



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년08월04일
(11) 등록번호 10-1645882
(24) 등록일자 2016년07월28일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) G06K 17/00 (2006.01)
(52) CPC특허분류
H04L 63/1483 (2013.01)
G06K 17/00 (2013.01)
(21) 출원번호 10-2015-0073535
(22) 출원일자 2015년05월27일
심사청구일자 2015년05월27일
(56) 선행기술조사문헌
KR101115250 B1
이민수 외 2인, 한국정보과학회 2010 한국컴퓨터
종합학술대회 논문집 제37권 제1호(D) “검색 엔
진 기반의 안티 피싱 기법” (2010.06. 공개)

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이문규
경기도 부천시 원미구 계남로 81, 2222동 702호(상동, 진달래마을)
(74) 대리인
양성보

전체 청구항 수 : 총 2 항

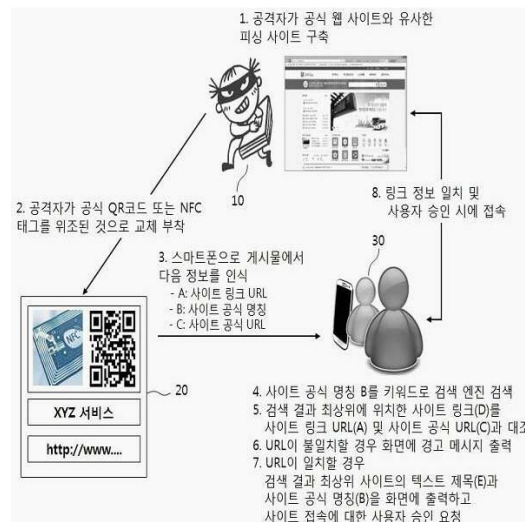
심사관 : 문형섭

(54) 발명의 명칭 문자 인식과 검색 순위 정보를 이용한 피싱 방지 방법 및 시스템

(57) 요약

문자 인식과 검색 순위 정보를 이용한 피싱 방지 방법 및 시스템이 개시된다. 피싱 방지 방법은, 사용자 단말을 통해 QR 코드 또는 NFC 태그로부터 인식된 제1 사이트 URL과 상기 사용자 단말의 문자 인식 기능에서 인식된 텍스트로서 제1 사이트 명칭과 제2 사이트 URL을 수신하는 단계; 상기 제1 사이트 명칭을 키워드로 하는 검색 요청을 검색 엔진으로 전송하는 단계; 상기 검색 요청에 따라 수행된 검색 결과를 수신하여 상기 검색 결과에 포함된 제3 사이트 URL을 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 비교하는 단계; 및 URL 비교 결과에 따라 상기 제1 사이트 URL을 이용한 사이트 접속 여부를 결정하는 단계를 포함한다.

대표도



이 발명을 지원한 국가연구개발사업

과제고유번호 1711026579

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신기술인력양성사업

연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술개발 및 연구 인력양성

기 여 율 1/1

주관기관 숭실대학교 산학협력단

연구기간 2012.06.01 ~ 2015.12.31

명세서

청구범위

청구항 1

컴퓨터로 구현되는 피싱 방지 방법에 있어서,

사용자 단말을 통해 QR 코드 또는 NFC 태그로부터 인식된 제1 사이트 URL과 상기 사용자 단말의 문자 인식 기능에서 인식된 텍스트로서 제1 사이트 명칭과 제2 사이트 URL을 수신하는 단계;

상기 제1 사이트 명칭을 키워드로 하는 검색 요청을 검색 엔진으로 전송하는 단계;

상기 검색 요청에 따라 수행된 검색 결과를 수신하여 상기 검색 결과에 포함된 제3 사이트 URL을 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 비교하는 단계; 및

URL 비교 결과에 따라 상기 제1 사이트 URL을 이용한 사이트 접속 여부를 결정하는 단계

를 포함하고,

상기 사용자 단말에서는 상기 QR 코드 또는 상기 NFC 태그, 상기 제1 사이트 명칭과 상기 제2 사이트 URL을 포함하는 게시물을 대상으로 하여, 카메라를 통해 상기 QR 코드를 인식하거나 NFC 리더기를 통해 상기 NFC 태그를 인식하고, 상기 문자 인식 기능을 이용하여 상기 게시물에 포함된 상기 제1 사이트 명칭과 상기 제2 사이트 URL을 인식하고,

상기 수신하는 단계는,

상기 사용자 단말로부터 상기 게시물에 대한 인식 결과로서 상기 QR 코드 또는 상기 NFC 태그, 그리고 상기 제1 사이트 명칭과 상기 제2 사이트 URL을 수신하고,

상기 비교하는 단계는,

상기 검색 결과에서 최상위에 노출된 사이트 URL 또는 최상위부터 둘 이상의 순위에 노출된 사이트 URL을 상기 제3 사이트 URL로 하여 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 비교하고,

상기 결정하는 단계는,

상기 제3 사이트 URL이 상기 제1 사이트 URL과 상기 제2 사이트 URL 중 적어도 하나와 불일치하는 경우 상기 제1 사이트 URL에 대하여 피싱 사이트를 경고하는 메시지를 상기 사용자 단말에 표시하는 단계; 및

상기 제3 사이트 URL이 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 모두 일치하는 경우 상기 검색 결과에서 상기 제3 사이트 URL에 해당되는 제2 사이트 명칭을 추출하여 상기 제1 사이트 명칭과 상기 제2 사이트 명칭을 상기 사용자 단말에 표시하는 단계

를 포함하는 피싱 방지 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

적어도 하나의 프로그램이 로딩된 메모리; 및

적어도 하나의 프로세서

를 포함하고,

상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라,

사용자 단말을 통해 QR 코드 또는 NFC 태그로부터 인식된 제1 사이트 URL과 상기 사용자 단말의 문자 인식 기능에서 인식된 텍스트로서 사이트 명칭과 제2 사이트 URL을 수신하는 과정;

