0133】일 실시예에 따르면, 상기 비정상 점수가 임계값을 넘은 후 기 설정된 시간 이내에 다시 상기 비정상 점수가 임계값을 넘는 경우에, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지될 수 있다.

【0134】일 실시예에 따르면, 상기 네트워크 엔티티는, 적어도 하나의 네트워크 스위치일 수 있다.

【0135】본 개시의 다양한 실시예에 따르면, 로그 데이터를 분석하는 전자 장치가 제공될 수 있다. 상기 전자 장치는, 적어도 하나의 트랜시버(transceiver); 상기 적어도 하나의 트랜시버에 통신적으로(communicatively) 결합된(coupled to) 적어도 하나의 프로세서; 및 상기 적어도 하나의 프로세서에 통신적으로 결합되어 명령어들(instructions)을 저장하는 적어도 하나의 메모리를 포함하고, 상기 명령어들은 상기 적어도 하나의 프로세서에 의해서 개별적으로(individually) 또는 임의의 조합(any combination)으로 실행되어, 상기 전자 장치가 네트워크 엔티티로부터 로그 데이터를 획득하고, 상기 획득한 로그 데이터로부터 로그 패턴과 이벤트

번호를 식별하고, 상기 로그 패턴의 발생 빈도에 기초하여, 상기 로그 패턴에 대해서 정상 상태에서의 상기 로그 패턴의 희귀도를 획득하고, 상기 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 상기 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득하고, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여, 상기 네트워크 엔티티의 비정상 상태를 탐지하도록 할 수 있다.

【0136】일 실시예에 따르면, 상기 명령어들은 상기 전자 장치가 상기 로그 패턴을, 상기 로그 데이터의 일부를 제거하거나 다른 단어로 대체하는 전처리(pre-processing) 단계 및 상기 로그 데이터 중 같은 형태의 로그 데이터를 상기 로그 패턴으로 압축하는 패턴 분석(pattern analysis) 단계를 통해 식별하고, 상기 이벤트 번호를, 상기 로그 패턴 중 유사한 로그 패턴들을 같은 이벤트로 분류하여 상기 이벤트 번호로 대응시키는 과정을 포함하는 이벤트 분류(event classification) 단계를 통해 식별하도록 할 수 있다.

【0137】일 실시예에 따르면, 상기 명령어들은 상기 전자 장치가 상기 로그 패턴의 희귀도를, 상기 획득한 로그 데이터의 개수, 상기 획득한 로그 데이터에서의 상기 로그 패턴의 개수, 상기 획득한 로그 데이터가 발생한 날짜 수 및 상기 획득한 로그 데이터에서의 상기 로그 패턴이 발생한 날짜 수를 이용하여 결정하도록 할 수 있다.

【0138】일 실시예에 따르면, 상기 명령어들은 상기 전자 장치가 상기 이벤트가 정상 상태에서 발생할 확률을, 최근에 발생한 이벤트 번호의 흐름을 포함하는 데이터를 정상 상태에서의 이벤트 번호의 흐름 데이터셋을 학습시킨 트랜스포머 모델에 입력하여 획득하도록 할 수 있다.

【0139】일 실시예에 따르면, 상기 명령어들은 상기 전자 장치가 상기 비정상 상태를, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 계산된 로그 패턴의 비정상 점수(Abnormal score)를 기반으로 탐지하도록 할 수 있다.

【0140】일 실시예에 따르면, 상기 명령어들은 상기 전자 장치가 상기 비정상 점수를, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도의 곱으로 결정하도록 할 수 있다.

【0141】일 실시예에 따르면, 상기 명령어들은 상기 전자 장치가 상기 비정상 점수가 연속하여 임계값(threshold)을 넘은 횟수가 기 설정된 횟수 이상이면, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지하도록 할 수 있다.

【0142】일 실시예에 따르면, 상기 명령어들은 상기 전자 장치가 상기 비정상 점수가 임계값을 넘은 후 기 설정된 시간 이내에 다시 상기 비정상 점수가 임계값을 넘는 경우에, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지하도록 할 수 있다.

【0143】일 실시예에 따르면, 상기 네트워크 엔티티는, 적어도 하나의 네트워크 스위치일 수 있다.

【0144】본 문서에 개시된 다양한 실시예들에 따른 전자 장치는 다양한 형태의 장치가 될 수 있다. 전자 장치는, 예를 들면, 휴대용 통신 장치(예: 스마트폰), 컴퓨터 장치, 휴대용 멀티미디어 장치, 휴대용 의료 기기, 카메라, 웨어러블 장치, 또는 가전 장치를 포함할 수 있다. 본 문서의 실시예에 따른 전자 장치는 전술한 기기들에 한정되지 않는다.

【0145】본 문서의 다양한 실시예들 및 이에 사용된 용어들은 본 문서에 기재된 기술적 특징들을 특정한 실시예들로 한정하려는 것이 아니며, 해당 실시예의 다양한 변경, 균등물, 또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 또는 관련된 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 아이템에 대응하는 명사의 단수 형은 관련된 문맥상 명백하게 다르게 지시하지 않는 한, 상기 아이템 한 개 또는 복수 개를 포함할 수 있다. 본 문서에서, "A 또는 B", "A 및 B 중 적어도 하나", "A 또는 B 중 적어도 하나", "A, B 또는 C", "A, B 및 C 중 적어도 하나", 및 "A, B, 또는 C 중 적어도 하나"와 같은 문구들 각각은 그 문구들 중 해당하는 문구에 함께 나열된 항목들 중 어느 하나, 또는 그들의 모든 가능한 조합을 포함할 수 있다. "제 1", "제 2", 또는 "첫째" 또는 "둘째"와 같은 용어들은 단순히 해당 구성요소를 다른 해당 구성요소와 구분하기 위해 사용될 수 있으며, 해당 구성요소들을 다른 측면(예: 중요성 또는 순서)에서 한정하지 않는다. 어떤(예: 제 1) 구성요소가 다른(예: 제 2) 구성요소에, "기능적

으로" 또는 "통신적으로"라는 용어와 함께 또는 이런 용어 없이, "커플드" 또는 "커넥티드"라고 언급된 경우, 그것은 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로(예: 유선으로), 무선으로, 또는 제 3 구성요소를 통하여 연결될 수 있다는 것을 의미한다.

