(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0091786
(43) 공개일자 2025년06월23일

(51) 국제특허분류(Int. Cl.)
G06F 21/14 (2013.01) *G06F 21/12* (2013.01)
(52) CPC특허분류
G06F 21/14 (2013.01)
G06F 21/128 (2013.01)
(21) 출원번호 10-2023-0182097
(22) 출원일자 2023년12월14일
심사청구일자 2023년12월14일

(71) 출원인
울산과학기술원
울산광역시 울주군 언양읍 유니스트길 50
(72) 발명자
전유석
울산광역시 울주군 언양읍 유니스트길 50
(74) 대리인
리앤목특허법인

전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **웹 페이지 추적기 탐지 장치, 웹 페이지 추적기 탐지 방법, 및 컴퓨터 프로그램**

(57) 요 약

본 개시의 실시예들에 따르면, 웹 페이지의 추적 스크립트에 의해 수집되는 데이터를 모니터링하여 개인 프라이버시가 훼손되는 데이터 수집에 대해서 제공할 수 있다. 또한, HTML 문서에 포함되는 분기 지점들 각각에 대한 스크립트를 실행시키는 하나 이상의 강제 실행 문을 생성하고, 강제 실행 문을 이용하여 추적 스크립트를 추출함으로써, 숨겨진 개인 정보 추적 스크립트를 검출할 수 있다. 또한, HTML 문서에 대한 정적 변수 흐름 데이터를 생성하고, 정적 변수 흐름 데이터를 이용하여 HTML 문서를 실행 시킴으로써, 실제 실행 전에 개인 정보에 대한 추적 스크립트를 검출할 수 있다. 또한, 추적 스크립트에 대한 정보를 사용자에게 제공함으로써, 렌더링된 웹 사이트 외에 웹 사이트에서 이루어지는 숨겨진 추적 기능을 확인할 수 있다.

대 표 도 - 도1

1



이 발명을 지원한 국가연구개발사업

과제고유번호	1781000016
과제번호	KISA-2022-002
부처명	개인정보보호위원회
과제관리(전문)기관명	한국인터넷진흥원
연구사업명	개인정보보호강화기술연구개발(R&D)
연구과제명	브라우저상 수집되는 정보주체의 온라인 행태정보 탐지 및 자기 통제기술 개발
기 여 율	1/1
과제수행기관명	숭실대학교 산학협력단
연구기간	2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

추적기 탐지 장치가, 접속하고자 하는 웹 사이트의 HTML 문서를 수신하고, 상기 HTML 문서를 분석하여, 추적 스크립트를 추출하는 단계;

상기 추적기 탐지 장치가, 상기 추적 스크립트에 포함된 사용자 소스 정보와 싱크 영역을 고려하여 상기 추적 스크립트의 유해 여부를 판단하는 단계; 및

상기 추적기 탐지 장치가, 유해한 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이하는 단계;를 포함하는, 추적기 탐지 방법.

청구항 2

제1항에 있어서,

상기 추적 스크립트를 추출하는 단계는,

상기 HTML 문서를 동적 분석하여 정적 변수 흐름 데이터를 생성하고, 상기 정적 변수 흐름 데이터를 이용하여 사용자 소스 정보 및 싱크 영역 정보를 추출하는 단계를 더 포함하는, 추적기 탐지 방법.

청구항 3

제2항에 있어서,

상기 정적 변수 흐름 데이터는,

프로그램을 실행하지 않고 프로그램의 실행 과정에서의 변수에 대한 값의 흐름에 대한 데이터인, 추적기 탐지 방법.

청구항 4

제2항에 있어서,

상기 추적 스크립트를 추출하는 단계는,

상기 HTML 문서에 강제 실행 문을 따른 동적 분석을 수행하여, 상기 HTML 문서에 포함된 분기 지점에서의 모든 경우들에 대해서 실행되도록 하는 단계를 더 포함하는, 추적기 탐지 방법.

청구항 5

제1항에 있어서,

상기 유해 여부를 판단하는 단계는

상기 추적 스크립트의 사용자 소스 정보가 기 설정된 사용자 소스 정보의 테이블에 포함되고, 상기 싱크 영역 정보가 기 설정된 싱크 영역 정보의 테이블에 포함되는 경우인지 여부를 판단하여, 상기 추적 스크립트의 유해 여부를 판단하는, 추적기 탐지 방법.

청구항 6

통신부, 메모리 및 프로세서를 포함하고,

상기 프로세서가, 접속하고자 하는 웹 사이트의 HTML 문서를 수신하고, 상기 HTML 문서를 분석하여, 추적 스크립트를 추출하고,

상기 추적 스크립트에 포함된 사용자 소스 정보와 싱크 영역을 고려하여 상기 추적 스크립트의 유해 여부를 판단하며,

유해한 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이하는, 추적기 탐지 장치.

청구항 7

제6항에 있어서,

상기 프로세서가,

상기 HTML 문서를 동적 분석하여 정적 변수 흐름 데이터를 생성하고, 상기 정적 변수 흐름 데이터를 이용하여 사용자 소스 정보 및 싱크 영역 정보를 추출하는, 추적기 탐지 장치.

청구항 8

제7항에 있어서,

상기 정적 변수 흐름 데이터는,

프로그램을 실행하지 않고 프로그램의 실행 과정에서의 변수에 대한 값의 흐름에 대한 데이터인, 추적기 탐지 장치.

청구항 9

제7항에 있어서,

상기 프로세서가,

상기 HTML 문서에 강제 실행 문을 따른 동적 분석을 수행하여, 상기 HTML 문서에 포함된 분기 지점에서의 모든 경우들에 대해서 실행되도록 하는, 추적기 탐지 장치.

청구항 10

제6항에 있어서,

상기 프로세서가,

상기 추적 스크립트의 사용자 소스 정보가 기 설정된 사용자 소스 정보의 테이블에 포함되고, 상기 싱크 영역 정보가 기 설정된 싱크 영역 정보의 테이블에 포함되는 경우인지 여부를 판단하여, 상기 추적 스크립트의 유해 여부를 판단하는, 추적기 탐지 장치.

청구항 11

컴퓨터를 이용하여 제1항 내지 제5항 중 어느 한 항의 방법을 실행시키기 위하여 컴퓨터 판독 가능한 저장 매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 개시의 명세서는, 추적기 탐지 장치, 추적기 탐지 방법, 및 컴퓨터 프로그램에 관한 것으로, 웹 페이지에 대한 데이터를 판독하여 추적 스크립트를 검출하고, 추적 스크립트에 대한 출력 메시지를 생성하여 제공하는 점을 특징으로 한다.

배 경 기 술

[0002] 인터넷 또는 온라인 분석의 맥락에서 웹 페이지 추적기(tracker)는 방문자 및 특정 웹 사이트와의 상호 작용에 대한 데이터를 모니터링하거나 수집하는데 사용되는 도구 또는 시스템을 말한다.