상기 사이트 명칭을 키워드로 하는 검색 요청을 검색 엔진으로 전송하는 과정;

상기 검색 요청에 따라 수행된 검색 결과를 수신하여 상기 검색 결과에 포함된 제3 사이트 URL을 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 비교하는 과정; 및

URL 비교 결과에 따라 상기 제1 사이트 URL을 이용한 사이트 접속 여부를 결정하는 과정

을 처리하고,

상기 사용자 단말에서는 상기 QR 코드 또는 상기 NFC 태그, 상기 제1 사이트 명칭과 상기 제2 사이트 URL을 포함하는 게시물을 대상으로 하여, 카메라를 통해 상기 QR 코드를 인식하거나 NFC 리더기를 통해 상기 NFC 태그를 인식하고, 상기 문자 인식 기능을 이용하여 상기 게시물에 포함된 상기 제1 사이트 명칭과 상기 제2 사이트 URL을 인식하고,

상기 수신하는 과정은,

상기 사용자 단말로부터 상기 게시물에 대한 인식 결과로서 상기 QR 코드 또는 상기 NFC 태그, 그리고 상기 제1 사이트 명칭과 상기 제2 사이트 URL을 수신하고,

상기 비교하는 과정은,

상기 검색 결과에서 최상위에 노출된 사이트 URL 또는 최상위부터 둘 이상의 순위에 노출된 사이트 URL을 상기 제3 사이트 URL로 하여 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 비교하고,

상기 결정하는 과정은,

상기 제3 사이트 URL이 상기 제1 사이트 URL과 상기 제2 사이트 URL 중 적어도 하나와 불일치하는 경우 상기 제1 사이트 URL에 대하여 피싱 사이트를 경고하는 메시지를 상기 사용자 단말에 표시하고,

상기 제3 사이트 URL이 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 모두 일치하는 경우 상기 검색 결과에서 상기 제3 사이트 URL에 해당되는 제2 사이트 명칭을 추출하여 상기 제1 사이트 명칭과 상기 제2 사이트 명칭을 상기 사용자 단말에 표시하는 것

을 특징으로 하는 피싱 방지 시스템.

발명의 설명

기술 분야

[0001] 본 발명의 실시예들은 피싱(phishing)으로 인한 피해를 방지하기 위한 기술에 관한 것이다.

배경 기술

[0002] 스마트폰 사용이 일반화되면서, 사용자가 정상 사이트로 오인하기 쉬운 가짜 사이트로 접근하도록 하는 피싱(phishing), 특히 문자 메시지에 포함된 URL을 클릭하게 유도하는 변형된 형태의 피싱인 스미싱(smishing) 등의 공격에 의한 피해가 발생하고 있다.

[0003] 이러한 피싱 방지를 위한 기술의 일 예로서, 한국등록특허 제10-0745044호(등록일 2007년 07월 26일)에는 사용자가 사이트 접속 시 참조 모니터가 접근 사이트를 식별하고 사용자 접속 URL이 기 저장된 피싱 사이트 데이터베이스에 존재하면 피싱 경고를 보고할 뿐만 아니라, 만약 접속 URL이 존재하지 않으면 정상 사이트 DB에 존재하는 URL 정보들과의 유사도를 비교하여 일정 수준의 임계값 이상이면 피싱 사이트를 보고해 주는 피싱 사이트 접속 방지 장치 및 방법이 개시되어 있다.

발명의 내용

해결하려는 과제

- [0004] 스마트폰의 QR 코드(quick response code) 인식 기능이나 NFC(near field communication) 기능을 이용한 사이트 접속 시 사용자가 의도하지 않는 피싱 사이트로의 접속을 방지할 수 있는 피싱 방지 방법 및 시스템을 제공한다.
- [0005] 스마트폰에서 쉽게 제공 가능한 문자 인식 기능과 웹브라우저의 검색 엔진 검색 기능을 조합하여 안내판 상에 공개된 QR 코드나 NFC 태그를 통한 피싱 사이트로의 접속에 대처할 수 있는 피싱 방지 방법 및 시스템을 제공한다.

과제의 해결 수단

- [0006] 컴퓨터로 구현되는 피싱 방지 방법에 있어서, 사용자 단말을 통해 QR 코드 또는 NFC 태그로부터 인식된 제1 사이트 URL과 상기 사용자 단말의 문자 인식 기능에서 인식된 텍스트로서 제1 사이트 명칭과 제2 사이트 URL을 수신하는 단계; 상기 제1 사이트 명칭을 키워드로 하는 검색 요청을 검색 엔진으로 전송하는 단계; 상기 검색 요청에 따라 수행된 검색 결과를 수신하여 상기 검색 결과에 포함된 제3 사이트 URL을 상기 제1 사이트 URL 및 상기 제2 사이트 URL와 비교하는 단계; 및 URL 비교 결과에 따라 상기 제1 사이트 URL을 이용한 사이트 접속 여부를 결정하는 단계를 포함하는 피싱 방지 방법을 제공한다.
- [0007] 일 측면에 따르면, 상기 결정하는 단계는, 상기 제3 사이트 URL이 상기 제1 사이트 URL과 상기 제2 사이트 URL 중 적어도 하나와 불일치하는 경우 상기 제1 사이트 URL에 대하여 피싱 사이트를 경고하는 메시지를 상기 사용자 단말에 표시하는 단계를 포함할 수 있다.
- [0008] 다른 측면에 따르면, 상기 결정하는 단계는, 상기 제3 사이트 URL이 상기 제1 사이트 URL 및 상기 제2 사이트 URL과 모두 일치하는 경우 상기 검색 결과에서 상기 제3 사이트 URL에 해당되는 제2 사이트 명칭을 추출하여 상기 제1 사이트 명칭과 상기 제2 사이트 명칭을 상기 사용자 단말에 표시하는 단계를 더 포함할 수 있다.]
- [0009] 또 다른 측면에 따르면, 상기 제3 사이트 URL은 상기 검색 결과에서 최상위에 노출된 사이트 URL 또는 최상위부터 둘 이상의 순위에 노출된 사이트 URL을 포함할 수 있다.
- [0010] 적어도 하나의 프로그램이 로딩된 메모리; 및 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라, 사용자 단말을 통해 QR 코드 또는 NFC 태그로부터 인식된 제1 사이트 URL과 상기 사용자 단말의 문자 인식 기능에서 인식된 텍스트로서 사이트 명칭과 제2 사이트 URL을 수신하는 과정; 상기 사이트 명칭을 키워드로 하는 검색 요청을 검색 엔진으로 전송하는 과정; 상기 검색 요청에 따라 수행된 검색 결과를 수신하여 상기 검색 결과에 포함된 제3 사이트 URL을 상기 제1 사이트 URL 및 상기 제2 사이트 URL와 비교하는 과정; 및 URL 비교 결과에 따라 상기 제1 사이트 URL을 이용한 사이트 접속 여부를 결정하는 과정을 처리하는 피싱 방지 시스템을 제공한다.