【0146】 본 문서의 다양한 실시예들에서 사용된 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구현된 유닛을 포함할 수 있으며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로와 같은 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는, 상기 부품의 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 일실시예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.

【0147】본 문서의 다양한 실시예들은 기기(machine)(예: 전자 장치(101))의해 읽을 수 있는 저장 매체(storage medium)(예: 내장 메모리(136) 또는 외장 메모리(138))에 저장된 하나 이상의 명령어들을 포함하는 소프트웨어(예: 프로그램(140))로서 구현될 수 있다. 예를 들면, 기기(예: 전자 장치(101))의 프로세서(예: 프로세서(120))는, 저장 매체로부터 저장된 하나 이상의 명령어들 중 적어도 하나의 명령을 호출하고, 그것을 실행할 수 있다. 이것은 기기가 상기 호출된 적어도 하나의 명령어에 따라 적어도 하나의 기능을 수행하도록 운영되는 것을 가능하게 한다. 상기 하나 이상의 명령어들은 컴파일러에 의해 생성된 코드 또는 인터프리터에 의해 실행될 수 있는 코드를 포함할 수 있다. 기기로 읽을 수 있는 저장 매체는, 비일시적(non-transitory) 저장 매체의 형태로 제공될 수 있다. 여기서,

'비일시적'은 저장 매체가 실재(tangible)하는 장치이고, 신호(signal)(예: 전자기파)를 포함하지 않는다는 것을 의미할 뿐이며, 이 용어는 데이터가 저장 매체에 반영구적으로 저장되는 경우와 임시적으로 저장되는 경우를 구분하지 않는다.

【0148】 일실시예에 따르면, 본 문서에 개시된 다양한 실시예들에 따른 방법은 컴퓨터 프로그램 제품(computer program product)에 포함되어 제공될 수 있다. 컴퓨터 프로그램 제품은 상품으로서 판매자 및 구매자 간에 거래될 수 있다. 컴퓨터 프로그램 제품은 기기로 읽을 수 있는 저장 매체(예: compact disc read only memory(CD-ROM))의 형태로 배포되거나, 또는 어플리케이션 스토어(예: 플레이 스토어TM)를 통해 또는 두 개의 사용자 장치들(예: 스마트 폰들) 간에 직접, 온라인으로 배포(예: 다운로드 또는 업로드)될 수 있다. 온라인 배포의 경우에, 컴퓨터 프로그램 제품의 적어도 일부는 제조사의 서버, 어플리케이션 스토어의 서버, 또는 중계 서버의 메모리와 같은 기기로 읽을 수 있는 저장 매체에 적어도 일시 저장되거나, 임시적으로 생성될 수 있다.

【0149】 다양한 실시예들에 따르면, 상기 기술한 구성요소들의 각각의 구성요소(예: 모듈 또는 프로그램)는 단수 또는 복수의 개체를 포함할 수 있으며, 복수의 개체 중 일부는 다른 구성요소에 분리 배치될 수도 있다. 다양한 실시예들에 따르면, 전술한 해당 구성요소들 중 하나 이상의 구성요소들 또는 동작들이 생략되거나, 또는 하나 이상의 다른 구성요소들 또는 동작들이 추가될 수 있다. 대체적으로 또는 추가적으로, 복수의 구성요소들(예: 모듈 또는 프로그램)은 하나의 구성요소로 통합될 수 있다. 이런 경우, 통합된 구성요소는 상기 복수의 구성요소들 각각의

구성요소의 하나 이상의 기능들을 상기 통합 이전에 상기 복수의 구성요소들 중 해당 구성요소에 의해 수행되는 것과 동일 또는 유사하게 수행할 수 있다. 다양한 실시예들에 따르면, 모듈, 프로그램 또는 다른 구성요소에 의해 수행되는 동작들은 순차적으로, 병렬적으로, 반복적으로, 또는 휴리스틱하게 실행되거나, 상기 동작들 중 하나 이상이 다른 순서로 실행되거나, 생략되거나, 또는 하나 이상의 다른 동작들이 추가될 수 있다.

【청구범위】

【청구항 1】

전자 장치에 의해 로그 데이터를 분석하는 방법에 있어서,

네트워크 엔티티로부터 상기 로그 데이터를 획득하는 단계;

상기 획득한 로그 데이터로부터 로그 패턴과 이벤트 번호를 식별하는 단계;

상기 로그 패턴의 발생 빈도에 기초하여, 상기 로그 패턴에 대해서 정상 상태에서의 상기 로그 패턴의 희귀도를 획득하는 단계;

상기 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 상기 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득하는 단계; 및

상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여, 상기 네트워크 엔티티의 비정상 상태를 탐지하는 단계를 포함하는, 방법.

