(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년12월07일
(11) 등록번호 10-2336384
(24) 등록일자 2021년12월02일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 16/955* (2019.01)
G16Y 40/50 (2020.01)
(52) CPC특허분류
H04L 63/302 (2013.01)
G06F 16/955 (2019.01)
(21) 출원번호 10-2020-0150252
(22) 출원일자 2020년11월11일
심사청구일자 2020년11월11일
(56) 선행기술조사문헌
KR1020080052097 A*
KR1020150054322 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인천대학교 산학협력단
인천광역시 연수구 아카데미로 119 (송도동)
(72) 발명자
전광길
인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웰카운티2단지)
(74) 대리인
특허법인충정

전체 청구항 수 : 총 9 항 심사관 : 홍기완

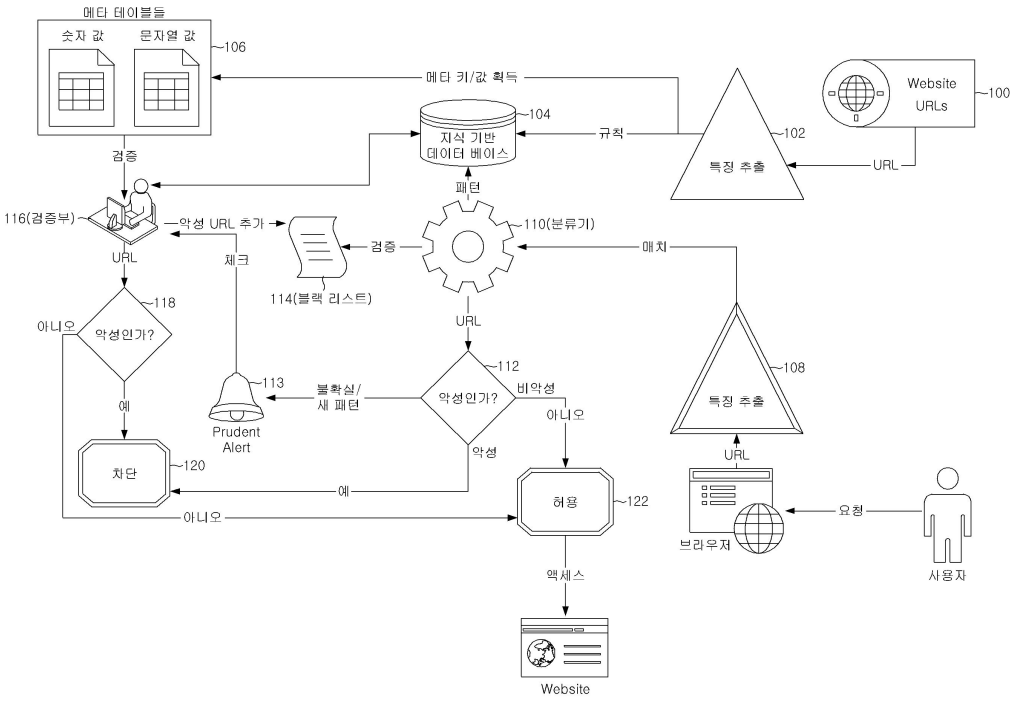
(54) 발명의 명칭 **사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법**

(57) 요 약

본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은, (A) 비악성(NM) URL들에 대한 지식기반 데이터베이스를 구축하는 단계; (B) 상기 비악성(NM) URL들로부터 추출된 특징들을 사용하여 분류기를 학습시키는 단계; (C) 수신되는 URL로부터 특징들을 추출하고 상기 특징들을 사용하여 상기 분류기 및 블랙리스

(뒷면에 계속)

대 표 도



트에 기반하여 상기 수신되는 URL을 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL로 분류하는 단계; (D) 상기 수신되는 URL이 불확실한(U) URL인 것으로 분류된 경우, 상기 지식기반 데이터베이스에 기반하여 상기 수신되는 URL이 악성(M) URL인지 비악성(NM) URL 인지를 검증하는 단계; (E) 상기 수신되는 URL이 악성(M)으로 검증된 경우, 상기 악성으로 검증된 URL을 악성(M) URL로서 상기 블랙리스트에 추가하는 단계; 및 (F) 상기 수신되는 URL이 비악성(NM)으로 검증된 경우, 상기 비악성으로 검증된 URL을 비악성(NM) URL로서 상기 지식기반 데이터베이스에 저장하는 단계를 포함한다.

(52) CPC특허분류
G16Y 40/50 (2020.01)
H04L 63/101 (2013.01)
H04L 63/1441 (2013.01)
H04L 63/308 (2013.01)

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

(A) 비악성(NM) URL들에 대한 지식기반 데이터베이스를 구축하는 단계;

(B) 상기 비악성(NM) URL들로부터 추출된 특징들을 사용하여 분류기를 학습시키는 단계;

(C) 수신되는 URL로부터 특징들을 추출하고 상기 특징들을 사용하여 상기 분류기 및 블랙리스트에 기반하여 상기 수신되는 URL을 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL로 분류하는 단계;

(D) 상기 수신되는 URL이 불확실한(U) URL인 것으로 분류된 경우, 상기 지식기반 데이터베이스에 기반하여 상기 수신되는 URL이 악성(M) URL인지 비악성(NM) URL 인지를 검증하는 단계;

(E) 상기 수신되는 URL이 악성(M)으로 검증된 경우, 상기 악성으로 검증된 URL을 악성(M) URL로서 상기 블랙리스트에 추가하는 단계; 및

(F) 상기 수신되는 URL이 비악성(NM)으로 검증된 경우, 상기 비악성으로 검증된 URL을 비악성(NM) URL로서 상기 지식기반 데이터베이스에 저장하는 단계를 포함하고,

상기 단계 (A)는,

(A-1) 상기 비악성(NM) URL들을 수집하는 단계; 및

(A-2) 상기 수집된 비악성 URL들로부터 특징들을 추출하고, 상기 추출된 특징들에 기반하여 키-값 쌍들 및 키-값 패턴 시퀀스를 획득하여 메타 테이블을 형성하며 상기 메타 테이블을 상기 지식기반 데이터베이스에 저장하는 단계를 포함하는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 단계 (B)는,

상기 비악성 URL들로부터 추출된 특징들을 사용하여 상기 분류기를 학습시켜 비악성 URL 또는 악성 URL을 분류하기 위한 분류 모델을 생성하는 단계를 포함하고,

상기 단계 (C)는,

수신되는 URL로부터 특징들을 추출하고 상기 특징들을 사용하여 상기 분류 모델 및 상기 블랙리스트에 기반하여 상기 수신되는 URL을 악성(M) URL, 비악성(NM) URL또는 불확실한(U) URL로 분류하는 단계를 포함하는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 4

청구항 3에 있어서,

상기 단계 (C) 다음에,

(G) 상기 분류 결과가 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL 인지를 판별하는 단계;

