



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0035572
(43) 공개일자 2013년04월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) G06F 21/20 (2006.01)
(21) 출원번호 10-2011-0099952
(22) 출원일자 2011년09월30일
심사청구일자 2011년09월30일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
김희강
서울특별시 서초구 양재동
(74) 대리인
특허법인충현

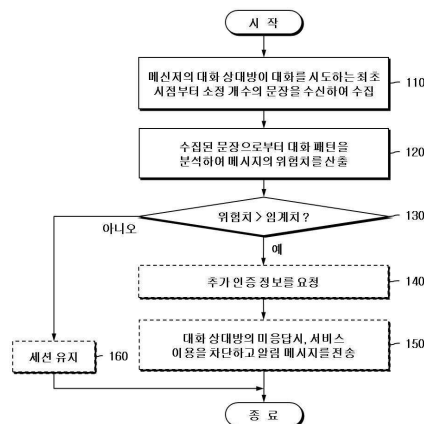
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 메신저 피싱을 탐지하는 장치 및 방법

(57) 요약

본 발명은 메신저 피싱을 탐지하는 장치 및 방법에 관한 것으로, 본 발명의 일 실시예에 따른 피싱 탐지 장치가 메신저를 통한 피싱을 탐지하는 방법은, 메신저의 대화 상대방이 대화를 시도하는 최초 시점부터 소정 개수의 문장을 수신하여 수집
의 문장을 수신하여 수집하고, 수집된 문장으로부터 대화 패턴을 분석하여 메시지의 위험치를 산출하며, 산출된 위험치가 미리 설정된 임계치 이상인지 여부를 판단함으로써 메신저 피싱을 탐지한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 ITAC1090111100020001000100100

부처명 정보통신산업진흥원

연구사업명 대학IT연구센터육성지원사업

연구과제명 [정부지원금]스마트 그리드 보안 연구센터(스마트 그리드 보안기술 개발)

주관기관 고려대학교 산학협력단

연구기간 2011.01.01 ~ 2011.12.31

특허청구의 범위

청구항 1

피싱 탐지 장치가 메시지를 통한 피싱을 탐지하는 방법에 있어서,

상기 메시지의 대화 상대방이 대화를 시도하는 최초 시점으로부터 상기 피싱 탐지 장치가 소정 개수의 문장을 수신하여 수집하는 단계;

상기 피싱 탐지 장치가 상기 수집된 문장으로부터 대화 패턴을 분석하여 메시지의 위험치를 산출하는 단계; 및

상기 산출된 위험치가 미리 설정된 임계치 이상인지 여부를 상기 피싱 탐지 장치가 판단하는 단계;를 포함하는 방법.

청구항 2

제 1 항에 있어서,

상기 대화 패턴을 분석하는 단계는,

상기 수집된 문장 내에 포함된 키워드들에 대한 시간적인 순서와 위험도를 고려하여 수행되는 것을 특징으로 하는 방법.

청구항 3

제 1 항에 있어서,

상기 수집된 문장으로부터 추출되는 키워드는, 인사말, 접속어 및 금융 관련 용어로 구분되는 것을 특징으로 하는 방법.

청구항 4

제 1 항에 있어서,

상기 대화 패턴을 분석하는 단계는,

형태소 분석을 이용하여 상기 수집된 문장 내에서 키워드를 추출하는 단계;

상기 추출된 키워드 중, 경어가 아닌 인사말이 존재하는지 여부를 판단하는 단계;

상기 경어가 아닌 인사말이 존재하는 경우, 상기 인사말 이후에 추출된 키워드 중, 화제를 전환하는 접속어가 존재하는지 여부를 판단하는 단계;

상기 접속어가 존재하는 경우, 상기 접속어 이후에 추출된 키워드 중, 금융 관련 용어가 존재하는지 여부를 판단하는 단계; 및

상기 금융 관련 용어가 존재하는 경우, 상기 금융 관련 용어 이후에 추출된 키워드 중, 금융 거래 정보가 존재하는지 여부를 판단하는 단계;를 포함하는 방법.

청구항 5

제 1 항에 있어서,

상기 대화 패턴을 분석하여 메시지의 위험치를 산출하는 단계는,

형태소 분석을 이용하여 상기 수집된 문장 내에서 키워드를 추출하는 단계;

상기 추출된 키워드가 미리 정의된 피싱 대화 패턴에 해당하는지 여부를 판단하는 단계;

상기 피싱 대화 패턴에 해당하는 키워드가 미리 정의된 피싱 단계에 순차적으로 대응되는지 여부를 판단하는 단계; 및

상기 피싱 단계에 대응되는 각각의 키워드에 대하여 가중치를 부여하고, 상기 부여된 가중치를 합산하는 단계;

를 포함하는 방법.

청구항 6

제 5 항에 있어서,

상기 피싱 단계의 시간적인 순서가 뒤로 갈수록 상기 가중치에 상대적으로 높은 값이 부여되는 것을 특징으로 하는 방법.

청구항 7

제 1 항에 있어서,

상기 판단 결과 상기 산출된 위험치가 상기 임계치 이상인 경우,

상기 피싱 탐지 장치가 상기 대화 상대방에게 추가 인증 정보를 요청하는 단계;를 더 포함하는 방법.

청구항 8

제 7 항에 있어서,

소정 시간 내에 상기 대화 상대방이 상기 추가 인증 정보 요청에 대해 응답하지 않는 경우,

상기 대화 상대방의 계정에 대한 서비스 이용을 차단하는 단계; 및

상기 계정의 사용자 정보를 참조하여 알림 메시지를 전송하는 단계;를 더 포함하는 방법.

청구항 9

제 1 항에 있어서,

상기 피싱 탐지 장치가 상기 대화 상대방의 IP 주소를 수집하는 단계;

상기 피싱 탐지 장치가 상기 IP 주소에 대하여 지역 정보를 추출하는 단계; 및

상기 피싱 탐지 장치가 상기 추출된 지역 정보에 기초하여 상기 메시지의 위험치에 위험 가중치를 부여하는 단계;를 더 포함하는 방법.

청구항 10

제 9 항에 있어서,

상기 메시지의 위험치에 위험 가중치를 부여하는 단계는,

지역 정보와 위험 가중치를 사상시켜 저장된 위험 지역 테이블을 이용하여 상기 추출된 지역 정보에 대응하는 위험 가중치를 산출하는 단계; 및

상기 산출된 메시지의 위험치에 상기 산출된 위험 가중치를 합산하는 단계;를 포함하는 방법.

청구항 11

제 1 항에 있어서,

상기 피싱 탐지 장치는 메신저 서버 또는 상기 메시지를 수신하는 클라이언트에 설치되는 것을 특징으로 하는 방법.

청구항 12

제 1 항 내지 제 11 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

기술분야

[0001] 본 발명은 메신저 피싱을 탐지하는 기술에 관한 것으로, 특히 메신저를 통해 대화 상대방이 메신저 사용자를 고의로 기만하여 경제적인 이익을 취하려 하는 메신저 피싱 행위를 상대방과의 대화 도중 탐지하여 이를 배척하기 위한 장치, 방법 및 이를 기록한 기록매체에 관한 것이다.

배경 기술

[0002] 피싱(Phishing)이란 '개인정보(Private data)를 낚는다(fishing)'라는 의미의 합성어로, 통상적인 피싱은 불특정 다수에게 메일을 발송해 위장된 홈페이지로 접속하도록 한 뒤 인터넷 이용자들의 금융정보 등을 빼내는 신종 사기 수법을 말한다.

