(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월02일
(11) 등록번호 10-2440180
(24) 등록일자 2022년08월31일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06K 9/62* (2022.01)
G06N 3/02 (2019.01) *H04L 65/40* (2022.01)
(52) CPC특허분류
G06F 21/6245 (2013.01)
G06F 21/6227 (2013.01)
(21) 출원번호 10-2020-0181420
(22) 출원일자 2020년12월22일
심사청구일자 2020년12월22일
(65) 공개번호 10-2022-0090332
(43) 공개일자 2022년06월29일
(56) 선행기술조사문헌
KR101054107 B1*
(뒷면에 계속)
전체 청구항 수 : 총 7 항

(73) 특허권자
연세대학교 원주산학협력단
강원도 원주시 흥업면 연세대길 1
(72) 발명자
황상원
서울특별시 노원구 공릉로34길 62 태강아파트 1010동 1103호
김민아
서울특별시 관악구 은천로28가길 46 소망스튜디오 203호
(뒷면에 계속)
(74) 대리인
특허법인지원

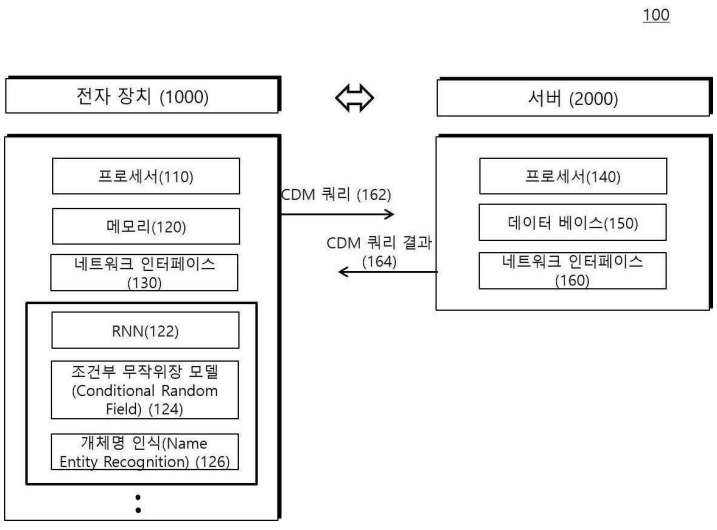
심사관 : 구대성

(54) 발명의 명칭 **CDM 패킷을 이용하여 개인정보 노출 여부를 결정하는 방법 및 장치**

(57) 요 약

본 개시는 개인 정보 노출 여부를 결정하는 방법 및 이를 수행하는 전자 장치에 관한 것이다. 일 실시 예에 의하면, 전자 장치가 개인 정보 노출여부를 결정하는 방법은 상기 전자 장치와 연결된 서버로 쿼리를 전송하는 단계; 상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 상기 서버로부터 전송되는 패킷을 획득하는 단계; 및 상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별하는 단계; 를 포함할 수 있다.

대 표 도



(52) CPC특허분류
G06K 9/62 (2022.01)
G06N 3/02 (2019.01)
H04L 67/02 (2022.05)

(72) 발명자
포비체카
강원도 원주시 일산로 20 원주의과대학 기숙사 2213호
권찬우
서울특별시 동작구 사당로20가길 7-3, 402호

(56) 선행기술조사문헌
KR1020080029123 A*
KR1020120068519 A*
KR1020140049148 A*
KR1020140115602 A*
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	191035
과제번호	HI19C1035
부처명	보건복지부
과제관리(전문)기관명	보건산업진흥원
연구사업명	CDM 기반 정밀의료 데이터 통합 플랫폼 기술개발
연구과제명	분산 연구 네트워크 상시 모니터링 기술 개발
기 여 율	1/1
과제수행기관명	연세대학교 원주산학협력단
연구기간	2019.07.25 ~ 2021.12.31

명 세 서

청구범위

청구항 1

전자 장치가 개인정보 노출 여부를 결정하는 방법에 있어서,

상기 전자 장치와 연결된 서버로 CDM(Common Data Model) 데이터를 쿼리 결과로써 요청하기 위한 CDM 쿼리를 전송하는 단계;

상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 HTTPS를 통해 상기 서버에 접속하고, 상기 접속된 서버로부터 전송되는 패킷을 획득하는 단계; 및

상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별하는 단계; 를 포함하고,

상기 패킷을 획득하는 단계는,

WIRE SHARK를 응용한 ALTO 시스템을 이용해, 상기 획득된 패킷 내 데이터를 PCAP 파일로 저장하는 단계를 포함하며,

상기 신경망 모델은,

순환 신경망 모델(Recurrent Neural Network) 구조이고, 문법의 기초가 되는 품사를 구분하기 위한 조건부 무작위장(Conditional Random Field) 모델 및 개체명 인식(Named Entitiy Recognition) 모델을 포함하는 것을 특징으로 하는, 방법.

청구항 2

제1항에 있어서, 상기 방법은

상기 개인 정보가 노출되었는지 여부에 대한 시각 컨텐츠를 생성하는 단계; 및

상기 생성된 시각 컨텐츠를 상기 전자 장치의 화면상에 표시하는 단계; 를 포함하는, 방법.

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

제1항에 있어서, 상기 개인 정보가 노출되었는지 여부를 식별하는 단계는

상기 PCAP 파일을 상기 신경망 모델에 입력하는 단계; 및

상기 신경망 모델의 출력 값에 기초하여 상기 전자 장치의 사용자에 대한 상기 개인 정보가 노출되었는지 여부를 식별하는 단계; 를 포함하는, 방법.