(H) 상기 URL이 악성(M) URL인 것으로 판별된 경우, 상기 URL을 차단하는 단계; 및

(I) 상기 URL이 비악성(NM) URL인 것으로 판별된 경우, 상기 URL을 허용하는 단계를 더 포함하고,

상기 단계 (D) 다음에, (J) 상기 검증 결과가 악성(M) 또는 비악성(NM) 인지를 판별하는 단계를 더 포함하는

것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 5

청구항 1에 있어서,

상기 단계 (D)는,

(D-1) 상기 수신되는 URL의 쿼리 경로(query path)로부터 키-값 쌍들 및 키-값 패턴 시퀀스 순서를 획득하는 단계;

(D-2) 상기 URL의 키 및 값들이 상기 지식기반 데이터베이스의 메타 테이블의 경계 내에 있고 동일한 시퀀스 순서로 있는지를 판정하는 단계; 및

(D-3) 상기 URL의 키 및 값들이 상기 지식기반 데이터베이스의 메타 테이블의 경계 내에 있고 동일한 시퀀스 순서로 있는 경우, 상기 수신되는 URL을 비악성(NM) URL인 것으로 검증하고, 그렇지 않은 경우 상기 수신되는 URL을 악성(M) URL인 것으로 검증하는 단계를 포함하는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 6

청구항 1에 있어서,

상기 단계 (C)는,

(C-1) 상기 수신되는 URL에서 첫번째 슬래시(/) 이전 영역인 도메인 영역을 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴들과 비교하는 단계; 및

(C-2) 상기 수신되는 URL의 도메인 영역이 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴과 일치하고 상기 블랙리스트에 없는 경우 상기 수신되는 URL을 비악성(NM) URL로 분류하고, 상기 수신되는 URL의 도메인 영역이 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴과 일치하지 않고 상기 블랙리스트에 없는 경우 상기 수신되는 URL을 불확실한(U) URL로 분류하며, 그 이외의 경우에는 상기 수신되는 URL을 악성(M) URL로 분류하는 단계를 포함하는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 7

청구항 1에 있어서,

상기 특징들은 프로토콜, 서브도메인, 도메인, 서픽스(suffix), 경로(path), 호스트명(hostname), URL의 쿼리 경로(query path)의 키-값 쌍들을 포함하는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 8

청구항 1에 있어서,

상기 메타 테이블은 상기 URL의 쿼리 부분(query part)을 명시하고 문자열 변수를 키(key) 및 값(value)으로 나누는 데이터 구조를 포함하고,

상기 값들은 쿼리 문자열 내의 키(key)의 속성에 의존하는 문자열 또는 숫자를 포함하며,

상기 메타 테이블은 숫자 값 테이블(NVTs: numerical value tables) 및 문자열 값 테이블(SVTs: string value tables)을 포함하는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 9

청구항 8에 있어서,

상기 숫자 값 테이블(NVTs)은 시퀀스 번호 필드, 키(key) 필드, 최소값 필드 및 최대값 필드를 포함하고,

상기 시퀀스 번호 필드는 상기 URL의 쿼리 부분으로부터 추출된 모든 키들(keys)의 시퀀스를 나타내고,

상기 키(key) 필드는 상기 URL로부터 추출된 모든 키의 타이틀(key's title)을 나타내며,

상기 최소값 필드는 특정 시퀀스 번호의 각 키-값 쌍의 최소 값을 나타내고,

상기 최대값 필드는 특정 시퀀스 번호의 모든 키-값 쌍의 최대 값을 나타내며,

상기 문자열 값 테이블(SVTs)은 시퀀스 번호 필드, 키(key) 필드 및 값 목록 필드를 포함하고,

상기 시퀀스 번호 필드는 상기 URL의 쿼리 부분으로부터 추출된 모든 키들(keys)의 시퀀스를 나타내고,

상기 키(key) 필드는 상기 URL로부터 추출된 모든 키의 타이틀(key's title)을 나타내며,

상기 값 목록 필드는 문자열 값들의 목록을 나타내는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

청구항 10

청구항 1에 있어서,

상기 분류기는 나이브 베이즈(Naive Bayes) 분류기를 포함하는 것을 특징으로 하는 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 관한 것이다.

배 경 기 술

[0002] 오늘날, 사물인터넷(IoT: Internet of Things) 디바이스가 확산되고 있고, 가트너의 연구에 따르면, 2020년까지 거의 204억개의 IoT 디바이스들이 사용될 예정이라고 한다.

[0003] 공유 IoT 네트워크의 일부 디바이스가 URL을 기반으로 하기 때문에, 이러한 IoT 디바이스의 확산으로 인해 일반 사용자가 악성 URL(uniform resource locator)을 통해 다양한 유형의 보안 공격의 피해자가 되게 하는 보안 취약성이 증가하고 있다.

[0004] URL은 공유 IoT 네트워크에서 특정 리소스를 찾고 액세스하는 데 사용되는 프로토콜에 의해 형성된다. 악성 URL은 스캠(scam), 악성 코드(malware), 스팸, 피싱 등과 같은 수많은 악성 활동을 지원한다. 악성 URL 공격으로 인해 개인 자격 증명 손실, 재정적 손해, 데이터 도난, 온라인 뱅킹, 전자 상거래 및 소셜 네트워크 사용과 같은 온라인 비즈니스에 대한 사용자 신뢰 상실을 포함한 높은 위험이 발생하는 것으로 관찰되었다.

[0005] 악성 URL을 통한 피싱 공격 및 스팸 공격으로 인하여 수많은 사용자가 피해을 보고 있다. 위의 우려 사항에 비추어 악성 URL 공격을 식별하기 위한 몇 가지 접근 방식이 개발되었다.

[0006] 이러한 접근 방식은 1) 블랙리스트 기반 접근 방식과 2) 머신 러닝(ML) 기반 접근 방식의 두 가지 주요 유형으로 분류할 수 있다. 전통적으로 블랙리스트 접근 방식은 가장 널리 사용되는 악성 URL 탐지 방법이며 일반적으로 최신 웹 브라우저의 도구 모음에 설치된다. 블랙리스트 기반 접근 방식은 안티 바이러스 그룹 또는 네트워크 보안 팀이 확인한 알려진 악성 URL 목록을 유지한다. 이러한 차단된 URL들은 종종 피시탱크(PhishTank) 및 스푸프가드(SpoofGuard)와 같은 크라우드 소싱 시스템을 통해 수집된다. 블랙리스트에 있는 URL 탐지 접근 방식은 단순한 데이터베이스 매칭 메커니즘으로 인해 빠르며 일반적으로 최소 FP(false positive) 비율을 가질 것으로 예상된다. 가장 큰 단점은 완전하지 않고 블랙리스트가 항상 최신 상태로 유지되는 것이 거의 비현실적이라는 것이다.

[0007] 따라서 이 접근 방식은 새로 생성된 악성 URL에 대해 실패한다. 이러한 한계를 해결하기 위해 수많은 연구에서 다양한 ML 기반 접근 방식을 조사했다. 일반적으로 악성 URL 탐지를 위한 ML 기반 접근 방식은 두 단계로 구성된다. 첫 번째는 어휘 및 호스트 기반 특징 선택을 획득하는 것이고 두 번째는 이러한 특징을 사용하여 악성 URL을 탐지하는 예측 모델을 훈련시키는 것이다.