[0003] 피싱의 대표적인 수법으로 금융기관이 보내온 메시지처럼 위장해 카드 번호나 비밀번호 등 민감한 개인 자료를 요구하는 유형이 널리 알려져 있다. 이 경우, 메일 본문에는 개인정보를 입력하도록 촉구하는 안내문과 웹사이트로의 링크가 기재되어 있는데, 해당 링크를 클릭하면 그 금융기관의 정규 웹사이트와 개인정보입력용 팝업 윈도우가 표시된다. 피싱의 경우, 메인 윈도우에 표시되는 사이트는 진정한 정규 웹사이트이지만, 팝업 페이지는 위장된 웹페이지라는 점이 특징적이다. 따라서, 정규 웹사이트를 보고 안심한 사용자가 팝업에 표시된 입력란에 인증번호나 비밀번호, 신용카드번호 등의 개인 금융 정보를 입력하여 송신하면 피싱을 시도하는 자에게 해당 정보가 송신되게 된다. 이러한 방법 외에도, 피싱 수법은 URL에 사용되는 특수한 서식을 이용하여, 마치 진정한 도메인에 링크되어 있는 것처럼 보이게 하거나, 팝업 윈도우의 어드레스바를 비표시로 하는 등의 교묘한 기술을 이용하고 있어 피해 사례가 증가하고 있다. 이하에서 인용된 비특허문헌에는 이러한 피싱의 다양한 유형과 이에 대한 대응 방안이 소개되어 있다.

[0004] 한편, 근래에 들어 메신저 피싱(messenger phishing)이라는 새로운 유형이 피싱이 등장하였다. 메신저 피싱이란, 문자 그대로 메신저를 이용한 피싱으로서, 타인의 메신저 아이디를 도용하여 로그인한 뒤 등록된 지인에게 메시지를 보내 금전을 요구하는 행위 등을 의미하는 것으로, 사회 공학적 해킹 기법의 한 종류이다. 즉, 메신저 피싱에서 피싱을 시도하는 대화 상대방은 인터넷 메신저 또는 채팅이 가능한 온라인 서비스에서 불법적으로 타인의 계정을 알아내어 접속한 뒤, 메신저 또는 서비스 내에 등록되어 있는 친구 목록을 살펴보고, 현재 접속하고 있는 사람에게 말을 걸어 지인인 것처럼 가장하여 부정하게 금전적인 이익을 얻게 된다. 이를 위해, 메신저 피싱 용의자는 타 사용자의 메신저 계정에 접속하여 메신저에 등록되어 있는 친구 목록을 살펴보고 접속하고 있는 사람에게 대화를 걸어 돈을 빌려달라고 하며 계좌이체 또는 무통장 입금을 유도한다.

[0005] 이러한 메신저 피싱은 용의자가 기계나 프로그램이 아닌 사람이라는 점에서, 보다 자연스럽고 사기 행위의 감지가 어렵다는 특징이 있다. 특히, 프로그램에 의해 획일적이고 순차적인 피싱 행위가 이루어지는 것이 아니기 때문에 기계적인 대응이 어려우며, 그 예방에 있어서도 전적으로 사용자의 주의가 요구되는 수준에 머물러 있다는 점이 문제점으로 지적된다. 따라서, 날이 갈수록 창궐하는 메신저 피싱을 정확하게 탐지하여 이에 적절히 대응할 수 있는 기술적 수단이 요구되는 바이다.

선행기술문헌

비특허문헌

[0006] (비특허문헌 0001) 피싱(Phishing) 위협 및 대응 방안, 이응용, 김윤정, 조규민, 정보통신산업진흥원, 2006.

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하고자 하는 기술적 과제는, 메신저 피싱에 대한 대응이 전적으로 사용자의 주의 수준에 머물러 있는 한계를 극복하고, 일부 메신저 피싱 탐지 기술들이 금융과 관련된 특정 단어가 입력될 경우 이에 반응하여 기계적인 경고 메시지를 표시함으로써 문맥상 메신저 피싱이 아닌 상황에서도 불필요한 경고 메시지가 노출되는 문제점을 해결하며, 빈번한 경고 메시지 노출에 의해 오히려 사용자의 주의가 저하되어 메신저 피싱 위협에 노출되는 부작용을 해소하고자 한다.

과제의 해결 수단

[0008] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 피싱 탐지 장치가 메신저를 통한 피싱을 탐

지하는 방법은, 상기 메신저의 대화 상대방이 대화를 시도하는 최초 시점으로부터 상기 피싱 탐지 장치가 소정 개수의 문장을 수신하여 수집하는 단계; 상기 피싱 탐지 장치가 상기 수집된 문장으로부터 대화 패턴을 분석하여 메시지의 위험치를 산출하는 단계; 및 상기 산출된 위험치가 미리 설정된 임계치 이상인지 여부를 상기 피싱 탐지 장치가 판단하는 단계;를 포함한다.

[0009] 상기된 메신저를 통한 피싱을 탐지하는 방법에서 상기 대화 패턴을 분석하는 단계는, 상기 수집된 문장 내에 포함된 키워드들에 대한 시간적인 순서와 위험도를 고려하여 수행된다. 또한, 수집된 문장으로부터 추출되는 키워드는, 인사말, 접속어 및 금융 관련 용어로 구분되는 것이 바람직하다.

[0010] 상기된 메신저를 통한 피싱을 탐지하는 방법에서 상기 대화 패턴을 분석하는 단계는, 형태소 분석을 이용하여 상기 수집된 문장 내에서 키워드를 추출하는 단계; 상기 추출된 키워드 중, 경어가 아닌 인사말이 존재하는지 여부를 판단하는 단계; 상기 경어가 아닌 인사말이 존재하는 경우, 상기 인사말 이후에 추출된 키워드 중, 화제를 전환하는 접속어가 존재하는지 여부를 판단하는 단계; 상기 접속어가 존재하는 경우, 상기 접속어 이후에 추출된 키워드 중, 금융 관련 용어가 존재하는지 여부를 판단하는 단계; 및 상기 금융 관련 용어가 존재하는 경우, 상기 금융 관련 용어 이후에 추출된 키워드 중, 금융 거래 정보가 존재하는지 여부를 판단하는 단계;를 포함한다.

[0011] 상기된 메신저를 통한 피싱을 탐지하는 방법에서 상기 대화 패턴을 분석하여 메시지의 위험치를 산출하는 단계는, 형태소 분석을 이용하여 상기 수집된 문장 내에서 키워드를 추출하는 단계; 상기 추출된 키워드가 미리 정의된 피싱 대화 패턴에 해당하는지 여부를 판단하는 단계; 상기 피싱 대화 패턴에 해당하는 키워드가 미리 정의된 피싱 단계에 순차적으로 대응되는지 여부를 판단하는 단계; 및 상기 피싱 단계에 대응되는 각각의 키워드에 대하여 가중치를 부여하고, 상기 부여된 가중치를 합산하는 단계;를 포함한다.

[0012] 또한, 상기된 메신저를 통한 피싱을 탐지하는 방법에서 상기 판단 결과 상기 산출된 위험치가 상기 임계치 이상인 경우, 상기 피싱 탐지 장치가 상기 대화 상대방에게 추가 인증 정보를 요청하는 단계;를 더 포함한다.

[0013] 나아가, 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 피싱 탐지 장치가 메신저를 통한 피싱을 탐지하는 방법은, 상기 피싱 탐지 장치가 상기 대화 상대방의 IP 주소를 수집하는 단계; 상기 피싱 탐지 장치가 상기 IP 주소에 대하여 지역 정보를 추출하는 단계; 및 상기 피싱 탐지 장치가 상기 추출된 지역 정보에 기초하여 상기 메시지의 위험치에 위험 가중치를 부여하는 단계;를 더 포함한다.

[0014] 상기된 메신저를 통한 피싱을 탐지하는 방법들에서, 상기 피싱 탐지 장치는 메신저 서버 또는 상기 메시지를 수신하는 클라이언트에 설치되는 것이 바람직하다.

