



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2024년05월09일

(11) 등록번호 10-2664072

(24) 등록일자 2024년05월02일

(51) 국제특허분류(Int. Cl.)

G06F 21/57 (2013.01) G06F 21/55 (2013.01)

G06F 21/64 (2013.01) H04L 9/00 (2022.01)

(52) CPC특허분류

G06F 21/57 (2013.01)

G06F 21/55 (2013.01)

(21) 출원번호 10-2022-0159876

(22) 출원일자 2022년11월25일

심사청구일자 2022년11월25일

(56) 선행기술조사문헌

JP2022535785 A\*

KR1020210041310 A\*

KR1020220141276 A

US20220318399 A1

\*는 심사관에 의하여 인용된 문헌

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

오학주

서울특별시 강남구 압구정로 151, 122동 1002호(압구정동, 현대아파트)

소순범

서울특별시 성북구 개운사길 75-30, 203호(안암동5가)

(74) 대리인

이대호, 박건홍

전체 청구항 수 : 총 22 항

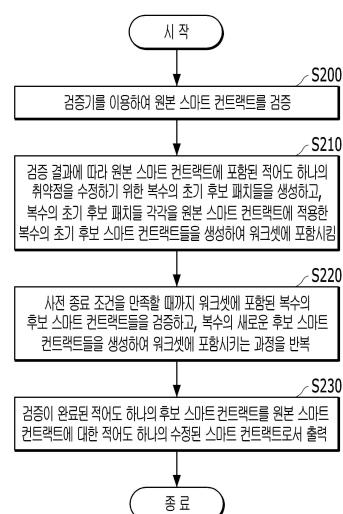
심사관 : 구대성

(54) 발명의 명칭 스마트 컨트랙트 취약점 수정 방법 및 장치

## (57) 요약

본 개시의 실시예에 따라, 컴퓨팅 장치에 의해 수행되는, 스마트 컨트랙트 취약점 수정 방법으로서, 검증기를 이용하여 원본 스마트 컨트랙트를 검증하는 단계; 상기 원본 스마트 컨트랙트에 대한 검증 결과에 따라 상기 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 초기 후보 패치들을 생성하고, 상기 생성된 복수의 초기 후보 패치들을 상기 원본 스마트 컨트랙트에 적용한 복수의 초기 후보 스마트 컨트랙트들을 생성하는 단계, 사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하는 단계; 및 검증 완료된 적어도 하나의 후보 스마트 컨트랙트들을 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력하는 단계를 포함한다.

## 대표도 - 도2



(52) CPC특허분류

*G06F 21/64* (2013.01)

*H04L 9/50* (2022.05)

이 발명을 지원한 국가연구개발사업

|             |                           |
|-------------|---------------------------|
| 과제고유번호      | 1711152676                |
| 과제번호        | 2019-0-01697-004          |
| 부처명         | 과학기술정보통신부                 |
| 과제관리(전문)기관명 | 정보통신기획평가원                 |
| 연구사업명       | 정보보호핵심원천기술개발              |
| 연구과제명       | 블록체인 플랫폼 보안취약점 자동분석 기술 개발 |
| 기 여 율       | 30/100                    |
| 과제수행기관명     | 고려대학교산학협력단                |
| 연구기간        | 2022.01.01 ~ 2022.12.31   |

이 발명을 지원한 국가연구개발사업

|             |                                          |
|-------------|------------------------------------------|
| 과제고유번호      | 1711152551                               |
| 과제번호        | 2020-0-01337-003                         |
| 부처명         | 과학기술정보통신부                                |
| 과제관리(전문)기관명 | 정보통신기획평가원                                |
| 연구사업명       | SW컴퓨팅산업원천기술개발                            |
| 연구과제명       | (SW 스탭) 실용화 수준의 고성능 소프트웨어 오류 자동 수정 기술 개발 |
| 기 여 율       | 30/100                                   |
| 과제수행기관명     | 고려대학교산학협력단                               |
| 연구기간        | 2022.01.01 ~ 2022.12.31                  |

이 발명을 지원한 국가연구개발사업

|             |                                      |
|-------------|--------------------------------------|
| 과제고유번호      | 1711160653                           |
| 과제번호        | 2022-0-00277-001                     |
| 부처명         | 과학기술정보통신부                            |
| 과제관리(전문)기관명 | 정보통신기획평가원                            |
| 연구사업명       | 정보보호핵심원천기술개발                         |
| 연구과제명       | SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발 |
| 기 여 율       | 30/100                               |
| 과제수행기관명     | 고려대학교산학협력단                           |
| 연구기간        | 2022.04.01 ~ 2022.12.31              |

이 발명을 지원한 국가연구개발사업

|             |                         |
|-------------|-------------------------|
| 과제고유번호      | 1711159611              |
| 과제번호        | 2020-0-01819-003        |
| 부처명         | 과학기술정보통신부               |
| 과제관리(전문)기관명 | 정보통신기획평가원               |
| 연구사업명       | 정보통신방송혁신인재양성(R&D)       |
| 연구과제명       | ICT명품인재양성(고려대학교)        |
| 기 여 율       | 10/100                  |
| 과제수행기관명     | 고려대학교산학협력단              |
| 연구기간        | 2022.01.01 ~ 2022.12.31 |

---

## 명세서

### 청구범위

#### 청구항 1

컴퓨팅 장치에 의해 수행되는, 스마트 컨트랙트 취약점 수정 방법으로서,

검증기를 이용하여 원본 스마트 컨트랙트를 검증하는 단계;

상기 원본 스마트 컨트랙트에 대한 검증 결과에 따라 상기 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 초기 후보 패치들을 생성하고, 상기 생성된 복수의 초기 후보 패치들을 상기 원본 스마트 컨트랙트에 적용한 복수의 초기 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시키는 단계;

사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하는 단계; 및

검증이 완료된 적어도 하나의 후보 스마트 컨트랙트들을 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력하는 단계를 포함하고,

상기 원본 스마트 컨트랙트에 대한 검증 결과는,

상기 원본 스마트 컨트랙트로부터 탐지된 취약점에 대한 정보를 나타내는 제1 취약점(vulnerability) 보고서 및 상기 원본 스마트 컨트랙트로부터 탐지된 퇴행에 대한 정보를 나타내는 제1 퇴행(regression) 보고서를 포함하는,

취약점 수정 방법.

#### 청구항 2

제1항에 있어서, 상기 사전 종료 조건을 만족할 때까지 상기 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 상기 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하는 단계는,

상기 워크셋에서 최소 비용 점수를 갖는 후보 패치 및 후보 스마트 컨트랙트를 선택하는 제1 단계;

상기 워크셋에서 선택된 후보 스마트 컨트랙트 및 상기 선택된 후보 스마트 컨트랙트에 적용된 후보 패치를 삭제하는 제2 단계;

상기 검증기를 이용하여, 상기 선택된 후보 스마트 컨트랙트를 검증하는 제3 단계;

상기 선택된 후보 스마트 컨트랙트에 대한 검증 결과에 따라 수정 진행 상태에 대한 변수들을 갱신하는 제4 단계; 및

복수의 새로운 후보 패치들 및 복수의 새로운 후보 패치들 각각이 적용된 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 복수의 새로운 후보 패치들 및 상기 복수의 새로운 후보 스마트 컨트랙트들을 상기 워크셋에 포함시키는 제5 단계; 및

상기 사전 종료 조건이 만족되면 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 후보 스마트 컨트랙트들을 출력하는 제6 단계를 포함하고,

상기 사전 종료 조건이 만족되지 않으면 상기 워크셋에 포함된 복수의 후보 패치들 및 복수의 후보 스마트 컨트랙트들을 대상으로 상기 제1 단계 내지 상기 제5 단계를 반복적으로 수행하는 루프(loop) 동작이 수행되는,

취약점 수정 방법.

#### 청구항 3

제2항에 있어서, 상기 최소 비용 점수를 갖는 후보 패치 및 후보 스마트 컨트랙트를 선택하는 제1 단계는,

상기 복수의 후보 스마트 컨트랙트들 각각에 적용된 후보 패치에 대한 비용 점수를 결정하는 단계; 및

상기 결정된 비용 점수 중 상기 최소 비용 점수를 갖는 후보 패치 및 상기 최소 비용 점수를 갖는 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하는 단계를 포함하는,

취약점 수정 방법.

#### 청구항 4

제1항에 있어서, 상기 사전 종료 조건은,

사전 설정된 타임아웃(time-out)에 도달하는 경우, 또는 상기 워크셋에 저장되었던 모든 후보 스마트 컨트랙트에 대한 검증이 완료된 경우, 또는 정답 스마트 컨트랙트를 발견하는 경우 중 어느 하나를 포함하는,

취약점 수정 방법.

#### 청구항 5

제2항에 있어서, 상기 수정 진행 상태에 대한 변수들은,

상기 원본 스마트 컨트랙트에 대하여 상기 후보 패치가 적용되었고, 비퇴행적이고, 탐지된 취약점의 수가 현재 까지 최소이고, 적용된 후보 패치의 크기가 현재까지 최소인 조건들을 만족하는 후보 스마트 컨트랙트들의 집합, 상기 조건들을 만족하는 후보 스마트 컨트랙트들에서 탐지된 취약점의 수, 상기 조건들을 만족하는 후보 스마트 컨트랙트들에 적용된 패치의 크기를 포함하는,

취약점 수정 방법.