【청구항 2】

제1 항에 있어서,

상기 획득한 로그 데이터로부터 상기 로그 패턴을 식별하는 단계는,

상기 로그 데이터의 일부를 제거하거나 다른 단어로 대체하는 전처리(pre-processing) 단계 및 상기 로그 데이터 중 같은 형태의 로그 데이터를 상기 로그

패턴으로 압축하는 패턴 분석(pattern analysis) 단계를 포함하고,

상기 획득한 로그 데이터로부터 상기 이벤트 번호를 식별하는 단계는,

상기 로그 패턴 중 유사한 로그 패턴들을 같은 이벤트로 분류하여 상기 이벤트 번호로 대응시키는 과정을 포함하는 이벤트 분류(event classification) 단계를 포함하는, 방법.

【청구항 3】

제1 항에 있어서,

상기 로그 패턴의 희귀도는,

상기 획득한 로그 데이터의 개수, 상기 획득한 로그 데이터에서의 상기 로그 패턴의 개수, 상기 획득한 로그 데이터가 발생한 날짜 수 및 상기 획득한 로그 데이터에서의 상기 로그 패턴이 발생한 날짜 수를 이용하여 결정되는 것인, 방법.

【청구항 4】

제1 항에 있어서,

상기 이벤트가 정상 상태에서 발생할 확률은,

최근에 발생한 이벤트 번호의 흐름을 포함하는 데이터를, 정상 상태에서의 이벤트 번호의 흐름 데이터셋을 학습시킨 트랜스포머 모델에 입력하여 획득되는 것인, 방법.

【청구항 5】

제1 항에 있어서,

상기 비정상 상태는,

상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 계산된 로그 패턴의 비정상 점수(Abnormal score)를 기반으로 탐지되는 것인, 방법.

【청구항 6】

제5 항에 있어서,

상기 비정상 점수는,

상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도의 곱으로 결정되는 것인, 방법.

【청구항 7】

제5 항에 있어서,

상기 비정상 점수가 연속하여 임계값(threshold)을 넘은 횟수가 기 설정된 횟수 이상이면, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지되는 것인, 방법.

【청구항 8】

제5 항에 있어서,

상기 비정상 점수가 임계값을 넘은 후 기 설정된 시간 이내에 다시 상기 비정상 점수가 임계값을 넘는 경우에, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지되는 것인, 방법.

【청구항 9】

제1 항에 있어서,

상기 네트워크 엔티티는, 적어도 하나의 네트워크 스위치인, 방법.

【청구항 10】

전자 장치에 있어서,

적어도 하나의 트랜시버(transceiver);

상기 적어도 하나의 트랜시버에 통신적으로(communicatively) 결합된(coupled to) 적어도 하나의 프로세서; 및

상기 적어도 하나의 프로세서에 통신적으로 결합되어 명령어들(instructions)을 저장하는 적어도 하나의 메모리를 포함하고,

상기 명령어들은 상기 적어도 하나의 프로세서에 의해서 개별적으로

(individually) 또는 임의의 조합(any combination)으로 실행되어, 상기 전자 장치가:

네트워크 엔티티로부터 로그 데이터를 획득하고,

상기 획득한 로그 데이터로부터 로그 패턴과 이벤트 번호를 식별하고,

상기 로그 패턴의 발생 빈도에 기초하여, 상기 로그 패턴에 대해서 정상 상태에서의 상기 로그 패턴의 희귀도를 획득하고,

상기 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 상기 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득하고,

상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여, 상기 네트워크 엔티티의 비정상 상태를 탐지하도록 하는, 전자 장치.

【청구항 11】

제10 항에 있어서,

상기 명령어들은 상기 전자 장치가:

상기 로그 패턴을, 상기 로그 데이터의 일부를 제거하거나 다른 단어로 대체하는 전처리(pre-processing) 단계 및 상기 로그 데이터 중 같은 형태의 로그 데이터를 상기 로그 패턴으로 압축하는 패턴 분석(pattern analysis) 단계를 통해 식별하고,

상기 이벤트 번호를, 상기 로그 패턴 중 유사한 로그 패턴들을 같은 이벤트로 분류하여 상기 이벤트 번호로 대응시키는 과정을 포함하는 이벤트 분류(event classification) 단계를 통해 식별하도록 하는, 전자 장치.

【청구항 12】

제10 항에 있어서,

상기 명령어들은 상기 전자 장치가:

상기 로그 패턴의 희귀도를, 상기 획득한 로그 데이터의 개수, 상기 획득한 로그 데이터에서의 상기 로그 패턴의 개수, 상기 획득한 로그 데이터가 발생한 날짜 수 및 상기 획득한 로그 데이터에서의 상기 로그 패턴이 발생한 날짜 수를 이용하여 결정하도록 하는, 전자 장치.

【청구항 13】

제10 항에 있어서,

상기 명령어들은 상기 전자 장치가:

상기 이벤트가 정상 상태에서 발생할 확률을, 최근에 발생한 이벤트 번호의 흐름을 포함하는 데이터를 정상 상태에서의 이벤트 번호의 흐름 데이터셋을 학습시킨 트랜스포머 모델에 입력하여 획득하도록 하는, 전자 장치.

【청구항 14】

제10 항에 있어서,

상기 명령어들은 상기 전자 장치가:

상기 비정상 상태를, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 계산된 로그 패턴의 비정상 점수(Abnormal score)를 기반으로 탐지하도록 하는, 전자 장치.

【청구항 15】

제14 항에 있어서,

상기 명령어들은 상기 전자 장치가:

상기 비정상 점수를, 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도의 곱으로 결정하도록 하는, 전자 장치.

【청구항 16】

제14 항에 있어서,

상기 명령어들은 상기 전자 장치가:

상기 비정상 점수가 연속하여 임계값(threshold)을 넘은 횟수가 기 설정된

횟수 이상이면, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지하도록 하는 것인, 전자 장치.