[0003] 웹 페이지의 추적기의 주요 목적은, 웹 사이트 관리자, 또는 마케팅 담당자에게 웹 사이트의 성능 및 사용에 대한 분석을 제공하기 위한 것이다. 웹 페이지의 추적기를 통해서, 웹 사이트의 관리자는 웹 페이지의 방문자에 대한 분석 데이터를 획득할 수 있다. 웹 사이트의 관리자는 웹 페이지를 본 횟수, 웹 페이지 상에서의 이동 경로 등의 데이터를 획득할 수 있다. 웹 사이트의 관리자는, 웹 페이지를 추천한 소스(검색 엔진, 소셜 미디어 플

랫폼, 직접 트래픽 등)에 대한 정보를 획득할 수 있다. 웹 사이트의 관리자는, 구매, 양식 작성, 뉴스레터 가입 등의 전환 이벤트를 모니터링할 수 있다. 웹 사이트의 관리자는, 버튼 클릭, 다운로드, 동영상 시청 등의 시청자 참여에 대한 데이터, 페이지 로드 시간, 서버 응답 시간 등의 웹 페이지에 대한 성능 지표에 대한 데이터를 획득할 수 있다.

[0004] 이러한 추적기는 웹 페이지에 설치되어 사용자 단말 또는 사용자 행위에 대한 데이터를 수집하고 분석할 수 있다.

[0005] 웹 페이지의 추적기가 어떠한 데이터를 획득하여 가는지에 대해서 사용자가 알기는 어렵기 때문에, 개인 프라이버시를 해치는 정보를 수집할 수 있다.

[0006] 따라서, 개인 프라이버시를 보호하기 위해서, 웹 페이지 추적기에 의해 수집되는 데이터에 대해서 감시할 필요성이 대두되고 있다.

발명의 내용

해결하려는 과제

[0007] 본 명세서에서 개시되는 실시예들은, 웹 페이지의 추적 스크립트에 의해 수집되는 데이터를 미리 판독하고 웹 페이지에서 작동되는 유해한 추적 스크립트에 대해서 미리 모니터링하는데 목적이 있다.

과제의 해결 수단

[0008] 본 개시의 실시예들에 따른 방법은, 추적기 탐지 장치가, 접속하고자 하는 웹 사이트의 HTML 문서를 수신하고, 상기 HTML 문서를 분석하여, 추적 스크립트를 추출하는 단계; 상기 추적기 탐지 장치가, 상기 추적 스크립트에 포함된 사용자 소스 정보와 싱크 영역을 고려하여 상기 추적 스크립트의 유해 여부를 판단하는 단계; 상기 추적기 탐지 장치가, 유해한 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이하는 단계;를 포함할 수 있다.

[0009] 상기 추적 스크립트를 추출하는 단계는, 상기 HTML 문서를 동적 분석하여 정적 변수 흐름 데이터를 생성하고, 상기 정적 변수 흐름 데이터를 이용하여 사용자 소스 정보 및 싱크 영역 정보를 추출하는 단계를 더 포함할 수 있다.

[0010] 상기 정적 변수 흐름 데이터는, 프로그램을 실행하지 않고 프로그램의 실행 과정에서의 변수에 대한 값의 흐름에 대한 데이터일 수 있다.

[0011] 상기 추적 스크립트를 추출하는 단계는, 상기 HTML 문서에 강제 실행 문을 따른 동적 분석을 수행하여, 상기 HTML 문서에 포함된 분기 지점에서의 모든 경우들에 대해서 실행되도록 하는 단계를 더 포함할 수 있다.

[0012] 상기 유해 여부를 판단하는 단계는 상기 추적 스크립트의 사용자 소스 정보가 기 설정된 사용자 소스 정보의 테이블에 포함되고, 상기 싱크 영역 정보가 기 설정된 싱크 영역 정보의 테이블에 포함되는 경우인지 여부를 판단하여, 상기 추적 스크립트의 유해 여부를 판단할 수 있다.

[0013] 본 개시의 실시예들에 따른 장치가, 통신부, 메모리 및 프로세서를 포함하고, 상기 프로세서가, 접속하고자 하는 웹 사이트의 HTML 문서를 수신하고, 상기 HTML 문서를 분석하여, 추적 스크립트를 추출하고, 상기 추적 스크립트에 포함된 사용자 소스 정보와 싱크 영역을 고려하여 상기 추적 스크립트의 유해 여부를 판단하며, 유해한 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이할 수 있다.

[0014] 본 발명의 실시예에 따른 컴퓨터 프로그램은 컴퓨터를 이용하여 본 발명의 실시예에 따른 방법 중 어느 하나의 방법을 실행시키기 위하여 매체에 저장될 수 있다.

[0015] 이 외에도, 본 발명을 구현하기 위한 다른 방법, 다른 시스템 및 상기 방법을 실행하기 위한 컴퓨터 프로그램을 기록하는 컴퓨터 판독 가능한 기록 매체가 더 제공된다.

[0016] 전술한 것 외의 다른 측면, 특징, 이점이 이하의 도면, 특허청구범위 및 발명의 상세한 설명으로부터 명확해 질 것이다.

발명의 효과

[0017] 전술한 과제 해결 수단 중 어느 하나에 의하면, 웹 페이지의 추적 스크립트에 의해 수집되는 데이터를 미리 판

독하고 웹 페이지에서 작동되는 유해한 추적 스크립트에 대해서 미리 모니터링할 수 있다.

[0018] 또한, HTML 문서에 포함되는 분기 지점들 각각에 대한 스크립트를 실행시키는 하나 이상의 강제 실행 문을 생성하고, 강제 실행 문을 이용하여 추적 스크립트를 추출함으로써, 숨겨진 개인 정보 추적 스크립트를 검출할 수 있다.

[0019] 또한, HTML 문서에 대한 정적 변수 흐름 데이터를 생성하고, 정적 변수 흐름 데이터를 이용하여 HTML 문서를 실행 시킴으로써, 실제 실행 전에 개인 정보에 대한 추적 스크립트를 검출할 수 있다.

[0020] 또한, 추적 스크립트에 대한 정보를 사용자에게 제공함으로써, 렌더링된 웹 사이트 외에 웹 사이트에서 이루어지는 숨겨진 추적 기능을 확인할 수 있다.

도면의 간단한 설명

[0021] 도 1은, 본 개시의 실시예들에 따른 추적기 자동 감시 장치의 네트워크 환경에 대한 예시 도면이다.

도 2는, 본 개시의 실시예들에 따른 추적기 자동 감시 장치(100)의 블록도이다.

도 3은 메모리(120)의 블록도이다.

도 4는 행동 탐지부(121)의 블록도이다.

도 5는 본 개시의 실시예들에 따른 추적 스크립트의 행동을 탐지하는 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하 첨부된 도면들에 도시된 본 발명에 관한 실시 예를 참조하여 본 발명의 구성 및 작용을 상세히 설명한다.

[0023] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시 예를 가질 수 있는 바, 특정 실시 예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 본 발명의 효과 및 특징, 그리고 그것들을 달성하는 방법은 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 다양한 형태로 구현될 수 있다.