#### 청구항 6

삭제

#### 청구항 7

제1항에 있어서, 상기 탐지된 취약점에 대한 정보는,

상기 탐지된 취약점의 타입, 상기 탐지된 취약점을 포함하고 있는 함수의 시그니처(signature), 상기 취약점이 탐지된 라인의 숫자, 또는 상기 라인에서 탐지된 취약점이 존재하는 표현식이나 명령문 중 적어도 하나를 포함하는,

취약점 수정 방법.

#### 청구항 8

제1항에 있어서, 상기 탐지된 퇴행에 대한 정보는,

사전에 정의된 퇴행의 종류들 중 상기 탐지된 퇴행의 종류 또는 상기 탐지된 퇴행을 포함하는 함수의 시그니처를 포함하는,

취약점 수정 방법.

#### 청구항 9

제1항에 있어서, 상기 복수의 초기 후보 패치들을 생성하고, 상기 복수의 초기 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 단계는,

상기 제1 취약점 보고서에 기반하여 상기 원본 스마트 컨트랙트에 존재하는 적어도 하나의 취약점을 수정하기 위한 패치 컴포넌트 집합을 결정하는 단계;

상기 결정된 패치 컴포넌트 집합을 이용하여 상기 복수의 초기 후보 패치들을 생성하는 단계;

상기 복수의 초기 후보 패치들을 상기 원본 스마트 컨트랙트에 적용하여 상기 복수의 초기 후보 스마트 컨트랙트들을 생성하는 단계; 및

상기 복수의 초기 후보 패치들 및 상기 복수의 초기 후보 스마트 컨트랙트들을 상기 워크셋에 포함시키는 단계를 포함하는,

취약점 수정 방법.

#### 청구항 10

제9항에 있어서, 상기 패치 컴포넌트 집합을 결정하는 단계는,

복수의 취약점들을 수정하기 위해 사전 설정된 복수의 수정 템플릿들을 이용하여 상기 원본 스마트 컨트랙트에 존재하는 적어도 하나의 취약점을 수정하기 위한 수정 템플릿 시퀀스를 결정하는 단계; 및

상기 결정된 수정 템플릿 시퀀스를 이용하여 상기 패치 컴포넌트 집합을 결정하는 단계를 포함하는,

취약점 수정 방법.

#### 청구항 11

제2항에 있어서, 상기 선택된 후보 스마트 컨트랙트에 대한 검증 결과는,

상기 선택된 후보 스마트 컨트랙트로부터 탐지된 취약점에 대한 정보를 나타내는 제2 취약점 보고서 및 상기 선택된 후보 스마트 컨트랙트로부터 탐지된 퇴행에 대한 정보를 나타내는 제2 퇴행 보고서를 포함하는,

취약점 수정 방법.

#### 청구항 12

제3항에 있어서, 상기 복수의 후보 스마트 컨트랙트들 각각에 적용된 후보 패치에 대한 비용 점수를 결정하는 단계는,

상기 복수의 후보 스마트 컨트랙트들 각각에 대한 검증 결과에 기반하여 학습된 제1 통계 모델을 이용하거나, 과거 수정 이력들에 기반하여 학습된 제2 통계 모델을 이용하여 상기 복수의 후보 패치들에 대한 예상 안전성 점수를 산출하는 단계; 및

상기 산출된 예상 안전성 점수를 이용하여 상기 복수의 후보 패치들에 대한 비용 점수를 결정하는 단계를 포함하는,

취약점 수정 방법.

#### 청구항 13

제12항에 있어서, 상기 과거 수정 이력들은,

복수의 추상화된 과거 후보 패치들 및 상기 복수의 추상화된 과거 후보 패치들 각각이 정답 패치에 가까운 정도를 수치화한 안전성 점수를 포함하고,

상기 복수의 추상화된 과거 후보 패치들 각각은,

과거 원본 스마트 컨트랙트에 적용되었던 복수의 후보 패치들을 포함하는,

취약점 수정 방법.

#### 청구항 14

제12항에 있어서, 상기 제1 통계 모델은,

상기 복수의 후보 패치들 각각에 기반하여 상기 복수의 후보 패치들 각각이 정답 패치에 가까운 정도를 수치화한 안전성 점수를 산출하도록 학습되는,

취약점 수정 방법.

#### 청구항 15

제13항에 있어서, 상기 제2 통계 모델은,

상기 복수의 추상화된 과거 후보 패치들 각각에 대한 안전성 점수를 산출하도록 학습되는,

취약점 수정 방법.

#### 청구항 16

제12항에 있어서, 상기 복수의 후보 패치들 각각에 대한 상기 비용 점수를 결정하는 단계는,

상기 제1 통계 모델을 이용하여 상기 복수의 새로운 후보 패치들 각각에 대한 제1 안전성 점수를 결정하는 단계;

상기 복수의 새로운 후보 패치들 각각에 대한 패널티 점수를 결정하는 단계; 및

상기 결정된 제1 안전성 점수에서 상기 결정된 패널티 점수를 감소시킨 값의 음수 값을 상기 비용 점수로 결정하는 단계를 포함하는,

취약점 수정 방법.

#### 청구항 17

제12항에 있어서, 상기 복수의 후보 패치들 각각에 대한 상기 비용 점수를 결정하는 단계는,

상기 제2 통계 모델을 이용하여 상기 복수의 새로운 후보 패치들 각각에 대한 제2 안전성 점수를 결정하는 단계;

상기 복수의 새로운 후보 패치들 각각에 대한 패널티 점수를 결정하는 단계; 및

상기 결정된 제2 안전성 점수에서 상기 결정된 패널티 점수를 감소시킨 값의 음수 값을 상기 비용 점수로 결정하는 단계를 포함하는,

취약점 수정 방법.

#### 청구항 18

제12항에 있어서, 상기 최소 비용 점수를 갖는 후보 패치 및 상기 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하는 단계는,

상기 제1 통계 모델 또는 상기 제2 통계 모델을 이용하여 상기 워크셋에 포함된 복수의 후보 패치들 중 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하는 단계인,

취약점 수정 방법.

#### 청구항 19

제18항에 있어서, 상기 제1 통계 모델 또는 상기 제2 통계 모델을 이용하여 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 결정하는 단계는,

상기 결정된 비용 점수 중 상기 최소 비용 점수를 갖는 후보 패치에서 높은 비용 점수를 갖는 후보 패치 순으로 적어도 하나의 정답 후보 패치를 결정하는 단계; 및

상기 적어도 하나의 정답 후보 패치 중 상기 최소 비용 점수를 갖는 후보 패치를 상기 정답 패치일 가능성이 가장 큰 새로운 후보 패치로 결정하는 단계를 포함하는,

취약점 수정 방법.

#### 청구항 20

제18항에 있어서,

상기 제1 통계 모델을 이용하여 상기 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하기 전에, 상기 복수의 후보 스마트 컨트랙트들 각각에 대한 검증 결과를 이용하여 상기 제1 통계 모델을 학습시키기 위한 제1 학습 데이터 세트를 생성하는 단계; 및

상기 생성된 제1 학습 데이터 세트를 이용하여 상기 제1 통계 모델을 학습시키는 단계를 포함하고,

상기 제1 학습 데이터 세트는,

상기 복수의 후보 스마트 컨트랙트들 각각에 적용된 후보 패치에 대한 특징 벡터(feature vector) 및 상기 후보 패치에 대한 안전성 점수를 포함하는,

취약점 수정 방법.

## 청구항 21

제18항에 있어서,

상기 제2 통계 모델을 이용하여 상기 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하기 전에, 복수의 과거 후보 스마트 컨트랙트들 각각에 대한 검증 결과를 이용하여 상기 제2 통계 모델을 학습시키기 위한 제2 학습 데이터 세트를 생성하는 단계; 및

상기 생성된 제2 학습 데이터 세트를 이용하여 상기 제2 통계 모델을 학습시키는 단계를 포함하고,

상기 제2 학습 데이터 세트는,

복수의 추상화된 과거 후보 패치들 각각에 대한 특징 벡터 및 복수의 추상화된 과거 후보 패치들 각각에 대한 안전성 점수를 포함하는,

취약점 수정 방법.

## 청구항 22

컴퓨터 판독가능 저장 매체 저장된 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은 하나 이상의 프로세서에서 실행되는 경우, 스마트 컨트랙트 취약점 수정을 위한 이하의 동작들을 수행하도록 하며, 상기 동작들은:

검증기를 이용하여 원본 스마트 컨트랙트를 검증하는 동작;

상기 원본 스마트 컨트랙트에 대한 검증 결과에 따라 상기 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 초기 후보 패치들을 생성하고, 상기 생성된 복수의 초기 후보 패치들을 상기 원본 스마트 컨트랙트에 적용한 복수의 초기 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시키는 동작;

사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하는 동작; 및

검증이 완료된 적어도 하나의 후보 스마트 컨트랙트들을 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력하는 동작을 포함하고,

상기 원본 스마트 컨트랙트에 대한 검증 결과는,

상기 원본 스마트 컨트랙트로부터 탐지된 취약점에 대한 정보를 나타내는 제1 취약점(vulnerability) 보고서 및 상기 원본 스마트 컨트랙트로부터 탐지된 퇴행에 대한 정보를 나타내는 제1 퇴행(regression) 보고서를 포함하는,

컴퓨터 판독가능 저장매체에 저장된 컴퓨터 프로그램.