[0015] 한편, 이하에서는 상기 기재된 피싱 탐지 장치가 메신저를 통한 피싱을 탐지하는 방법들을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

발명의 효과

[0016] 본 발명의 다양한 실시예들은 피싱을 시도하는 대화 상대방의 초반 메시지로부터 대화 패턴을 분석하여 메시지의 위험도를 산출함으로써 피싱 탐지 장치의 도움을 받아 메신저 피싱을 자동으로 탐지할 수 있고, 특정 단어에 대한 기계적인 반응이 아닌 문맥을 고려한 경고 메시지를 정확하게 노출함으로써 사용자의 주의 수준을 높일 수 있으며, 대화 상대방의 접속 IP 주소를 동시에 고려함으로써 메신저 피싱 탐지의 정확도를 향상시킬 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일 실시예에 따른 피싱 탐지 장치가 메신저를 통한 피싱을 탐지하는 방법을 도시한 흐름도이다.

도 2는 본 발명의 일 실시예에 따른 도 1의 피싱 탐지 방법에서 대화 패턴을 분석하여 메시지의 위험치를 산출하는 과정을 보다 구체적으로 도시한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 도 1의 피싱 탐지 방법에서 대화 상대방으로부터 수신되지 메시지의 시간적인 순서와 위험도를 고려하여 대화 패턴을 분석하는 과정을 보다 구체적으로 도시한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 피싱 탐지 장치가 메신저를 통한 피싱을 탐지하는 방법에서 대화 상대방의 IP 주소에 기반한 위험 가중치를 고려하여 메시지의 위험치를 산출하는 과정을 도시한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 메신저를 통한 피싱을 탐지하는 장치가 클라이언트에 구현된 경우를 예시한

시스템 블록도이다.

도 6은 본 발명의 일 실시예에 따른 메신저를 통한 피싱을 탐지하는 장치가 서버에 구현된 경우를 예시한 시스템 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0018] 본 발명의 실시예들을 설명하기에 앞서, 우선 본 발명의 실시예들이 구현되는 기술 분야, 즉 메신저 피싱에 대응한 보안 시스템의 운영 환경에 대해 간략히 소개하고, 이러한 실시예들이 구현되는 환경의 특징으로부터 안출될 수 있는 본 발명의 기본적인 아이디어를 제시하고자 한다.
- [0019] 앞서 간략히 소개한 바와 같이, 메신저 피싱은 본질적으로 실제 사람이 대화 상대방으로서, 메신저 사용자의 판단을 흐리게 하는 대화를 전송하게 된다. 이러한 일련의 대화 과정을 통해 메신저 피싱을 시도하는 용의자 내지 범죄자는 메신저 사용자로부터 자연스럽게 개인 금융 정보를 획득할 수 있게 된다. 따라서, 이러한 사람에 의한 대화 내용만으로 대화 상대방이 메신저 피싱을 시도하고 있는지를 판단하는 것은 기술적으로 매우 어려운 문제에 해당한다.
- [0020] 현재 메신저 피싱에 대한 보안 시스템으로는 금융과 관련된 특정 단어가 입력될 경우, 기계적으로 메신저 대화창에 경고 메시지를 표시하는 방법이 활용되고 있다. 예를 들어, '은행'이라는 단어가 입력되면 메신저 프로그램은 자동으로 메신저 피싱을 주의하라는 경고 메시지를 표시하게 된다. 그러나, 대화 상대방이 입력한 단어가 '은행(bank)'이 아닌 식물 '은행나무(ginkgo)'의 열매를 의미하는 경우였다면, 이러한 경고 메시지는 매우 부적절한 것이며, 대화를 방해하는데 지나지 않을 것이다. 따라서, 이러한 문제점으로 인해 실제의 메신저 피싱이 발생하는 상황보다 더 많은 경우에 불필요한 경고 메시지가 표시되게 되고, 메신저 사용자가 이러한 경고 메시지에 지속적이고 반복적으로 노출되게 될 경우 오히려 주의 수준이 저하될 우려가 존재한다.
- [0021] 한편, 대화 상대방의 접속 IP 주소가 국내가 아닌 해외의 IP 주소인 경우, 단순히 메신저 대화창에 해외 지역으로부터의 접속을 이유로 메신저 피싱을 주의하라는 경고 메시지를 기계적으로 표시하는 방법이 활용될 수도 있다. 그러나, 이러한 기계적인 IP 주소의 적용의 경우, 해외에 거주하는 지인과의 대화에 불필요한 경고 메시지를 표시함으로써 메신저 사용자 및 대화 상대방에게 불쾌감을 줄 수 있다. 이러한 경우 역시, 일반 사용자들이 보통의 대화 상대방과 일상적인 대화 중임에도 불구하고 지속적이고 반복적으로 경고 메시지가 노출됨으로 인해, 오히려 메신저 사용자의 주의 수준이 저하되는 결과를 야기할 수 있다.
- [0022] 나아가, 해외에 거주하는 불법적인 사용자가 메신저 피싱을 위해 프록시 서버(proxy server)나 가상 사설망(virtual private network, VPN) 등과 같은 네트워크 우회 수단을 이용하여 접속하거나 IP를 변조하여 접근할 경우, 마치 국내에서 접속한 것처럼 위장할 수 있어 메신저 피싱 여부를 정확하게 탐지할 수 없다는 한계가 존재한다.
- [0023] 따라서, 이하에서 제시되는 본 발명의 실시예들은 메신저 또는 채팅이 가능한 온라인 서비스에서 피싱 시도를 탐지하고, 적절한 시기에 경고를 하거나 자동으로 상대방을 검증함으로써 메신저 피싱 사고를 예방할 수 있는 기술적 수단을 제안하고자 한다. 이를 위해 본 발명의 실시예들은 크게 두 가지의 기술 요소를 포함할 수 있다.
- [0024] 첫째, 본 발명의 실시예들은 대화 상대방이 전송하는 메시지로부터 문맥을 고려하여 대화 패턴을 분석함으로써 대화 메시지의 위험 정도를 정량적으로 산출할 수 있다. 특히, 이러한 대화 패턴을 분석함에 있어, 메신저 피싱에 사용되는 용어들의 순서와 유형을 미리 정의하여 두고, 대화 상대방으로부터 실시간으로 입력되는 메시지가 정의된 규칙에 따르는지 여부를 검사함으로써 메시지의 위험치를 객관적으로 산출하게 된다.
- [0025] 둘째, 본 발명의 실시예들은 상기된 대화 패턴의 분석과 더불어 대화 상대방의 접속 IP 주소를 고려할 수 있다. 즉, 대화 상대방의 접속 IP만으로 메신저 피싱으로 간주하는 것이 아니라, 실제 대화의 내용에 메신저 피싱으로 추정되는 위험 요소가 존재하는지 여부와 대화 상대방이 위험 지역으로 분류된 IP 주소 대역으로부터 접속하고 있는지 여부를 동시에 고려함으로써 메신저 피싱 여부의 탐지 성능을 크게 향상시킬 수 있다.
- [0026] 이하에서는 도면을 참조하여 대화 패턴에 기반하여 메신저 피싱 시도를 탐지하는 본 발명의 실시예들을 보다 구체적으로 설명한다.
- [0027] 도 1은 본 발명의 일 실시예에 따른 피싱 탐지 장치가 메신저를 통한 피싱을 탐지하는 방법을 도시한 흐름도로써, 다음과 같은 단계들을 포함한다.
- [0028] 110 단계에서, 피싱 탐지 장치는 메신저의 대화 상대방이 대화를 시도하는 최초 시점으로부터 일정 개수의 문장

을 수신하여 수집한다. 메신저 피싱은 그 시작이 모두 대화 상대방(피싱을 시도하는 용의자 내지 범죄자)에 의해 이루어진다는 특징을 갖는다. 따라서, 메신저 사용자(보통의 사용자)가 먼저 대화를 시작하는 경우는 메신저 피싱으로 간주하지 않는다. 또한, 메신저 피싱을 시도하는 대화 상대방은 자신이 의도한 바대로 대화를 이끌어 가야 하기 때문에 대화를 시도한 이후 초반 대화 내에서 일정한 패턴 내지 경향을 갖는다. 따라서, 피싱 탐지 장치는 메신저의 대화 상대방이 대화를 시도한 이후, 일정 개수의 문장에 집중하여 이를 수집할 필요가 있다.