[0024] 이하, 첨부된 도면을 참조하여 본 발명의 실시 예들을 상세히 설명하기로 하며, 도면을 참조하여 설명할 때 동일하거나 대응하는 구성 요소는 동일한 도면부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0025] 이하에서, “상부” 나 “상”이라고 기재된 것은 접촉하여 바로 위에 있는 것 뿐만 아니라 비접촉으로 위에 있는 것도 포함할 수 있다.

[0026] 이하의 실시 예에서, 제1, 제2 등의 용어는 한정적인 의미가 아니라 하나의 구성 요소를 다른 구성 요소와 구별하는 목적으로 사용되었다.

[0027] 이하의 실시 예에서, 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0028] 이하의 실시 예에서, 포함하다 또는 가지다 등의 용어는 명세서상에 기재된 특징, 또는 구성요소가 존재함을 의미하는 것이고, 하나 이상의 다른 특징들 또는 구성요소가 부가될 가능성을 미리 배제하는 것은 아니다.

[0029] 도면에서는 설명의 편의를 위하여 구성 요소들이 그 크기가 과장 또는 축소될 수 있다. 예컨대, 도면에서 나타난 각 구성의 크기 및 두께는 설명의 편의를 위해 임의로 나타내었으므로, 본 발명이 반드시 도시된 바에 한정되지 않는다.

[0030] 또한, 본 명세서에 기재된 “…부”, “…영역” 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미할 수 있다.

[0031] 본 개시의 실시예에서, 추적기(tracker)는 웹 사이트의 소유자 및 관리자가 사이트 트래픽에 대한 정보를 수집하는 프로그램으로, 웹 사이트에 접속하는 사용자 단말 장치로부터 데이터를 획득하여 정해진 저장소에 저장하도록 처리할 수 있다.

[0032] 여기서, HTML 문서는, 웹 브라우저에 표시되도록 설계된 표준 텍스트 문서로서, 웹 페이지의 구조를 만드는데 사용되는 프로그래밍 언어 형식을 말한다. HTML 문서는, 꺽쇠괄호(<, >)로 둘러싸인 태그인 HTML 요소로 구성되며, 제목, 단락, 링크, 이미지 등과 같은 웹 페이지의 다양한 구성요소들을 포함할 수 있다.

[0033] 여기서, 문서를 판독하는 것(read, decipher)은, 문서의 텍스트를 읽어드리고, 소정의 규약, 규칙에 따라서 문

서의 내용을 읽어서 해독하는 것을 의미한다.

[0034] 여기서, 문서를 파싱(parsing)하는 것은, 정해진 태그, 형식 등을 고려하여, 문서의 내용(context)을 읽는 것을 말한다.

[0035] 여기서, 추적 스크립트는, 웹 사이트에 접속한 사용자 행동을 추적하고, 사용자 행동에 대한 데이터를 수집하는 프로그래밍 코드를 말한다.

[0036] 도 1은, 본 개시의 실시예들에 따른 네트워크 환경(10)을 설명하는 도면이다.

[0037] 사용자 단말기(10)는, 추적기 탐지 모듈이 설치되어 웹 페이지의 구문을 분석하여 추적기(wab page tracker)의 행동을 탐지할 수 있다. 추적기의 행동으로는, 웹 사이트 추천 소스, 전환 이벤트, 버튼 클릭, 다운로드 등의 사용자 행동과 관련된 정보를 수집하는 것을 포함할 수 있다. 사용자 단말기(10)는, 프로세서, 통신부, 메모리를 포함하는 컴퓨팅 장치를 말한다. 사용자 단말기(10)는, 네트워크 망에 접속하여 웹 서버(20)와 통신할 수 있다.

[0038] 사용자 단말기(10)는, 웹 사이트에 접속하는 입력에 대응하여, 웹 사이트에 대한 코드를 포함하는 HTML 형식의 문서를 수신하고, HTML 형식의 문서를 판독하여 웹 사이트를 디스플레이하여 출력부를 통해 보여줄 수 있다. HTML 형식의 문서는 자바스크립트로 작성될 수 있다. 자바 스크립트(Java script)는 웹 페이지에서 동적으로 변경되는 콘텐츠(contents)를 만들고 멀티미디어를 제어하는 등 다양한 작업을 수행할 수 있도록 하는 언어로서, HTML 문서 내에서 <script src= …>와 같은 태그를 붙여 표현될 수 있다. 사용자 단말기(10)는, HTML 문서 내에서, 스크립트의 로드(load), 파싱과 실행이 동기적으로(sunchronously) 처리할 수 있다. HTML 문서는 자바 스크립트 형식의 태그를 포함하여 구현될 수 있다. 자바 스크립트에서는, 콜백 함수, 프로미스, async await 등의 비동기 작업을 처리하는 코드, 사용자의 클릭, 스크롤바 이동 등의 행위 및 시스템 이벤트에 반응하여 실행되는 코드 등이 있으며, 이러한 형식이 코드가 HTML 문서에 포함되어 동작될 수 있다. 이러한 자바스크립트 형식이 코드는 HTML 문서의 판독(read, decipher, parse) 이후에 실행될 수 있다.

[0039] 이를 통해, 웹 페이지를 로딩하고 디스플레이하는 과정에서, 웹 서버(20)의 관리자에 의해 숨겨진 자바 스크립트 형식의 코드가 사용자 단말기(10)에서 강제적으로 실행될 수 있다.

[0040] 사용자 단말기(10)는 추적기 탐지 모듈이 설치되어 있어 웹 페이지에 대응하는 HTML 문서에 포함된 추적 스크립트를 검출하고, 추적 스트립트에 의해 추적 행동을 탐지하여 추적 행동에 대한 정보를 별개의 출력 윈도우로 디스플레이할 수 있다.

[0041] 관리자는, 웹 사이트에서 제공되는 하나 이상의 웹 페이지들에 대한 문서들을 생성하여 웹 서버(20)에 업로드할 수 있다. 웹 서버(20)는, 서버 프로그램이 설치되어 있어, 접속한 사용자 단말기(10)에게 웹 사이트에 대한 프로그래밍 문서(구문)들에 따른 동작이 제공되도록 할 수 있다. 웹 서버(20)는, 통신부, 메모리 및 프로세서를 포함하는 컴퓨팅 장치로서, 접속한 사용자 단말기(10)에게 웹 사이트를 제공하는 기능을 수행하는 장치를 말한다. 웹 서버(20)는, 클라우드 시스템으로 구현될 수 있다.

[0042] 도 2은, 본 개시의 실시예들에 따른 추적기 탐지 장치(100)의 블록도이다.