## 청구항 23

스마트 컨트랙트 취약점 수정을 위한 컴퓨팅 장치로서,

적어도 하나의 프로세서; 및

메모리를 포함하며,

상기 적어도 하나의 프로세서는:

검증기를 이용하여 원본 스마트 컨트랙트를 검증하고,

상기 원본 스마트 컨트랙트에 대한 검증 결과에 따라 상기 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 후보 패치들을 생성하고, 상기 생성된 복수의 후보 패치들을 상기 원본 스마트 컨트

랙트에 적용한 복수의 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시키고,  
 사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하고,  
 검증이 완료된 적어도 하나의 후보 스마트 컨트랙트들을 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력하도록 구성되고,  
 상기 원본 스마트 컨트랙트에 대한 검증 결과는,  
 상기 원본 스마트 컨트랙트로부터 탐지된 취약점에 대한 정보를 나타내는 제1 취약점(vulnerability) 보고서 및 상기 원본 스마트 컨트랙트로부터 탐지된 퇴행에 대한 정보를 나타내는 제1 퇴행(regression) 보고서를 포함하는,  
 컴퓨팅 장치.

## 발명의 설명

### 기술 분야

[0001] 본 개시는 스마트 컨트랙트의 보안에 관한 것으로, 구체적으로 스마트 컨트랙트에 존재하는 취약점을 수정하기 위한 방법 및 장치에 관한 것이다.

### 배경 기술

[0002] 일반적으로, 스마트 컨트랙트(Smart Contract)는 프로그래밍 언어로 작성된 디지털 계약서(digital contract)를 의미한다. 이러한 스마트 컨트랙트는 신뢰할 수 있는 제3 중개인의 개입이 필요하지 않으므로, 기존 문서 기반 계약 과정에서 소요되던 시간과 비용을 획기적으로 절감해줄 수 있다. 이로 인해, 스마트 컨트랙트는 금융, 유통망 관리 등의 많은 분야에서 활용성이 높아지고 있다.

[0003] 그러나, 스마트 컨트랙트는 블록체인으로의 배포 후 코드 수정이 불가능하며, 단 하나의 보안 취약점이 존재하더라도 이를 악용하게 되면 막대한 재산 피해로 이어질 수 있다는 문제점이 있다.

[0004] 이러한 스마트 컨트랙트의 안전성 문제를 해결하기 위해 다수의 보안 취약점 탐지 기술들이 연구되었으나, 이러한 기술들로 탐지된 취약점을 개발자가 수동으로 수정하므로, 수정하는데 오랜 시간이 소요되고, 개발자의 실수로 인해 새로운 취약점이 추가될 수도 있다.

[0005] 이로 인해, 탐지된 취약점을 자동으로 수정하는 기술들도 연구되었으나, 이러한 기술들은 대부분 한 종류의 수정 전략을 이용하므로, 다양한 타입 또는 패턴의 취약점을 수정하는데 적용하기 어렵다. 또한, 여러 가지 수정 전략을 활용하는 기술도 연구되었으나, 이러한 기술은 일부 프로그램 실행 경우만을 고려하여 테스트되므로, 수정에 대한 안전성이 보장되지 않는다.

[0006] 따라서, 스마트 컨트랙트에 대하여 다양한 종류의 취약점을 탐지하고, 탐지된 취약점을 자동으로 수정하면서 수정된 스마트 컨트랙트에 대한 안전성을 보장하기 위한 스마트 컨트랙트 취약점 수정 방법 및 장치가 요구된다.

## 선행기술문헌

### 특허문헌

[0007] (특허문헌 0001) 일본 공개특허 제2022-535785호

## 발명의 내용

### 해결하려는 과제

[0008] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 스마트 컨트랙트 취약점 수정 방법 및 장치를 제공하고자 한다.

[0009] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과

제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

## 과제의 해결 수단

- [0010] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 실시예에 따라, 컴퓨팅 장치에 의해 수행되는, 스마트 컨트랙트 취약점 수정 방법은, 검증기를 이용하여 원본 스마트 컨트랙트를 검증하는 단계, 상기 원본 스마트 컨트랙트에 대한 검증 결과에 따라 상기 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 초기 후보 패치들을 생성하고, 상기 생성된 복수의 초기 후보 패치들을 상기 원본 스마트 컨트랙트에 적용한 복수의 초기 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시키는 단계, 사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하는 단계 및 검증 완료된 적어도 하나의 후보 스마트 컨트랙트들을 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력하는 단계를 포함할 수 있다.
- [0011] 또한, 상기 사전 종료 조건을 만족할 때까지 상기 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 상기 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하는 단계는, 상기 워크셋에서 최소 비용 점수를 갖는 후보 패치 및 후보 스마트 컨트랙트를 선택하는 제1 단계, 상기 워크셋에서 선택된 후보 스마트 컨트랙트 및 상기 선택된 후보 스마트 컨트랙트에 적용된 후보 패치를 삭제하는 제2 단계, 상기 검증기를 이용하여, 상기 선택된 후보 스마트 컨트랙트를 검증하는 제3 단계, 상기 선택된 후보 스마트 컨트랙트에 대한 검증 결과에 따라 수정 진행 상태에 대한 변수들을 갱신하는 제4 단계, 복수의 새로운 후보 패치들 및 복수의 새로운 후보 패치들 각각이 적용된 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 복수의 새로운 후보 패치들 및 상기 복수의 새로운 후보 스마트 컨트랙트들을 상기 워크셋에 포함시키는 제5 단계 및 상기 사전 종료 조건이 만족되면 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 후보 스마트 컨트랙트들을 출력하는 제6 단계를 포함하고, 상기 사전 종료 조건이 만족되지 않으면 상기 워크셋에 포함된 복수의 후보 패치들 및 복수의 후보 스마트 컨트랙트들을 대상으로 상기 제1 단계 내지 상기 제5 단계를 반복적으로 수행하는 루프(loop) 동작이 수행될 수 있다.
- [0012] 또한, 상기 최소 비용 점수를 갖는 후보 패치 및 후보 스마트 컨트랙트를 선택하는 제1 단계는, 상기 복수의 후보 스마트 컨트랙트들 각각에 적용된 후보 패치에 대한 비용 점수를 결정하는 단계 및 상기 결정된 비용 점수 중 상기 최소 비용 점수를 갖는 후보 패치 및 상기 최소 비용 점수를 갖는 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하는 단계를 포함할 수 있다.
- [0013] 또한, 상기 사전 종료 조건은, 사전 설정된 타임아웃(time-out)에 도달하는 경우, 또는 상기 워크셋에 저장되었던 모든 후보 스마트 컨트랙트에 대한 검증이 완료된 경우, 또는 정답 스마트 컨트랙트를 발견하는 경우 중 어느 하나를 포함할 수 있다.
- [0014] 또한, 상기 수정 진행 상태에 대한 변수들은, 상기 원본 스마트 컨트랙트에 대하여 상기 후보 패치가 적용되었고, 비퇴행적이고, 탐지된 취약점의 수가 현재까지 최소이고, 적용된 후보 패치의 크기가 현재까지 최소인 조건들을 만족하는 후보 스마트 컨트랙트들의 집합, 상기 조건들을 만족하는 후보 스마트 컨트랙트들에서 탐지된 취약점의 수, 상기 조건들을 만족하는 후보 스마트 컨트랙트들에 적용된 패치의 크기를 포함할 수 있다.
- [0015] 또한, 상기 원본 스마트 컨트랙트에 대한 검증 결과는, 상기 원본 스마트 컨트랙트로부터 탐지된 취약점에 대한 정보를 나타내는 제1 취약점(vulnerability) 보고서 및 상기 원본 스마트 컨트랙트로부터 탐지된 퇴행에 대한 정보를 나타내는 제1 퇴행(regression) 보고서를 포함할 수 있다.
- [0016] 또한, 상기 탐지된 취약점에 대한 정보는, 상기 탐지된 취약점의 타입, 상기 탐지된 취약점을 포함하고 있는 함수의 시그니처(signature), 상기 취약점이 탐지된 라인의 숫자, 또는 상기 라인에서 탐지된 취약점이 존재하는 표현식이나 명령문 중 적어도 하나를 포함할 수 있다.
- [0017] 또한, 상기 탐지된 퇴행에 대한 정보는, 사전에 정의된 퇴행의 종류들 중 상기 탐지된 퇴행의 종류 또는 상기 탐지된 퇴행을 포함하는 함수의 시그니처를 포함할 수 있다.
- [0018] 또한, 상기 복수의 초기 후보 패치들을 생성하고, 상기 복수의 초기 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 단계는, 상기 제1 취약점 보고서에 기반하여 상기 원본 스마트 컨트랙트에 존재하는 적어도 하나의 취약점을 수정하기 위한 패치 컴포넌트 집합을 결정하는 단계, 상기 결정된 패치 컴포넌트 집합을 이용하여 상기 복수의 초기 후보 패치들을 생성하는 단계, 상기 복수의 초기 후보 패치들을 상기 원본 스마트 컨

트랙트에 적용하여 상기 복수의 초기 후보 스마트 컨트랙트들을 생성하는 단계 및 상기 복수의 초기 후보 패치들 및 상기 복수의 초기 후보 스마트 컨트랙트들을 상기 워크셋에 포함시키는 단계를 포함할 수 있다.