【청구항 17】

제14 항에 있어서,

상기 명령어들은 상기 전자 장치가:

상기 비정상 점수가 임계값을 넘은 후 기 설정된 시간 이내에 다시 상기 비정상 점수가 임계값을 넘는 경우에, 상기 네트워크 엔티티가 상기 비정상 상태라고 탐지하도록 하는, 전자 장치.

【청구항 18】

제10 항에 있어서,

상기 네트워크 엔티티는, 적어도 하나의 네트워크 스위치인, 전자 장치.

【요약서】

【요약】

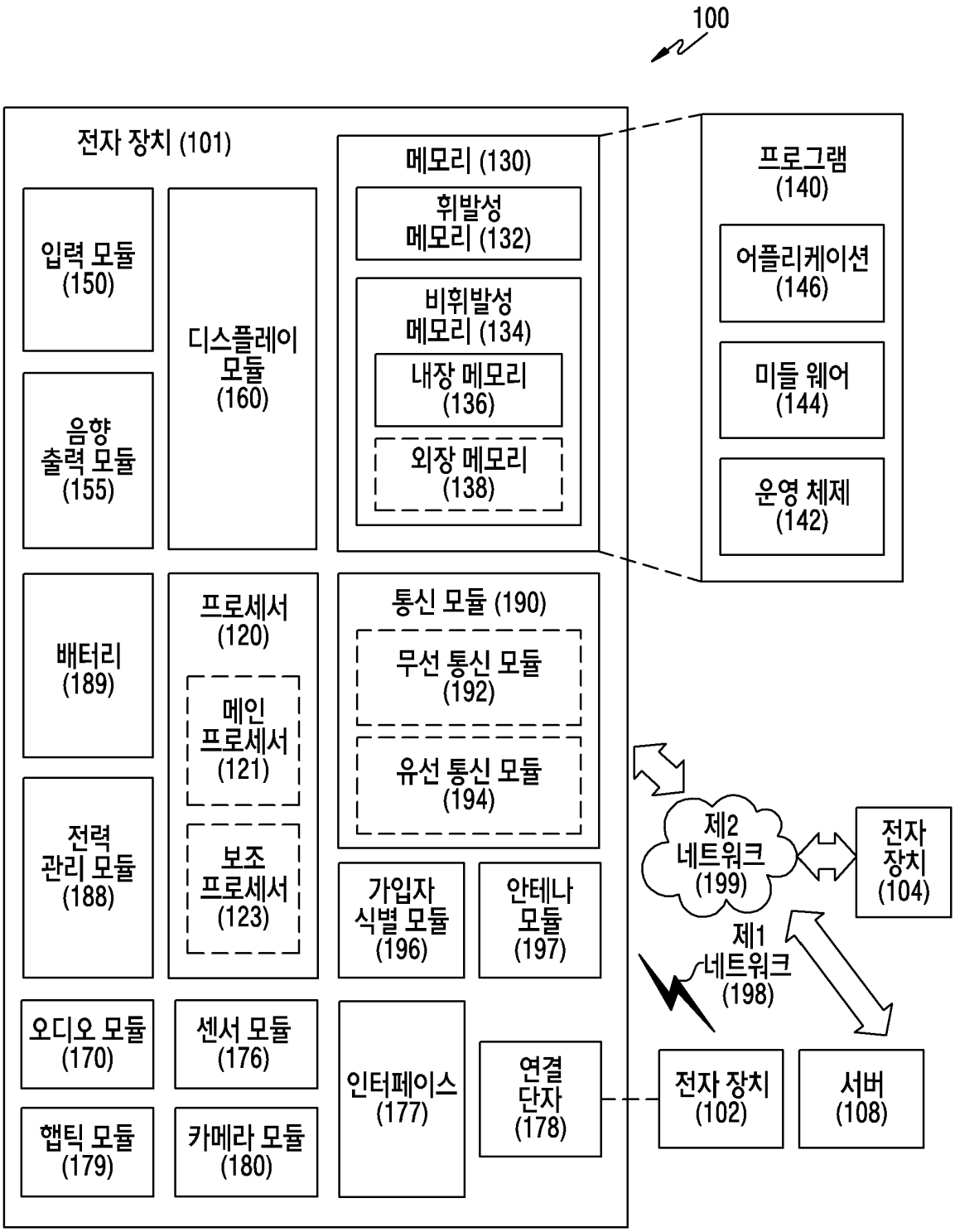
본 개시는 네트워크 엔티티의 상태를 탐지하는 방법과 장치에 관한 것이다. 본 개시는 로그 데이터를 분석하여 네트워크 엔티티의 상태를 탐지하는 방법과 장치에 관한 것이다. 구체적으로, 본 개시의 일 실시예에 따른 전자 장치에 의해 수행되는 방법은, 네트워크 엔티티로부터 로그 데이터를 획득하는 단계; 상기 획득한 로그 데이터로부터 로그 패턴과 이벤트 번호를 식별하는 단계; 상기 로그 패턴의 발생 빈도에 기초하여, 상기 로그 패턴에 대해서 정상 상태에서의 상기 로그 패턴의 희귀도를 획득하는 단계; 상기 이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 상기 이벤트 번호에 대응하는 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득하는 단계; 및 상기 로그 패턴의 희귀도, 상기 이벤트가 정상 상태에서 발생할 확률 및 상기 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여, 상기 네트워크 엔티티의 비정상 상태를 탐지하는 단계를 포함한다.