[0043] 추적기 탐지 장치(100)는 컴퓨팅 장치로서, 웹 페이지에 대응하는 문서에 포함된 추적 스크립트를 검출하고, 추적 스크립트에 의해 추적 행동을 검출할 수 있다. 추적기 탐지 장치(100)는, 추적 스크립트의 유해 여부를 판단하여, 유해한 추적 스크립트에 대한 정보를 생성할 수 있다. 추적기 탐지 장치(100)는, 상기 추적 행동에 대한 정보를 출력 데이터로 생성하여, 디스플레이 할 수 있다. 추적기 탐지 장치(100)는, 도 1의 사용자 단말기(10)와 대체 가능하다.

[0044] 본 개시의 실시예들에 따르면, 추적 스크립트는, 추적기 탐지 장치(100)에 대한 사용자 소스 정보를 추출하고, 추출된 사용자 정보를 싱크(sink) 영역으로 유출하는 기능을 수행하는 구문을 말한다. 추적 스크립트는, 브랜치(branch) 형식의 구문으로 삽입될 수 있으므로, 브랜치 형식의 구문에 대해서는, 강제 입력을 통해 분기되는 복수의 구문들을 실행 시켜 확인될 수 있다.

[0045] 여기서, 사용자 소스 정보는, 웹 페이지에 있는 추적기의 출처 또는 시작 시점을 나타내는 것으로, 데이터 수집을 담당하는 스크립트, 픽셀 또는 기타 구성요소를 포함할 수 있다. 사용자 소스 정보는, 추적기가 로드되는 도메인 또는 서버와 연결되는 것을 말한다. 사용자 소스 정보의 예시로는 URL, host, 쿠키, DOM 원소(입력 필드 값 등), event listener 등이 있을 수 있다. DOM 원소는, event listener는 DOM 원소가 클릭된 후의 onclick 이벤트 등이 있을 수 있다. 추적 스크립트를 판단하는데 유용한 DOM 원소는, 패스워드 등과 같은 입력값을 입력

하는 입력 필드를 말한다.

[0046] 여기서, 싱크 영역은 웹 페이지 추적기를 통해 수집된 데이터가 전송되는 대상 또는 엔드 포인트를 말한다. 싱크 영역은, 사용자 데이터를 처리하고 저장하는 서버, 분석 플랫폼, 또는 기타 외부 엔터티를 포함할 수 있다. 싱크 영역에 대한 정보는 추적기의 동작을 통해 수집된 데이터를 수신하고 저장하는 장치와 연결되는 것으로, 추적기의 동작을 식별하는데 이용될 수 있다. 안전하지 않은 싱크 영역으로는 jQuery, XMLHttpRequest, fetch, DOM 원소 등의 src 속성, 또는 storage, LocalStorage 등의 저장소 속성을 가지는 것일 수 있다.

[0047] 추적기 탐지 장치(100)는 웹 페이지의 문서를 판독하여 추적 스크립트를 추출하고, 추적 스크립트에 대한 유해 여부를 판단하여, 유해한 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이할 수 있다. 추적기 탐지 장치(100)는, 유해한 추적 스크립트에 대한 정보를 추적기 감시 리스트에 추가하여, 업데이트할 수 있다.

[0048] 추적기 탐지 장치(100)는, 프로세서(110), 메모리(120), 통신부(130), 및 입출력부(140)를 포함할 수 있다.

[0049] 본 개시의 일 실시 예에 따르면, 프로세서(110)는 통상적으로, 추적기 탐지 장치(100)의 전반적인 동작을 제어한다. 예를 들어, 프로세서(110)는 추적기 탐지 장치(100)에 저장된 명령어들을 실행시킴으로써, 추적기 탐지 장치(100)가 포함하는 구성요소들을 전반적으로 제어할 수 있다.

[0050] 본 개시의 일 실시 예에 따르면, 메모리(120)는 프로세서(110)의 처리 및 제어를 위한 프로그램을 저장할 수 있고, 추적기 탐지 장치(100)로 입력되거나 추적기 탐지 장치(100)로부터 출력되는 데이터를 저장할 수도 있다. 메모리(120)는 프로그램 코드를 분석하여 생성된 데이터, 프로그램을 검증, 테스트하기 위한 명령어들을 저장할 수 있다. 메모리(120)는 상기의 정보들을 저장한 데이터베이스를 포함할 수 있다.

[0051] 본 개시의 일 실시 예에 따르면, 메모리(120)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. 또한 본 개시의 일 실시 예에 따르면, 메모리(120)에 저장된 프로그램들은 그 기능에 따라 복수 개의 모듈들로 분류할 수 있다.

[0052] 본 개시의 일 실시 예에 따르면, 통신부(130)는 프로세서(110)의 외부 장치와 통신을 수행할 수 있다. 예를 들어, 통신부(130)는 프로세서(110)의 제어에 의해 보안이 필요한 프로그램이 저장된 전자 장치와 통신을 수행할 수 있다. 또한, 통신부(130)는 외부 인터페이스와의 통신을 통해 자율주행 프로그램이 저장된 전자 장치에 접근하여 웹 사이트와 관련된 데이터를 수신할 수 있다.

[0053] 입출력부(140)는 입출력 장치와의 인터페이스를 위한 수단일 수 있다. 예를 들어, 입력 장치는 키보드 또는 마우스 등의 장치를, 그리고 출력 장치는 어플리케이션의 통신 세션을 표시하기 위한 디스플레이와 같은 장치를 포함할 수 있다. 다른 예로 입출력부(140)는 터치스크린과 같이 입력과 출력을 위한 기능이 하나로 통합된 장치와의 인터페이스를 위한 수단일 수도 있다. 보다 구체적인 예로, 추적기 탐지 장치(100)의 프로세서(110)는 메모리(120)에 로딩되거나, 저장된 컴퓨터 프로그램의 명령을 처리함에 있어서 서비스 화면이나 컨텐츠가 입출력부(140)를 통해 디스플레이에 표시될 수 있다.

[0054] 또한, 다른 실시 예들에서, 추적기 탐지 장치(100)는 도 2의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다. 예를 들어, 상술한 입출력 장치 중 적어도 일부를 포함하도록 구현되거나 또는 내부 구성요소들에 전력을 공급하는 배터리 및 충전 장치, 각종 센서, 데이터베이스 등과 같은 다른 구성요소들을 더 포함할 수도 있다.

[0055] 도 3은 메모리(120)의 블록도이다.

[0056] 메모리(120)는, 행동 탐지부(121), 및/또는 웹 브라우저(122)를 포함할 수 있다.

[0057] 행동 탐지부(121)는 웹 브라우저(122)에서, 접속하고자 하는 웹 페이지의 HTML 문서를 파싱하면서 DOM(document Object Model)을 생성할 수 있다. 행동 탐지부(121)는, HTML 문서에서 추적 스크립트를 추출하고 추적 스크립트에 대한 유해 여부를 판단할 수 있다.

[0058] 행동 탐지부(121)는, 유해한 것으로 판단된 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이할 수 있다.