- [0019] 또한, 상기 패치 컴포넌트 집합을 결정하는 단계는, 복수의 취약점들을 수정하기 위해 사전 설정된 복수의 수정 템플릿들을 이용하여 상기 원본 스마트 컨트랙트에 존재하는 적어도 하나의 취약점을 수정하기 위한 수정 템플릿 시퀀스를 결정하는 단계; 및 상기 결정된 수정 템플릿 시퀀스를 이용하여 상기 패치 컴포넌트 집합을 결정하는 단계를 포함할 수 있다.
- [0020] 또한, 상기 선택된 후보 스마트 컨트랙트에 대한 검증 결과는, 상기 선택된 후보 스마트 컨트랙트로부터 탐지된 취약점에 대한 정보를 나타내는 제2 취약점 보고서 및 상기 선택된 후보 스마트 컨트랙트로부터 탐지된 퇴행에 대한 정보를 나타내는 제2 퇴행 보고서를 포함할 수 있다.
- [0021] 또한, 상기 복수의 후보 스마트 컨트랙트들 각각에 적용된 후보 패치에 대한 비용 점수를 결정하는 단계는, 상기 복수의 후보 스마트 컨트랙트들 각각에 대한 검증 결과에 기반하여 학습된 제1 통계 모델을 이용하거나, 과거 수정 이력들에 기반하여 학습된 제2 통계 모델을 이용하여 상기 복수의 후보 패치들에 대한 예상 안전성 점수를 산출하는 단계 및 상기 산출된 예상 안전성 점수를 이용하여 상기 복수의 후보 패치들에 대한 비용 점수를 결정하는 단계를 포함할 수 있다.
- [0022] 또한, 상기 과거 수정 이력들은, 복수의 추상화된 과거 후보 패치들 및 상기 복수의 추상화된 과거 후보 패치들 각각이 정답 패치에 가까운 정도를 수치화한 안전성 점수를 포함하고, 상기 복수의 과거 후보 패치들 각각은, 과거 원본 스마트 컨트랙트에 적용되었던 복수의 후보 패치들을 포함할 수 있다.
- [0023] 또한, 상기 제1 통계 모델은, 상기 복수의 후보 패치들 각각에 기반하여 상기 복수의 후보 패치들 각각이 정답 패치에 가까운 정도를 수치화한 안전성 점수를 산출하도록 학습될 수 있다.
- [0024] 또한, 상기 제2 통계 모델은, 상기 복수의 추상화된 과거 후보 패치들 각각에 대한 안전성 점수를 산출하도록 학습될 수 있다.
- [0025] 또한, 상기 복수의 후보 패치들 각각에 대한 상기 비용 점수를 결정하는 단계는, 상기 제1 통계 모델을 이용하여 상기 복수의 새로운 후보 패치들 각각에 대한 제1 안전성 점수를 결정하는 단계, 상기 복수의 새로운 후보 패치들 각각에 대한 패널티 점수를 결정하는 단계 및 상기 결정된 제1 안전성 점수에서 상기 결정된 패널티 점수를 감소시킨 값의 음수 값을 상기 비용 점수로 결정하는 단계를 포함할 수 있다.
- [0026] 또한, 상기 복수의 후보 패치들 각각에 대한 상기 비용 점수를 결정하는 단계는, 상기 제2 통계 모델을 이용하여 상기 복수의 새로운 후보 패치들 각각에 대한 제2 안전성 점수를 결정하는 단계, 상기 복수의 새로운 후보 패치들 각각에 대한 패널티 점수를 결정하는 단계 및 상기 결정된 제2 안전성 점수에서 상기 결정된 패널티 점수를 감소시킨 값의 음수 값을 상기 비용 점수로 결정하는 단계를 포함할 수 있다.
- [0027] 또한, 상기 최소 비용 점수를 갖는 후보 패치 및 상기 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하는 단계는, 상기 제1 통계 모델 또는 상기 제2 통계 모델을 이용하여 상기 워크셋에 포함된 복수의 후보 패치들 중 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하는 단계일 수 있다.
- [0028] 또한, 상기 제1 통계 모델 또는 상기 제2 통계 모델을 이용하여 상기 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 결정하는 단계는, 상기 결정된 비용 점수 중 상기 최소 비용 점수를 갖는 후보 패치에서 높은 비용 점수를 갖는 후보 패치 순으로 상기 적어도 하나의 후보 패치를 결정하는 단계 및 상기 적어도 하나의 정답 후보 패치 중 상기 최소 비용 점수를 갖는 후보 패치를 상기 정답 패치일 가능성이 가장 큰 새로운 후보 패치로 결정하는 단계를 포함할 수 있다.
- [0029] 또한, 상기 제1 통계 모델을 이용하여 상기 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하기 전에, 상기 복수의 후보 스마트 컨트랙트들 각각에 대한 검증 결과를 이용하여 상기 제1 통계 모델을 학습시키기 위한 제1 학습 데이터 세트를 생성하는 단계 및 상기 생성된 제1 학습 데이터 세트를 이용하여 상기 제1 통계 모델을 학습시키는 단계를 포함하고, 상기 제1 학습 데이터 세트는, 상기 복수의 후보 스마트 컨트랙트들 각각에 적용된 후보 패치에 대한 특징 벡터 (feature vector) 및 상기 후보 패치에 대한 안전성 점수를 포함할 수 있다.
- [0030] 또한, 상기 제2 통계 모델을 이용하여 상기 정답 패치일 가능성이 가장 큰 후보 패치 및 상기 정답 패치일 가능성이 가장 큰 후보 패치가 적용된 후보 스마트 컨트랙트를 선택하기 전에, 복수의 과거 후보 스마트 컨트랙트들

각각에 대한 검증 결과를 이용하여 상기 제2 통계 모델을 학습시키기 위한 제2 학습 데이터 세트를 생성하는 단계 및 상기 생성된 제2 학습 데이터 세트를 이용하여 상기 제2 통계 모델을 학습시키는 단계를 포함하고, 상기 제2 학습 데이터 세트는, 복수의 추상화된 과거 후보 패치들 각각에 대한 특징 벡터 및 복수의 추상화된 과거 후보 패치들 각각에 대한 안전성 점수를 포함할 수 있다.

[0031] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 실시예에 따라, 컴퓨터 판독가능 저장 매체 저장된 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은 하나 이상의 프로세서에서 실행되는 경우, 스마트 컨트랙트 취약점 수정을 위한 이하의 동작들을 수행하도록 하며, 상기 동작들은, 검증기를 이용하여 원본 스마트 컨트랙트를 검증하는 동작, 상기 원본 스마트 컨트랙트에 대한 검증 결과에 따라 상기 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 초기 후보 패치들을 생성하고, 상기 생성된 복수의 초기 후보 패치들을 상기 원본 스마트 컨트랙트에 적용한 복수의 초기 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시키는 동작, 사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하는 동작 및 검증 완료된 적어도 하나의 후보 스마트 컨트랙트들을 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력하는 동작을 포함할 수 있다.

[0032] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 실시예에 따라, 스마트 컨트랙트 취약점 수정을 위한 컴퓨팅 장치로서, 적어도 하나의 프로세서 및 메모리를 포함하며, 상기 적어도 하나의 프로세서는, 검증기를 이용하여 원본 스마트 컨트랙트를 검증하고, 상기 원본 스마트 컨트랙트에 대한 검증 결과에 따라 상기 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 후보 패치들을 생성하고, 상기 생성된 복수의 후보 패치들을 상기 원본 스마트 컨트랙트에 적용하여 복수의 초기 후보 스마트 컨트랙트들을 생성하고, 사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 상기 워크셋에 포함시키는 과정을 반복하고, 검증이 완료된 적어도 하나의 후보 스마트 컨트랙트들을 상기 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력하도록 구성될 수 있다.

[0033] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

### 발명의 효과

[0034] 본 개시의 몇몇 실시예에 따르면, 본 개시의 스마트 컨트랙트 취약점 수정 방법 및 장치는 취약점 탐지부터 수정까지 전자동화가 가능하고, 수정을 위해 소요되는 시간을 줄이면서 개발자의 실수를 최소화할 수 있다.

[0035] 또한, 본 개시의 스마트 컨트랙트 취약점 수정 방법 및 장치는 스마트 컨트랙트의 안전성을 향상시키고, 기존 취약점 탐지 및/또는 수정 기술 대비 신속하고 정확도 있는 취약점 탐지 및 수정이 가능하다.

[0036] 또한, 본 개시의 스마트 컨트랙트 취약점 수정 방법 및 장치는 스마트 컨트랙트 뿐만 아니라, 다른 종류의 프로그램(C, Java 등)을 위한 오류 수정 기술에 적용될 수 있으며, 이에 따라 해당 오류 수정 기술의 속도 및 정확성을 개선시킬 수 있다.

[0037] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

### 도면의 간단한 설명

[0038] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 구체적인 세부사항들 없이 실시될 수 있음은 명백할 것이다.

도 1은 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정을 위한 장치의 블록 구성도이다.

도 2는 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정 방법의 일례를 설명하기 위한 흐름도이다.

도 3은 본 개시의 실시예에 따른 정답 스마트 컨트랙트 혹은 비퇴행적이고 원본 스마트 컨트랙트의 취약점이 일

부 수정되어 적어도 원본 스마트 컨트랙트보다 더 안전한 스마트 컨트랙트를 결정하는 방법의 일례를 설명하기 위한 흐름도이다.