【대표도】

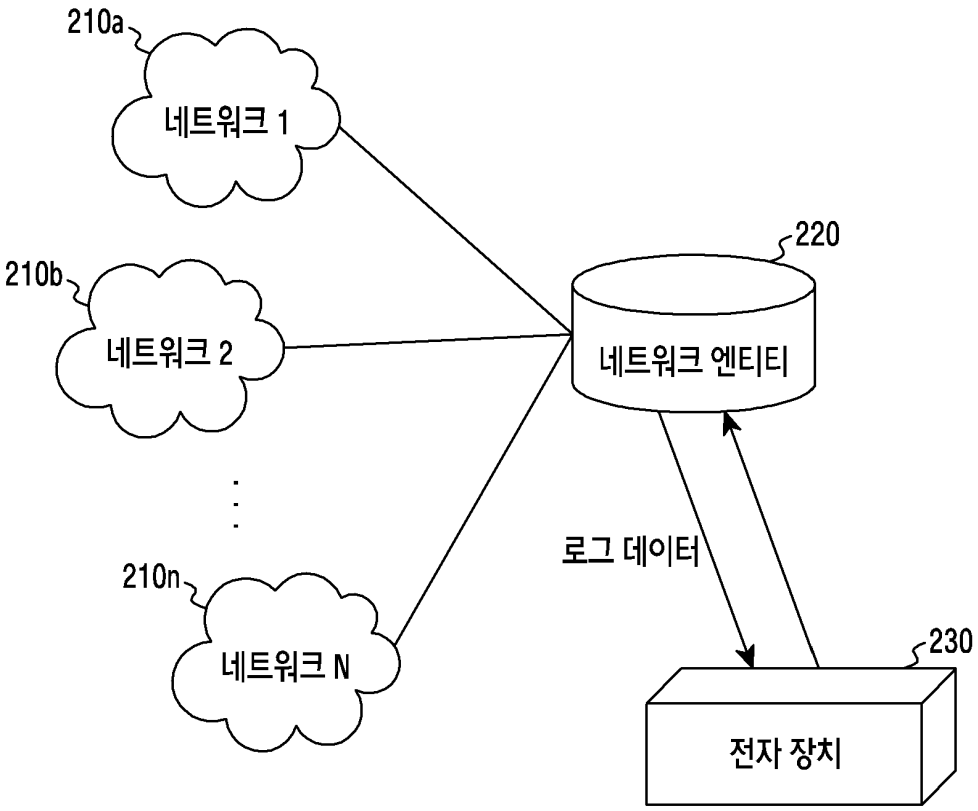
도 3

【도면】

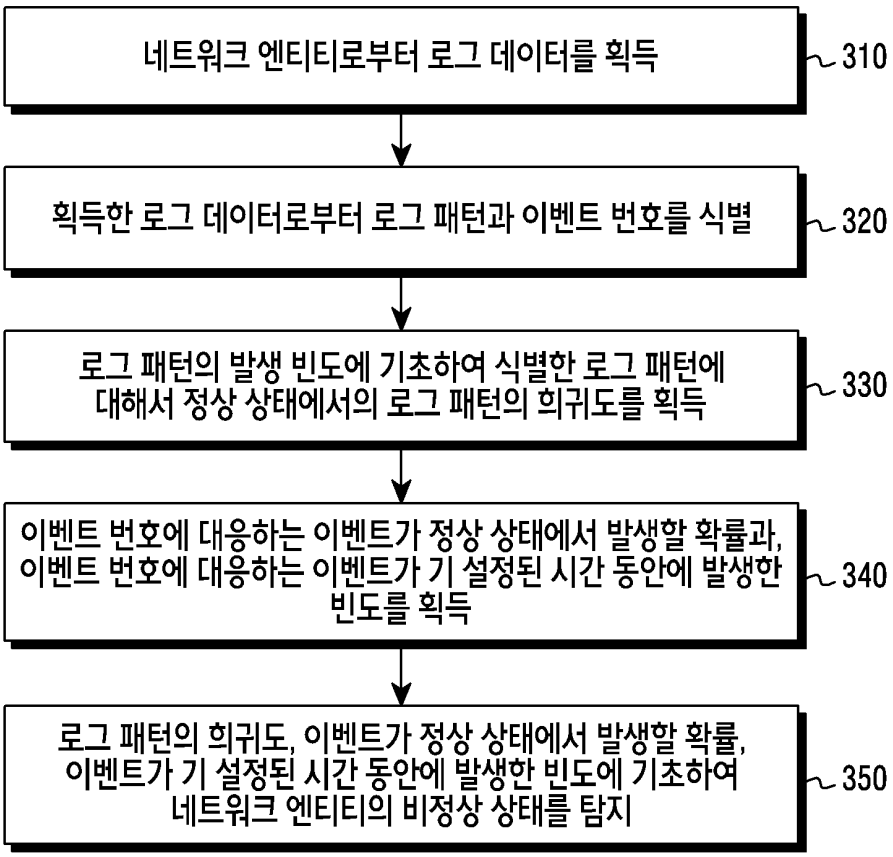
【도 1】


100
전자 장치 (101)
입력 모듈 (150)
음향 출력 모듈 (155)
디스플레이 모듈 (160)
메모리 (130)
휘발성 메모리 (132)
비휘발성 메모리 (134)
내장 메모리 (136)
외장 메모리 (138)
프로그램 (140)
어플리케이션 (146)
미들 웨어 (144)
운영 체제 (142)
배터리 (189)
전력 관리 모듈 (188)
프로세서 (120)
메인 프로세서 (121)
보조 프로세서 (123)
통신 모듈 (190)
무선 통신 모듈 (192)
유선 통신 모듈 (194)
가입자 식별 모듈 (196)
안테나 모듈 (197)
오디오 모듈 (170)
센서 모듈 (176)
햅틱 모듈 (179)
카메라 모듈 (180)
인터페이스 (177)
연결 단자 (178)
제2 네트워크 (199)
전자 장치 (104)
제1 네트워크 (198)
전자 장치 (102)
서버 (108)