[0059] 행동 탐지부(121)는, 자바 스크립트 형식의 추적 스크립트를 분석하여, 추적 스크립트에 포함된 사용자 소스 정

보, 및/또는 싱크 영역 정보를 추출하고, 사용자 소스 정보 및/또는 싱크 영역 정보가 정해진 테이블에 포함되는지 여부를 통해 추적 스크립트의 유해 여부를 판단할 수 있다. 추적 스크립트는 사용자 소스 정보를 싱크 영역 정보로 전송하도록 구현되는 코드일 수 있으나, 이에 한정하지 않고, 장치의 다른 저장 영역에 접근하여 데이터를 획득하고 이를 외부의 장치로 전송하도록 구현된 코드를 말한다.

[0060] 추적 스크립트는 안전하지 않은 소스 정보를 안전하지 않은 싱크 영역으로 전송하도록 구현될 수 있다. 행동 탐지부(121)는, 안전하지 않은 소스 정보를 안전하지 않은 싱크 영역으로 전송하도록 구현되는 추적 스크립트를 유해한 것으로 판단할 수 있다. 안전하지 않은 소스 정보는, 사용자의 개인 정보를 포함하는 것으로, 기 설정된 소스 테이블에 포함된 정보로 결정될 수 있다. 안전하지 않은 소스 정보는, 사용자에 의해 설정된 정보 또는, 일반적으로 웹 서버로 제공되지 않는 개인 정보를 포함할 수 있다. 사용자는, 유출되길 원치 않고 보호하고자 하는 개인 정보에 대해서 미리 설정할 수 있다. 예를 들어, 전화번호, 검색이력, 로그인 정보에서 패스워드 정보, 플러그인 정보, 장바구니에 추가된 정보, 구매한 정보 등의 개인 정보가 외부의 웹 서버로 전송될 수 있다. 사용자는, 전화번호, 검색이력, 로그인 정보에서 패스워드 정보, 플러그인 정보, 장바구니에 추가된 정보, 구매한 정보 등의 개인 정보의 리스트에 대해서 선택 입력을 통해서 안전하지 않은 소스 정보를 설정할 수 있다.

[0061] 여기서, 소스 테이블은, 안전하지 않은 소스 정보를 포함할 수 있다. 안전하지 않은 싱크 영역은, 개인 정보를 수신하는 장치에 대한 정보를 말한다. 안전하지 않은 싱크 영역은, 기 설정된 싱크 테이블에 포함된 정보를 기초로 결정될 수 있다. 여기서, 싱크 테이블은 안전하지 않은 싱크 영역에 대한 정보를 포함할 수 있다. 안전하지 않은 싱크 영역으로는 jQuery, XMLHttpRequest, fetch, DOM 원소 등의 src 속성, 또는 storage, LocalStorage 등의 저장소 속성을 가지는 것이 있을 수 있다.

[0062] 보다 구체적으로, 행동 탐지부(121)는, 추적 스크립트에 포함된 브랜치 형식의 구문에 대해서 강제 입력을 통해 분기되는 복수의 구분들을 실행시켜 추적 스크립트의 유해 여부를 판단할 수 있다. 예를 들어, if 및 else 로 분기되는 추적 스크립트의 경우, if로 분기되는 입력값을 강제적으로 입력하여 if 이하의 스크립트를 실행시키고, else로 분기되는 입력값을 강제적으로 입력하여 else 이하의 스크립트를 실행시킬 수 있다. 이 외에도, 다양한 조건문들을 포함하는 추적 스크립트에 대해서 입력값을 강제적으로 입력하여 각각의 조건문 이하의 명령어들을 실행시켜, 추적 스크립트의 유해 여부를 판단할 수 있다.

[0063] 행동 탐지부(121)는, 정적 분석을 수행하여, 사용자 소스 정보가 싱크 영역으로 유출되는 흐름이 발생되는지 여부를 기초로 추적 스크립트의 유해 여부를 판단할 수 있다.

[0064] 상기에서 기술한 방법 중 적어도 하나의 방법을 실행시켜, 행동 탐지부(121)는, 추적 스크립트의 유해 여부를 판단하고, 유해한 추적 스크립트로 판단된 경우, 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이할 수 있다.

[0065] 행동 탐지부(121)는, 장치(100)에 설치된 웹 브라우저(122)에 내재되어 접속하는 웹 페이지의 추적 스크립트의 유해 여부를 판단하도록 동작될 수 있다.

[0066] 행동 탐지부(121)는 웹 사이트의 스크립트에 포함된 추적 스크립트 중에서, 유해한 추적 스크립트가 있는지 여부를 판단할 수 있다. 추적 스크립트가 탐지된 경우, 탐지된 추적 스크립트에 대한 정보를 제공하는 출력 데이터를 생성할 수 있다.

[0067] 도 4는 행동 탐지부(121)의 블록도이다.

[0068] 행동 탐지부(121)는, 접속되는 웹 페이지의 구문을 판독하여 추적 스크립트를 추출하고, 추적 스크립트의 유해 여부를 판단하여 이에 대한 출력 메시지를 제공하는 것으로, 소프트웨어 적으로 구현된 것일 수 있다. 안정성 판단부(121)는, 기능을 구현하는 명령어들의 집합 또는 이러한 명령어들을 컴파일하여 생성된 프로그램의 형태일 수 있다. 안정성 판단부(121)는, 웹 서버 연결부(1211), 추적 행위 체크부(1212), 출력 데이터 생성부(1213)를 포함할 수 있다. 웹 서버 연결부(1211), 추적 행위 체크부(1212), 출력 데이터 생성부(1213) 중 적어도 하나는, 소정의 코드로 작성된 명령어들의 집합 또는, 이러한 명령어들을 컴파일하여 생성된 프로그램의 형태일 수 있다.

[0069] 웹 서버 연결부(1211)는 접속하고자 하는 웹 페이지의 HTML 문서를 수신하고, HTML 문서를 파싱하여 DOM을 생성할 수 있다.

[0070] 추적 행위 체크부(1212)는 HTML 문서를 분석하여, 추적 스크립트를 추출할 수 있다. 추적 행위 체크부(1212)는 HTML 문서를 분석하여, 사용자 소스 정보가, 싱크 영역으로 유출되는 데이터 흐름을 가지는 스크립트를 추적 스

크립트로 추출할 수 있다. 추적 행위 체크부(1212)는, 기 저장된 사용자 소스 정보의 테이블을 이용하여 사용자 소스 정보 인지 여부를 결정할 수 있다. 추적 행위 체크부(1212)는, 기 저장된 싱크 영역 정보의 테이블을 이용하여 싱크 영역 정보인지 여부를 결정할 수 있다. 추적 행위 체크부(1212)는, 추적 스크립트를 분석하여, 추적 스크립트에서 사용되는 데이터의 변수 흐름 데이터를 생성할 수 있다. 추적 행위 체크부(1212)는, 싱크 영역 정보로 할당되는 데이터 및/또는 변수로 이동되는 데이터 및/또는 변수를 검색하고, 상기 데이터 및/또는 변수가 변수 흐름 데이터를 이용하여 사용자 소스 정보를 가지도록 구현되는 경우인지 여부를 결정할 수 있다. 추적 행위 체크부(1212)는, 변수 흐름 데이터를 이용하여 싱크 영역 정보로 할당되는 데이터 및/또는 변수로 이동되는 하나 이상의 제1 변수를 검색하고, 제1 변수로 접근가능한 하나 이상의 제2 변수를 추출할 수 있다. 제2 변수 중에서, 사용자 소스 정보가 할당되는 제3 변수를 포함하는 스크립트를 추적 스크립트로 추출할 수 있다.