발명의 효과

- [0011] 본 발명의 실시예에 따르면, QR 코드나 NFC 태그로부터 읽어온 URL을 바로 접속하는 대신, 스마트폰에서 쉽게 제공 가능한 문자 인식 기능과 웹브라우저의 검색 엔진 검색 기능을 조합하여 해당 URL의 사이트 확인을 통한 필터링을 거침으로써 QR 코드나 NFC 태그를 이용한 피싱에 효과적으로 대처할 수 있고 사용자가 의도하지 않는 피싱 사이트로의 접속을 방지할 수 있다.

도면의 간단한 설명

- [0012] 도 1은 QR 코드나 NFC 태그를 이용한 피싱 공격의 예시를 설명하기 위한 도면이다.
- 도 2는 본 발명의 일 실시예에 있어서, 피싱 방지 환경의 예를 설명하기 위한 도면이다.
- 도 3은 본 발명의 일 실시예에 있어서, 문자 인식과 검색 순위 정보를 이용한 피싱 방지 시스템의 내부 구성을 설명하기 위한 블록도이다.
- 도 4는 본 발명의 일 실시예에 있어서, 안전성이 개선된 게시물 구성의 일 예를 도시한 것이다.
- 도 5는 본 발명의 일 실시예에 있어서, 문자 인식과 검색 순위 정보를 이용한 피싱 방지 방법을 도시한 순서도

이다.

도 6은 본 발명의 일 실시예에 있어서, QR 코드 또는 NFC 태그 번조에 의한 피싱 공격에 대처하는 과정을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0014] 최근에는 스마트폰에 여러 가지 부가 기능들이 추가되면서, QR 코드 인식 기능, NFC 기능 등을 이용한 편리한 서비스들이 등장하고 있다.

[0015] 예를 들어, 버스 안내 서비스는 버스 정류장에 설치된 안내판에 QR 코드가 부착되거나 NFC 태그가 내장되어 있어 스마트폰 사용자가 안내판의 QR 코드를 스캔하거나 안내판에 내장된 NFC 태그를 접촉하면 노선 정보, 실시간 버스 정보 등 버스와 관련된 유용한 정보를 제공할 수 있다. 유사한 서비스로, 문화재 등의 안내판에 QR 코드가 부착되어 있고 QR 코드를 스마트폰으로 스캔하면 해당 문화재에 관한 좀 더 자세한 정보를 제공할 수 있다.

[0016] 이러한 서비스들은 대부분 QR 코드 또는 NFC 태그에 내장된 URL 정보를 스마트폰 내의 어플리케이션이 인식한 후, 해당 URL을 스마트폰의 웹브라우저가 방문하게 하는 방식으로 구성되어 있다.

[0017] 그러나, 안내판에 부착된 QR코드나 NFC 태그는 공개된 장소에 방치되어 있어 공격자가 만들어낸 가짜 사이트에 관한 URL을 담은 번조 QR코드 또는 번조 NFC 태그로 쉽게 대체가 가능하다. 이러한 경우, 피싱이나 스미싱 공격에 의한 피해로 이어질 수 있다.

[0018] 더욱이, 일반적인 피싱은 사용자가 웹사이트의 URL 내용을 정확히 확인하면 어느 정도 방지가 가능하며, 스미싱은 의심스러운 문자 메시지 상의 URL을 클릭하지 않으면 방지할 수 있으나, 공개된 안내판 상의 QR 코드나 NFC 태그를 물리적으로 대체하는 공격은 사용자가 대처하기 매우 어렵다.

[0019] 본 발명은 스마트폰에서 쉽게 제공 가능한 문자 인식 기능과 웹브라우저의 검색 엔진 검색 기능을 이용하여 QR 코드나 NFC 태그를 이용한 피싱에 대처할 수 있는 피싱 방지 방법 및 시스템에 관한 것이다.

[0020] 먼저, 도 1을 참조하여 QR 코드나 NFC 태그를 이용한 피싱 공격 과정을 설명하기로 한다.

[0021] 1. 공격자(10)는 공식 서비스 사이트와 유사한 형태를 가지도록 가짜 사이트(이하, '피싱 사이트'라 칭함)를 구축하고, 피싱 사이트의 URL을 담고 있는 위조 QR 코드 또는 위조 NFC 태그를 생성한다. 이때, QR 코드의 생성은 QR 코드 생성 프로그램을 이용하여 URL을 인코딩 한 코드를 인쇄하면 되고, NFC 태그는 시중에서 쉽게 구할 수 있는 저가의 NFC 태그에 NFC 기능을 지원하는 스마트폰으로 URL을 기록(write)하면 된다.

[0022] 2. 공격자(10)는 안내판(30) 상의 원본 QR 코드 또는 NFC 태그 위에 위조 QR 코드 또는 위조 NFC 태그를 스티커 형태로 부착하거나, 일반인들에게 노출되어 있는 임의의 시설물 등에 위조 QR 코드 또는 위조 NFC 태그가 내장된 스티커를 부착할 수 있다.