[0008] 기존 접근 방식은 ML 알고리즘을 사용하여 악성 URL의 분류 및 탐지에 대해 우수한 성능 결과를 보였지만 실제로 이러한 접근 방식에는 다음과 같은 한계가 있다.

[0009] 1) 대부분 Bag-of-Words(BOW) 특징에 의존하여, URL에 특정 단어의 존재에 대한 도움만 제공한다. 2) URL의 문

자열에 있는 문자의 순서를 효과적으로 추적할 수 없다. 3) 일반적으로 도메인 전문가가 URL에서 특정 특징의 중요성을 결정해야 하는 광범위한 수동 특징 엔지니어링이 필요하므로 사람의 개입이 필요하다. 4) 새로운 단어(보이지 않는 특징)를 효율적으로 감지하지 못한다. 그리고 5) 성공적인 지식기반 시스템(KBS: knowledge-based system)을 개발하려면 인간 전문가가 필요하기 때문에 지식기반 시스템을 이용하여 악성 URL을 탐지하는 데 덜 집중한다. 따라서, 악성 URL을 효율적으로 탐지하기 위해서는 앞서 언급한 한계를 극복할 수 있는 기술이 필요하다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) KR 10-1398740 B1

발명의 내용

해결하려는 과제

[0011] 본 발명이 해결하고자 하는 과제는 사물인터넷(IoT)상에서 악성 URL을 자동으로 그리고 효율적으로 정확하게 탐지하기 위한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법을 제공하는 것이다.

과제의 해결 수단

[0012] 상기 과제를 해결하기 위한 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은,

[0013] (A) 비악성(NM) URL들에 대한 지식기반 데이터베이스를 구축하는 단계;

[0014] (B) 상기 비악성(NM) URL들로부터 추출된 특징들을 사용하여 분류기를 학습시키는 단계;

[0015] (C) 수신되는 URL로부터 특징들을 추출하고 상기 특징들을 사용하여 상기 분류기 및 블랙리스트에 기반하여 상기 수신되는 URL을 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL로 분류하는 단계;

[0016] (D) 상기 수신되는 URL이 불확실한(U) URL인 것으로 분류된 경우, 상기 지식기반 데이터베이스에 기반하여 상기 수신되는 URL이 악성(M) URL인지 비악성(NM) URL 인지를 검증하는 단계;

[0017] (E) 상기 수신되는 URL이 악성(M)으로 검증된 경우, 상기 악성으로 검증된 URL을 악성(M) URL로서 상기 블랙리스트에 추가하는 단계; 및

[0018] (F) 상기 수신되는 URL이 비악성(NM)으로 검증된 경우, 상기 비악성으로 검증된 URL을 비악성(NM) URL로서 상기 지식기반 데이터베이스에 저장하는 단계를 포함한다.

[0019] 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 단계 (A)는,

[0020] (A-1) 상기 비악성(NM) URL들을 수집하는 단계; 및

[0021] (A-2) 상기 수집된 비악성 URL들로부터 특징들을 추출하고, 상기 추출된 특징들에 기반하여 키-값 쌍들 및 키-값 패턴 시퀀스를 획득하여 메타 테이블을 형성하며 상기 메타 테이블을 상기 지식기반 데이터베이스에 저장하는 단계를 포함할 수 있다.

[0022] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 단계 (B)는,

[0023] 상기 비악성 URL들로부터 추출된 특징들을 사용하여 상기 분류기를 학습시켜 비악성 URL 또는 악성 URL을 분류하기 위한 분류 모델을 생성하는 단계를 포함하고,

[0024] 상기 단계 (C)는,

[0025] 수신되는 URL로부터 특징들을 추출하고 상기 특징들을 사용하여 상기 분류 모델 및 상기 블랙리스트에 기반하여 상기 수신되는 URL을 악성(M) URL, 비악성(NM) URL또는 불확실한(U) URL로 분류하는 단계를 포함할 수 있다.

[0026] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은, 상기 단계 (C) 다음에,

[0027] (G) 상기 분류 결과가 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL 인지를 판별하는 단계;

[0028] (H) 상기 URL이 악성(M) URL인 것으로 판별된 경우, 상기 URL을 차단하는 단계; 및

[0029] (I) 상기 URL이 비악성(NM) URL인 것으로 판별된 경우, 상기 URL을 허용하는 단계를 더 포함하고,

[0030] 상기 단계 (D) 다음에, (J) 상기 검증 결과가 악성(M) 또는 비악성(NM) 인지를 판별하는 단계를 더 포함할 수 있다.

[0031] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 단계 (D)는,

[0032] (D-1) 상기 수신되는 URL의 쿼리 경로(query path)로부터 키-값 쌍들 및 키-값 패턴 시퀀스 순서를 획득하는 단계;

[0033] (D-2) 상기 URL의 키 및 값들이 상기 지식기반 데이터베이스의 메타 테이블의 경계 내에 있고 동일한 시퀀스 순서로 있는지를 판정하는 단계; 및

[0034] (D-3) 상기 URL의 키 및 값들이 상기 지식기반 데이터베이스의 메타 테이블의 경계 내에 있고 동일한 시퀀스 순서로 있는 경우, 상기 수신되는 URL을 비악성(NM) URL인 것으로 검증하고, 그렇지 않은 경우 상기 수신되는 URL을 악성(M) URL인 것으로 검증하는 단계를 포함할 수 있다.

[0035] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 단계 (C)는,

[0036] (C-1) 상기 수신되는 URL에서 첫번째 슬래시(/) 이전 영역인 도메인 영역을 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴들과 비교하는 단계; 및

[0037] (C-2) 상기 수신되는 URL의 도메인 영역이 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴과 일치하고 상기 블랙리스트에 없는 경우 상기 수신되는 URL을 비악성(NM) URL로 분류하고, 상기 수신되는 URL의 도메인 영역이 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴과 일치하지 않고 상기 블랙리스트에 없는 경우 상기 수신되는 URL을 불확실한(U) URL로 분류하며, 그 이외의 경우에는 상기 수신되는 URL을 악성(M) URL로 분류하는 단계를 포함할 수 있다.

[0038] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 특징들은 프로토콜, 서브도메인, 도메인, 서픽스(suffix), 경로(path), 호스트명(hostname), URL의 쿼리 경로(query path)의 키-값 쌍들을 포함할 수 있다.

[0039] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 메타 테이블은 상기 URL의 쿼리 부분(query part)을 명시하고 문자열 변수를 키(key) 및 값(value)으로 나누는 데이터 구조를 포함하고,

[0040] 상기 값들은 쿼리 문자열 내의 키(key)의 속성에 의존하는 문자열 또는 숫자를 포함하며,

[0041] 상기 메타 테이블은 숫자 값 테이블(NVTs: numerical value tables) 및 문자열 값 테이블(SVTs: string value tables)을 포함할 수 있다.