[0071] 추적 행위 체크부(1212)는, 자바 스크립트 형식의 추적 스크립트를 분석하여, 추적 스크립트에 포함된 사용자 소스 정보, 및/또는 싱크 영역 정보를 추출할 수 있다.

[0072] 추적 행위 체크부(1212)는, 사용자 소스 정보 및/또는 싱크 영역 정보가 정해진 테이블에 포함되는지 여부를 통해 추적 스크립트의 유해 여부를 판단할 수 있다. 안전하지 않은 소스 정보 또는 안전하지 않은 싱크 영역을 포함하는 추적 스크립트를 유해한 것으로 판단할 수 있다. 안전하지 않은 소스 정보는, 기 설정된 소스 테이블에 포함된 정보를 포함하는 것을 말한다. 여기서, 소스 테이블은, 안전하지 않은 소스 정보를 포함할 수 있다. 안전하지 않은 싱크 영역은, 기 설정된 싱크 테이블에 포함된 정보를 포함하는 것으로, 싱크 테이블은 안전하지 않은 싱크 영역에 대한 정보를 포함할 수 있다. 안전하지 않은 싱크 영역으로는 jQuery, XMLHttpRequest, fetch, DOM 원소 등의 src 속성, 또는 storage, LocalStorage 등의 저장소 속성을 가지는 것일 수 있다.

[0073] 추적 행위 체크부(1212)는 추적 스크립트에 포함된 브랜치 형식의 구문에 대해서 강제 입력을 통해 분기되는 복수의 구문들을 실행시켜 추적 스크립트의 유해 여부를 판단할 수 있다. 예를 들어, if 및 else 로 분기되는 추적 스크립트의 경우, if로 분기되는 입력값을 강제적으로 입력하여 if 이하의 스크립트를 실행시키고, else로 분기되는 입력값을 강제적으로 입력하여 else 이하의 스크립트를 실행시킬 수 있다. 이 외에도, 다양한 조건문들을 포함하는 추적 스크립트에 대해서 입력값을 강제적으로 입력하여 각각의 조건문 이하의 명령어들을 실행시켜, 추적 스크립트의 유해 여부를 판단할 수 있다. 각각의 조건문 이하의 명령어들이 사용자 소스 정보 및/또는 싱크 영역 정보를 추출하고, 사용자 소스 정보 및/또는 싱크 영역 정보가 정해진 테이블에 포함되는지 여부를 통해 유해한지 여부를 판단할 수 있다.

[0074] 추적 행위 체크부(1212)는 추적 스크립트를 포함하는 코드 영역을 정적 분석하고, 추적 스크립트를 포함하는 코드 영역을 강제 실행 시키는 모듈을 이용하여 추적 스크립트에 포함된 브랜치 형식의 복수의 구문들을 실행 시킬 수 있다.

[0075] 추적 행위 체크부(1212)는 정적 분석을 수행하여, 사용자 소스 정보가 싱크 영역으로 유출되는 흐름이 발생되는지 여부를 기초로 추적 스크립트의 유해 여부를 판단할 수 있다. 추적 행위 체크부(1212)는, 정적 변수 흐름 데이터를 이용하여, 사용자 소스 정보가 싱크 영역으로 유출되는 흐름이 발생되는지 여부를 판단할 수 있다. 여기서, 정적 변수 흐름 데이터는, 프로그램을 실행하지 않고 프로그램의 실행 과정에서의 변수에 대한 값(value)의 흐름에 대한 데이터로, 정적 분석 방법에 의해 생성될 수 있다. 정적 변수 흐름 데이터는, SVFG(static value flow graph)일 수 있으나 이에 한정되지 않는다. 정적 변수 흐름 데이터는, 노드, 엔터티, 흐름 에지, 유형 정보 등을 포함할 수 있다. 정적 변수 흐름 데이터는 프로그램의 실행 과정에서 변수에 대한 값이 어떻게 변화하는지에 대한 데이터, 하나의 변수에 대한 값을 변화시키는 코드들 사이의 관계를 포함할 수 있다. 추적 행위 체크부(1212)는 HTML 문서를 동적으로 분석하여, 흐름 데이터, 예를 들어, 정적 변수 흐름 데이터를 생성할 수 있다. HTML 문서에 포함된 모든 코드들을 실행시키는 강제 실행 문을 생성하여, 강제 실행 문(명령어)를 이용하여 HTML 문서에 대한 흐름 데이터를 생성할 수 있다. 강제 실행 문은, 문서에 존재하는 분기 지점들에 대해서, 모든 경우들로 각각 실행되도록 하는 명령어들을 말한다. 예를 들어, if에 해당하는 입력값, else에 해당하는 입력값이 강제적으로 입력되도록 하는 명령어들을 강제 실행 문이라고 한다. HTML 문서에 포함된 조건문들을 판독하여, 각 조건문에서의 대상값을 변경하는 코드를 각 조건문 실행 전에 실행시키는 강제 실행 문을 HTML 문서에 삽입한 후 HTML 문서를 실행시킬 수 있다. 예를 들어, if 조건에 해당하는 제1 강제 실행 문을 삽입한 HTML 문서를 실행시키고, else 조건에 해당하는 제2 강제 실행문을 삽입한 HTML 문서를 실행시키도록 구현될 수 있다.

[0076] 상기에서 기술한 방법 중 적어도 하나의 방법을 실행시켜, 추적 행위 체크부(1212)는 추적 스크립트에 대한 유해 여부를 판단할 수 있다.

[0077] 출력 데이터 생성부(1213)는 유해한 것으로 판단된 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스

플레이할 수 있다.

[0078] 출력 데이터 생성부(1213)는 추적 스크립트를 포함하는 웹 사이트 정보, 추적 스크립트에서 획득하는 사용자 소스 정보, 추적 스크립트에 포함된 싱크 영역 정보를 포함하는 출력 데이터를 생성할 수 있다. 예를 들어, 사용자의 검색 이력의 쿠키를 A 페이지에 전송하고 있다. '사용자의 방문 페이지들의 쿠키 데이터가 A 스토리지에 저장되고 있다'. '당신이 B 사이트에 방문한 이력이 C 서버로 전송되고 있다'와 같은 출력 데이터가 생성될 수 있다.