[0023] 3. 사용자(피해자)(30)는 공개된 안내판이나 시설물 등에 부착된 QR 코드 또는 NFC 태그의 위조 여부를 인지하지 못한 채로 위조 QR 코드 또는 위조 NFC 태그 정보를 스마트폰으로 읽는다.

[0024] 4. 사용자(30)의 스마트폰에서 웹브라우저가 별도의 필터링 없이 위조 QR 코드 또는 위조 NFC 태그로부터 읽어들인 정보에 포함된 URL로 접속함으로써 피싱 사이트에 접속하게 되어 피해가 발생한다.

[0025] 본 명세서에서는 사용자의 스마트폰이 QR 코드 및 NFC 태그로부터 읽어들인 URL을 바로 접속하는 대신, 자동 필터링을 통과하고 사용자의 명시적 승인을 득한 경우에 접속하게 함으로써 피싱 공격을 차단하는 기술을 제안한다.

[0026] 도 2는 본 발명의 일 실시예에 있어서, 피싱 방지 환경의 예를 설명하기 위한 도면이다. 도 2는 사용자 단말(201) 및 피싱 방지 시스템(200)을 나타내고 있다. 도 2에서 화살표는 구성 요소 간에 유/무선 네트워크(2)를 이용하여 데이터가 송수신될 수 있음을 의미한다.

[0027] 사용자 단말(201)은 본 명세서에서 설명되는 특징들 중 하나 이상의 특징을 수행하도록 구성된 하나 이상의 프로세스들을 실행할 수 있다. 사용자 단말(201)은 피싱 방지 시스템(200)과 관련된 웹/모바일 사이트의 접속 또는 서비스 전용 어플리케이션의 설치 및 실행이 가능한 모든 단말 장치를 의미할 수 있다. 이때, 사용자 단말(201)은 웹/모바일 사이트 또는 전용 어플리케이션의 제어 하에 서비스 화면 구성, 데이터 입력, 데이터

송수신, 데이터 저장 등 서비스 전반의 동작을 수행할 수 있다.

- [0028] 사용자 단말(201)의 예로는 스마트폰(smart phone), 태블릿(tablet), 웨어러블 컴퓨터(wearable computer), 노트북 컴퓨터(laptop computer), 랩탑 컴퓨터(laptop computer) 등의 모바일 통신 디바이스를 포함할 수 있지만 이러한 것으로만 한정되는 것은 아니다.
- [0029] 사용자 단말(201)은 네트워크(2)(예를 들어, 인터넷 혹은 로컬 영역 네트워크 등)에 직접적으로 혹은 간접적으로 결합될 수 있다. 예를 들어, 노트북 컴퓨터이나 개인용 컴퓨터는 유선 네트워크 연결을 통해 네트워크(2)에 직접적으로 결합될 수 있다. 랩탑 컴퓨터는 랩탑 컴퓨터와 무선 액세스 포인트(Wireless Access Point)(즉, WAP) 간에 확립된 무선 통신 채널을 통해 네트워크(2)에 무선으로 결합될 수 있다. 스마트폰이나 태블릿 등은 스마트폰과 셀룰러 네트워크/브리지 간에 확립된 무선 통신 채널을 통해 네트워크(2)에 무선으로 결합될 수 있다. 이때, 네트워크(2)는 하나 이상의 2차 네트워크들(미도시)과 통신할 수 있으며, 2차 네트워크들의 예로는 로컬 영역 네트워크(Local Area Network), 와이드 영역 네트워크(Wide Area Network), 또는 인트라넷(intranet)을 포함할 수 있지만 이러한 것으로만 한정되는 것은 아니다.
- [0030] 사용자 단말(201)은 상기에서 설명한 네트워크(2)를 통해 피싱 방지 시스템(200)과 서로 인터페이스 할 수 있다.
- [0031] 피싱 방지 시스템(200)은 본 명세서에서 설명되는 특징들 중 하나 이상의 특징을 수행하도록 구성된 하나 이상의 프로세서들을 실행할 수 있다. 특히, 피싱 방지 시스템(200)은 사용자 단말(201)에서 제공하는 문자 인식 기능과 웹브라우저의 검색 엔진 검색 기능을 이용하여 피싱 사이트를 필터링 할 수 있다.
- [0032] 피싱 방지 시스템(200)은 서버 컴퓨터에 해당되는 것으로, 서버 컴퓨터의 예로는 서버 컴퓨팅 디바이스, 개인용 컴퓨터, 서버 컴퓨터, 일련의 서버 컴퓨터들, 미니 컴퓨터, 및/또는 메인프레임 컴퓨터를 포함할 수 있지만 이러한 것으로만 한정되는 것은 아니다. 서버 컴퓨터는 분산형 시스템일 수 있고, 그리고 서버 컴퓨터의 동작들은 하나 이상의 프로세서들 상에서 동시에 그리고/또는 순차적으로 실행될 수 있다.
- [0033] 상기한 피싱 방지 시스템(200)은 적어도 일부의 구성 요소가 사용자 단말(201) 상에 설치되는 어플리케이션 형태로 구현될 수 있으며, 이에 한정되는 것은 아니며 클라이언트-서버 환경에서 피싱 방지 서비스를 제공하는 서비스 플랫폼에 포함되는 형태로 구현되는 것 또한 가능하다.
- [0034] 도 3은 본 발명의 일 실시예에 있어서, 피싱 방지 시스템의 내부 구성을 설명하기 위한 블록도이다.
- [0035] 도 3에 도시한 바와 같이, 본 실시예에 따른 피싱 방지 시스템(200)은 프로세서(310), 버스(320), 네트워크 인터페이스(330), 및 메모리(340) 및 데이터베이스(350)를 포함할 수 있다. 메모리(340)는 운영체제(341) 및 필터링 처리 루틴(342)를 포함할 수 있다. 다른 실시예들에서 피싱 방지 시스템(200)은 도 3의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다.
- [0036] 메모리(340)는 컴퓨터에서 판독 가능한 기록 매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 또한, 메모리(340)에는 운영체제(341)와 필터링 처리 루틴(342)을 위한 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 드라이브 메커니즘(drive mechanism, 미도시)을 이용하여 메모리(340)와는 별도의 컴퓨터에서 판독 가능한 기록 매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록 매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록 매체(미도시)를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록 매체가 아닌 네트워크 인터페이스(330)를 통해 메모리(340)에 로딩될 수도 있다.
- [0037] 버스(320)는 피싱 방지 시스템(200)의 구성요소들간의 통신 및 데이터 전송을 가능하게 할 수 있다. 버스(320)는 고속 시리얼 버스(high-speed serial bus), 병렬 버스(parallel bus), SAN(Storage Area Network) 및/또는 다른 적절한 통신 기술을 이용하여 구성될 수 있다.
- [0038] 네트워크 인터페이스(330)는 피싱 방지 시스템(200)을 컴퓨터 네트워크에 연결하기 위한 컴퓨터 하드웨어 구성요소일 수 있다. 네트워크 인터페이스(330)는 피싱 방지 시스템(200)을 무선 또는 유선 커넥션을 통해 컴퓨터 네트워크에 연결시킬 수 있다.
- [0039] 프로세서(310)는 기본적인 산술, 로직 및 피싱 방지 시스템(200)의 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(340) 또는 네트워크 인터페이스(330)에 의해, 그리고 버스(320)를 통해 프로세서(310)로 제공될 수 있다. 프로세서(310)는 본 명세서에서 설명되는 특징들 중 하나