[0042] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 숫자 값 테이블(NVTs)은 시퀀스 번호 필드, 키(key) 필드, 최소값 필드 및 최대값 필드를 포함하고,

[0043] 상기 시퀀스 번호 필드는 상기 URL의 쿼리 부분으로부터 추출된 모든 키들(keys)의 시퀀스를 나타내고,

[0044] 상기 키(key) 필드는 상기 URL로부터 추출된 모든 키의 타이틀(key's title)을 나타내며,

[0045] 상기 최소값 필드는 특정 시퀀스 번호의 각 키-값 쌍의 최소 값을 나타내고,

[0046] 상기 최대값 필드는 특정 시퀀스 번호의 모든 키-값 쌍의 최대 값을 나타내며,

[0047] 상기 문자열 값 테이블(SVTs)은 시퀀스 번호 필드, 키(key) 필드 및 값 목록 필드를 포함하고,

[0048] 상기 시퀀스 번호 필드는 상기 URL의 쿼리 부분으로부터 추출된 모든 키들(keys)의 시퀀스를 나타내고,

[0049] 상기 키(key) 필드는 상기 URL로부터 추출된 모든 키의 타이틀(key's title)을 나타내며,

[0050] 상기 값 목록 필드는 문자열 값들의 목록을 나타낼 수 있다.

[0051] 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 있어서, 상기 분류기는 나이브 베이즈(Naive Bayes) 분류기를 포함할 수 있다.

발명의 효과

[0052] 본 발명의 일 실시예에 의한 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 의하면, 사물인터넷(IoT)상에서 악성 URL을 자동으로 그리고 효율적으로 정확하게 탐지할 수 있다.

도면의 간단한 설명

[0053] 도 1은 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법의 개략도.

도 2는 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법의 흐름도.

도 3은 도 2에 도시된 검증 단계의 상세 흐름도.

도 4는 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법이 수행되는 예시적인 장치를 도시한 도면.

발명을 실시하기 위한 구체적인 내용

[0054] 본 발명의 목적, 특정한 장점들 및 신규한 특징들은 첨부된 도면들과 연관되어지는 이하의 상세한 설명과 바람직한 실시예들로부터 더욱 명백해질 것이다.

[0055] 이에 앞서 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이고 사전적인 의미로 해석되어서는 아니되며, 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있는 원칙에 입각하여 본 발명의 기술적 사상에 부합되는 의미와 개념으로 해석되어야 한다.

[0056] 본 명세서에서 각 도면의 구성요소들에 참조번호를 부가함에 있어서, 동일한 구성 요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 번호를 가지도록 하고 있음에 유의하여야 한다.

[0057] 또한, "제1", "제2", "일면", "타면" 등의 용어는, 하나의 구성요소를 다른 구성요소로부터 구별하기 위해 사용되는 것으로, 구성요소가 상기 용어들에 의해 제한되는 것은 아니다.

[0058] 이하, 본 발명을 설명함에 있어, 본 발명의 요지를 불필요하게 흐릴 수 있는 관련된 공지 기술에 대한 상세한 설명은 생략한다.

[0059] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시형태를 상세히 설명하기로 한다.

[0060] URL(Uniform Resource Locator)은 웹(월드 와이드 웹) 또는 인터넷에서 특정 리소스를 찾는 데 사용되는 식별자 이름이다. URL은 웹에서 사용할 수 있는 리소스에 대한 고유한 문자열 표현을 포함한다. URL은 사용 가능한 웹 리소스에 액세스하는 데 사용되는 프로토콜(예를 들어 HTTP 및 HTTPS)로 구성되며, 도메인, IP 주소 및 리소스 경로의 형태일 수 있다. URL의 일반적인 구조는 <protocol>://[<sub-domain>].<base-domain>.<top-level domain>/<path>와 같이 작성될 수 있다.

[0061] 피싱(phishing), 스푸핑(spoofed), 스캠(scam)과 같은 악의적인 활동에 사용되는 URL은 악성 URL 또는 블랙 URL로 알려져 있다. 이러한 공격은 일반 사용자가 악성 사이트를 방문하도록 유도하는 링크, 이미지, 파일 또는 이메일을 사용자가 클릭하도록 합법적인 것처럼 보이게 한다.

[0062] 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에서는 다음과 같은 설계 목표를 해결한다.

[0063] 1) FP(False Positive) 또는 오류율은 최소가 되어야 궁극적으로 모델의 정확도가 높아진다. 2) 악성 URL의 분류를 지원할 수 있도록 유연해야 한다. 3) 또한 새로 생성된 악성 URL을 탐지하고 그에 따라 자동으로 데이터베이스를 업데이트할 수 있다.

[0064] 도 1은 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법의 개요도이다.

[0065] 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에는 다음과 같은 주요 구성 요소들이 있다. 1) 데이터 세트, 특징 추출 및 분석; 2) 메타 테이블; 3) 지식기반(KB) 데이터베이스 구축 및 분류

프로세스; 4) 신중한 분석; 및 5) 가상 전문가 역할을 하는 검증부.

[0067] **데이터 세트, 특징 추출 및 분석**

[0068] 이 섹션에서는 데이터 준비 및 수집 프로세스를 설명한다. 2017년 8월부터 2018년 3월까지 7개월 동안 다중 사용자 클라이언트 서버 지원 웹 사이트에서 73,322개의 무해한 비악성 URL을 수집하였다.

[0069] 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은 서버 측에서 구현되었으며 대상 웹 사이트 활동을 실시간으로 추적했다. 논의한 바와 같이, 모든 웹 페이지의 URL에서 특징 추출부(102)에 의해 특징들이 추출되었다. 추출된 모든 특징들은 전처리되는데, 전처리 과정에서 값과 함께 추출된 특징들이 키-값 쌍(key-value pairs)으로 변환되고 또한 키-값 패턴 시퀀스(key-value pattern sequence)가 기록된 다음, 지식기반 데이터베이스(104)에 저장된다.

[0070] 지식기반 데이터베이스(104)의 구조는 m×n 행렬이다. 여기서 m은 각 특징의 데이터를 반영하는 튜플(tuple)을 의미하고, n은 행렬에서 상기 특징의 타이틀을 나타내는 열을 나타낸다. 표 1은 획득된 데이터 세트와 추출된 특징들을 나타낸 것이다.

표 1

[0071]

Description	Values
Total URLs	107,586
Total number of benign URLs	73,322
Total number of malicious URLs	34,264
Number of features	34
List of features	Protocol, subdomain, domain, suffix, path, hostname, and key-values pairs of query path in URL. E.g., Key_1=$Value_1$,.....Key_n= $Value_n$
URL's sequence	Path + Query sequence e.g., index.php?key_1=$value_1$..key_n= $value_n$
Class Labels	{M, NM} e.g., M=Malicious and NM= Non Malicious

[0073] **메타 테이블**

[0074] 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에서는 URL에서 메타 데이터를 얻기 위하여 메타 테이블(106)을 형성하였다. 메타 테이블(106)은 기본적으로 각각의 진정한 URL의 쿼리 부분(query part)을 명시하고 모든 쿼리 문자열 변수를 키(key)와 값(values)의 두 부분으로 나누는 데이터 구조이다.