청구항 7

개인정보 노출 여부를 결정하는 전자 장치에 있어서,

네트워크 인터페이스;

디스플레이;

하나 이상의 인스트럭션을 저장하는 메모리; 및

상기 하나 이상의 인스트럭션을 실행하는 적어도 하나의 프로세서; 를 포함하고,

상기 적어도 하나의 프로세서는 상기 하나 이상의 인스트럭션을 실행함으로써,

상기 전자 장치와 연결된 서버로 CDM(Common Data Model) 데이터를 쿼리 결과로써 요청하기 위한 CDM 쿼리를 전송하고,

상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 HTTPS를 통해 상기 서버에 접속하고, 상기 접속된 서버로부터 전송되는 패킷을 획득하고,

상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별하고,

상기 적어도 하나의 프로세서는,

WIRE SHARK를 응용한 ALTO 시스템을 이용해, 상기 획득된 패킷 내 데이터를 PCAP 파일로 저장하고,

상기 신경망 모델은,

순환 신경망 모델(Recurrent Neural Network) 구조이고, 문법의 기초가 되는 품사를 구분하기 위한 조건부 무작위장(Conditional Random Field) 모델 및 개체명 인식(Named Entitiy Recognition) 모델을 포함하는 것을 특징으로 하는, 전자 장치.

청구항 8

제7항에 있어서, 상기 적어도 하나의 프로세서는

상기 하나 이상의 인스트럭션을 실행함으로써,

상기 개인 정보가 노출되었는지 여부에 대한 시각 컨텐츠를 생성하고

상기 생성된 시각 컨텐츠를 상기 전자 장치의 화면상에 표시하는, 전자 장치.

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

제7항에 있어서, 상기 적어도 하나의 프로세서는

상기 PCAP 파일을 상기 신경망 모델에 입력하고,

상기 신경망 모델의 출력 값에 기초하여 상기 전자 장치의 사용자에 대한 상기 개인 정보가 노출되었는지 여부를 식별하는, 전자 장치.

청구항 13

전자 장치가 개인정보 노출 여부를 결정하는 방법에 있어서,

상기 전자 장치와 연결된 서버로 CDM(Common Data Model) 데이터를 쿼리 결과로써 요청하기 위한 CDM 쿼리를 전송하는 단계;

상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 HTTPS를 통해 상기 서버에 접속하고, 상기 접속

된 서버로부터 전송되는 패킷을 획득하는 단계; 및

상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별하는 단계; 를 포함하고,

상기 패킷을 획득하는 단계는,

WIRE SHARK를 응용한 ALTO 시스템을 이용해, 상기 획득된 패킷 내 데이터를 PCAP 파일로 저장하는 단계를 포함하며,

상기 신경망 모델은,

순환 신경망 모델(Recurrent Neural Network) 구조이고, 문법의 기초가 되는 품사를 구분하기 위한 조건부 무작위장(Conditional Random Field) 모델 및 개체명 인식(Named Entitiy Recognition) 모델을 포함하는 것을 특징으로 하는, 방법을 수행하도록 하는 프로그램이 저장된 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 개시는 개인 정보 노출 여부를 결정하는 방법 및 장치에 관한 것이다. 보다 상세하게는 CMD 쿼리 결과 내 패킷을 이용하여 개인 정보 노출 여부를 결정하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 개인정보 노출을 분석할 때 가장 중요한 것은 문서 내 개인정보의 유무를 확인하는데 있다. 기존 개인 정보를 판별하는 방법 중 하나로 정규식(Regular expression)을 많이 활용하였으나, 개인 정보의 다형성을 판단할 수 없다는 한계가 있다.

[0003] 예를 들어, 대한민국의 주소를 정규식으로 표현하기 위해서 하기 수학식 1과 같은 정규식이 필요할 수 있다.

수학식 1

[0004] ***/(([가-힣A-Za-z·₩d~₩-₩.]{2,}(로|길).[₩d]+)|([가-힣A-Za-z·₩d~₩-₩.]+(읍|동)₩s)[₩d]+)/***

[0005] 그러나, 상기 수학식 1과 같은 정규식은 실제 주소가 아닌 다른 일반 단어도 주소로 판별하거나, 실제 주소이지만 형태가 조금 다른 주소의 경우에 주소로 판별하지 못하는 한계가 있다. 상술한 예와 마찬가지로, 개인 정보 또한 다양한 형태를 가지고 있기 때문에 정규식으로 개인 정보를 구분하는 데는 한계가 있다.

[0006] 따라서, 다양한 형태의 개인 정보를 식별하고, 개인 정보 노출 여부를 검출할 수 있는 기술 개발이 요구되고 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국등록특허 제2101456호

발명의 내용

해결하려는 과제

[0008] 일 실시 예에 따르면, 개인정보 노출 여부를 결정하는 방법 및 이를 수행하는 전자 장치가 제공될 수 있다.

[0009] 일 실시 예에 의하면, 신경망 모델을 이용하여 개인정보 노출 여부를 결정하는 방법 및 이를 수행하는 전자 장치가 제공될 수 있다.

과제의 해결 수단

[0010] 상술한 기술적 과제를 달성하기 위한 본 개시의 일 실시 예에 따라, 전자 장치가 개인 정보 노출 여부를 결정하는 방법은 상기 전자 장치와 연결된 서버로 쿼리를 전송하는 단계; 상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 상기 서버로부터 전송되는 패킷을 획득하는 단계; 및 상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별하는 단계; 를 포함할 수 있다.

[0011] 상술한 기술적 과제를 달성하기 위한 또 다른 실시 예에 의하면, 개인정보 노출 여부를 결정하는 전자 장치는 네트워크 인터페이스; 디스플레이; 하나 이상의 인스트럭션을 저장하는 메모리; 및 상기 하나 이상의 인스트럭션을 실행하는 적어도 하나의 프로세서; 를 포함하고, 상기 적어도 하나의 프로세서는 상기 하나 이상의 인스트럭션을 실행함으로써, 상기 전자 장치와 연결된 서버로 쿼리를 전송하고, 상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 상기 서버로부터 전송되는 패킷을 획득하고, 상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별하는, 전자 장치가 제공될 수 있다.