이상의 특징을 수행하기 위한 프로그램 코드를 실행하도록 구성될 수 있다. 이러한 프로그램 코드는 메모리 (340)와 같은 기록 장치에 저장될 수 있다.

- [0040] 도 4는 본 발명의 일 실시예에 있어서, 안전성이 개선된 게시물 구성의 일 예를 도시한 것이다.
- [0041] QR 코드나 NFC 태그로 구성된 공식 게시물에 대해 QR 코드나 NFC 태그를 변조하여 물리적으로 대체하는 피싱 공격에 대처하기 위한 일환으로, 도 4에 도시한 바와 같이 QR 코드나 NFC 태그(401)를 포함하는 게시물에 해당 QR 코드나 NFC 태그(401)에 내장된 사이트의 공식 명칭(402)과 공식 URL(403)에 해당되는 텍스트를 추가적으로 인쇄하는 방식을 적용한다.
- [0042] 상기한 구성에 따라 QR 코드나 NFC 태그를 이용한 게시물에 해당 게시물에 대한 안내 정보(즉, 서비스의 공식 명칭)와 QR 코드나 NFC 태그에 내장된 URL 정보를 텍스트로 추가 게시함으로써 QR 코드 또는 NFC 태그 변조에 의한 피싱 공격에 쉽게 대처할 수 있도록 한다.
- [0043] 도 5는 본 발명의 일 실시예에 있어서, 피싱 방지 방법을 도시한 순서도이다. 일 실시예에 따른 피싱 방지 방법은 도 3을 통해 설명한 프로세서(310)에 의해 각각의 단계가 수행될 수 있다.
- [0044] 사용자 단말에서는 도 4와 같이 구성된 게시물에 대하여 카메라를 통해 QR 코드를 스캔하여 QR 코드에 담긴 사이트 링크 URL을 인식하거나, NFC 리더기를 통해 NFC 태그를 읽어 NFC 태그에 담긴 사이트 링크 URL을 인식할 수 있다. 특히, 본 실시예에서 사용자 단말은 문자 인식 기능을 이용하여 게시물에 인쇄된 텍스트, 즉 사이트 공식 명칭과 사이트 공식 URL을 함께 인식할 수 있다.
- [0045] 단계(510)에서 프로세서(310)는 사용자 단말에서 QR 코드나 NFC 태그를 이용한 게시물을 인식하는 경우 사용자 단말로부터 QR 코드 또는 NFC 태그에서 인식된 사이트 링크 URL(A)을 수신할 수 있고, 아울러 문자 인식 기능을 통해 인식된 사이트 공식 명칭(B)과 사이트 공식 URL(C)을 수신할 수 있다.
- [0046] 단계(520)에서 프로세서(310)는 사용자 단말로부터 수신된 정보 중 사이트 공식 명칭(B)을 키워드로 인터넷 검색 엔진 상의 검색을 수행할 수 있다. 예를 들어, 프로세서(310)는 사용자 단말 상의 웹 브라우저를 통한 검색 엔진 검색 기능을 이용할 수 있으며, 이때 사이트 공식 명칭(B)을 키워드로 한 검색을 검색 엔진에 요청하여 검색 결과를 수신할 수 있다.
- [0047] 단계(530)에서 프로세서(310)는 검색 결과 목록에서 최상위에 노출된 사이트 링크 URL(D)를 사용자 단말로부터 수신된 사이트 링크 URL(A) 및 사이트 공식 URL(C)과 대조할 수 있다.
- [0048] 단계(540)에서 프로세서(310)는 단계(530)에서의 대조 결과를 사용자 단말로 제공하고 사용자의 승인 여부에 따라 QR 코드 또는 NFC 태그에서 인식된 사이트 링크 URL(A)를 통한 사이트 접속 여부를 결정할 수 있다. 이때, 프로세서(310)는 단계(530)에서의 대조 결과와 함께, 검색 결과 목록에서 최상위에 위치한 사이트의 텍스트 제목(E)과 사용자 단말로부터 수신된 사이트 공식 명칭(B)을 사용자 단말로 제공할 수 있다.
- [0049] 도 6을 참조하여, QR 코드 또는 NFC 태그 변조에 의한 피싱 공격에 대처하는 과정을 상세히 설명하기로 한다. 이하에서는 피싱 방지 시스템(200)이 사용자 단말(201) 상에 설치된 어플리케이션(이하, '피싱 방지 앱'이라 칭함)의 형태로 구현될 수 있다.
- [0050] 1. 공격자(10)는 공식 서비스 사이트와 유사한 형태를 가지도록 피싱 사이트를 구축한다.
- [0051] 2. 공격자(10)는 피싱 사이트의 URL을 담고 있는 위조 QR 코드 또는 위조 NFC 태그를 만들어 원본 QR 코드 또는 NFC 태그를 포함하는 게시물(20)에 부착하거나 임의 시설물 등에 부착한다.
- [0052] 3. 사용자(30)의 스마트폰에서 QR 코드 또는 NFC 태그를 인식하는 경우 피싱 방지 앱은 스마트폰의 문자 인식 기능을 이용하여 카메라 영상으로부터 게시물(20)에 포함된 텍스트를 인식한다. QR 코드 방식의 경우 이 과정은 별도 과정이 아니며, 사용자가 게시물(20) 사진을 찍는 동시에 QR 코드가 자동 인식될 수 있다. 피싱 방지 앱은 스마트폰을 통해 QR 코드 또는 NFC 태그를 인식함으로써 QR 코드 또는 NFC 태그에 포함된 URL 텍스트 정보인 사이트 링크 URL(A)을 인식할 수 있으며, 아울러 문자 인식 기능을 통해 게시물(20)에 포함된 텍스트, 즉 사이트 공식 명칭(B)과 사이트 공식 URL(C)을 인식할 수 있다. 만약에, QR 코드 또는 NFC 태그로 구성된 게시물(20)에 사이트 공식 명칭(B)과 사이트 공식 URL(C)이 없거나 정상적으로 인식되지 않는 경우 경고 메시지(예컨대, "피싱의 위험성이 있습니다." 등)를 화면에 출력하여 사용자에게 보여줄 수 있다. 피싱 방지 앱은 안전성 레벨을 설정하는 기능을 제공할 수 있으며, 안정성 레벨이 "높음"으로 설정된 경우 경고 메시지 전달과 동시에 사이트 링크 URL(A)로의 접근을 차단하는 것도 가능하다.