[0075] 값(values)은 쿼리 문자열의 키(key) 속성에 따라 숫자 또는 문자열이 될 수 있다. 따라서 메타 테이블은 숫자값 테이블(NVT: numerical value tables)과 문자열 값 테이블(SVT: string value tables)로 구분된다. NVT는 시퀀스 번호 필드(seq. #), 키 필드(key), 최소값 필드(Min. Val.) 및 최대값 필드(Max. Val.)로 구성된다. SVT는 시퀀스 번호 필드(seq. #), 키 필드(key) 및 값 목록 필드(List of values)로 구성된다. 표 2 및 표 3은 각각 MVT 및 SVT에 대한 메타 데이터 및 구조를 나타낸다.

표 2

[0076]

Fields	Description
Seq. #	This column in the MVT keeps track of the sequence of all the keys extracted from the query part of URL.
Key	It contains all the key's title which are extracted from the URL
Min. Val.	This field contains the minimum value of each key-value pair in a specified sequence number.
Max.Val.	It holds the maximum value of every key-value pair in a specified sequence number.

표 3

[0077]

Fields	Description
Seq. #	This column in the MVT keeps track of the sequence of all the keys extracted from the query part of URL.
Key	It contains all the key's title which are extracted from the URL
List of values	This column contain the list of string values. E.g., key1={string1, string2, …..stringN}, key2={….} etc.

[0079] **지식기반(KB) 데이터베이스 구축 및 분류 프로세스**

[0080] 처음에는 클래스 레이블 NM(비악성 URL)이 수동으로 할당된 웹 사이트에서 합법적인 73,322개의 비악성 URL이 획득되었다. 기준 분류기(110)를 사용하여 NM URL 패턴을 생성하고 지식기반(KB) 데이터베이스(104)를 구축하였다. 지식기반 데이터베이스(104)의 기존 패턴과 일치하지 않는 새로운 패턴이 URL에서 발생할 때마다 이를 악성(M)으로 분류한다.

[0081] 전체 데이터 세트에 대해 동일한 프로세스가 실행된다. 마지막으로 73,322 및 34,264개의 URL이 도 1에 나와있는 모델의 적용을 위해 전처리된 데이터 세트로 결합되었다. 신중한 프롬프트(113)는 비정상적인 URL 패턴을 의미한다. 이러한 비정상적인 URL 패턴이 시스템에 의해 감지될 때마다 항상 신중한 프롬프트(113) 또는 경고를 생성한다. 기본적으로 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법의 신중한 프롬프트(113)는 기존 지식기반의 역량을 넘어서는 새로운 유형의 악성 URL을 쉽게 탐지하기 때문에 새로운 유형의 악성 URL을 쉽게 처리할 수 있다.

[0082] 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에서는 신중한 프롬프트(113)를 생성하는 방법을 개발하였다. 이 방법은 다음 절차를 기반으로 한다. 수신되는 URL이 지식기반 데이터베이스(104)에 저장된 URL 패턴과 일치하지 않을 때마다, 예를 들어 판정부(112)에 의해 URL이 불확실한 새 패턴을 나타내는 경우 신중한 프롬프트(113)가 생성된다. 이 프롬프트(113)는 새로운 유형의 URL 패턴 감지를 검증부(116)에게 알린다.

[0084] **가상 전문가 역할을 하는 검증부**

[0085] URL은 공개적으로 사용 가능하고 다른 출처에서 얻은 잘 알려진 악성 블랙리스트 URL(114)에 기반하여 확인된다. 이 URL이 블랙리스트(114)의 URL과 일치하지 않으면 검증부(116)로 전송된다. 검증부(116)는 인간 전문가의 개입에 필요한 추가 비용과 시간을 피하는 데 도움이 되는 가상 전문가의 역할을 한다.

[0086] 검증부(116)에는 두 개의 메타 데이터 테이블, 즉 NVT 및 SVT가 포함된 메타 테이블이 미리 유지되어 있다. 판정부(112)에 의해 URL이 새로운 패턴을 나타내는 불확실한 URL인 것으로 판정되면, 신중한 프롬프트(113)가 생성되고, 검증부(116)는 최종적으로 공개적으로 사용 가능한 전세계 블랙리스트 URL(114)에 존재하지 않는 불확실한 URL이 비악성 URL인지 또는 악성 URL인지를 검증한다. 판정부(118)는 검증부(116)의 검증 결과가 악성인지 비악성인지를 판정한다.

[0087] 한편, 판정부(112, 118)에 의해 URL이 악성 URL인 것으로 판정되면 차단부(120)에 의해 URL이 차단되고, 판정부

(112, 118)에 의해 URL이 비악성 URL인 것으로 판정되면 허용부(122)에 의해 URL이 허용된다.

[0088] 도 2는 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법의 흐름도이고, 도 3은 도 2에 도시된 검증 단계의 상세 흐름도이며, 도 4는 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법이 수행되는 예시적인 장치를 도시한 도면이다.

[0089] 도 2에 도시된 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은 도 4에 도시된 장치에 의해 수행될 수 있고, 특히 프로세서(400)에 의해 수행된다. 한편, 도 4에 도시된 데이터 저장부(402)는 프로세서(400)에 의해 처리되는 데이터를 저장하기 위한 것으로, 지식기반 데이터베이스 및 블랙리스트를 포함한다.

[0090] 도 2에 도시된 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은 프로세서(400)에 의해 실행되고, 비악성(NM: nonmalicious) URL들에 대한 지식기반 데이터베이스를 구축하는 단계(S200, S202, S204), 상기 비악성(NM) URL들로부터 추출된 특징들을 사용하여 분류기를 학습시키는 단계(S206), 수신되는 URL로부터 특징들을 추출하고 상기 특징들을 사용하여 상기 분류기 및 블랙리스트에 기반하여 상기 수신되는 URL을 악성(M: malicious) URL, 비악성(NM) URL 또는 불확실한(U: unsure) URL로 분류하는 단계(S208), 상기 분류 결과가 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL 인지를 판별하는 단계(S210), 상기 URL이 악성(M) URL인 것으로 판별된 경우, 상기 URL을 차단하는 단계(S212), 상기 URL이 비악성(NM) URL인 것으로 판별된 경우, 상기 URL을 허용하는 단계(S214), 상기 수신되는 URL이 불확실한(U) URL인 것으로 판별된 경우, 상기 지식기반 데이터베이스에 기반하여 상기 수신되는 URL이 악성(M) URL인지 비악성(NM) URL 인지를 검증하는 단계(S216), 상기 검증 결과가 악성(M) 또는 비악성(NM) 인지를 판별하는 단계(S218), 상기 검증 결과가 악성(M)인 경우, 상기 악성으로 검증된 URL을 악성(M) URL로서 상기 블랙리스트에 추가하는 단계(S220), 및 상기 검증 결과가 비악성(NM)인 경우, 상기 비악성으로 검증된 URL을 비악성(NM) URL로서 상기 지식기반 데이터베이스에 저장하는 단계(S222)를 포함한다.

[0091] 도 2 내지 도 4를 참조하면, 단계 S200에서, 프로세서(400)가, 비악성(NM) URL들을 수집하고, 단계 S202에서, 수집된 비악성 URL들로부터 특징들을 추출한다. 표 1에 기재된 바와 같이, 상기 특징들은 프로토콜, 서브도메인, 도메인, 서픽스(suffix), 경로(path), 호스트명(hostname), URL의 쿼리 경로(query path)의 키-값 쌍들을 포함한다.