도 4는 본 개시의 실시예에 따라 제1 통계 모델을 학습시키기 위한 제1 학습 데이터를 생성하는 방법을 설명하기 위한 예시도이다.

도 5는 본 개시의 실시예에 따라 제1 통계 모델을 학습시키기 위한 방법을 설명하기 위한 예시도이다.

도 6은 본 개시의 실시예에 따라 제1 통계 모델을 이용하여 적어도 하나의 정답 후보 패치를 결정하기 위한 방법의 일례를 설명하기 위한 흐름도이다.

도 7은 본 개시의 실시예에 따라 제2 통계 모델을 학습시키기 위한 제2 학습 데이터를 생성하는 방법을 설명하기 위한 예시도이다.

도 8은 본 개시의 실시예에 따라 제2 통계 모델을 학습시키기 위한 방법을 설명하기 위한 예시도이다.

도 9는 본 개시의 실시예에 따라 제2 통계 모델을 이용하여 적어도 하나의 정답 후보 패치를 결정하기 위한 방법의 일례를 설명하기 위한 흐름도이다.

도 10은 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정 동작을 의사코드로 표현한 일례를 나타내는 예시도이다.

도 11은 본 개시의 실시예에 따른 수정 진행 상태를 결정하기 위한 변수들을 갱신하는 동작을 의사코드로 표현한 일례를 나타내는 예시도이다.

도 12는 본 개시의 실시예에 따른 통계 모델을 학습하기 위해 사용되는 데이터 및 통계 모델을 획득하기 위한 동작을 의사코드로 표현한 일례를 나타내는 예시도이다.

도 13은 본 개시의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도이다.

### 발명을 실시하기 위한 구체적인 내용

[0039] 다양한 실시예들이 이제 도면을 참조하여 설명된다. 본 명세서에서, 다양한 설명들이 본 개시의 이해를 제공하기 위해서 제시된다. 그러나, 이러한 실시예들은 이러한 구체적인 설명 없이도 실행될 수 있음이 명백하다.

[0040] 본 명세서에서 사용되는 용어 "컴포넌트", "모듈", "시스템" 등은 컴퓨터-관련 엔티티, 하드웨어, 펌웨어, 소프트웨어, 소프트웨어 및 하드웨어의 조합, 또는 소프트웨어의 실행을 지칭한다. 예를 들어, 컴포넌트는 프로세서 상에서 실행되는 처리과정(procedure), 프로세서, 객체, 실행 스레드, 프로그램, 및/또는 컴퓨터일 수 있지만, 이들로 제한되는 것은 아니다. 예를 들어, 컴퓨팅 장치에서 실행되는 애플리케이션 및 컴퓨팅 장치 모두 컴포넌트일 수 있다. 하나 이상의 컴포넌트는 프로세서 및/또는 실행 스레드 내에 상주할 수 있다. 일 컴포넌트는 하나의 컴퓨터 내에 로컬화 될 수 있다. 일 컴포넌트는 2개 이상의 컴퓨터들 사이에 분배될 수 있다. 또한, 이러한 컴포넌트들은 그 내부에 저장된 다양한 데이터 구조들을 갖는 다양한 컴퓨터 판독가능한 매체로부터 실행할 수 있다. 컴포넌트들은 예를 들어 하나 이상의 데이터 패킷들을 갖는 신호(예를 들면, 로컬 시스템, 분산 시스템에서 다른 컴포넌트와 상호작용하는 하나의 컴포넌트로부터의 데이터 및/또는 신호를 통해 다른 시스템과 인터넷과 같은 네트워크를 통해 전송되는 데이터)에 따라 로컬 및/또는 원격 처리들을 통해 통신할 수 있다.

[0041] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0042] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하는 것으로 이해되어야 한다. 다만, "포함한다" 및/또는 "포함하는"이라는 용어는, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0043] 그리고, "A 또는 B 중 적어도 하나"이라는 용어는, "A만을 포함하는 경우", "B 만을 포함하는 경우", "A와 B의

구성으로 조합된 경우"를 의미하는 것으로 해석되어야 한다.

- [0044] 당업자들은 추가적으로 여기서 개시된 실시예들과 관련되어 설명된 다양한 예시적 논리적 블록들, 구성들, 모듈들, 회로들, 수단들, 로직들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양쪽 모두의 조합들로 구현될 수 있음을 인식해야 한다. 하드웨어 및 소프트웨어의 상호교환성을 명백하게 예시하기 위해, 다양한 예시적 컴포넌트들, 블록들, 구성들, 수단들, 로직들, 모듈들, 회로들, 및 단계들은 그들의 기능성 측면에서 일반적으로 위에서 설명되었다. 그러한 기능성이 하드웨어로 또는 소프트웨어로서 구현되는지 여부는 전반적인 시스템에 부과된 특정 어플리케이션(application) 및 설계 제한들에 달려 있다. 숙련된 기술자들은 각각의 특정 어플리케이션들을 위해 다양한 방법들로 설명된 기능성을 구현할 수 있다. 다만, 그러한 구현의 결정들이 본 개시내용의 영역을 벗어나게 하는 것으로 해석되어서는 안된다.
- [0045] 제시된 실시예들에 대한 설명은 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 발명을 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이다. 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어나지 않고 다른 실시예들에 적용될 수 있다. 그리하여, 본 발명은 여기에 제시된 실시예들로 한정되는 것이 아니다. 본 발명은 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.
- [0046] 본 개시에서 '원본 스마트 컨트랙트'는 적어도 하나의 취약점(vulnerability)이 존재하는 스마트 컨트랙트를 의미할 수 있다.
- [0047] 본 개시에서 '후보 패치'는 원본 스마트 컨트랙트에 존재하는 적어도 하나의 취약점을 수정하기 위해 원본 스마트 컨트랙트에 적용될 수 있는 패치(patch)를 의미할 수 있다.
- [0048] 본 개시에서 '후보 스마트 컨트랙트'는 원본 스마트 컨트랙트에 후보 패치가 적용된 스마트 컨트랙트를 의미할 수 있다.
- [0049] 본 개시에서 '정답 스마트 컨트랙트'는 비퇴행적이고, 취약점이 존재하지 않는(즉, 취약점의 부재가 검증기에 의해 증명된) 후보 스마트 컨트랙트를 의미할 수 있다.
- [0050] 본 개시에서 '정답 패치'는 정답 스마트 컨트랙트에 적용된 후보 패치를 의미할 수 있다.
- [0051] 본 개시에서 '검증기'는 원본 또는 후보 스마트 컨트랙트에 대한 검증을 수행하는 도구로서, 원본 또는 후보 스마트 컨트랙트에 대한 취약점 탐지 및 퇴행 탐지를 수행할 수 있다.
- [0052] 본 개시에서 '취약점 탐지'는 원본 또는 후보 스마트 컨트랙트에 취약점이 존재하는지를 검증하는 과정을 의미할 수 있다.
- [0053] 본 개시에서 '퇴행 탐지'는 원본 또는 후보 스마트 컨트랙트에 퇴행(regression)이 존재하는지 검증하는 과정을 의미할 수 있다.
- [0054] 도 1은 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정을 위한 장치의 블록 구성도이다. 도 1에 도시된 장치(100)의 구성은 간략화하여 나타낸 예시일 뿐이다. 본 개시의 일 실시예에서 장치(100)는 장치(100)의 컴퓨팅 환경을 수행하기 위한 다른 구성들이 포함될 수 있고, 개시된 구성들 중 일부만이 장치(100)를 구성할 수도 있다.
- [0055] 장치(100)는 통신부(110), 메모리(120) 및 프로세서(130)를 포함할 수 있다. 다만, 상술한 구성 요소들은 장치(100)를 구현하는데 있어서 필수적인 것은 아니어서, 장치(100)는 위에서 열거된 구성요소들보다 많거나, 또는 적은 구성요소들을 가질 수 있다. 여기서, 각각의 구성 요소들은 별개의 칩이나 모듈이나 장치로 구성될 수 있고, 하나의 장치 내에 포함될 수도 있다.
- [0056] 본 개시의 실시예에 따른 통신부(110)는 네트워크 접속을 위한 임의의 형태의 유/무선 인터넷 모듈을 포함할 수 있다. 또한, 통신부(110)는 근거리 통신(short range communication) 모듈을 포함할 수 있다. 근거리 통신 기술로 블루투스(Bluetooth), RFID(Radio Frequency Identification), 적외선 통신(IrDA, infrared Data Association), UWB(Ultra-Wideband), ZigBee 등이 이용될 수 있다.
- [0057] 본 명세서에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 다른 네트워크들에서도 사용될 수 있다.
- [0058] 본 개시의 몇몇 실시예에 따르면, 통신부(110)는 장치(100)가 외부 장치와 통신이 가능하도록 연결한다.
- [0059] 본 개시의 일 실시예에 따르면, 저장부(120)는 프로세서(130)가 생성하거나 결정한 임의의 형태의 정보 및 통신

부(110)가 수신한 임의의 형태의 정보를 저장할 수 있다. 본 개시의 몇몇 실시예에 따르면, 저장부(120)는 스마트 컨트랙트 취약점 수정을 위한 다양한 데이터를 저장할 수 있다.