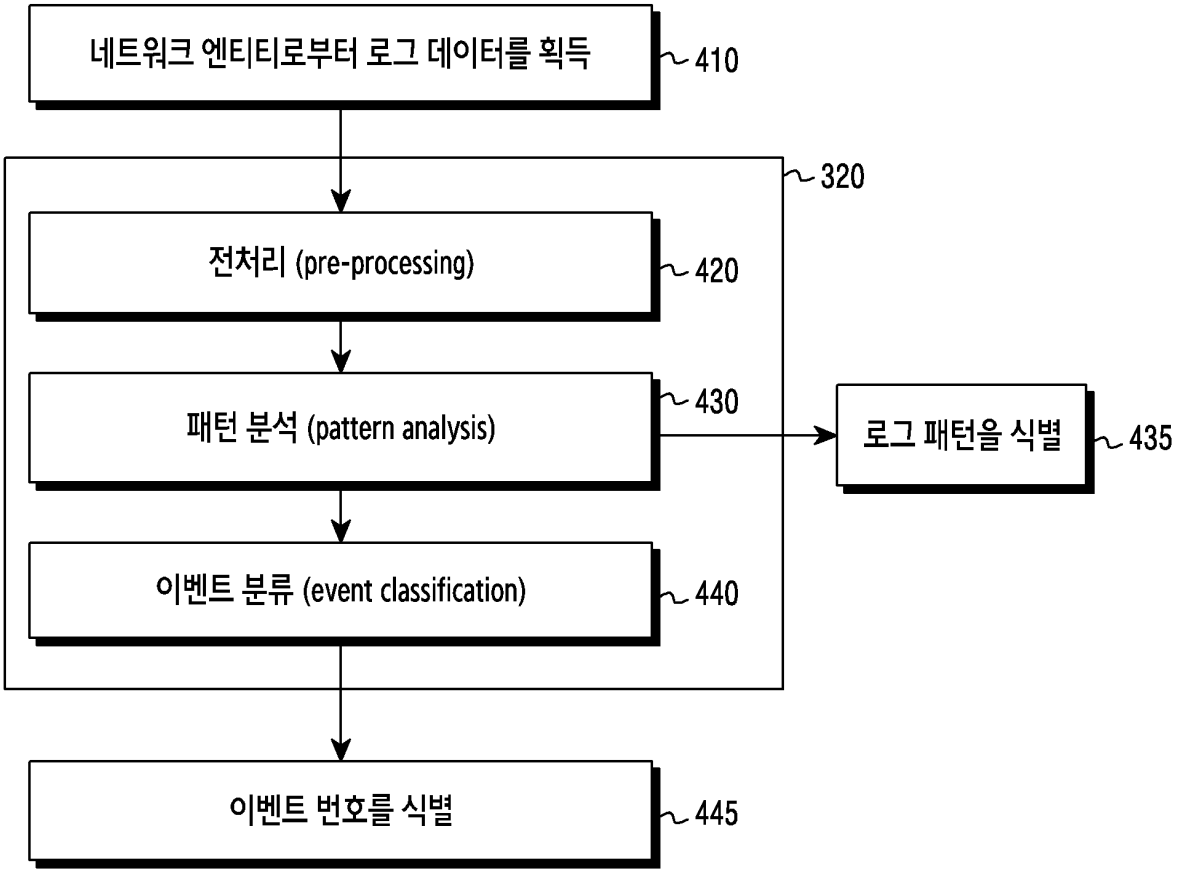
【도 2】



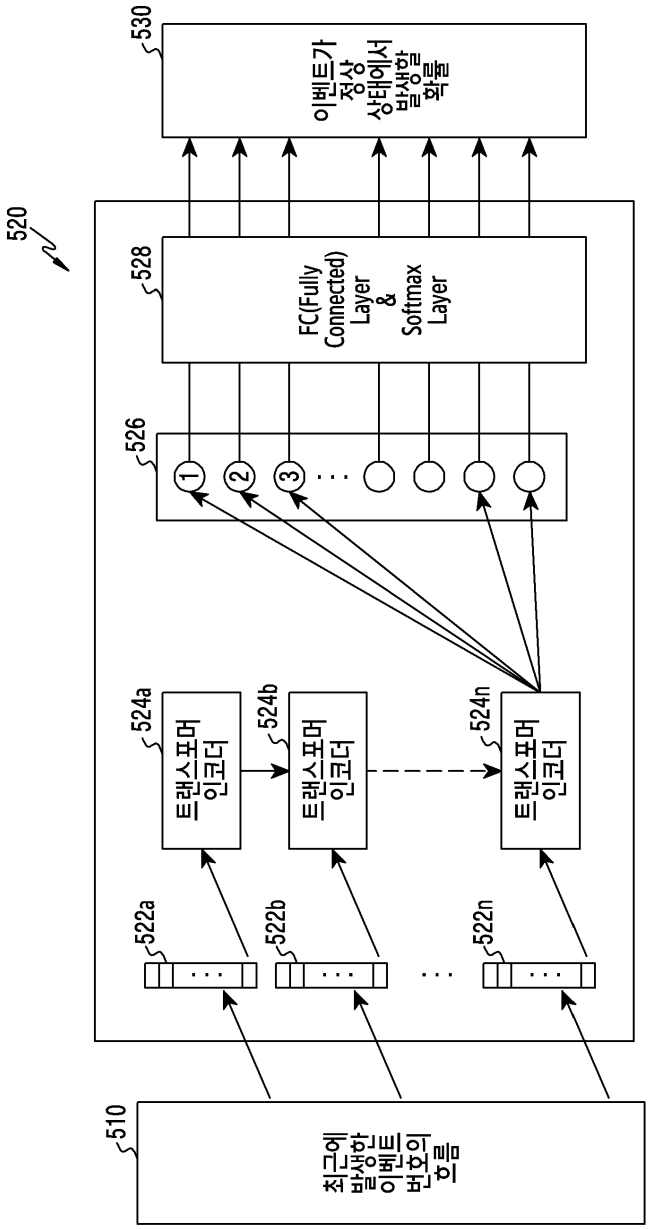
【도 3】


네트워크 엔티티로부터 로그 데이터를 획득
310
획득한 로그 데이터로부터 로그 패턴과 이벤트 번호를 식별
320
로그 패턴의 발생 빈도에 기초하여 식별한 로그 패턴에 대해서 정상 상태에서의 로그 패턴의 희귀도를 획득
330
이벤트 번호에 대응하는 이벤트가 정상 상태에서 발생할 확률과, 이벤트 번호에 대응하는 이벤트가 기 설정된 시간 동안에 발생한 빈도를 획득
340
로그 패턴의 희귀도, 이벤트가 정상 상태에서 발생할 확률, 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 네트워크 엔티티의 비정상 상태를 탐지
350