[0012] 또한, 상술한 기술적 과제를 달성하기 위한 또 다른 실시 예에 따라 전자 장치가 개인정보 노출 여부를 결정하는 방법에 있어서, 상기 전자 장치와 연결된 서버로 쿼리를 전송하는 단계; 상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 상기 서버로부터 전송되는 패킷을 획득하는 단계; 및 상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별하는 단계; 를 포함하는, 방법을 수행하도록 하는 프로그램이 저장된 컴퓨터로 읽을 수 있는 기록매체가 제공될 수 있다.

도면의 간단한 설명

[0013] 도 1은 일 실시 예에 따른 전자 장치가 개인 정보 노출을 검사하는 과정을 개략적으로 설명하기 위한 도면이다.

도 2는 일 실시 예에 따른 전자 장치가 개인 정보 노출을 결정하는 방법의 흐름도이다.

도 3은 일 실시 예에 따른 전자 장치가 서버로부터 패킷을 획득하는 방법의 흐름도이다.

도 4는 일 실시 예에 따른 전자 장치가 신경망 모델을 이용하여 쿼리를 학습하는 과정을 설명하기 위한 도면이다.

도 5는 일 실시 예에 따른 전자 장치의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 명세서에서 사용되는 용어에 대해 간략히 설명하고, 본 개시에 대해 구체적으로 설명하기로 한다.

[0015] 본 개시에서 사용되는 용어는 본 개시에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0016] 명세서 전체에서 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에 기재된 "...부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0017] 아래에서는 첨부한 도면을 참고하여 본 개시의 실시예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 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.

[0018] 도 1은 일 실시 예에 따른 전자 장치가 개인 정보 노출을 검사하는 과정을 개략적으로 설명하기 위한 도면이다.

[0019] 일 실시 예에 의하면, 개인 정보 검출 시스템(100)은 전자 장치(1000) 및 서버(2000)를 포함할 수도 있다. 일 실시 예에 의하면, 개인 정보 검출 시스템(100)은 전자 장치(1000) 및 서버(2000)사이에 송수신되는 패킷을 분석함으로써, 전자 장치(1000)의 사용자의 개인 정보 노출 여부 또는 서버의 전체적인 보안 위험을 검출할 수 있다.

[0020] 일 실시 예에 의하면, 전자 장치(1000)는 서버(2000)로 CDM 쿼리(162)를 전송하고, 전송된 쿼리(162)에 응답하여 CDM 쿼리 결과(164)를 획득할 수 있다. 일 실시 예에 의하면, CDM(Common Data Model)은 공통 데이터 모델로써 서로 다른 구조의 데이터를 활용하기 쉽게 표준화한 데이터 구조를 의미할 수 있다. 일 실시 예에 의하면, 전자 장치(1000) 또는 서버(2000) 중 적어도 하나가 관리하는 쿼리 및 쿼리에 대한 결과와 관련된 데이터들은 공통 데이터 모델 구조로 관리될 수 있다.

[0021] 일 실시 예에 의하면, 전자 장치(1000)는 서버(2000)로부터 획득되는 패킷을 분석함으로써, 패킷 내의 개인 정보가 노출되었는지 여부를 결정할 수 있다. 일 실시 예에 의하면, 전자 장치(1000)는 패킷 분석의 대표적인 오픈 소스인 ALTO(WIRE SHARK)를 이용하여 패킷을 분석할 수 있다. 또한, 전자 장치(1000)는 WIRE SHARK 를 응용한 ALTO 시스템과 연동하여 패킷의 전반적인 분석 과정을 수행할 수도 있다. 일 실시 예에 의하면, ALTO 시스템은 패킷 분석뿐만 아니라, 서버(2000)의 전체적인 보안 위험을 검출하는데 사용될 수도 있다. 일 실시 예에 의하면, 전자 장치(1000)는 개인 정보 토출 검사 결과, 또는 노출 위험에 대한 정보등을 시각적인 컨텐츠로 생성하고, 생성된 컨텐츠를 출력할 수도 있다.

[0022] 일 실시 예에 의하면, 전자 장치(1000)는 패킷 분석 결과에 대한 정보를, 신경망 모델에 입력함으로써 개인 정보 노출 여부를 식별할 수 있다. 일 실시 예에 의하면 전자 장치는 RNN 구조의 개체명 인식(NER) 모델에 패킷 분석 결과를 입력함으로써, 패킷 내 개인 정보 노출 여부를 결정할 수도 있다. 일 실시 예에 의하면 RNN으로 구성된 개체 인식 모델은 품사 판별기 (CRF)를 통하여, 구분되는 품사에 기초하여 학습될 수도 있다. 일 실시 예에 의하면 품사 판별기(CRF) 모델은 국립 국어원에서 제공되는 세종 말뭉치에 기초하여 학습될 수 있다.

[0023] 일 실시 예에 의하면, 전자 장치(1000)는 프로세서(110), 메모리(120) 및 네트워크 인터페이스(130)를 포함할 수 있다. 프로세서(110)는 메모리(120)내 하나 이상의 인스트럭션을 수행함으로써, 패킷 내 개인 정보가 노출되었는지 여부를 결정하는 방법을 수행할 수 있다. 일 실시 예에 의하면, 메모리(120)는 인공 지능 학습 알고리즘에 따라 학습될 수 있는 복수의 인공 지능 모델을 포함할 수 있다. 네트워크 인터페이스(130)는 서버(2000)와의 사이에 또는 개인 정보 검출 시스템 외의 기타 시스템과의 사이에 데이터, 패킷, 쿼리, 쿼리 결과를 송수신할 수 있다.