- [0053] 4. 피싱 방지 앱은 QR 코드 또는 NFC 태그가 인식됨에 따라 스마트폰으로부터 게시물(20)에서 인식된 사이트 링크 URL(A)와 사이트 공식 명칭(B) 및 사이트 공식 URL(C)을 수신할 수 있으며, 이에 스마트폰의 웹 브라우저를 통해 게시물(20)에서 인식된 사이트 공식 명칭(B)을 키워드로 인터넷 검색 엔진 상의 검색을 수행한다.
- [0054] 5. 피싱 방지 앱은 검색 결과 상의 최상위(또는 상위 일정 순위(예컨대, 1위에서 3위까지))에 노출된 사이트 링크 URL(D)을 게시물(20)에서 인식된 사이트 링크 URL(A) 및 사이트 공식 URL(C)과 일치하는지 대조한다. 예를 들어, 서비스 공식 명칭(B)가 "경기도 시내버스 도착 안내 서비스"이고, 사이트 공식 URL(C)가 "www.gbise.go.kr"라면 먼저 "경기도 시내버스 도착 안내 서비스"를 키워드로 검색 엔진(예컨대, 구글, 네이버 등)에서 검색을 수행한다. 이때, 검색 결과 "경기버스정보", "경기도 버스정보시스템"이라는 사이트 이름이 최상위에 위치하며 최상위 사이트 링크 URL(D)가 모두 "www.gbise.go.kr"이라고 할 때 최상위 사이트 링크 URL(D)와 사이트 공식 URL(C)은 모두 일치하게 되며, 게시물(20)에 포함된 NFC 또는 QR 코드가 원본일 경우 사이트 링크 URL(A)와도 일치하게 된다. 검색 과정은 스마트폰의 화면에 보여지는 것은 아니며 스마트폰 내부적으로 수행하는 것이다.
- [0055] 6. 피싱 방지 앱은 5. 단계의 대조 결과에 따라 사이트 링크 URL(A), 사이트 공식 URL(C), 최상위 사이트 링크 URL(D)이 불일치하는 경우 스마트폰의 화면 상에 경고 메시지(예컨대, "피싱의 위험성이 매우 높다." 등)를 표시하여 사용자에게 보여줄 수 있다. 마찬가지로, 피싱 방지 앱은 안전성 레벨을 설정하는 기능을 제공할 수 있으며, 안전성 레벨이 "높음"으로 설정된 경우 경고 메시지 전달과 동시에 사이트 링크 URL(A)로의 접근을 차단하는 것도 가능하다.
- [0056] 7. 피싱 방지 앱은 5. 단계의 대조 결과에 따라 사이트 링크 URL(A), 사이트 공식 URL(C), 최상위 사이트 링크 URL(D)이 모두 일치하는 경우 검색 결과 상의 최상위(또는 상위 일정 순위)에 위치한 사이트의 텍스트 제목(E)을 추출한 후 추출된 최상위 사이트 명칭(E)을 서비스 공식 명칭(B)과 함께 스마트폰의 화면 상에 표시하고 사용자에게 사이트 링크 URL(A)에 대한 접속 승인을 요청할 수 있다. 예컨대, "게시물에 인쇄된 서비스 명칭은 '경기도 시내버스 도착 안내 서비스'이며, 자동 인식된 서비스 명칭은 '경기버스정보'입니다. 해당 서비스에 접속하시겠습니까? (Y/N)"와 같은 메시지를 사용자에게 보여줄 수 있다.
- [0057] 8. 피싱 방지 앱은 사용자(30)가 접속을 승인하는 경우 스마트폰의 웹 브라우저를 통해 게시물(20)에서 인식된 사이트 링크 URL(A)의 사이트에 접속할 수 있다.
- [0058] 상기한 과정의 피싱 방지 방법에 따르면, 다음과 같이 피싱을 방지할 수 있다.
- [0059] 1. 공격자가 게시물에서 사이트 공식 명칭(B)과 사이트 공식 URL(C)은 그대로 두고 QR 코드 또는 NFC 태그만을 위조하는 경우, QR 코드 또는 NFC 태그에서 인식된 사이트 링크 URL(A)이 사이트 공식 URL(C) 및/또는 최상위 사이트 링크 URL(D)과 일치하지 않기 때문에 피싱 방지가 가능하다.
- [0060] 2. 공격자가 QR 코드 또는 NFC 태그와 함께 사이트 공식 URL(C)을 위조하는 경우, QR 코드 또는 NFC 태그에서 인식된 사이트 링크 URL(A)와 사이트 공식 URL(C)이 일치하더라도 최상위 사이트 링크 URL(D)과 일치하지 않기 때문에 피싱 방지가 가능하다.
- [0061] 3. 공격자가 게시물에서 QR 코드 또는 NFC 태그와 함께 사이트 공식 명칭(B)과 사이트 공식 URL(C)을 모두 위조하는 경우, 즉 정식 서비스와 유사한 명칭의 피싱 사이트를 개설하여 위조한 QR 코드 또는 NFC 태그로 게시물을 만들고 해당 게시물에 위조한 사이트 명칭과 URL을 인쇄한 경우, 검색 엔진의 유사 키워드 검색 기능에 의하여 피싱 사이트보다는 방문 빈도가 월등히 높은 정식 서비스 사이트가 검색 결과의 상위에 위치할 확률이 높다. 따라서, 사이트 공식 URL(C)이 최상위 사이트 링크 URL(D)과 일치하지 않게 되므로 피싱 방지가 가능하다. 이러한 경우 사이트 공식 URL(C)을 대신하여 검색 결과 최상위 사이트 링크 URL(D)로 연결을 유도하는 것도 가능하다. 만약, 검색 엔진의 유사 키워드 검색 기능을 우회하기 위해 피싱 사이트의 명칭을 정식 서비스 명칭과 상이하게 구성할 경우, 사용자는 게시물에 본인이 원하는 서비스와 매우 다른 이름의 서비스가 인쇄된 것을 인지할 것이므로 역시 피싱 방지가 가능하다.
- [0062] 상기한 피싱 방지 방법은 도 2 내지 도 5를 통해 설명한 피싱 방지 시스템의 상세 내용을 바탕으로 보다 단축된 동작들 또는 추가의 동작들을 포함할 수 있다. 또한, 둘 이상의 동작이 조합될 수 있고, 동작들의 순서나 위치가 변경될 수 있다.
- [0063] 이와 같이, 본 발명의 실시예에 따르면, QR 코드나 NFC 태그로부터 읽어온 URL을 바로 접속하는 대신, 스마트폰에서 쉽게 제공 가능한 문자 인식 기능과 웹 브라우저의 검색 엔진 검색 기능을 조합하여 해당 URL의 사이트 확