[0092] 단계 S204에서, 프로세서(400)가, 추출된 특징들에 기반하여 키-값 쌍들 및 키-값 패턴 시퀀스를 획득하여 메타 테이블을 형성하고 상기 메타 테이블을 지식기반 데이터베이스로서 데이터 저장부(402)에 저장한다.

[0093] 상기 메타 테이블은 상기 URL의 쿼리 부분(query part)을 명시하고 문자열 변수를 키(key) 및 값(value)으로 나누는 데이터 구조를 포함하며, 상기 값들은 쿼리 문자열 내의 키(key)의 속성에 의존하는 문자열 또는 숫자를 포함한다.

[0094] 표 2 및 표 3에 기재된 바와 같이, 상기 메타 테이블은 숫자 값 테이블(NVTs: numerical value tables) 및 문자열 값 테이블(SVTs: string value tables)을 포함한다.

[0095] 표 2에 기재된 바와 같이, 상기 숫자 값 테이블(NVTs)은 시퀀스 번호 필드, 키(key) 필드, 최소값 필드 및 최대값 필드를 포함하고, 상기 시퀀스 번호 필드는 상기 URL의 쿼리 부분으로부터 추출된 모든 키들(keys)의 시퀀스를 나타내고, 상기 키(key) 필드는 상기 URL로부터 추출된 모든 키의 타이틀(key's title)을 나타내며, 상기 최소값 필드는 특정 시퀀스 번호의 각 키-값 쌍의 최소 값을 나타내고, 상기 최대값 필드는 특정 시퀀스 번호의 모든 키-값 쌍의 최대 값을 나타낸다.

[0096] 표 3에 기재된 바와 같이, 상기 문자열 값 테이블(SVTs)은 시퀀스 번호 필드, 키(key) 필드 및 값 목록 필드를 포함하고, 상기 시퀀스 번호 필드는 상기 URL의 쿼리 부분으로부터 추출된 모든 키들(keys)의 시퀀스를 나타내고, 상기 키(key) 필드는 상기 URL로부터 추출된 모든 키의 타이틀(key's title)을 나타내며, 상기 값 목록 필드는 문자열 값들의 목록을 나타낸다.

[0097] 단계 S206에서, 프로세서(400)가, 상기 추출된 특징들을 사용하여 분류기를 학습시켜 비악성 URL 또는 악성 URL을 분류하기 위한 분류 모델을 생성한다. 상기 분류기는 나이브 베이즈(Naive Bayes) 분류기를 포함한다.

[0098] 단계 S208에서, 프로세서(400)가, 수신되는 URL로부터 특징들을 추출하고 상기 특징들을 사용하여 상기 분류 모델 및 상기 블랙리스트에 기반하여 상기 수신되는 URL을 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL로 분류한다.

[0099] 한편, 상기 단계 S208은, 상기 수신되는 URL에서 첫번째 슬래시(/) 이전 영역인 도메인 영역을 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴들과 비교하는 단계 및 상기 수신되는 URL의 도메인 영역이 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴과 일치하고 상기 블랙리스트에 없는 경우 상기 수신되는 URL을 비악성(NM) URL로 분류하고, 상기 수신되는 URL의 도메인 영역이 상기 지식기반 데이터베이스에 저장되어 있는 비악성 URL 패턴과 일치하지 않고 상기 블랙리스트에 없는 경우 상기 수신되는 URL을 불확실한(U) URL로 분류하며, 그 이외의 경우에는 상기 수신되는 URL을 악성(M) URL로 분류하는 단계를 포함한다.

[0100] 단계 S210에서, 상기 분류 결과가 악성(M) URL, 비악성(NM) URL 또는 불확실한(U) URL 인지를 판별하고, 상기 URL이 악성(M) URL인 것으로 판별된 경우 단계 S212에서 상기 URL을 차단한다.

[0101] 상기 URL이 비악성(NM) URL인 것으로 판별된 경우 단계 S214에서 상기 URL을 허용한다.

[0102] 상기 URL이 불확실한(U) URL인 것으로 판별된 경우 단계 S216에서 상기 지식기반 데이터베이스에 기반하여 상기 URL이 악성(M) URL인지 비악성(NM) URL 인지를 검증한다.

[0103] 한편, 도 3에 도시된 바와 같이, 상기 단계 S216은, 상기 수신되는 URL의 쿼리 경로(query path)로부터 키-값 쌍들 및 키-값 패턴 시퀀스 순서를 획득하는 단계(S300), 상기 URL의 키 및 값들이 상기 지식기반 데이터베이스의 메타 테이블의 경계 내에 있고 동일한 시퀀스 순서로 있는지를 판정하는 단계(S302) 및 상기 URL의 키 및 값들이 상기 지식기반 데이터베이스의 메타 테이블의 경계 내에 있고 동일한 시퀀스 순서로 있는 경우, 상기 수신되는 URL을 비악성(NM) URL인 것으로 판정하고(S304), 그렇지 않은 경우 상기 수신되는 URL을 악성(M) URL인 것으로 판정하는 단계(S306)를 포함한다.

[0104] 다시 도 2를 참조하면, 단계 S218에서 상기 검증 결과가 악성(M) 또는 비악성(NM) 인지를 판별한다.

[0105] 상기 검증 결과가 악성(N)인 경우 단계 S220에서 상기 악성으로 검증된 URL을 악성(M) URL로서 상기 블랙리스트에 추가하고 단계 S212로 진행하여 상기 악성 URL로 검증된 URL을 차단한다.

[0106] 상기 검증 결과가 비악성(NM)인 경우 단계 S222에서 상기 비악성으로 검증된 URL을 비악성(NM) URL로서 상기 지식기반 데이터베이스에 추가하고 단계 S214로 진행하여 상기 비악성 URL로 검증된 URL을 허용한다.

[0107] 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에서는 악성 URL 탐지를 위한 효율적인 접근 방식을 소개하였다. 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은 클라이언트 측에서 장치를 설치하거나 구성할 필요없이 서버 측에서 설계 및 구현된다. 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법은 웹 브라우저를 지원할 수 있는 경우 핸드 헬드 장치에서 URL을 감지하고 분류할 수 있다. 또한, 본 발명의 일 실시예에 의한 사물인터넷(IoT)상에서 악성 URL 자동 탐지 방법에 의하면 제3자 서비스나 도구없이 URL에서 특징을 추출하여 악성 URL 또는 비악성 URL을 신속하고 정확하게 그리고 효율적으로 분류할 수 있다.

[0108] 이상 본 발명을 구체적인 실시예를 통하여 상세하게 설명하였으나, 이는 본 발명을 구체적으로 설명하기 위한 것으로, 본 발명은 이에 한정되지 않으며, 본 발명의 기술적 사상 내에서 당 분야의 통상의 지식을 가진 자에 의해 그 변형이나 개량이 가능함은 명백하다고 할 것이다.