[0024] 일 실시 예에 의하면, 메모리(120)는 RNN(Recurrent Neural Network) 모델(122), 조건부 무작위장 모델(Conditional Random Field)(124), 개체명 인식 모델(Name Entity Recognition)(126) 모델을 포함할 수 있다. 일 실시 예에 의하면, 조건부 무작위장 모델(CRF)(126)은 신경망 모델로 구성됨으로써, 통계적 모델링 방법에 따라 스트링(STRING) 형식의 문장으로부터 품사를 식별할 수 있다. 일 실시 예에 의하면, 조건부 무작위장 모델(126)은 (단어, 품사), (단어, 품사) 형식으로 문장을 구성하는 단어와 품사를 식별할 수 있다. 일 실시 예에 의하면 조건부 무작위장 모델(126)은 시퀀셜 라벨링을 위해 POTENTIAL FUNCTION을 이용하넌 SOFT MAX REGRESSION일 수 있다.

[0025] 일 실시 예에 의하면, 개체명 인식 모델(126)은 RNN으로 구성되는 모델로써, 정규화된 개인 정보뿐만 아니라, 개인 정보로 판별될 수 있는 단어들을 유추하여 구분할 수 있다. 일 실시 예에 의하면 개체 인식 모델은 기계학습의 한 분류인 NLP, 자연어처리 기술에 사용될 수 있다. 개체명 인식 모델은 미리 정의된 사람, 회사, 장소, 시간 단위 등에 해당하는 단어(개체명)를 문서에서 추출하여 인식하는데 사용될 수 있다.

[0026] 또 다른 실시 예에 의하면, 전자 장치(1000)가 이용하는 인공 신경망(Artificial Neural Network)은 생물학적 신경망에 착안된 컴퓨팅 시스템을 지칭할 수 있다. 인공 신경망은 미리 정의된 조건에 따라 작업을 수행하는 고전적인 알고리즘과 달리, 다수의 샘플들을 고려함으로써 작업을 수행하는 것을 학습할 수 있다. 인공 신경망은 인공 뉴런(neuron)들이 연결된 구조를 가질 수 있고, 뉴런들 간의 연결은 시냅스(synapse)로 지칭될 수 있다. 뉴런은 수신된 신호를 처리할 수 있고, 처리된 신호를 시냅스를 통해서 다른 뉴런에 전송할 수 있다. 뉴런의 출력은 액티베이션(activation)으로 지칭될 수 있고, 뉴런 및/또는 시냅스는 변동될 수 있는 가중치(weight)를 가질 수 있고, 가중치에 따라 뉴런에 의해 처리된 신호의 영향력이 증가하거나 감소할 수 있다.

[0027] 예를 들어, 인공 신경망은 복수의 신경망 레이어들로 구성될 수 있다. 복수의 신경망 레이어들 각각은 복수의 가중치들(weight values, weights)을 갖고 있으며, 이전(previous) 레이어의 연산 결과와 복수의 가중치들 간의

연산을 통해 신경망 연산을 수행한다. 복수의 신경망 레이어들이 갖고 있는 복수의 가중치들은 인공 신경망의 학습 결과에 의해 최적화될 수 있다.

[0028] 예를 들어, 학습 과정 동안 인공지능 모델에서 획득한 손실(loss) 값 또는 코스트(cost) 값이 감소 또는 최소화되도록 복수의 가중치들이 수정 및 갱신될 수 있다. 본 개시에 따른 인공 신경망은 심층 신경망(DNN:Deep Neural Network)을 포함할 수 있으며, 예를 들어, CNN (Convolutional Neural Network), DNN (Deep Neural Network), RNN (Recurrent Neural Network), RBM (Restricted Boltzmann Machine), DBN (Deep Belief Network), BRDNN(Bidirectional Recurrent Deep Neural Network) 또는 심층 Q-네트워크 (Deep Q-Networks) 등이 있으나, 전술한 예에 한정되지 않는다.

[0029] 일 실시 예에 의하면, 전자 장치(1000)는 서버(2000)와 연동함으로써 쿼리 및 쿼리에 대한 결과를 송수신하며, 쿼리 결과로써 패킷 내 개인 정보 노출 여부를 검사할 수도 있다. 일 실시 예에 의하면, 서버(2000)는 프로세서(140), 데이터 베이스(150) 및 네트워크 인터페이스(160)를 포함할 수 있다. 프로세서(140)는 데이터 베이스(150)내 하나 이상의 인스트럭션을 실행함으로써, 서버(2000)로 하여금, 전자 장치와 연동하여 패킷 내 개인 정보를 분석하도록 할 수 있다. 일 실시 예에 의하면, 네트워크 인터페이스(160)는 전자 장치(1000)와의 사이에 또는 기타 개인 정보 노출 여부를 검사하기 위한 시스템 과의 사이에 데이터, 패킷, 쿼리, 쿼리 결과를 송수신할 수 있다.

[0030] 일 실시 예에 의하면, 프로세서(140)는 전자 장치(1000)로부터 CDM 쿼리(162)를 획득하고, 획득된 쿼리에 응답하여 쿼리 결과(164)를 전자 장치(1000)로 전송할 수도 있다. 일 실시 예에 의하면 서버(2000)가 전송한 CDM 쿼리 결과로써 패킷은 ALTO 시스템에 의해 분석됨으로써 서버(2000)전체의 보안 위험을 검사하는데 사용될 수도 있다.

[0031] 도 2는 일 실시 예에 따른 전자 장치가 개인 정보 노출을 결정하는 방법의 흐름도이다.

[0032] S210에서, 전자 장치(1000)는 전자 장치(1000)와 연결된 서버(2000)로 쿼리를 전송할 수 있다. 일 실시 예에 의하면, 전자 장치(1000)는 CDM(Common Data Model) 데이터를 쿼리 결과로써 요청하기 위한 CDM 쿼리를 서버로 전송할 수도 있다. S220에서, 전자 장치(1000)는 쿼리에 대한 쿼리 결과로써, 전송된 쿼리에 응답하여 서버로부터 전송되는 패킷을 획득할 수 있다. 일 실시 예에 의하면, 전자 장치(1000)는 HTTPS를 통해 서버로부터 쿼리 결과를 획득할 수도 있다.