[0079] 출력 데이터 생성부(1213)는, 추적 스크립트에 대한 정보를 출력하면서 웹 사이트에 대한 방문을 계속적으로 수행할지 여부를 묻는 사용자 인터페이스를 생성하여 제공할 수 있다. 출력 데이터 생성부(1213)는 제1 웹 사이트를 접속하는 신호에 대응하여 제1 웹사이트의 스크립트를 판독하고, 제1 웹 사이트의 스크립트에서, 제1 추적 스크립트를 추출하며, 제1 추적 스크립트가 유해한 것으로 판단된 경우, 제1 추적 스크립트에 대한 사용자 인터페이스를 생성하여 제공할 수 있다. 사용자 인터페이스는, 접속 계속 또는 접속 중단 중 하나를 선택할 수 있는 아이템을 포함할 수 있다. 제1 추적 스크립트에 대한 사용자 인터페이스를 통해 획득된 사용자 입력에 대응하여 제1 웹 사이트의 접속이 중단될 수 있다.

[0080] 도 5는 본 개시의 실시예들에 따른 추적 스크립트의 행동을 탐지하는 방법의 흐름도이다.

[0081] S110에서는, 추적기 탐지 장치(100)는 접속하고자 하는 웹 페이지의 HTML 문서를 수신하고, HTML 문서를 파싱하여 DOM을 생성할 수 있다.

[0082] S120에서는, 추적기 탐지 장치(100)는 HTML 문서를 분석하여, 추적 스크립트를 추출할 수 있다. 추적 스크립트는, 사용자 소스 정보와 싱크 영역 정보에 대한 구문을 포함하는 것일 수 있다. 추적기 탐지 장치(100)는 기 저장된 사용자 소스 정보의 테이블을 이용하여 사용자 소스 정보 인지 여부를 결정할 수 있다. 추적기 탐지 장치(100)는 기 저장된 싱크 영역 정보의 테이블을 이용하여 싱크 영역 정보인지 여부를 결정할 수 있다. 추적기 탐지 장치(100)는 추적 스크립트를 분석하여, 추적 스크립트에서 사용되는 데이터의 정적 변수 흐름 데이터를 생성할 수 있다. 추적기 탐지 장치(100)는 싱크 영역 정보로 할당되는 데이터 및/또는 변수로 이동되는 데이터 및/또는 변수를 검색하고, 상기 데이터 및/또는 변수가 변수 흐름 데이터를 이용하여 사용자 소스 정보를 가지도록 구현되는 경우인지 여부를 결정할 수 있다. 추적기 탐지 장치(100)는 변수 흐름 데이터를 이용하여 싱크 영역 정보로 할당되는 데이터 및/또는 변수로 이동되는 하나 이상의 제1 변수를 검색하고, 제1 변수로 접근가능한 하나 이상의 제2 변수를 추출할 수 있다. 제2 변수 중에서, 사용자 소스 정보가 할당되는 제3 변수를 포함하는 스크립트를 추적 스크립트로 추출할 수 있다.

[0083] S130에서는, 추적기 탐지 장치(100)는 자바 스크립트 형식의 추적 스크립트를 분석하여, 추적 스크립트에 포함된 사용자 소스 정보, 및/또는 싱크 영역 정보를 추출하고, 사용자 소스 정보 및/또는 싱크 영역 정보가 정해진 테이블에 포함되는지 여부를 통해 추적 스크립트의 유해 여부를 판단할 수 있다. 안전하지 않은 소스 정보 또는 안전하지 않은 싱크 영역을 포함하는 추적 스크립트를 유해한 것으로 판단할 수 있다. 안전하지 않은 소스 정보는, 기 설정된 소스 테이블에 포함된 정보를 포함하는 것을 말한다. 여기서, 소스 테이블은, 안전하지 않은 소스 정보를 포함할 수 있다. 안전하지 않은 싱크 영역은, 기 설정된 싱크 테이블에 포함된 정보를 포함하는 것으로, 싱크 테이블은 안전하지 않은 싱크 영역에 대한 정보를 포함할 수 있다. 안전하지 않은 싱크 영역으로는 jQuery, XMLHttpRequest, fetch, DOM 원소 등의 src 속성, 또는 storage, LocalStorage 등의 저장소 속성을 가지는 것일 수 있다.

[0084] 추적기 탐지 장치(100)는 추적 스크립트에 포함된 브랜치(branch) 형식의 구문에 대해서 강제 입력을 통해 분기되는 복수의 구문들을 실행시켜 추적 스크립트의 유해 여부를 판단할 수 있다. 예를 들어, if 및 else 로 분기되는 추적 스크립트의 경우, if로 분기되는 입력값을 강제적으로 입력하여 if 이하의 스크립트를 실행시키고, else로 분기되는 입력값을 강제적으로 입력하여 else 이하의 스크립트를 실행시킬 수 있다. 이 외에도, 다양한 조건문들을 포함하는 추적 스크립트에 대해서 입력값을 강제적으로 입력하여 각각의 조건문 이하의 명령어들을 실행시켜, 추적 스크립트의 유해 여부를 판단할 수 있다.

[0085] 추적기 탐지 장치(100)는 추적 스크립트를 포함하는 코드 영역을 정적 분석하고, 추적 스크립트를 포함하는 코드 영역을 강제 실행 시키는 모듈을 이용하여 추적 스크립트에 포함된 브랜치 형식의 복수의 구문들을 실행 시킬 수 있다.

[0086] 추적기 탐지 장치(100)는 정적 분석을 수행하여, 사용자 소스 정보가 싱크 영역으로 유출되는 흐름이 발생되는지 여부를 기초로 추적 스크립트의 유해 여부를 판단할 수 있다. 추적기 탐지 장치(100)는 정적 변수 흐름 데이

터를 이용하여, 사용자 소스 정보가 싱크 영역으로 유출되는 흐름이 발생되는지 여부를 판단할 수 있다. 여기서, 정적 변수 흐름 데이터는, 프로그램을 실행하지 않고 프로그램의 실행 과정에서의 변수에 대한 값(value)의 흐름에 대한 데이터로, 정적 분석 방법에 의해 생성될 수 있다. 정적 변수 흐름 데이터는, SVFG(static value flow graph)일 수 있으나 이에 한정되지 않는다. 정적 변수 흐름 데이터는, 노드, 엔터티, 흐름 에지, 유형 정보 등을 포함할 수 있다. 정적 변수 흐름 데이터는 프로그램의 실행 과정에서 변수에 대한 값이 어떻게 변화하는지에 대한 데이터, 하나의 변수에 대한 값을 변화시키는 코드들 사이의 관계를 포함할 수 있다. 추적기 탐지 장치(100)는, HTML 문서를 동적으로 분석하여, 흐름 데이터, 예를 들어, 정적 변수 흐름 데이터를 생성할 수 있다. HTML 문서에 포함된 모든 코드들을 실행시키는 강제 실행 문을 생성하여, 강제 실행 문(명령어)를 이용하여 HTML 문서에 대한 흐름 데이터를 생성할 수 있다. 강제 실행 문은, 문서에 존재하는 분기 지점들에 대해서, 모든 경우들로 각각 실행되도록 하는 명령어들을 말한다. 예를 들어, if에 해당하는 입력값, else에 해당하는 입력값이 강제적으로 입력되도록 하는 명령어들을 강제 실행 문이라고 한다.