[0029] 이 때, 피싱 탐지 장치가 수집하는 대상 문장은 대략 10 내지 15개 정도의 문장인 경우가 보편적인 것으로 조사되었다. 따라서, 본 발명의 실시예들은 이러한 개수(대화 초반의 10 내지 15개의 문장)의 문장에 집중하여 수집하는 것이 바람직하다. 그러나, 이러한 수집 대상 문장의 개수는 본 발명이 구현되는 환경, 또는 사용 언어에 따라 유연하게 확장 내지 축소가 가능하다.

[0030] 120 단계에서, 피싱 탐지 장치는 110 단계를 통해 수집된 문장으로부터 대화 패턴을 분석하여 메시지의 위험치를 산출한다. 이 과정은 피싱 탐지 장치가 수집된 문장으로부터 대화의 문맥을 파악하는 단계에 해당한다. 이를 위해 피싱 탐지 장치는 수집된 문장의 형태소를 분석하여 이로부터 키워드를 추출하고, 추출된 키워드들에 대해 미리 정의된 규칙을 적용하여 현재 입력된 대화의 메시지가 메신저 피싱의 대화 패턴에 해당하는지 여부를 판단한다. 각각의 키워드들에는 이에 상응하는 위험치가 부여되어 있으며, 일련의 메신저 피싱 과정을 통해 수집된 대화 메시지에서부터 개별 위험치가 합산되어 결과값이 산출된다. 보다 구체적인 패턴 분석 과정은 이후에 도 2 및 도 3을 통해 자세히 설명하도록 한다.

[0031] 130 단계에서, 피싱 탐지 장치는 120 단계를 통해 산출된 위험치가 미리 설정된 임계치 이상인지 여부를 판단함으로써 메신저 피싱 시도를 탐지한다. 이러한 임계치는 메신저 제작자에 의해 미리 적절한 수준으로 설정되어 공급될 수 있으나, 필요에 따라서는 사용자에게 의해 그 수준의 조절이 가능하도록 구현될 수도 있다. 대화 상대방인 보통의 메신저 사용자이어서 산출된 위험치가 여전히 임계치 이하인 경우에는 160 단계로 진행하여 지속적으로 메신저 세션을 유지한다.

[0032] 반면, 산출된 위험치가 임계치 이상인 경우에는 메신저 피싱이 시도중인 것으로 판단된다. 이 때, 임계치 이상인 경우 전체에 대하여 일괄적으로 메신저 피싱을 알리는 경고 메시지가 표시될 수도 있지만, 산출된 위험치의 정도에 따라 구간을 나누어 위험 정도를 구분할 수도 있을 것이다. 후자의 경우, 구분된 위험 정도에 따라 대응 방법이 달라질 수도 있을 것이며, 필요에 따라서는 경고 메시지를 정상적인 메신저 사용자에게만 표시할 수도 있을 것이다. 예를 들어, 현재 메신저 사용자(보통 사용자)에게는 대화 상대방이 메신저 피싱을 시도하고 있다는 경고를 표시하고, 대화 상대방에 대한 대응 방법(세션 차단 내지 대화 상대방의 메신저 계정을 소유한 진정 소유자에게 SMS 전송 등이 될 수 있다.)을 선택하도록 제시할 수도 있다. 또한, 구분된 위험 정도가 최고 위험 수준인 경우에는 사이버수사대에 신고하는 대응안이 추가로 제시될 수도 있다.

[0033] 한편, 130 단계를 통한 판단 결과 120 단계를 통해 산출된 위험치가 미리 설정된 임계치 이상인 경우에, 140 단계에서는 피싱 탐지 장치가 대화 상대방에게 추가 인증 정보를 요청할 수 있다. 여기서, 추가 인증 정보는 현재 접속 중인 대화 상대방이 진정한 계정 사용자인지 여부를 식별할 수 있는 정보가 된다. 예를 들어, 메신저 서비스의 최초 가입시 사용되었던 휴대전화 번호나 이메일 주소가 존재하는 경우, 휴대전화나 이메일을 통해 인증 코드를 전송하고, 수신된 인증 코드를 제차 메신저 인증창에 입력할 것을 요구할 수 있다.

[0034] 또는, 메신저 서비스의 최초 가입시 자신만이 알 수 있는 질문에 대한 답변이 기재된 경우, 이를 현재 접속 중인 대화 상대방에게 표시하여 응답을 요구할 수도 있다. 예를 들어, 메신저 사용자가 실제로는 형이 없는데도 불구하고, "어제 우리 형 만났다면?"과 같은 질문을 자동으로 대화 상대방에게 표시할 수도 있다. 이 때, 대화 상대방의 응답을 보고, 사실과 다른 답변이 회신되거나 무응답으로 반응할 경우, 대화 상대방을 피싱을 시도하는 사람으로 간주할 수 있다.

[0035] 이상과 같은 인증 과정은 선택적으로 포함될 수 있으며, 앞서 제시한 다양한 대응안 중 하나로서 구현될 수 있다.

[0036] 150 단계에서, 만약 대화 상대방이 140 단계의 추가 인증 정보 요청에 대해 응답하지 않은 경우, 피싱 탐지 장치는 대화 상대방의 서비스 이용을 차단할 수 있다. 이를 위해 피싱 탐지 장치는 140 단계의 추가 인증 정보의 요청 이후 일정 시간을 대기한 후, 해당 시간 내에 응답이 없는 경우에 대화 상대방의 계정에 대한 서비스 이용을 차단하거나 세션을 종료할 수 있다.

[0037] 또한, 피싱 탐지 장치는 메신저 도용을 경고하는 알림 메시지를 진정 사용자(계정이 도용된 메신저 사용자)에게 전송할 수 있다. 이 경우, 피싱 탐지 장치는 해당 계정의 진정한 사용자 정보를 참조하여 SMS나 이메일을 통해

알림 메시지를 전송하는 것이 바람직하다. 이러한 알림 메시지 내에는 계정 도용의 의심 사실과 계정 도용에 대한 조치 방법을 안내하는 문구가 포함될 수 있다.