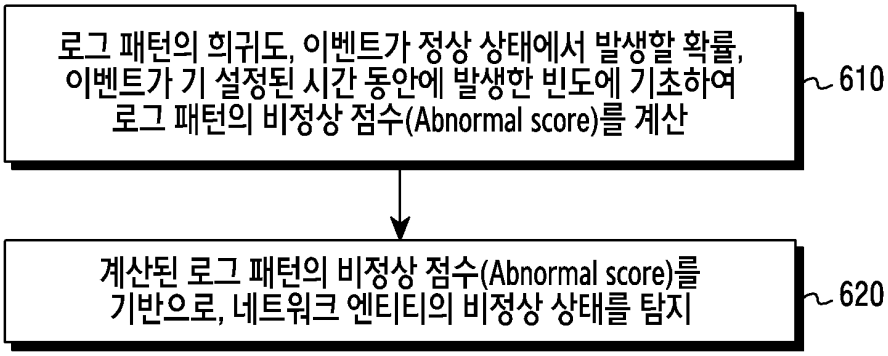
【도 4】


네트워크 엔티티로부터 로그 데이터를 획득
410
320
전처리 (pre-processing)
420
패턴 분석 (pattern analysis)
430
로그 패턴을 식별
435
이벤트 분류 (event classification)
440
이벤트 번호를 식별
445

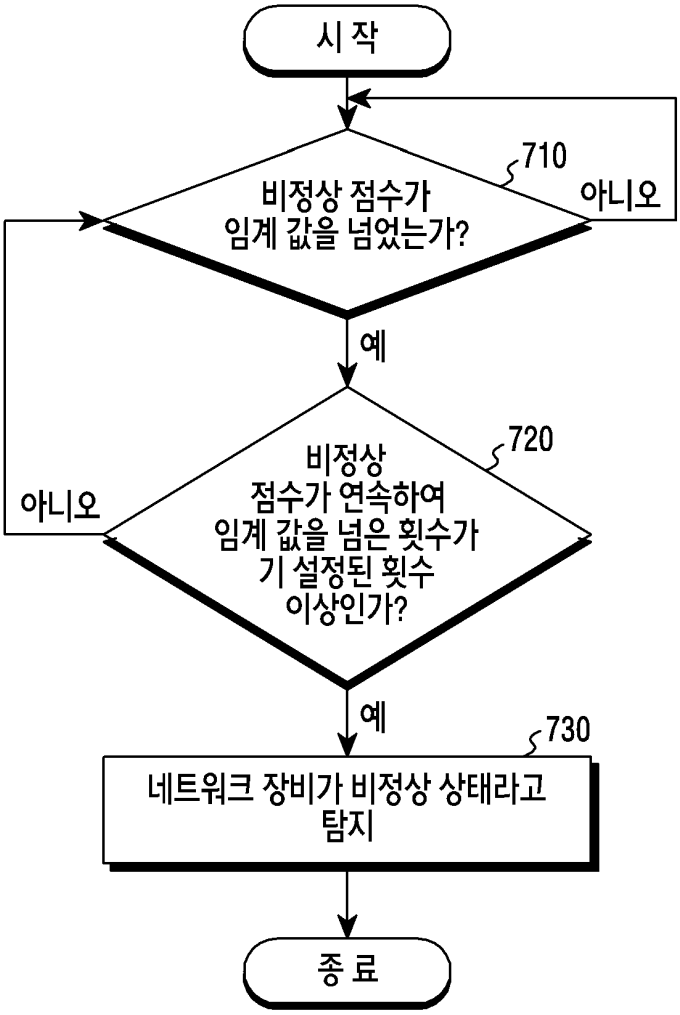
【도 5】


530
이벤트가 정상 상태에서 발생할 확률
520
528
FC(Fully Connected) Layer & Softmax Layer
526
1
2
3
524a
트랜스포머 인코더
524b
트랜스포머 인코더
524n
트랜스포머 인코더
522a
522b
522n
510
최근에 발생한 이벤트의 번호의 흐름