[0033] S230에서, 전자 장치(1000)는 획득된 패킷을 신경망 모델에 입력함으로써 패킷 내 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별할 수 있다. 또 다른 실시 예에 의하면, 전자 장치(1000)는 ALTO 시스템을 이용하여 분석된 패킷 분석 결과를 신경망 모델에 입력함으로써, 패킷 내 개인 정보가 노출되었는지 여부를 결정할 수도 있다.

[0034] 또 다른 실시 예에 의하면, 전자 장치(1000)는 개인 정보가 노출되었는지 여부에 대한 정보를 시각 컨텐츠로 생성하고, 생성된 시각 컨텐츠를 전자 장치의 디스플레이 화면상에 표시할 수도 있다. 일 실시 예에 의하면, 전자 장치(1000)는 개인 정보 노출 결과를 시각적 또는 오디오 형태의 컨텐츠로 출력할 수도 있다.

[0035] 도 3은 일 실시 예에 따른 전자 장치가 서버로부터 패킷을 획득하는 방법의 흐름도이다.

[0036] S310에서, 전자 장치(1000)는 HTTPS를 통해 서버(2000)에 접속할 수 있다. S320에서, 전자 장치(1000)는 접속된 서버(2000)를 통하여, 패킷을 획득할 수 있다. 보다 상세하게는, 전자 장치(1000)는 네트워크 인터페이스를 통하여 서버와 연결되고, 연결된 서버로부터 패킷을 획득할 수도 있다. S330에서, 전자 장치(1000)는 WIRE SHARK를 응용한 ALTO 시스템을 이용하여 획득된 패킷 내 데이터를 PCAP 파일로 저장할 수 있다. 전자 장치가 이용하는 와이어 샤크는 자유 및 오픈소스 패킷 분석 프로그램으로써 네트워크 문제, 분석, 소프트웨어 및 통신 프로토콜 개발에 사용될 수 있다. 전자 장치(1000)는 WIRE SHARK를 이용하여 서버로부터 획득된 패킷을 분석하고, 패킷 분석 결과(예컨대 PCAP 파일)를 소정의 신경망 모델에 입력할 수도 있다.

[0037] 도 4는 일 실시 예에 따른 전자 장치가 신경망 모델을 이용하여 쿼리를 학습하는 과정을 설명하기 위한 도면이다.

[0038] 일 실시 예에 의하면, 전자 장치(1000)는 서버로부터 획득된 패킷을 소정의 신경망 구조의 모델에 입력함으로써, 패킷 내 개인 정보 노출 여부를 결정할 수도 있다. 또 다른 실시 예에 의하면, 전자 장치(1000)는 WIRE SHARK를 이용하여 서버로부터 획득된 패킷을 분석하고, 분석 결과에 대한 정보를 소정의 신경망 모델에 입력할 수도 있다. 일 실시 예에 의하면, 신경망 모델은 문법의 기초가되는 품사를 구분하기 위한 조건부 무작

위장 모델 및 개체명 인식 모델을 포함할 수 있다.

[0039] 일반적으로 개인 정보 노출을 분석할 때 문서 내 개인 정보의 유무를 확인하여야 하는데, 기존 개인 정보를 판별하는 방법 중 하나로 정규식(Regular expression)이 많이 활용되었으나, 개인 정보의 다형성을 판단할 수 없다는 한계가 있었다. 그러나, 본 개시에 따른 전자 장치(1000)는 신경망 모델(430)을 이용하여 개체명 인식 모델(420)을 구성하고, 개체명 인식 모델을 이용하여 정규화된 개인 정보뿐만 아니라, 개인 정보로 판별될 수 있는 단어를 유추하여 구분할 수 있다. 따라서, 본 개시에 따른 전자 장치(1000)는 개인 정보로 판별될 수 있는 단어를 유추하여 구분함으로써 정규식의 단점을 보완할 수 있다.

[0040] 또한, 전자 장치(1000)는 정규식의 단점을 보완하기 위해, 신경망 모델(430)로 구성된 조건부 무작위장 모델(410, CRF)을 통해 문법의 기초가 되는 품사를 구분할 수 있다. 한글에 관한 품사 정보를 이용해야만 조건부 무작위장 모델을 학습할 수 있는데, 전자 장치(1000)는 국립 국어원에서 제공하는 세종 말뭉치를 이용하여 조건부 무작위장 모델을 학습시킬 수 있다. 전자 장치(1000)는 학습된 조건부 무작위장 모델을 이용하여 한글에 관한 품사 정보를 식별하고, 식별된 품사 정보에 기초하여 개체명 인식 모델(420)을 학습시킬 수 있다. 전자 장치(1000)는 학습된 개체명 인식 모델을 이용하여 패킷 내 개인 정보로 판별될 수 있는 단어를 효과적으로 구분할 수 있다.

[0041] 일 실시 예에 의하면, 조건부 무작위장 모델(410) 또는 개체명 인식 모델(420)을 구성하는 신경망 모델(430)은 심층 신경망(DNN:Deep Neural Network)을 포함할 수 있으며, 예를 들어, CNN (Convolutional Neural Network), DNN (Deep Neural Network), 순환신경망 RNN (Recurrent Neural Network), RBM (Restricted Boltzmann Machine), DBN (Deep Belief Network), BRDNN(Bidirectional Recurrent Deep Neural Network) 또는 심층 Q-네트워크 (Deep Q-Networks) 등을 포함할 수 있으나, 전술한 예에 한정되지 않는다. 일 실시 예에 의하면 신경망 모델(430)은 복수의 레이어들 및 상기 레이어들의 연결 강도에 관한 가중치(432)를 포함할 수 있다. 신경망 모델(430)은 가중치를 수정 및 갱신함으로써 학습될 수 있다.

[0042] 도 5는 일 실시 예에 따른 전자 장치의 블록도이다.

[0043] 일 실시 예에 의하면, 전자 장치(1000)는 프로세서(1300), 네트워크 인터페이스(1500) 및 메모리(1700)를 포함할 수 있다. 그러나 상술한 예에 한정되는 것은 아니고, 전자 장치(1000)는 출력부(디스플레이, 스피커)를 더 포함할 수도 있다.