- [0038] 이상에서 기술된 일련의 단계들은 피싱 탐지 장치를 통해 수행되는 것으로, 물리적으로는 적어도 하나 이상의 프로세서(processor)를 포함하여 구현될 수 있다. 즉, 피싱 탐지 장치는 전자적 형태로 입력되는 데이터를 수신하여 정의된 연산을 처리하고, 화면에 표시될 결과값을 산출한다. 이러한 처리 과정에서 본 실시예에는 하나 이상의 프로세서뿐만 아니라, 연산을 위한 임시 내지 영구적인 데이터들을 저장하는 메모리(memory)와 이러한 연산 과정을 정의하고 각각의 하드웨어를 적절히 제어하는 소프트웨어(software) 코드를 포함할 수 있다.
- [0039] 도 2는 본 발명의 일 실시예에 따른 도 1의 피싱 탐지 방법에서 대화 패턴을 분석하여 메시지의 위험치를 산출하는 과정을 보다 구체적으로 도시한 흐름도로서, 피싱 탐지 장치가 일정 개수의 문장을 수신하여 수집한 단계(110) 직후를 가정한다.
- [0040] 210 단계에서, 피싱 탐지 장치는 형태소 분석을 이용하여 문장 내에서 키워드를 추출한다. 즉, 수집된 문장 내에서 문맥상 유의미한 키워드들을 추출하여 패턴 분석의 대상으로 설정한다. 형태소를 분석하는 다양한 방법과 기술적 수단은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 적절히 선택되어 활용될 수 있으며, 본 발명의 본질을 흐릴 우려가 있는 바, 여기서는 그 구체적인 설명을 생략한다.
- [0041] 220 단계에서, 피싱 탐지 장치는 추출된 키워드로부터 대화 패턴을 분석한다. 보다 구체적으로, 221 단계에서는 추출된 키워드가 미리 정의된 피싱 대화 패턴에 해당하는지 여부를 판단하고, 이어서 222 단계를 통해 피싱 대화 패턴에 해당하는 키워드 또한 미리 정의된 피싱 단계에 순차적으로 대응되는지 여부를 판단한다. 즉, 221 단계 및 222 단계를 통한 대화 패턴을 분석하는 과정은, 110 단계를 통해 수집된 문장 내에 포함된 키워드들에 대한 시간적인 순서와 위험도를 고려하여 수행된다.
- [0042] 메신저 피싱의 경우, 피싱을 시도하는 대화 상대방은 최초의 대화 시작 시점부터 실질적인 금융 정보 요구 과정에 이르는 대화 내용에 대화를 이끌어가는 일련의 흐름과 논리가 발견되었는데, 220 단계에서는 이를 발굴하여 피싱 대화 패턴으로 정의한 것이다. 특히, 메신저 피싱을 위한 대화 패턴에서는 키워드의 유형과 순서에 특징이 존재하는데 양자는 독립적인 변인이 아니라 서로 일정한 상관 관계를 갖는다. 예를 들어, 대화를 시작하는 인사말(greeting)이 등장한 이후에야 비로소 일상적인 대화 시도가 이루어지고, 다시 금융과 관련된 이야기로 화제를 전환하는 키워드들이 나타나게 된다. 따라서, 이상의 예에서 '인사말' → '화제 전환' → '금융 관련 용어'는 순차적으로 대화 내에서 등장하게 되며, 이러한 순서는 반드시 지켜지게 된다. 만약, 대화 상대방이 '금융 관련 용어'를 사용한 직후, '화제를 전환하여' 다른 이야기를 진행한다면, 이러한 대화 상대방은 메신저 피싱을 시도하는 사람이 아닐 가능성이 크다. 따라서, 추출된 키워드로부터 판단된 대화 패턴이 반드시 미리 정의된 피싱 대화 패턴에 따른 순서와 일치하는지 여부를 검사할 필요성이 있다.
- [0043] 이제, 230 단계를 통해 피싱 탐지 장치는 피싱 단계에 대응되는 각각의 키워드에 대하여 가중치를 부여하고 부여된 가중치를 합산함으로써 메시지의 위험치를 산출한다. 즉, 대화의 전개 방향에 따라 정의된 피싱 단계마다 가중치가 부여되고, 대화 상대방으로부터 수집된 문장 전체를 통해 부여된 각각의 가중치들을 모두 합산하여 메시지의 위험치에 대한 결과값을 산출한다.
- [0044] 한편, 230 단계를 통한 가중치의 합산에 있어서, 피싱 단계의 시간적인 순서가 뒤로 갈수록 가중치에 상대적으로 높은 값이 부여되는 것이 바람직하다. 왜냐하면, 일반적으로 메신저 피싱의 경우 대화의 각 단계를 거치면서 위험도가 더욱 증가하기 때문이다. 예를 들어, 인사말 이후에 화제 전환을 나타내는 키워드가 등장한 경우에도, 보통의 사용자라면 주말에 있었던 야구 경기의 결과에 대해 이야기할 수 있을 것이다. 이러한 경우 메시지의 위험도는 더 이상 증가하지 않게 된다. 반면, 메신저 피싱을 시도하는 사용자라면, 대화의 진행에 따라 보다 높은 수준의 사용자 금융 정보를 요구하게 되므로, 230 단계를 통해 부여되는 가중치는 시간의 경과 및 대화의 흐름에 따라 증가하도록 설정되는 것이 바람직하다.
- [0045] 도 3은 본 발명의 일 실시예에 따른 도 1의 피싱 탐지 방법에서 대화 상대방으로부터 수신되지 메시지의 시간적인 순서와 위험도를 고려하여 대화 패턴을 분석하는 과정을 보다 구체적으로 도시한 흐름도로서, 도 2의 경우와 마찬가지로 피싱 탐지 장치가 일정 개수의 문장을 수신하여 수집한 단계(110) 직후를 가정하고 있다.
- [0046] 310 단계에서, 피싱 탐지 장치는 형태소 분석을 이용하여 문장 내에서 키워드를 추출한다. 이 때, 수집된 문장으로부터 추출되는 키워드는, 인사말, 접속어 및 금융 관련 용어로 구분되는 것이 바람직하나, 본 발명의 실시예들이 구현되는 환경에 따른 표본 조사를 통해 다양하게 확장 및 변경될 수 있다.
- [0047] 320 단계에서, 피싱 탐지 장치는 추출된 키워드에 대한 패턴 분석을 단계적으로 수행한다. 각각의 분석 과정을

정의된 순서에 따라 보다 구체적으로 설명한다.