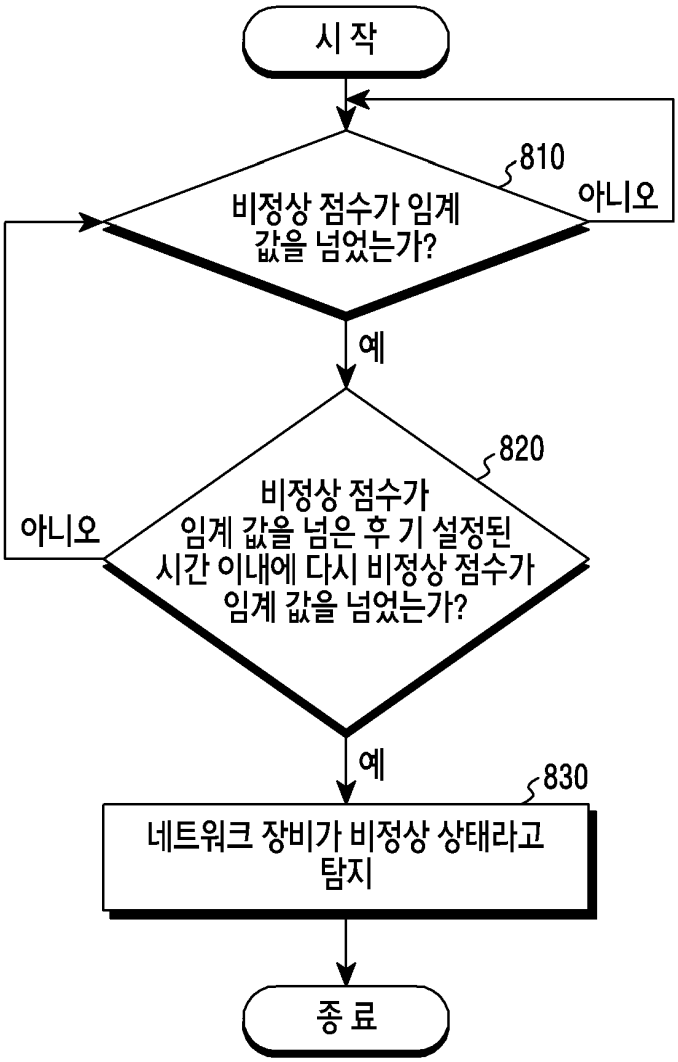
【도 6】


로그 패턴의 희귀도, 이벤트가 정상 상태에서 발생할 확률, 이벤트가 기 설정된 시간 동안에 발생한 빈도에 기초하여 로그 패턴의 비정상 점수(Abnormal score)를 계산
610
계산된 로그 패턴의 비정상 점수(Abnormal score)를 기반으로, 네트워크 엔티티의 비정상 상태를 탐지
620

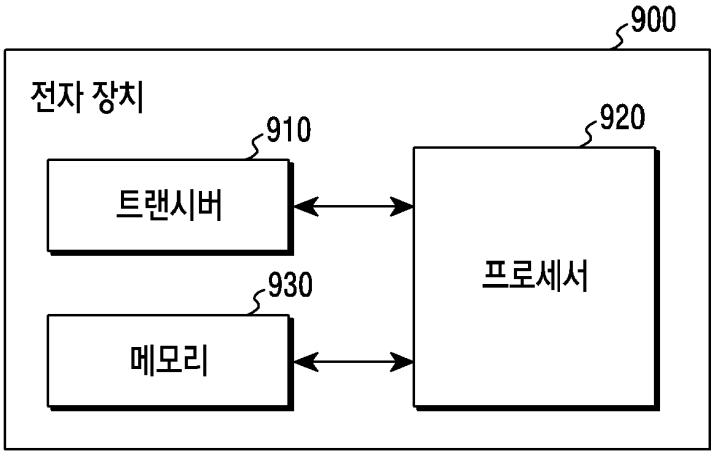
【도 7】


시 작
710
비정상 점수가
임계 값을 넘었는가?
아니오
예
720
비정상
점수가 연속하여
임계 값을 넘은 횟수가
기 설정된 횟수
이상인가?
아니오
예
730
네트워크 장비가 비정상 상태라고
탐지
종 료

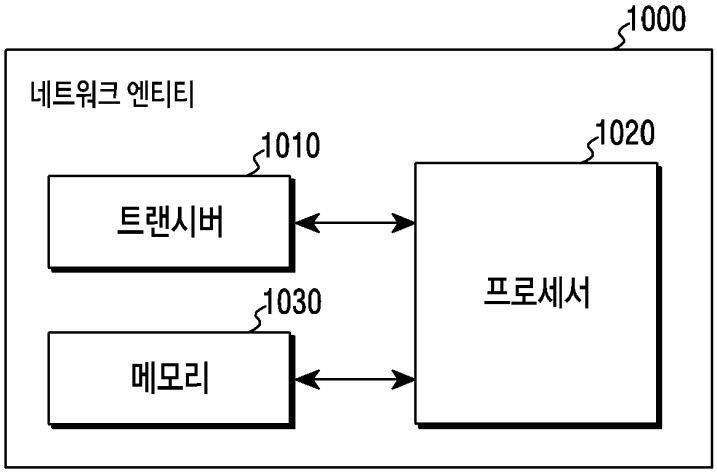
【도 8】


시 작
810
비정상 점수가 임계 값을 넘었는가?
아니오
예
820
비정상 점수가 임계 값을 넘은 후 기 설정된 시간 이내에 다시 비정상 점수가 임계 값을 넘었는가?
아니오
예
830
네트워크 장비가 비정상 상태라고 탐지
종 료

【도 9】


900
전자 장치
910
트랜시버
920
프로세서
930
메모리

【도 10】


1000
네트워크 엔티티
1010
트랜시버
1020
프로세서
1030
메모리