[0044] 일 실시 예에 의하면, 전자 장치(1000)는 소정의 신경망 모델을 생성하고, 생성된 신경망 모델을 학습시킬 수 있다. 전자 장치(1000)는 학습된 신경망 모델을 이용하여 서버로부터 패킷을 획득하고, 획득된 패킷 내 개인 정보들이 노출되었는지 여부를 결정할 수 있다.

[0045] 일 실시 예에 의하면, 전자 장치(1000)는 인공 신경망(Artificial Neural Network)을 학습 시키기 위한 학습 데이터를 생성할 수 있다. 일 실시 예에 의하면, 전자 장치(1000)는 생성된 학습 데이터를 이용하여 인공 신경망 내 레이어들 및 레이어들의 연결 강도에 관한 가중치(weight)를 수정 및 갱신함으로써 인공 신경망을 학습시킬 수 있다. 일 실시 예에 의하면, 전자 장치(1000)는 인공 신경망의 가중치를 처리하기 위한, AI 프로그램이 탑재되고 음성 인식 기능을 포함하는 스마트폰, 태블릿 PC, PC, 스마트 TV, 휴대폰, 미디어 플레이어, 서버, 마이크로 서버, 기타 모바일 또는 비모바일 컴퓨팅 장치일 수 있으나, 이에 제한되지 않는다.

[0046] 일 실시 예에 의하면, 프로세서(1300)는 메모리(1700)내 하나 이상의 인스트럭션을 수행함으로써 전자 장치(1000)의 전반적인 동작을 제어한다. 일 실시 예에 의하면, 프로세서(1300)는 메모리(1700)에 저장된 프로그램들을 실행함으로써 도 1 내지 도 4에 기재된 전자 장치(10000)의 기능을 수행할 수 있다. 프로세서(1300)는 하나 또는 복수의 프로세서로 구성될 수 있고, 하나 또는 복수의 프로세서는 CPU, AP, DSP(Digital Signal Processor) 등과 같은 범용 프로세서, GPU와 같은 그래픽 전용 프로세서일 수 있다. 일 실시 예에 의하면, 프로세서(1300)가 범용 프로세서 및 그래픽 전용 프로세서를 포함하는 경우, 각각의 범용 프로세서 및 그래픽 전용 프로세서는 별도의 칩으로 구현될 수도 있다.

[0047] 일 실시 예에 의하면, 프로세서(1300)가 복수의 프로세서 또는 그래픽 전용 프로세서로 구현될 때, 복수의 프로세서 또는 그래픽 전용 프로세서 중 적어도 일부는 전자 장치(1000) 및 전자 장치(1000)와 연결된 다른 전자 장치 또는 서버에 탑재될 수도 있다. 예를 들어, 프로세서(1300)는, 메모리(1700)에 저장된 프로그램들을 실행함으로써, 서버와 연동하여 패킷을 송수신하고, 패킷 내 개인 정보가 노출되었는지 여부를 결정할 수 있다.

[0048] 일 실시 예에 의하면, 프로세서(1300)는 상기 전자 장치와 연결된 서버로 쿼리를 전송하고, 상기 쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 상기 서버로부터 전송되는 패킷을 획득하고, 상기 획득된 패킷을

신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별할 수 있다.

[0049] 일 실시 예에 의하면, 프로세서(1300)는 상기 개인 정보가 노출되었는지 여부에 대한 시각 컨텐츠를 생성하고 상기 생성된 시각 컨텐츠를 상기 전자 장치의 화면상에 표시할 수 있다.

[0050] 일 실시 예에 의하면, 프로세서(1300)는 CDM(Common Data Model) 데이터를 쿼리 결과로써 요청하기 위한 CDM 쿼리를 전송할 수 있다.

[0051] 일 실시 예에 의하면, 프로세서(1300)는 HTTPS를 통해 상기 서버에 접속하고,

[0052] 상기 접속된 서버로부터 패킷을 획득하고, WIRE SHARK를 응용한 ALTO 시스템을 이용해, 상기 획득된 패킷 내 데이터를 PCAP 파일로 저장할 수 있다.

[0053] 일 실시 예에 의하면, 프로세서(1300)는 상기 PCAP 파일을 상기 신경망 모델에 입력하고, 상기 신경망 모델의 출력 값에 기초하여 상기 전자 장치의 사용자에 대한 상기 개인 정보가 노출되었는지 여부를 식별할 수 있다.

[0054] 네트워크 인터페이스(1500)는 전자 장치(1000)가 다른 장치(미도시) 및 서버(2000)와 통신을 하게 하는 하나 이상의 구성요소를 포함할 수 있다. 다른 장치(미도시)는 전자 장치(1000)와 같은 컴퓨팅 장치이거나, 센싱 장치일 수 있으나, 이에 제한되지 않는다. 예를 들어, 네트워크 인터페이스(1500)는 근거리 통신부, 이동 통신부를 포함할 수 있다.

[0055] 근거리 통신부(short-range wireless communication unit) 는, 블루투스 통신부, BLE(Bluetooth Low Energy) 통신부, 근거리 무선 통신부(Near Field Communication unit), WLAN(와이파이) 통신부, 지그비(Zigbee) 통신부, 적외선(IrDA, infrared Data Association) 통신부, WFD(Wi-Fi Direct) 통신부, UWB(ultra wideband) 통신부, 등을 포함할 수 있으나, 이에 한정되는 것은 아니다. 이동 통신부는, 이동 통신망 상에서 기지국, 외부의 단말, 서버 중 적어도 하나와 무선 신호를 송수신한다. 일 실시 예에 의하면, 네트워크 인터페이스(미도시)는 프로세서의 제어에 의하여, 서버로 쿼리 요청, CDM 쿼리 요청, 인공 신경망 내 가중치 값들, 상기 인공 신경망을 학습시키기 위한 학습 데이터등에 대한 요청을 전송하거나, 요청에 응답하여 쿼리 결과, 인공 신경망 학습 데이터, 인공 신경망의 학습 정보등을 수신할 수도 있다.