- [0048] 321 단계에서는 추출된 키워드 중, 경어가 아닌 인사말이 존재하는지 여부를 판단한다. 메신저 피싱을 시도할 때, 보통 용의자는 "자리에 있어?", "잘 지내지?" 등과 같은 반말로 인사를 건네는 것이 일반적으로 조사되었다. 따라서, 경어가 아닌 인사말에 대한 데이터베이스를 구축하고, 추출된 키워드가 이에 해당할 경우, 잠정적으로 메신저 피싱의 시작으로 간주할 수 있다. 물론 이 경우에는 앞서 도 2를 통해 설명한 바와 같이 상대적으로 위험 정도가 낮음을 의미하는 다소 낮은 값의 가중치가 부여될 수 있을 것이다.
- [0049] 322 단계에서, 피싱 탐지 장치는 321 단계를 통해 경어가 아닌 인사말이 존재하는 경우에 검사를 시도하게 되는데, 인사말 이후에 추출된 키워드 중, 화제를 전환하는 접속어가 존재하는지 여부를 판단하게 된다. 통상적으로 메신저 피싱을 시도하는 용의자는 인사말 이후에 기타 연관성이 없는 몇 마디의 말을 더 건넨 뒤, 반전형의 접속어(예를 들어, "근데", "부탁이 있는데", "다름이 아니라", "참 저기 있잖아" 등이 될 수 있다.)를 이용하여 화제를 전환하는 문장을 사용하는 경향이 있는 것으로 발견되었다. 따라서, 이러한 화제 전환형 접속어에 대한 데이터베이스를 구축하고, 추출된 키워드가 이에 해당할 경우, 메신저 피싱이 진행되었다고 간주할 수 있다. 이 경우에는 앞서 321 단계를 통해 부여된 가중치보다는 상대적으로 더 큰 값이 부여될 수 있다.
- [0050] 323 단계에서, 피싱 탐지 장치는 322 단계를 통해 접속어가 존재하는 경우에 검사를 시도하게 되는데, 접속어 이후에 추출된 키워드 중, 금융 관련 용어가 존재하는지 여부를 판단하게 된다. 메신저 피싱을 시도하는 용의자가 화제 전환 이후, 곧바로 금융 관련 용어(예를 들어, "계좌 이체", "인터넷 뱅킹" 등이 될 수 있다.)로 대화를 시도하는 경향이 있는 것으로 발견되었다. 따라서, 이러한 금융 관련 용어에 관한 데이터베이스를 구축하고, 추출된 키워드가 이에 해당할 경우, 메신저 피싱이 보다 진행되었다고 간주할 수 있다. 이 경우에는 앞서 322 단계를 통해 부여된 가중치보다는 상대적으로 더 큰 값이 부여될 수 있다.
- [0051] 마지막으로, 324 단계에서, 피싱 탐지 장치는 323 단계를 통해 금융 관련 용어가 존재하는 경우에 검사를 시도하게 되는데, 금융 관련 용어 이후에 추출된 키워드 중, 금융 거래 정보가 존재하는지 여부를 판단하게 된다. 비록 앞서 323 단계를 통해 기술한 바와 같이 대화 중에 금융 관련 용어가 등장했다고 할지라도, 대화 상대방이 메신저 피싱을 시도하는 것으로 단정적으로 결론내릴 수는 없다. 왜냐하면, 보통의 대화 상대방이 단순히 경제 상황에 대한 이야기를 하는 경우도 있기 때문이다. 따라서, 대화의 문맥을 정확하게 파악하여, 대화 상대방이 전개하는 금융 관련 이야기가 메신저 사용자로 하여금 경제적인 손해를 끼치려 하는 메신저 피싱 행위인지를 판단하는 과정이 필요하다. 이를 위해 본 발명의 실시예는 324 단계를 통해 메신저 사용자와 관련하여 경제적으로 손해를 끼칠 수 있는 금융 거래 행위에 대한 요청(예를 들어, "특정 은행 이름", "계좌 번호", "구체적인 부족 금액"이 될 수 있다.)이 있는지 여부를 재차 검사하게 된다. 따라서, 이러한 금융 거래 정보에 관한 데이터베이스를 구축하고, 추출된 키워드가 이에 해당할 경우, 비로소 메신저 피싱이 시도되고 있다고 간주할 수 있다. 물론, 필요에 따라서는 323 단계의 검사만으로도 메신저 피싱의 시도로 간주될 수도 있을 것이며, 이러한 결정은 설정된 보안 수준에 따라 유연하게 적용될 수 있다. 이제, 324 단계를 통해 금융 거래 정보가 존재한다고 판단된 경우에는 이상에서 부여된 가중치들에 비해 상대적으로 가장 큰 값이 부여될 수 있다.
- [0052] 마지막으로, 330 단계에서는 각각의 키워드에 대하여 부여된 가중치를 합산하여 메시지의 위험치를 산출하게 된다.
- [0053] 도 4는 본 발명의 일 실시예에 따른 피싱 탐지 장치가 메신저를 통한 피싱을 탐지하는 방법에서 대화 상대방의 IP 주소에 기반한 위험 가중치를 고려하여 메시지의 위험치를 산출하는 과정을 도시한 흐름도로서, 앞서 도 1 내지 도 3을 통해 기술한 대화 패턴을 분석하는 방법에 선택적이고 부가적으로 수행될 수 있다. 110 단계 및 120 단계는 도 1을 통해 설명한 바 있으므로, 여기서는 중복을 피해 410 단계 내지 430 단계에 집중하여 설명하도록 한다.
- [0054] 410 단계에서, 피싱 탐지 장치는 대화 상대방의 IP 주소를 수집한다.
- [0055] 420 단계에서, 피싱 탐지 장치는 410 단계를 통해 수집된 IP 주소에 대하여 지역 정보를 추출한다. 이 때, 지역 정보는 국가 코드 내지 도시 위치 정보가 될 수 있으며, 이러한 지역 정보는 GeoIP 등과 같은 데이터베이스를 이용해 추출될 수 있다. GeoIP는 주어진 호스트 또는 IP 주소에 대해 해당 주소의 국가, 도시 또는 ISP 정보를 반환할 수 있으며, 이를 위해 호스트/IP 주소를 국가/도시/ISP 정보와 사상시켜 저장한다. 요약하건대, 서버가 지역 정보를 추출하는 과정은, 수집된 접속 IP 주소를 이용하여 IP 주소 대역과 지역 정보를 사상시킨 데이터베이스에 질의하고, 질의에 대응하는 지역 정보를 응답받음으로써 수행된다. 또한, 편의상 응답받는 지역 정보는 국가 코드 또는 도시 코드 중 적어도 하나인 것이 바람직하다.

- [0056] 430 단계에서, 피싱 탐지 장치 420 단계를 통해 추출된 지역 정보에 기초하여 메시지의 위험치에 위험 가중치를 산출한다. 지역에 따라서는 메신저 피싱 우범 지역으로 설정된 지역이 있을 수 있으며, 대화 상대방이 해당 우범 지역에서 접속을 시도하는 경우에는 매우 높은 수준의 위험 가중치가 부여될 수 있다.
- [0057] 이제, 125 단계에서는 110 단계 및 120 단계를 통해 대화 패턴을 분석하여 산출된 메시지의 위험치에 410 단계 내지 430 단계를 통해 IP 주소를 분석하여 산출된 위험 가중치를 합산하게 된다. 이러한 구성을 통해 단지 IP 주소만을 통해 메신저 피싱 여부를 판단함으로써 야기될 수 있는 무분별한 경고 메시지를 감소시킬 수 있으며, 보다 정확한 메신저 피싱 여부를 탐지할 수 있다.
- [0058] 한편, 이상에서 도 1 내지 도 4를 통해 기술된 피싱 탐지 장치는 메신저 서버 또는 상기 메시지를 수신하는 클라이언트 어디에도 구현 내지 설치될 수 있다. 이러한 설치는 본 발명의 실시예들이 구현되는 통신 환경 내지 응용 프로그램의 특성에 따라 유연하게 결정될 수 있다. 이하에서는 이상의 2 가지 경우에 기초하여 각각의 구현예를 도 5 및 도 6을 통해 설명하고자 한다. 각각의 하드웨어 구성이 수행하는 역할은 앞서 도 1 내지 도 4를 통해 이미 구체적으로 설명하였으므로, 이하에서는 설명의 중복을 피하기 위해 하드웨어의 구성을 중심으로 해당 구성의 개괄적인 역할에 대해서만 약술하도록 한다.
- [0059] 도 5는 본 발명의 일 실시예에 따른 메신저를 통한 피싱을 탐지하는 장치가 클라이언트(20)에 구현된 경우를 예시한 시스템 블록도로서, 비록 메신저 서비스를 제공하기 위해 별도의 메신저 서버(미도시)가 활용될 수 있으나, 피싱 탐지에 집중하여 대화 상대방(10)과 클라이언트(20)만을 도시하였다. 또한, 본 시스템은 메신저 피싱이 탐지된 경우, 이를 진정 사용자(계정이 도용된 메신저 서비스 가입자를 의미한다.)에게 통지하기 위한 알람 서버(40)를 선택적으로 포함할 수 있다.
- [0060] 통신부(21)는 대화 상대방(10)과 메신저 사용자(20)가 서로 대화를 주고받을 수 있도록 데이터 및 메시지 패킷을 송수신하는 역할을 수행한다.
- [0061] 처리부(22)는 메신저의 대화 상대방이 대화를 시도하는 최초 시점으로부터 일정 개수의 문장을 수신하여 수집하고, 수집된 문장으로부터 대화 패턴을 분석하여 메시지의 위험치를 산출한다. 이 과정에서 미리 정의된 대화 패턴 분석 데이터베이스(23)를 참고할 수 있으며, 필요에 따라서는 새롭게 발견된 피싱 위험 패턴을 대화 패턴 분석 데이터베이스(23)에 갱신할 수도 있을 것이다. 처리부(22)는 이상의 과정을 통해 산출된 위험치가 미리 설정된 임계치 이상인지 여부를 판단함으로써 메신저 피싱을 탐지할 수 있다.
- [0062] 만약 메신저 피싱 시도가 탐지된 경우, 처리부(22)는 대화 상대방(10)에게 추가 인증 정보를 요청할 수 있으며, 일정 시간 내에 이러한 추가 인증 정보 요청에 대해 응답하지 못하는 경우, 대화 상대방(10)의 계정에 대한 서비스 이용을 차단하고, 계정의 사용자 정보를 참조하여 알람 서버(40)를 통해 진정 사용자에게 알람 메시지를 전송한다. 이 때, 알람 서버(40)는 진정 사용자의 계정 정보에 접근할 수 있어야 하고, 편의상 메신저 서비스의 서버와 동일한 하드웨어로 구성될 수도 있을 것이다.
- [0063] 한편, 처리부(22)는 통신부(21)를 통해 수신된 대화 상대방(10)의 메시지를 통해 대화 상대방(10)의 IP 주소를 수집하고, GeoIP 데이터베이스(24)를 참조하여 IP 주소에 대한 지역 정보를 추출할 수 있다. 이를 통해 처리부(22)는 추출된 지역 정보에 기초하여 메시지의 위험치에 대한 위험 가중치를 부여할 수 있다.
- [0064] 도 6은 본 발명의 일 실시예에 따른 메신저를 통한 피싱을 탐지하는 장치가 서버에 구현된 경우를 예시한 시스템 블록도로서, 대화 상대방(10)과 메신저 사용자(20) 이외에 별도의 서버(30)를 통해 메신저 피싱을 탐지하도록 구성되었다. 또한, 본 시스템은 메신저 피싱이 탐지된 경우, 이를 진정 사용자(계정이 도용된 메신저 서비스 가입자를 의미한다.)에게 통지하기 위한 알람 서버(40)를 선택적으로 포함할 수 있다.
- [0065] 이 경우, 서버(30)는 메신저 서비스를 제공하는 메신저 서버와 동일한 하드웨어로 구현되는 것이 바람직하나, 필요에 따라서는 구분된 하드웨어로서 구현될 수도 있을 것이다. 피싱을 탐지하는 서버(30)의 개별 구성요소인 통신부(31), 처리부(32), 대화 패턴 분석 데이터베이스(33) 및 GeoIP 데이터베이스(34)는 앞서 도 5를 통해 설명한 바와 동일하다.
- [0066] 상기된 본 발명의 실시예들에 따르면, 피싱을 시도하는 대화 상대방의 초반 메시지로부터 대화 패턴을 분석하여 메시지의 위험도를 산출함으로써 피싱 탐지 장치의 도움을 받아 메신저 피싱을 자동으로 탐지할 수 있고, 특정 단어에 대한 기계적인 반응이 아닌 문맥을 고려한 경고 메시지를 정확하게 노출함으로써 사용자의 주의 수준을 높일 수 있다.
- [0067] 본 발명의 실시예들에 따르면, 대화 전체를 분석할 필요 없이 메신저 피싱의 증후를 감지할 수 있는 초기 대화