[0109] 본 발명의 단순한 변형 내지 변경은 모두 본 발명의 영역에 속하는 것으로, 본 발명의 구체적인 보호 범위는 첨부된 청구범위에 의하여 명확해질 것이다.

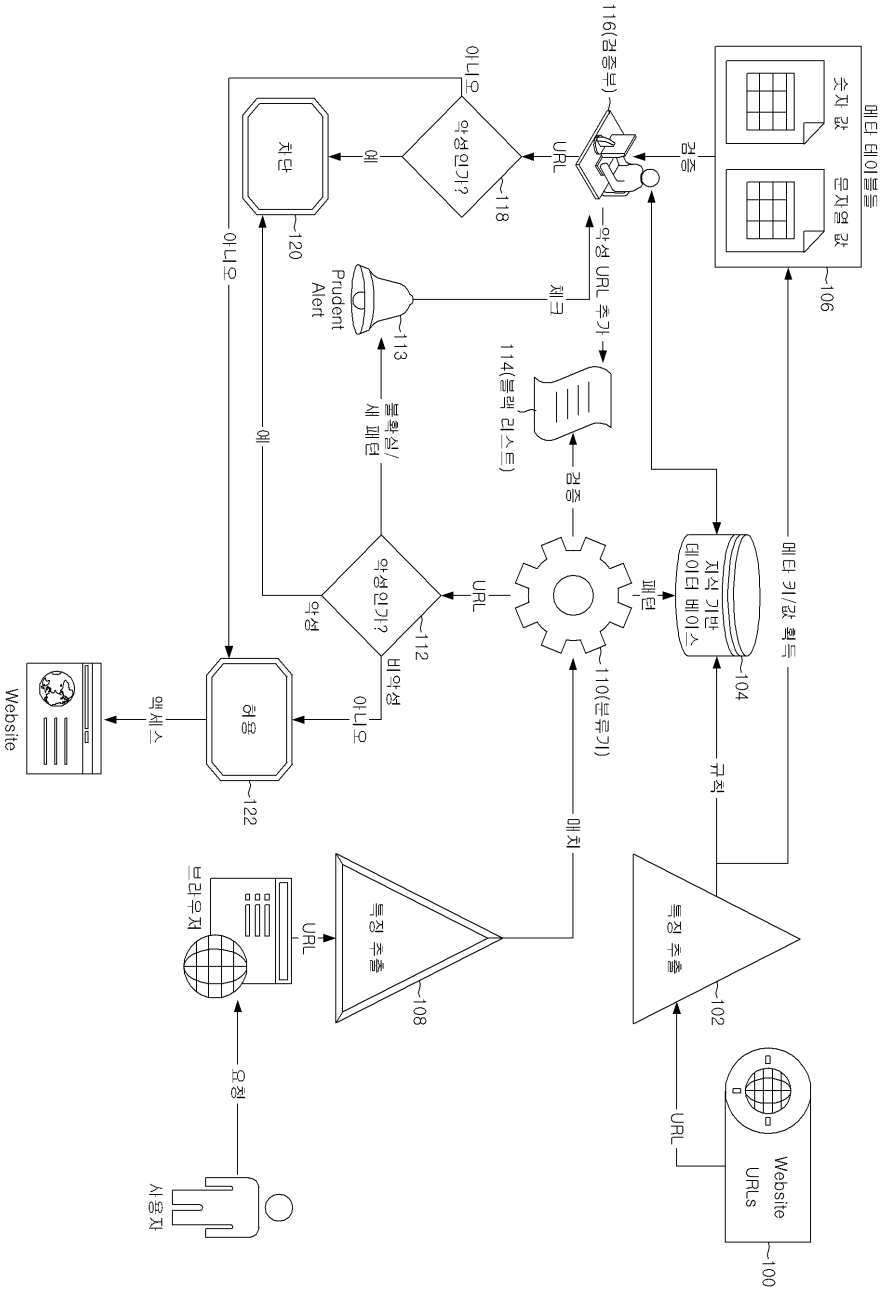
부호의 설명

[0110]

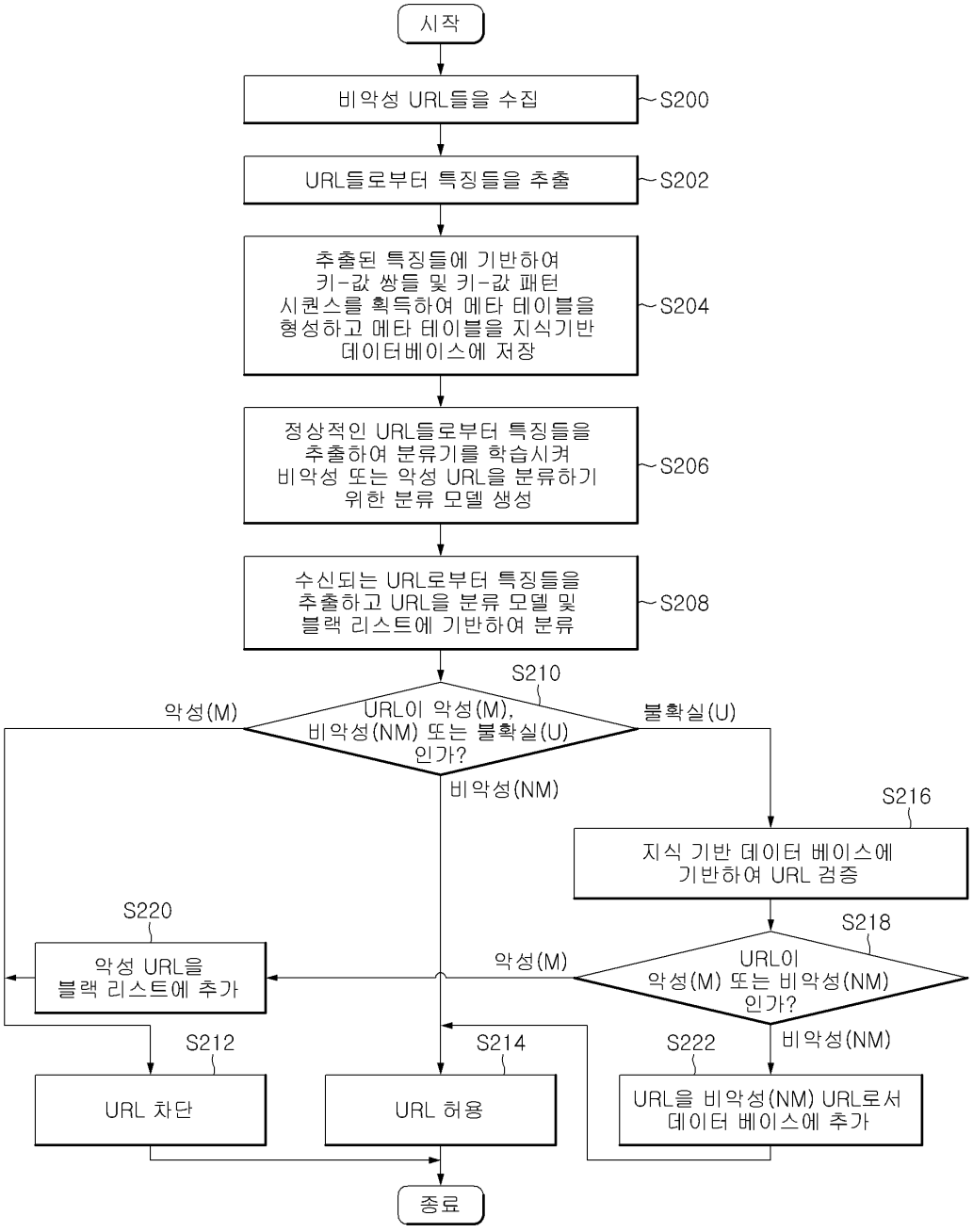
100 : 웹사이트 URL들	102, 108 : 특징 추출부
104 : 지식기반 데이터베이스	106 : 메타 테이블들
110 : 분류기	112, 118 : 판정부
113 : 신중한 프롬프트	114 : 블랙리스트
116 : 검증부	120 : 차단부
122 : 허용부	400 : 프로세서
402 : 데이터 저장부	