[0056] 메모리(1700)는, 프로세서(1300)의 처리 및 제어를 위한 프로그램을 저장할 수 있고, 전자 장치(1000)로 입력되거나 전자 장치(1000)로부터 출력되는 데이터를 저장할 수도 있다. 또한, 메모리(1700)는 인공 신경망을 구성하는 레이어들, 레이어들에 포함된 노드들 및 레이어들의 연결 강도에 관한 가중치들에 대한 정보를 저장할 수 있다. 또한, 메모리(1700)는 증강 데이터들을 더 저장할 수도 있다. 또한, 메모리(1700)는 인공 신경망 내 가중치들이 수정 및 갱신될 경우, 수정 및 갱신된 가중치에 관한 정보를 더 저장할 수 있다. 또한, 메모리(1700)는 개체명 인식 모델, 조건부 무작위장 모델, 신경망 모델에 대한 정보를 더 저장할 수도 있다.

[0057] 메모리(1700)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(RAM, Random Access Memory) SRAM(Static Random Access Memory), 롬(ROM, Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

[0058] 일 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 개시를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

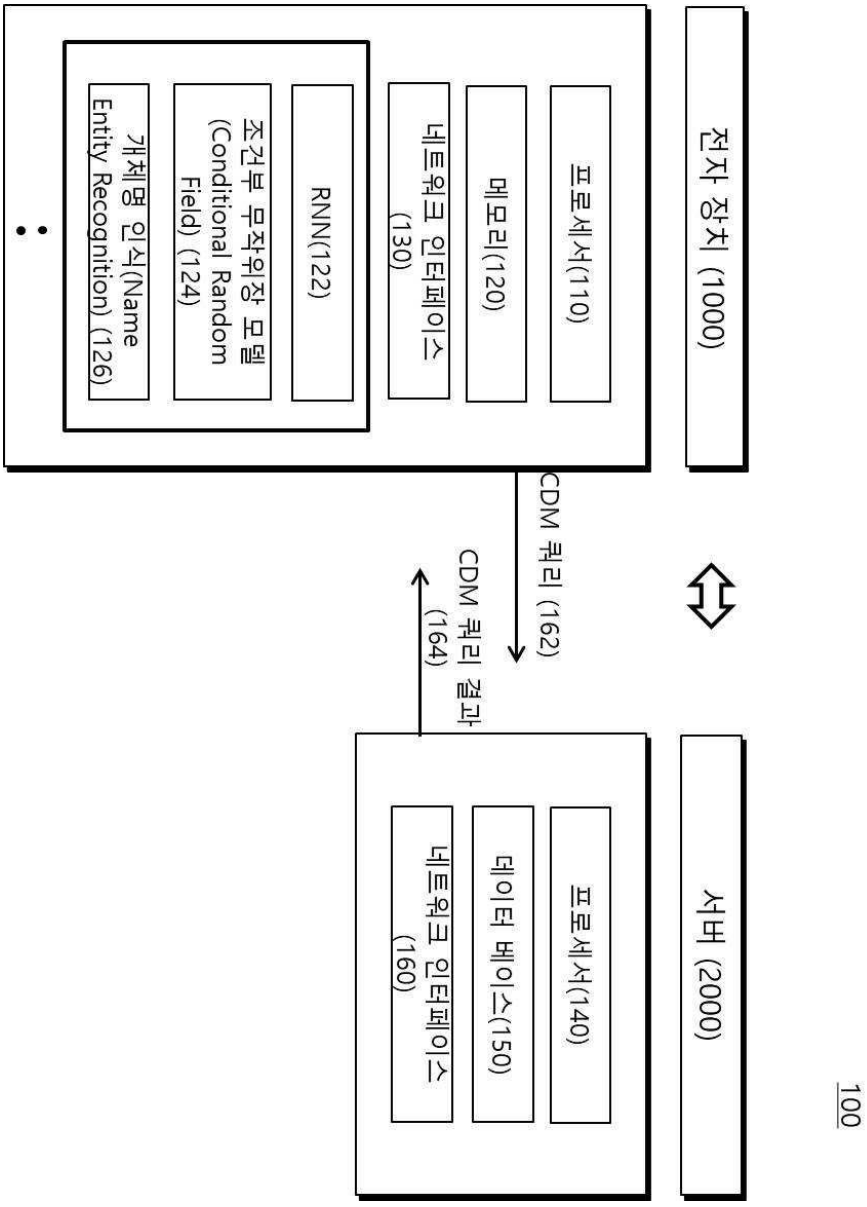
[0059] 또한, 상기 일 실시 예에 다른 방법을 수행하도록 하는 프로그램이 저장된 기록매체를 포함하는 컴퓨터 프로그램 장치가 제공될 수 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0060] 이상에서 본 개시의 실시예에 대하여 상세하게 설명하였지만 본 개시의 권리범위는 이에 한정되는 것은 아니고

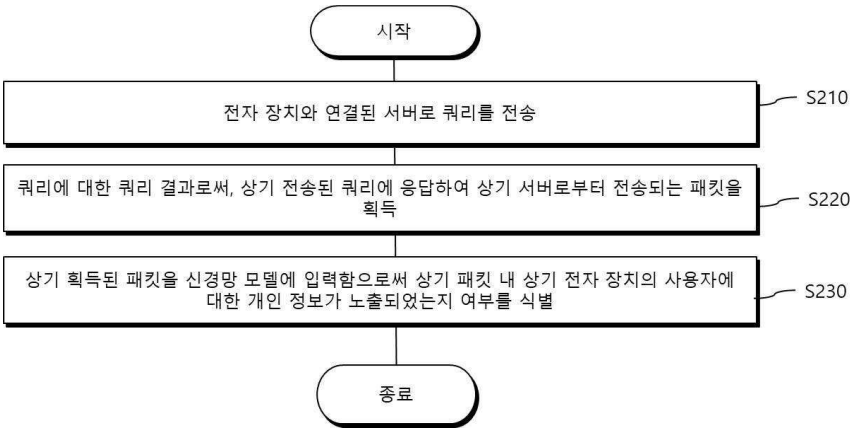
다음의 청구범위에서 정의하고 있는 본 개시의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 개시의 권리범위에 속한다.