패턴의 분석을 통해 메신저 피싱의 조기 탐지가 가능하다. 메신저 피싱을 시도하는 범죄자가 대화 문장을 다양하게 변경하더라도, 대화의 톤과 사용되는 단어의 분포 및 대화의 형태소를 분석하여 반말과 존댓말의 구별이 가능하고, 해당 대화가 메신저 피싱을 유도하는 패턴인지 여부를 판정할 수 있다는 장점을 갖는다. 특히, 본 발명의 실시예들은 단어 그 자체에 기계적으로 반응하는 것이 아닌, 패턴 분석에 기반한 탐지 시스템이므로, 정상적인 대화에서 경고 메시지가 상대적으로 적게 노출된다는 점이 차별화된다.

[0068] 또한, 대화 상대방의 접속 IP 주소를 동시에 고려함으로써 메신저 피싱 탐지의 정확도를 향상시킬 수 있을 뿐만 아니라, 진정 사용자인지 여부를 판단하기 위한 본인 인증이 자동으로 수행됨으로써, 본인 인증에 실패한 경우 자동으로 세션을 끊기 때문에 메신저 피싱의 피해를 효과적으로 줄일 수 있다.

[0069] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0070] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0071] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0072] 10 : 메신저 대화 상대방 (피싱을 시도하는 상대방)

20 : 메신저 사용자

30 : 메신저 서버 (피싱 탐지 장치)