[0087] 상기에서 기술한 방법 중 적어도 하나의 방법을 실행시켜, 추적기 탐지 장치(100)는 추적 스크립트에 대한 유해 여부를 판단할 수 있다.

[0088] S140에서는, 추적기 탐지 장치(100)는 유해한 것으로 판단된 추적 스크립트에 대한 정보를 출력 데이터로 생성하여 디스플레이할 수 있다.

[0089] 추적기 탐지 장치(100)는 추적 스크립트를 포함하는 웹 사이트 정보, 추적 스크립트에서 획득하는 사용자 소스 정보, 추적 스크립트에 포함된 싱크 영역 정보를 포함하는 출력 데이터를 생성할 수 있다. 예를 들어, 사용자의 검색 이력의 쿠키를 A 페이지에 전송하고 있다. 사용자의 방문 페이지들의 쿠키 데이터가 A 스토리지에 저장되고 있다. 당신이 B 사이트에 방문한 이력이 C 서버로 전송되고 있다와 같은 출력 데이터가 생성될 수 있다.

[0090] 다른 실시예에서, 추적기 탐지 장치(100)는 출력 데이터와 함께 웹 사이트에 대해서 접근할지 여부를 묻는 인터페이스를 생성하여 제공할 수 있다. 추적기 탐지 장치(100)는, 상기 인터페이스에 대해서 '아니오(no)' 의 사용자 입력이 획득되면, 웹 사이트에 접속하지 않고, 접속을 강제 종료 할 수 있다.

[0091] 다른 실시예에서, 추적기 탐지 장치(100)는, 유해한 추적 스크립트를 포함하는 웹 페이지를 렌더링하지 않고, 해당 웹 서버와의 접속을 강제 종료 할 수 있다.

[0092] 다른 실시예에서, 추적기 탐지 장치(100)는 유해한 추적 스크립트에 대한 범위를 사용자 입력에 의해 결정할 수 있다. 예를 들어, 사용자의 검색 이력, 방문 페이지 정보를 유출시키는 추적 스크립트를 유해한 것으로 설정할 수 있다. 이런 경우, 설정된 정보에 기초하여 사용자의 검색 이력, 방문 페이지 정보를 유출시키는 추적 스크립트를 유해한 것으로 판단할 수 있다.

[0093] 이에 한정되지 않고, 사용자 식별과 관련된 정보인, 접속 시점, 접속 사이트 정보, 웹 브라우저의 버전 정보, 장치의 모델 정보, 사용자의 위치 정보, 사용자의 패스워드 정보, 사용자의 아이디 정보 중 적어도 하나를 유출시키는 추적 스크립트를 유해한 것으로 판단할 수 있다.

[0094] S150에서는, 추적기 탐지 장치(100)는 HTML 문서에 대응하여, 웹 페이지를 렌더링할 수 있다.

[0095] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

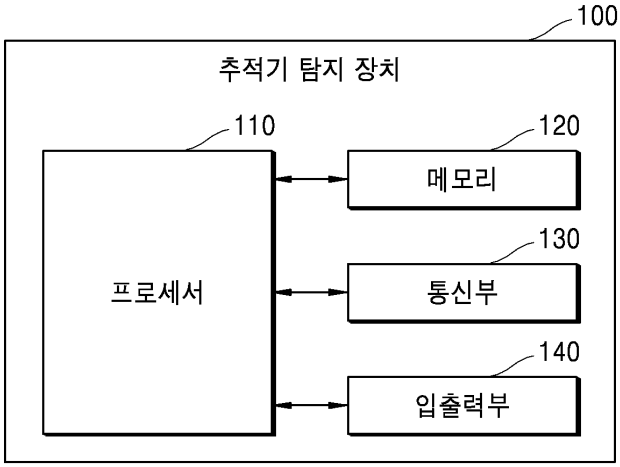
[0096] 따라서, 본 발명의 사상은 앞에서 설명된 실시예들에 국한하여 정해져서는 아니되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 또는 이로부터 등가적으로 변경된 모든 범위가 본 발명의 사상의 범주에 속한다고 할 것이다.

도면

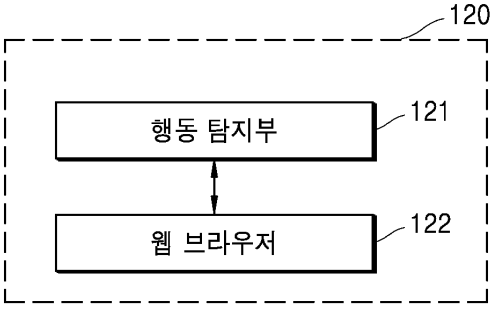
도면1



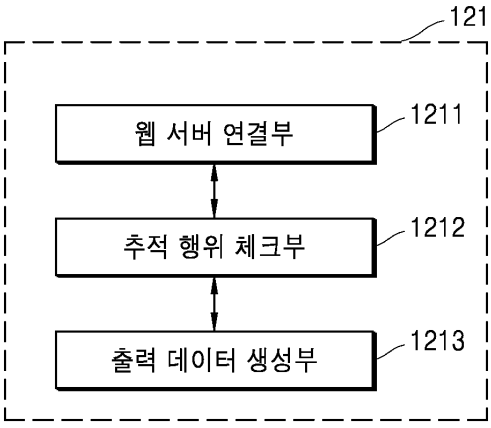
도면2



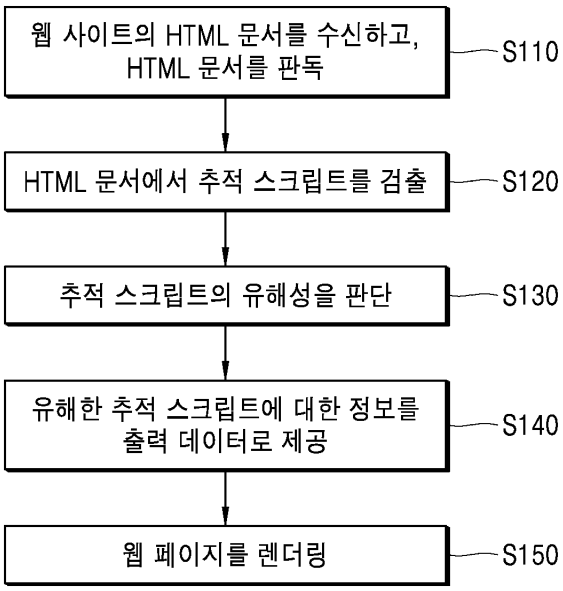
도면3



도면4


121
웹 서버 연결부
1211
추적 행위 체크부
1212
출력 데이터 생성부
1213

도면5


웹 사이트의 HTML 문서를 수신하고, HTML 문서를 판독
S110
HTML 문서에서 추적 스크립트를 검출
S120
추적 스크립트의 유해성을 판단
S130
유해한 추적 스크립트에 대한 정보를 출력 데이터로 제공
S140
웹 페이지를 렌더링
S150