- [0060] 저장부(120)는 프로세서의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들을 임시 또는 영구 저장할 수 있는 메모리 및/또는 영구저장매체를 포함할 수 있다. 저장부(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(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), 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. 이러한 메모리는 프로세서에 제어에 의하여 동작될 수 있다. 또한, 본 개시 내용에서 메모리 및 저장부는 서로 상호 교환 가능하게 사용될 수 있다. 장치(100)는 인터넷(internet) 상에서 상기 저장부(120)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다. 전술한 저장부에 대한 기재는 예시일 뿐, 본 개시는 이에 제한되지 않는다.
- [0061] 프로세서(130)는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치 (GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit), 신경 처리 장치(NPU: Neural Processing Unit) 등과 같이 메모리 상에 저장된 명령어들을 실행시킴으로써 스마트 컨트랙트 취약점 수정을 위한 임의의 형태의 프로세서를 포함할 수 있다.
- [0062] 프로세서(130)는 메모리(130)에 저장된 컴퓨터 프로그램을 판독하여 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정을 위한 데이터 처리를 수행할 수 있다.
- [0063] 구체적으로, 스마트 컨트랙트 취약점 수정을 위한 프로세서(130)는 검증기를 이용하여 원본 스마트 컨트랙트를 검증하고, 검증 결과에 따라 원본 스마트 컨트랙트를 수정하기 위한 복수의 초기 후보 패치들을 생성할 수 있다. 이어서, 프로세서(130)는 복수의 생성된 초기 후보 패치들 각각을 원본 스마트 컨트랙트에 적용한 복수의 초기 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시킬 수 있다.
- [0064] 프로세서(130)는 사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시키는 과정을 반복할 수 있다. 여기서, 사전 종료 조건은 사전 설정된 타임아웃에 도달하거나, 모든 후보 스마트 컨트랙트에 대한 검증이 완료되거나, 정답 스마트 컨트랙트를 발견하는 경우를 포함할 수 있다. 특히, 워크셋에 포함된 복수의 후보 스마트 컨트랙트들은 복수의 초기 후보 스마트 컨트랙트들 및 복수의 새로운 후보 스마트 컨트랙트들을 포함할 수 있다.
- [0065] 프로세서(130)는 검증이 완료된 적어도 하나의 후보 스마트 컨트랙트들을 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력할 수 있다.
- [0066] 원본 스마트 컨트랙트에 대한 취약점 수정을 가속화하기 위해 프로세서(130)는 인공지능 기반 모델을 이용하여 정답 패치일 가능성이 높은 적어도 하나의 후보 패치 및 해당 적어도 하나의 후보 패치를 원본 스마트 컨트랙트에 적용한 적어도 하나의 후보 스마트 컨트랙트를 결정하고, 적어도 하나의 결정된 후보 스마트 컨트랙트에 대해 우선적으로 검증을 수행할 수 있다.
- [0067] 이하에서는 도 2 내지 도 12를 참조하여 스마트 컨트랙트 취약점 수정을 위한 방법을 구체적으로 설명하도록 한다. 제시된 실시예에서 도 2 내지 도 12의 동작들은 스마트 컨트랙트 취약점 수정 장치(100)의 프로세서(130)에 의해서 수행될 수 있다.
- [0068] 도 2는 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정 방법의 일례를 설명하기 위한 흐름도이다.
- [0069] 도 2를 참조하면, 프로세서(130)는 검증기를 이용하여 원본 스마트 컨트랙트를 검증한다(S200).
- [0070] 구체적으로, 프로세서(130)는 검증기를 이용하여 원본 스마트 컨트랙트에 대한 취약점 탐지 및 퇴행 탐지를 수행하고, 원본 스마트 컨트랙트로부터 탐지된 취약점에 대한 정보를 나타내는 제1 취약점 보고서 및 원본 스마트 컨트랙트로부터 탐지된 퇴행에 대한 정보를 나타내는 제1 퇴행 보고서를 획득할 수 있다. 예를 들어, 제1 취약점 보고서는, 탐지된 취약점의 타입, 탐지된 취약점을 포함하고 있는 함수의 시그니처(signature), 취약점이 탐지된 라인의 숫자, 또는 라인에서 탐지된 취약점이 존재하는 표현식이나 명령문 중 적어도 하나를 포함할 수 있으나, 이에 한정되지 않는다. 또한, 제1 퇴행 보고서는 사전에 정의된 퇴행의 종류 중 원본 스마트 컨트랙트로부터 탐지된 퇴행의 종류 또는 탐지된 퇴행을 포함하는 함수의 시그니처를 포함할 수 있으나, 이에 한정되지 않는다.

- [0071] 프로세서(130)는 검증 결과에 따라 원본 스마트 컨트랙트에 포함된 적어도 하나의 취약점을 수정하기 위한 복수의 초기 후보 패치들을 생성하고, 복수의 초기 후보 패치들 각각을 원본 스마트 컨트랙트에 적용한 복수의 초기 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시킨다(S210).
- [0072] 구체적으로, 프로세서(130)는 제1 취약점 보고서 및 제1 퇴행 보고서를 이용하여 원본 스마트 컨트랙트에 존재하는 적어도 하나의 취약점을 수정하기 위해 사용되는 복수의 초기 후보 패치들을 생성할 수 있다.
- [0073] 이러한 초기 후보 패치를 생성하기 위해 프로세서(130)는 복수의 취약점들을 수정하기 위해 사전 설정된 복수의 수정 템플릿들을 이용할 수 있다. 여기서, 수정 템플릿은 패치의 기본 단위로서, 예를 들면 특정 명령문 앞 또는 뒤에 삽입 가능한 명령문 템플릿(예: Insert(1, s)) 또는 특정 표현식을 다른 표현식으로 교체하는 표현식 템플릿(예: Rep(1, e<sub>1</sub>, e<sub>2</sub>)) 등을 포함할 수 있다. 이러한 수정 템플릿은 취약점의 종류에 따라 달라지거나 확장될 수 있다.
- [0074] 프로세서(130)는 제1 취약점 보고서 및 제1 퇴행 보고서를 참조하고, 사전 설정된 복수의 수정 템플릿들을 활용하여 상기 원본 스마트 컨트랙트에 존재하는 취약점을 수정하기 위해 사용될 수 있는 수정 템플릿 시퀀스(즉, 패치 컴포넌트)를 결정할 수 있다. 예를 들어, 프로세서(130)는 제1 취약점 보고서에 기록된 적어도 하나의 취약점의 타입 및 위치를 참조하여 해당 취약점을 수정하기 위해 사용될 수 있는 수정 템플릿 시퀀스를 결정할 수 있다.
- [0075] 프로세서(130)는 이와 같이 결정된 수정 템플릿 시퀀스를 이용하여 패치 컴포넌트 집합을 결정하고, 패치 컴포넌트 집합을 이용하여 복수의 초기 후보 패치들을 생성할 수 있다. 예를 들어, 재진입 취약점(reentrancy vulnerability)을 수정하기 위해 프로세서(130)는 복수 개의 비-재진입 수정자(non-reentrant modifier)를 재진입 취약점에 대한 수정 템플릿 시퀀스로서 결정할 수 있다. 다시 말해서, 프로세서(130)는 여러 개의 수정 템플릿을 이용하여 하나의 패치 컴포넌트를 구성함으로써, 수정 루프 동작에 대한 효율성 및 속도를 향상시킬 수 있다. 다양한 실시예에서 프로세서(130)는 패치 컴포넌트 집합 중 단일 패치 컴포넌트를 포함하는 후보 패치를 생성하고, 복수의 패치 컴포넌트들을 포함하는 후보 패치를 생성할 수 있으나, 이에 한정되지 않는다. 프로세서(130)는 이와 같이 복수의 초기 후보 패치들 각각을 원본 스마트 컨트랙트에 적용하여 복수의 초기 후보 스마트 컨트랙트들을 생성하고, 워크셋에 복수의 초기 후보 패치들 및 복수의 초기 후보 스마트 컨트랙트들을 포함시킬 수 있다. 여기서, 워크셋은 검증하고자 하는 후보 패치 및 후보 스마트 컨트랙트에 대한 집합일 수 있다.
- [0076] 다음으로, 프로세서(130)는 사전 종료 조건을 만족할 때까지 워크셋에 포함된 복수의 후보 스마트 컨트랙트들을 검증하고, 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 워크셋에 포함시키는 과정을 반복한다(S220).
- [0077] 구체적으로, 프로세서(130)는 검증기를 이용하여 워크셋에 포함된 복수의 후보 스마트 컨트랙트들 각각에 대한 취약점 탐지 및 퇴행 탐지를 수행하고, 복수의 후보 스마트 컨트랙트들 각각으로부터 탐지된 취약점에 대한 정보를 나타내는 제2 취약점 보고서 및 복수의 후보 스마트 컨트랙트들 각각으로부터 탐지된 퇴행에 대한 정보를 나타내는 제2 퇴행 보고서를 생성할 수 있다. 예를 들어, 제2 취약점 보고서는, 탐지된 취약점의 타입, 탐지된 취약점을 포함하고 있는 함수의 시그니처, 취약점이 탐지된 라인의 숫자, 또는 라인에서 탐지된 취약점이 존재하는 표현식이나 명령문 중 적어도 하나를 포함할 수 있으나, 이에 한정되지 않는다. 또한, 제2 퇴행 보고서는 사전에 정의된 퇴행의 종류 중 복수의 후보 스마트 컨트랙트들 각각으로부터 탐지된 퇴행의 종류 또는 탐지된 퇴행을 포함하는 함수의 시그니처를 포함할 수 있으나, 이에 한정되지 않는다.
- [0078] 프로세서(130)는 검증이 완료된 적어도 하나의 후보 스마트 컨트랙트들을 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 스마트 컨트랙트들로서 출력한다(S230). 여기서, 수정된 스마트 컨트랙트는 원본 스마트 컨트랙트에 패치가 적용되어 원본 스마트 컨트랙트의 취약점이 적어도 일부 수정된 스마트 컨트랙트를 의미할 수 있다.
- [0079] 이하에서는 복수의 후보 스마트 컨트랙트들에 대한 검증 동작에 대하여 하기의 도 3을 참조하여 상세하게 설명하도록 한다.
- [0080] 도 3은 본 개시의 실시예에 따른 정답 스마트 컨트랙트(즉, 비퇴행적이고 취약점이 존재하지 않는 스마트 컨트랙트) 혹은 비퇴행적이고 원본 스마트 컨트랙트의 취약점이 일부 수정되어 적어도 원본 스마트 컨트랙트보다 더 안전한 스마트 컨트랙트를 결정하는 방법의 일례를 설명하기 위한 흐름도이다. 다시 말해서, 도 3은 도 2의 S220 및 S230을 구체화하는 흐름도이다.
- [0081] 도 3을 참조하면, 프로세서(130)는 워크셋에서 최소 비용 점수를 갖는 후보 패치 및 후보 스마트 컨트랙트를 선