인을 통한 필터링을 거침으로써 QR 코드나 NFC 태그를 이용한 피싱에 효과적으로 대처할 수 있고 사용자가 의도하지 않는 피싱 사이트로의 접속을 방지할 수 있다.

[0064] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨터 시스템을 통하여 수행될 수 있는 프로그램 명령(instruction) 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다.

[0065] 본 실시예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용의 어플리케이션으로 구성될 수 있다. 본 실시예에서의 피싱 방지와 관련된 앱은 독립적으로 동작하는 프로그램 형태로 구현되거나, 혹은 특정 어플리케이션의 인-앱(in-app) 형태로 구성되어 상기 특정 어플리케이션 상에서 동작이 가능하도록 구현될 수 있다.

[0066] 또한, 본 발명의 실시예에 따른 방법들은 피싱 방지 서비스를 제공하는 서버 시스템과 연관된 어플리케이션이 사용자 단말기를 제어하여 수행될 수 있다. 일 예로, 이러한 어플리케이션은 본 명세서에서 설명되는 특징들 중 하나 이상의 특징을 수행하도록 구성된 하나 이상의 프로세스들을 실행할 수 있다. 또한, 이러한 어플리케이션은 파일 배포 시스템이 제공하는 파일을 통해 사용자 단말기에 설치될 수 있다. 일 예로, 파일 배포 시스템은 사용자 단말기의 요청에 따라 상기 파일을 전송하는 파일 전송부(미도시)를 포함할 수 있다.

[0067] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0068] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