도면

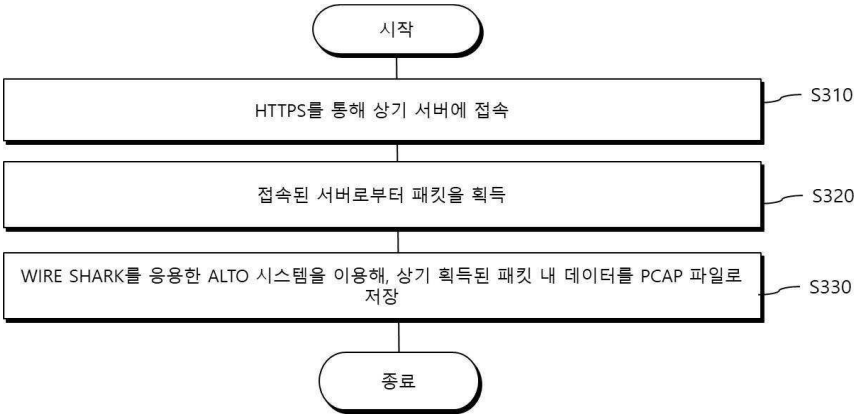
도면1



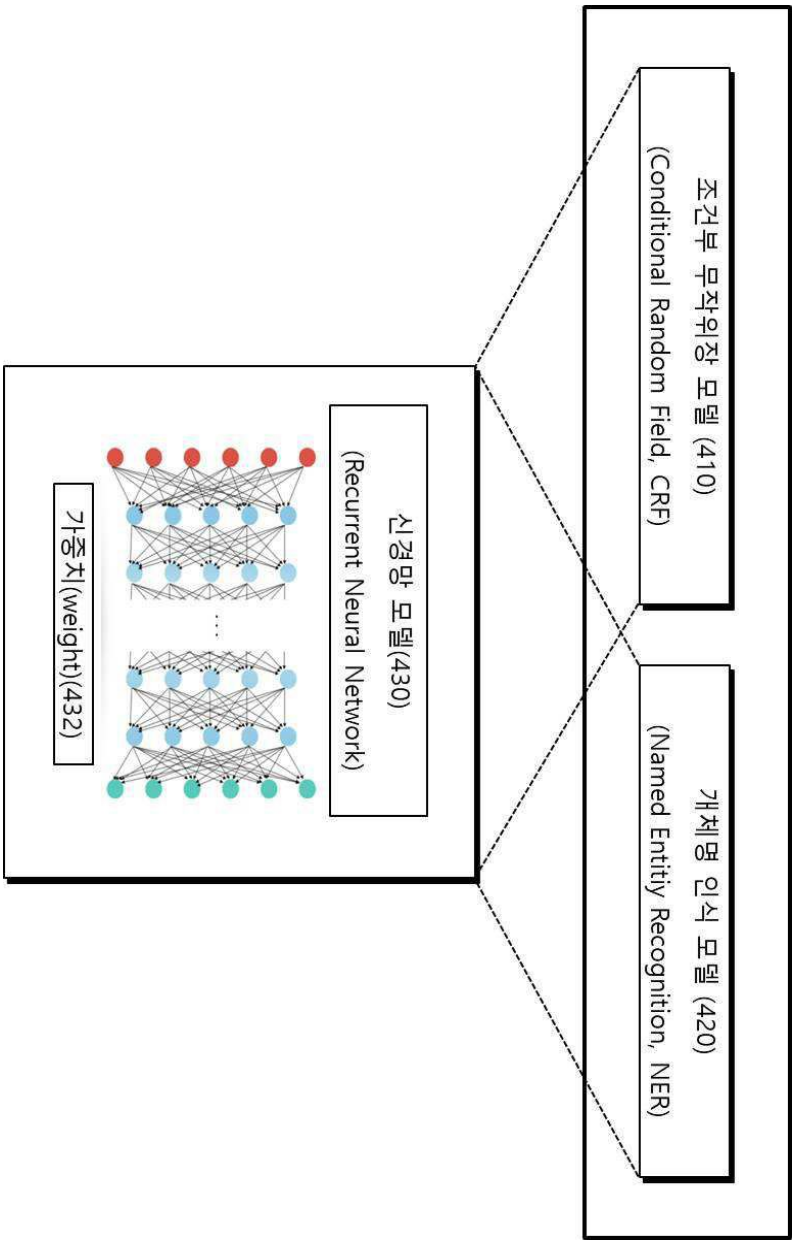
도면2


시작
전자 장치와 연결된 서버로 쿼리를 전송
S210
쿼리에 대한 쿼리 결과로써, 상기 전송된 쿼리에 응답하여 상기 서버로부터 전송되는 패킷을 획득
S220
상기 획득된 패킷을 신경망 모델에 입력함으로써 상기 패킷 내 상기 전자 장치의 사용자에 대한 개인 정보가 노출되었는지 여부를 식별
S230
종료

도면3


시작
HTTPS를 통해 상기 서버에 접속
S310
접속된 서버로부터 패킷을 획득
S320
WIRE SHARK를 응용한 ALTO 시스템을 이용해, 상기 획득된 패킷 내 데이터를 PCAP 파일로 저장
S330
종료

도면4


조건부 무작위장 모델 (410)
(Conditional Random Field, CRF)
개체명 인식 모델 (420)
(Named Entitiy Recognition, NER)
신경망 모델(430)
(Recurrent Neural Network)
가중치(weight)(432)

도면5