21, 31 : 통신부

22, 32 : 처리부

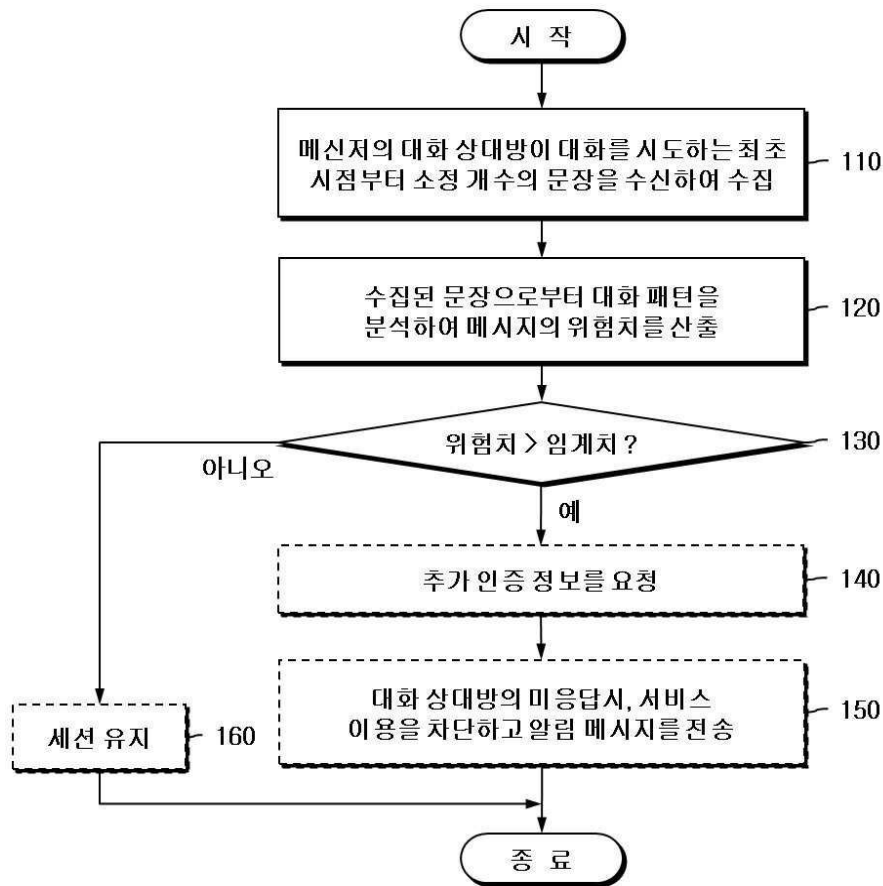
23, 33 : 대화 패턴 분석 DB

24, 34 : GeoIP DB

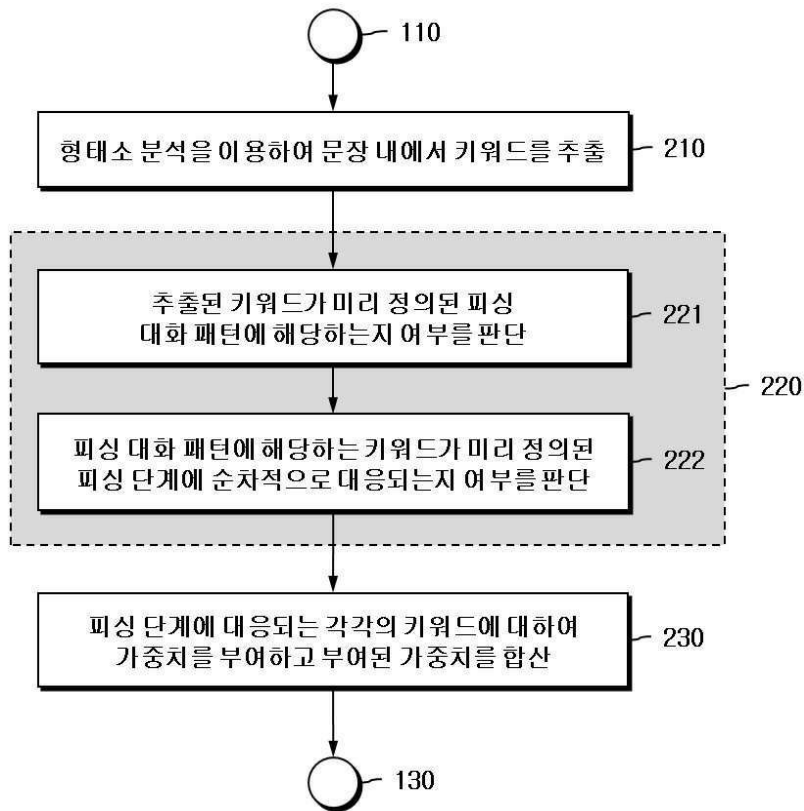
40 : 알림 서버

도면

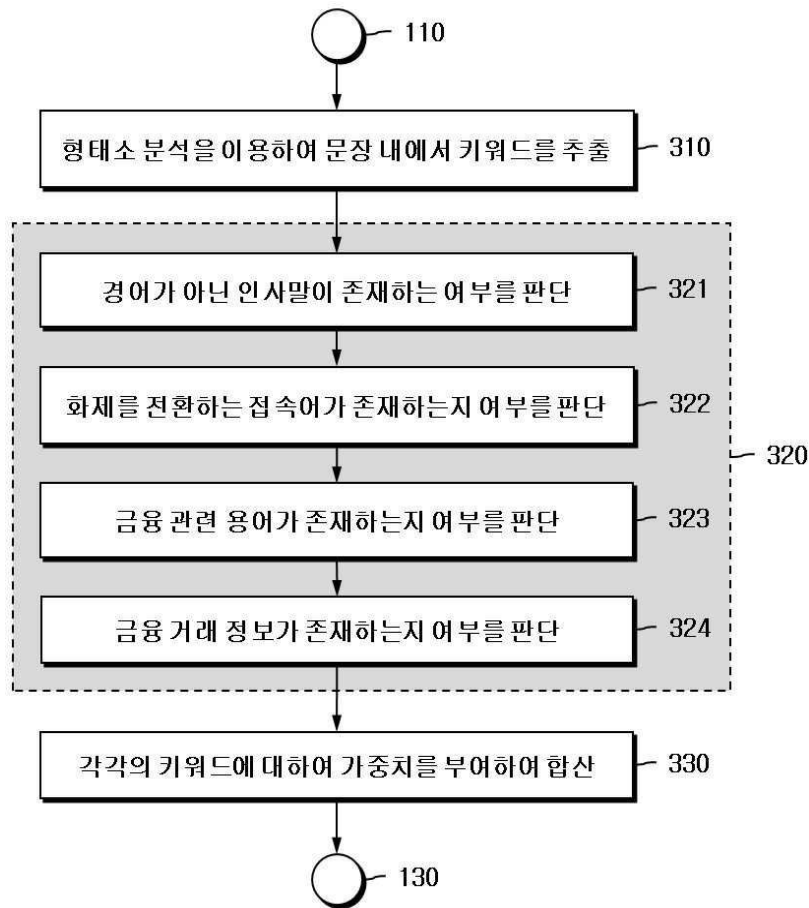
도면1



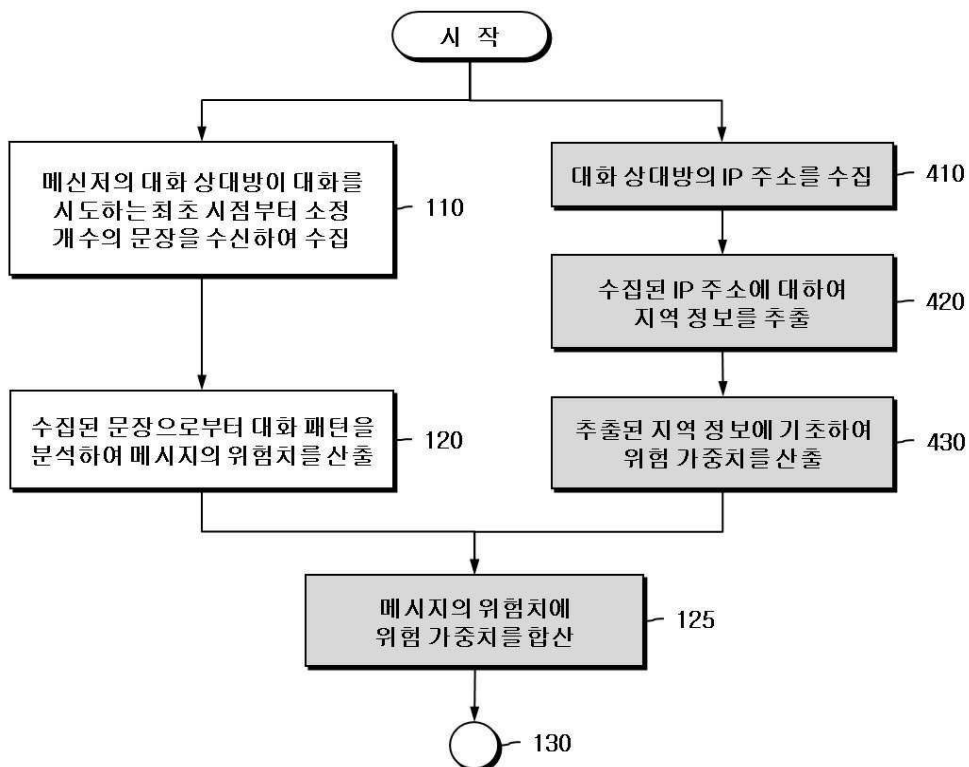
도면2



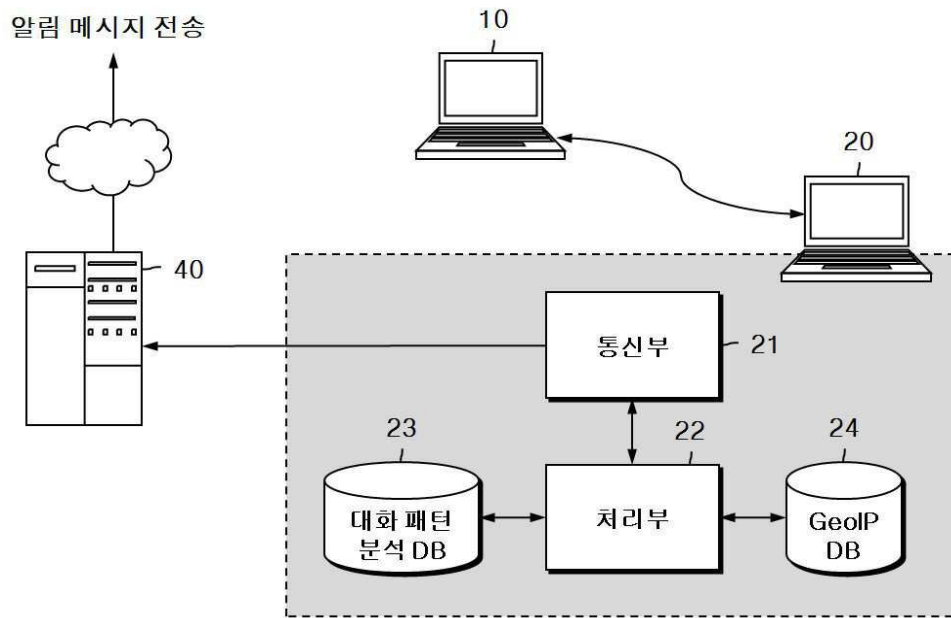
도면3



도면4



도면5



도면6