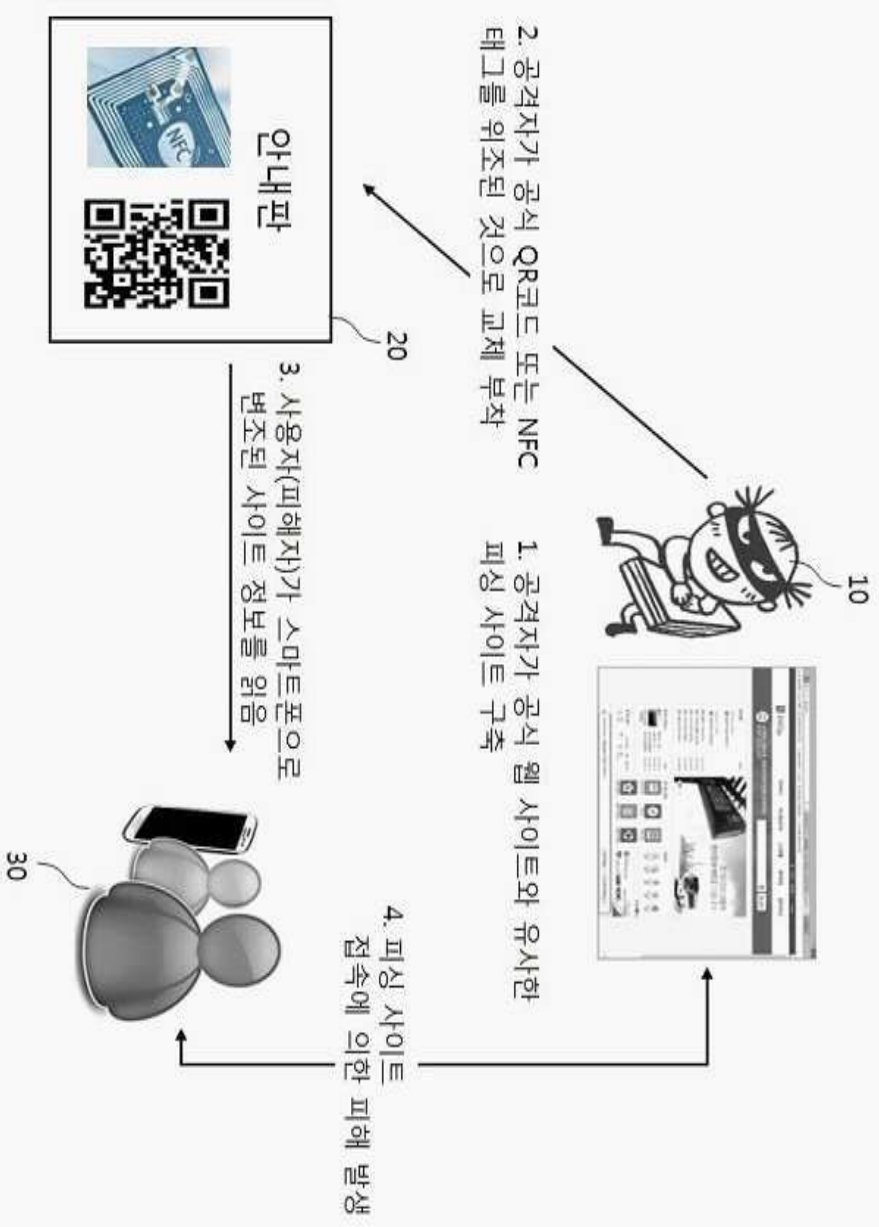
[0069] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0070] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0071] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

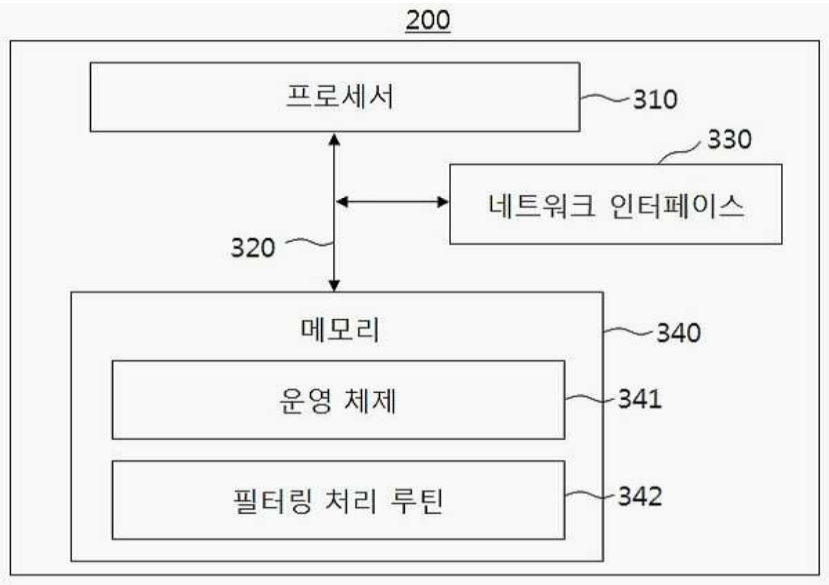
도면1



도면2



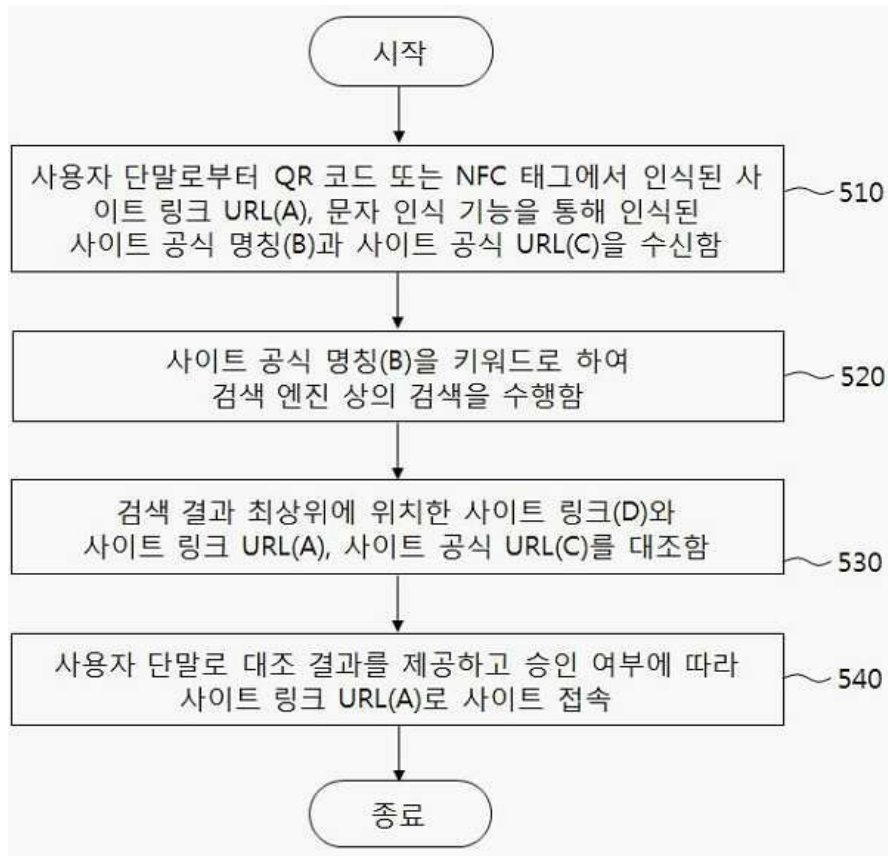
도면3



도면4



도면5



도면6