택한다(S300). 후보 패치에 대한 비용 점수를 산출하기 위해 프로세서(130)는 ' $\text{cost}(p) = |p| + \text{penalty}(p)$ '와 같은 제1 비용 계산식을 이용하여 비용 점수( $\text{cost}(p)$ )를 산출할 수 있으나, 이에 한정되지 않는다. 여기서,  $p$ 는 후보 패치를 의미하고,  $|p|$ 는 후보 패치의 크기를 의미하며,  $\text{penalty}(p)$ 는 정답 패치일 가능성이 낮은 후보 패치에 대하여 패널티 점수를 부과하는 함수를 의미할 수 있다.

[0082] 프로세서(130)는 워크셋에서 선택된 후보 패치 및 후보 스마트 컨트랙트를 삭제한다(S310). 여기서, 삭제된 후보 패치 및 후보 스마트 컨트랙트는 S300에서 선택된 최소 비용 점수를 갖는 후보 패치 및 후보 스마트 컨트랙트를 의미할 수 있다.

[0083] 프로세서(130)는 검증기를 이용하여, 선택된 후보 스마트 컨트랙트를 검증하고(S320), 검증 결과에 기반하여 수정 진행 상태를 추적하기 위한 변수들을 갱신한다(S330). 여기서, 수정 진행 상태에 대한 변수들은 수정된 후보 스마트 컨트랙트들 중에서 현재까지 패치 안전성과 패치 크기 측면에서 가장 우수한(즉, 비퇴행적이고, 탐지된 취약점의 수가 현재까지 최소이고, 비퇴행적이고, 탐지된 취약점의 수가 현재까지 최소이고, 적용된 후보 패치의 크기가 현재까지 최소인 조건들을 만족하는) 스마트 컨트랙트들의 집합, 해당 후보 스마트 컨트랙트들(즉, 현재까지 가장 우수한 후보 스마트 컨트랙트들)에서 탐지된 취약점의 수, 해당 후보 스마트 컨트랙트들(즉, 현재까지 가장 우수한 후보 스마트 컨트랙트들)에 적용된 패치의 크기를 포함할 수 있다.

[0084] 구체적으로, 프로세서(130)는 검증 완료된 후보 스마트 컨트랙트에 대해 검증 결과에 따라, 해당 후보 스마트 컨트랙트에서 탐지된 취약점의 수가 가장 우수한 후보 스마트 컨트랙트에서 탐지된 취약점의 수보다 작거나 같은지, 또는 해당 후보 스마트 컨트랙트의 패치 크기가 가장 우수한 후보 스마트 컨트랙트의 패치 크기보다 작거나 같은지를 결정할 수 있다. 해당 조건을 만족하는 경우 프로세서(130)는 검증 완료된 후보 스마트 컨트랙트를 가장 우수한 스마트 컨트랙트 집합에 포함시키고, 가장 우수한 후보 스마트 컨트랙트에서 탐지된 알람의 수를 검증 완료된 후보 스마트 컨트랙트에서 탐지된 알람의 수로 갱신하거나, 또는 가장 우수한 후보 스마트 컨트랙트에 적용된 패치의 크기를 검증 완료된 후보 스마트 컨트랙트에 적용된 패치의 크기로 갱신할 수 있다. 이에 대한 구체적인 설명은 도 11을 참조하여 후술하도록 한다.

[0085] 프로세서(130)는 복수의 새로운 후보 패치들 및 복수의 새로운 후보 패치들 각각이 적용된 복수의 새로운 후보 스마트 컨트랙트들을 생성하여 복수의 새로운 후보 패치들 및 복수의 새로운 후보 스마트 컨트랙트들을 워크셋에 포함시킨다(S340).

[0086] 프로세서(130)는 사전 종료 조건이 만족되는지 결정하여(S350) 사전 종료 조건이 만족되면 원본 스마트 컨트랙트에 대한 적어도 하나의 수정된 후보 스마트 컨트랙트들을 출력한다(S360). 구체적으로, 사전 종료 조건이 만족되면 프로세서(130)는 수정 루프 동작을 종료하고, S330에서의 현재까지 패치 안전성과 패치 크기 측면에서 가장 우수한 스마트 컨트랙트들의 집합을 출력할 수 있다. 여기서, 사전 종료 조건은 상술한 바와 같이 사전 설정된 타임아웃에 도달하는 경우, 워크셋에 저장되었던 모든 후보 스마트 컨트랙트에 대한 검증이 완료되는 경우, 또는 정답 스마트 컨트랙트를 발견하는 경우를 포함할 수 있다.

[0087] 종료 조건이 만족되지 않으면 프로세서(130)는 사전 종료 조건이 만족될 때까지 S300 내지 S350 까지의 수정 루프 동작을 반복적으로 수행할 수 있다.

[0088] 본 개시에서 검증기는 취약점(또는 버그(bug))의 부재를 증명할 수 있는 정형 검증(formal verification) 기술에 기반할 수 있으나, 이에 한정되지 않는다. 검증기가 정형 검증 기술에 기반한 것일 경우, 원본 스마트 컨트랙트에서 버그가 발견되었으나 후보 스마트 컨트랙트에서 해당 버그가 발견되지 않았다면, 해당 버그가 수정되었음이 보장될 수 있다.

[0089] 특히, 이러한 검증기는 후보 스마트 컨트랙트에 대해 취약점으로부터의 안전성(즉, 취약점의 부재)을 검증하는 안전성 검증(safety verification)을 수행하고, 후보 스마트 컨트랙트에 적용된 후보 패치가 올바른지를 검증하는 기능성 퇴행 탐지(functionality regression detection)를 수행할 수 있다. 여기서, 안전성 검증 동작은 후보 패치가 적용된 후보 스마트 컨트랙트에 대한 취약점 탐지를 수행하고, 이에 대한 취약점 보고서를 생성하는 동작일 수 있다. 기능성 퇴행 탐지는 사전에 정의된 퇴행 조건식을 이용하는 검증 동작일 수 있다. 검증기의 기능성 퇴행 탐지 동작에 대해서 예를 들어 살펴보면 다음과 같다.

[0090] 원본 스마트 컨트랙트에 ' $\text{require}(x \leq a); y := x - a$ '와 같은 명령문들로 구성된 함수가 존재한다고 가정한다. ' $x - a$ '에서의 언더 플로우 버그를 수정하기 위해 ' $\text{require}(x \geq a)$ '와 같은 후보 패치 명령문이 삽입되어 ' $\text{require}(x \leq a); \text{require}(x \geq a); y := x - a$ '로 구성되면 삽입된 후보 패치 명령문 이후 ' $x = a$ '라는 조건이 항상 성립되므로, 마지막 명령문에서  $y$ 에 항상 '0'이 할당되어버리는 기능성 퇴행이 후보 스마트 컨트랙트에 존재할 수 있다.

검증기는 전처리 단계에서  $\text{assert}(y==0)$ 과 같은 assertion 명령문을 마지막 명령문 바로 뒤에 삽입하여 ' $y==0$ '과 같은 퇴행 조건식(regression condition)을 테스트할 수 있다. 여기서, ' $y==0$ '은 'y가 항상 0 값을 할당받는지' 확인하기 위한 퇴행 조건식일 수 있다. 이어서, 검증기는 ' $x \leq a \wedge x \geq a \wedge y = x - a \rightarrow y = 0$ '과 같은 검증 조건식(verification condition)을 생성하고, 이에 대한 타당성(validity, 항상 참인 성질)을 확인할 수 있다. 검증 조건식이 타당하면 검증기는 해당 검증 결과를 포함하는 퇴행 보고서를 생성할 수 있다. 이와 같이 비정상적 프로그램 속성이 원본 스마트 컨트랙트에서 탐지되지 않고 후보 스마트 컨트랙트에서만 탐지될 경우, 후보 스마트 컨트랙트가 퇴행적인 것으로 판단함으로써, 프로세서(130)는 후보 스마트 컨트랙트에 적용된 후보 패치를 검증 대상에서 제외시킬 수 있다.