도면

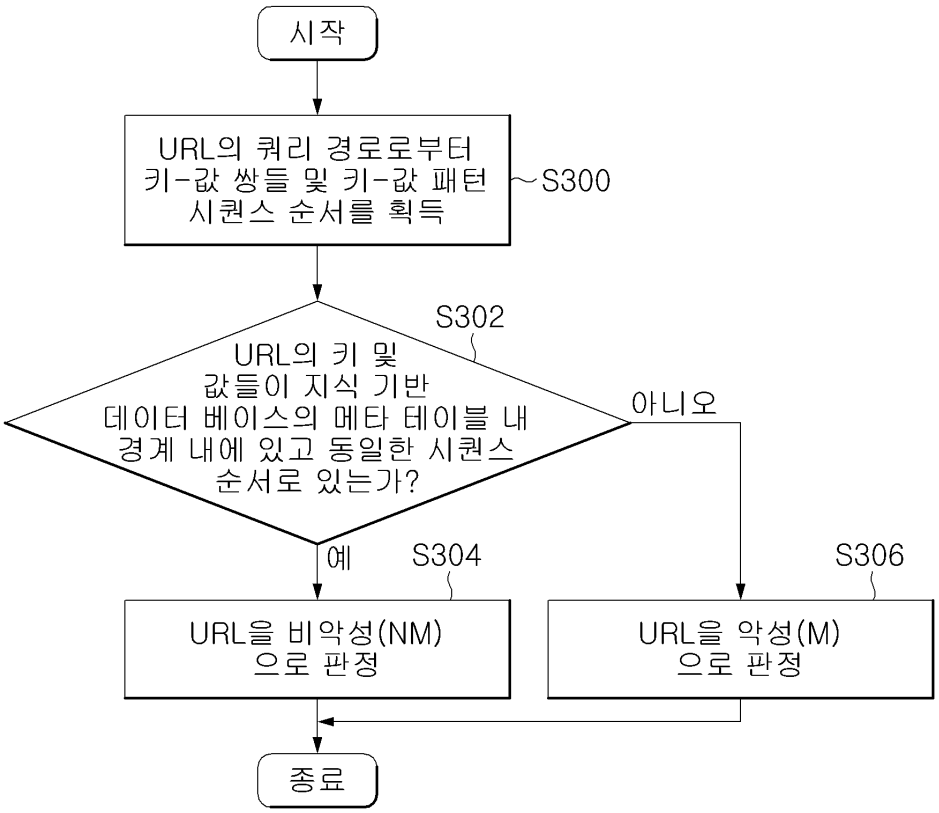
도면1


메타 데이터베이스
숫자 값
문자열 값
106
116(검증부)
검증
URL
악성인가?
118
아니오
예
차단
120
악성 URL 추가
체크
Prudent Alert
113
114(블랙 리스트)
검증
불확실/새 패턴
악성인가?
112
악성
비악성
아니오
예
URL
패턴
지식 기반 데이터 베이스
104
110(분류기)
메타 키/값 획득
규칙
특정 추출
102
URL
Website URLs
100
매칭
특정 추출
108
URL
브라우저
요청
사용자
허용
122
액세스
Website

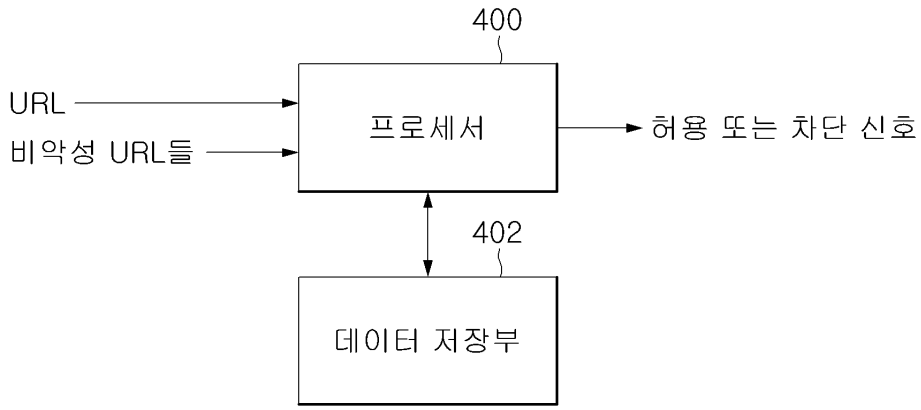
도면2


시작
비악성 URL들을 수집
S200
URL들로부터 특징들을 추출
S202
추출된 특징들에 기반하여 키-값 쌍들 및 키-값 패턴 시퀀스를 획득하여 메타 데이블을 형성하고 메타 데이블을 지식기반 데이터베이스에 저장
S204
정상적인 URL들로부터 특징들을 추출하여 분류기를 학습시켜 비악성 또는 악성 URL을 분류하기 위한 분류 모델 생성
S206
수신되는 URL로부터 특징들을 추출하고 URL을 분류 모델 및 블랙 리스트에 기반하여 분류
S208
S210
URL이 악성(M), 비악성(NM) 또는 불확실(U) 인가?
악성(M)
불확실(U)
비악성(NM)
S216
지식 기반 데이터 베이스에 기반하여 URL 검증
S218
URL이 악성(M) 또는 비악성(NM) 인가?
악성(M)
비악성(NM)
S220
악성 URL을 블랙 리스트에 추가
S212
URL 차단
S214
URL 허용
S222
URL을 비악성(NM) URL로서 데이터 베이스에 추가
종료

도면3


시작
URL의 쿼리 경로로부터 키-값 쌍들 및 키-값 패턴 시퀀스 순서를 획득
S300
S302
URL의 키 및 값들이 지식 기반 데이터 베이스의 메타 테이블 내 경계 내에 있고 동일한 시퀀스 순서로 있는가?
아니오
예
S304
S306
URL을 비악성(NM)으로 판정
URL을 악성(M)으로 판정
종료

도면4


400
URL
비악성 URL들
프로세서
허용 또는 차단 신호
402
데이터 저장부