[0091] 다양한 실시예에서 퇴행 조건식은 상술한 바와 같이 '0값 할당문'을 탐지하기 위한 assertion 이외에 데드코드 패치 탐지를 위한  $\text{assert}(\text{false})$ 와 같은 assertion 명령문이 이용될 수 있다. 또 다른 예로, '영향력이 없는 할당문'을 탐지하기 위한 퇴행 조건식이 디자인될 수도 있다. 이에 대해서 예시적으로 살펴보면, 원본 스마트 컨트랙트에 ' $\text{require}(x+a \leq x); x := x+a$ '와 같은 명령문들로 구성된 함수가 존재한다고 가정한다. ' $x+a$ '에서의 오버플로우 버그를 수정하기 위해 ' $\text{require}(x+a > x)$ '와 같은 후보 패치 명령문이 삽입되어 ' $\text{require}(x+a \leq x); \text{require}(x+a > x); x := x+a$ '로 구성되면 a가 항상 0이어야 하므로, 마지막 명령문에서 x 값이 변하지 않는 퇴행이 발생할 수 있다. 이러한 퇴행은 마지막 명령문 ' $x := x+a$ '를 ' $\text{pre} := x; x := x+a; \text{assert}(\text{pre} == x)$ '와 같이 변형하는 전처리를 수행하여 탐지될 수 있다. 다양한 실시예에서 검증 효율을 위해 퇴행 조건식을 포함하는 assertion 명령문은 스마트 컨트랙트 명령문들 중 일부에 삽입될 수 있다. 예를 들어, '0값 할당문'을 탐지하기 위한 assertion 명령문은 덧셈/뺄셈 연산이 수행되는 명령문들 뒤에 삽입될 수 있다.

[0092] 원본 스마트 컨트랙트에 대한 수정을 가속화하기 위한 방법으로, 프로세서(130)는 복수의 후보 스마트 컨트랙트들에 대한 검증 결과에 기반하여 학습된 제1 통계 모델 또는 원본 스마트 컨트랙트를 과거에 수정한 과거 수정 이력들을 나타내는 지식 데이터에 기반하여 학습된 제2 통계 모델을 이용할 수 있다.

[0093] 구체적으로, 프로세서(130)는 복수의 후보 패치들, 및 복수의 후보 스마트 컨트랙트들에 대한 검증 결과에 기반하여 제1 통계 모델을 학습시키고, 학습된 제1 통계 모델을 이용하여 복수의 후보 패치들 중 정답 패치일 가능성이 높은 적어도 하나의 후보 패치를 결정한 후, 결정된 후보 패치가 적용된 후보 스마트 컨트랙트에 대해 우선적으로 검증을 수행함으로써, 원본 스마트 컨트랙트에 대한 취약점 수정을 가속화시킬 수 있다. 하기에서는 도 4 및 도 5를 참조하여 제1 통계 모델에 대한 학습을 상세하게 설명하도록 한다.

[0094] 도 4는 본 개시의 실시예에 따라 제1 통계 모델을 학습시키기 위한 제1 학습 데이터를 생성하는 방법을 설명하기 위한 예시도이다.

[0095] 도 4를 참조하면, 프로세서(130)는 검증기(410)를 이용하여, S300에서 선택된 후보 스마트 컨트랙트(400)를 검증할 수 있다. 프로세서(130)는 검증 결과에 대한 보고서(즉, 검증 결과를 나타내는 취약점 보고서 및 퇴행 보고서)(420)를 획득하고, 획득된 검증 결과 보고서(420)를 이용하여 제1 통계 모델을 학습하기 위한 제1 학습 데이터(430)를 생성할 수 있다. 구체적으로, 프로세서(130)는 후보 스마트 컨트랙트(400)에 적용된 각 후보 패치에 대한 특징 벡터를 생성하고, 검증 결과 보고서(420)를 이용하여 각 후보 패치가 정답 패치에 가까운 정도를 수치화한 안전성 점수(safety score)를 결정할 수 있다. 프로세서(130)는 이와 같이 생성된 특징 벡터 및 안전성 점수를 포함하는 제1 학습 데이터(430)를 적어도 하나 생성할 수 있다.

[0096] 도 5는 본 개시의 실시예에 따라 제1 통계 모델을 학습시키기 위한 방법을 설명하기 위한 예시도이다.

[0097] 도 5를 참조하면, 프로세서(130)는 도 4에서 설명한 제1 학습 데이터를 포함하는 제1 학습 데이터 세트(500)를 이용하여 제1 통계 모델(510)을 학습시킬 수 있다. 여기서, 제1 학습 데이터 세트(500)는 적어도 하나의 제1 학습 데이터를 포함하고, 각 제1 학습 데이터는 후보 패치에 대한 특징 벡터 및 후보 패치에 대한 안전성 점수를 포함할 수 있다. 예를 들어, 프로세서(130)는 패치 컴포넌트 집합으로 매개 변수화된(parameterized) 특징 인코딩 함수를 이용하여 후보 패치를 특징 벡터(500)로 변환할 수 있다. 프로세서(130)는 지도 학습 알고리즘을 이용하여 제1 통계 모델(510)이 후보 패치에 대한 예상 안전성 점수를 산출하도록 학습할 수 있는데, 이러한 지도 학습 알고리즘은 선형 회귀 모델을 학습하기 위한 알고리즘일 수 있으나, 이에 한정되지 않는다.

[0098] 정답 패치일 가능성이 높은 후보 패치가 적용된 후보 스마트 컨트랙트를 우선적으로 검증하기 위해 프로세서(130)는 제1 통계 모델을 이용하여 워크셋에 포함된 후보 패치들 중에서 정답 패치일 가능성이 높은 순서대로 적어도 하나의 후보 패치를 결정할 수 있다. 하기에서는 이러한 적어도 하나의 후보 패치를 결정하기 위해 하기의 도 6을 참조하여 설명하도록 한다.

- [0099] 도 6은 본 개시의 실시예에 따라 제1 통계 모델을 이용하여 적어도 하나의 정답 후보 패치를 결정하기 위한 방법의 일례를 설명하기 위한 흐름도이다.
- [0100] 도 6을 참조하면, 프로세서(130)는 제1 통계 모델을 이용하여 복수의 후보 패치들에 대한 예상 안전성 점수를 산출하고(S600), 산출된 예상 안전성 점수를 이용하여 복수의 후보 패치들에 대한 비용 점수를 결정한다(S610). 구체적으로, 프로세서(130)는 복수의 후보 패치들 각각에 대한 특징 벡터를 생성하고, 생성된 특징 벡터에 기반하여 후보 패치에 대한 예상 안전성 점수를 산출하도록 학습된 제1 통계 모델을 이용하여 각 후보 패치에 대한 예상 안전성 점수를 산출할 수 있다. 예를 들어, 제1 통계 모델이 패치 p1의  $\langle 1, 0, 0 \rangle$ 과 같은 특징 벡터에 대한 안전성 점수를  $x$ ( $x$ 는 후술할 <수학식 1>에 의해 계산된 실수)로 산출하도록 학습되고, 패치 p2의  $\langle 0, 1, 0 \rangle$ 와 같은 특징 벡터에 대한 안전성 점수를  $y$ ( $y$ 는 후술할 <수학식 1>에 의해 계산된 실수,  $y$ 는  $x$ 와 같거나 다를 수 있음)로 산출하도록 학습된 경우 프로세서(130)는 제1 통계 모델을 이용하여 후보 패치의  $\langle 1, 1, 0 \rangle$ 과 같은 특징 벡터에 대한 예상 안전성 점수를  $z$ ( $z$ 는  $x$ ,  $y$ 와 같거나 다를 수 있는 실수)로 산출할 수 있다.
- [0101] 프로세서(130)는 산출된 예상 안전성 점수를 이용하여 비용 점수(cost(p))를 결정하기 위해 'cost(p) = -(score(p) - penalty(p))'와 같은 제2 비용 계산식을 이용할 수 있으나, 이에 한정되지 않는다. 여기서, score(p)는 후보 패치 p에 대한 예상 안전성 점수를 의미할 수 있다. 여기서, 제2 비용 계산식은 통계 모델들(즉, 제1 통계 모델 및 제2 통계 모델)을 기반으로 하며, 상술한 제1 비용 계산식에 비해 개선된 버전의 비용 계산식일 수 있다. 도 3에서 서술한 제1 비용 계산식은 통계 모델을 이용하지 않은 기본적인 비용 계산식에 해당한다. 원본 스마트 컨트랙트에 대한 수정을 가속화하기 위해서 프로세서(130)는 제2 비용 계산식을 이용하여 비용 점수를 산출할 수 있다.
- [0102] 다음으로, 프로세서(130)는 최소 비용 점수를 갖는 후보 패치에서 높은 비용 점수를 갖는 후보 패치 순으로 적어도 하나의 후보 패치를 결정한다(S620). 각 후보 패치에 대한 비용 점수가 통계 모델들의 활용에 기반한 상기 제2 비용 계산식에 의해 산출되었을 경우, 적어도 하나의 후보 패치가 적용된 후보 스마트 컨트랙트가 정답 스마트 컨트랙트일 가능성이 높은 순서대로 검증됨으로써, 수정 루프 동작에 대한 가속화가 이루어질 수 있다.
- [0103] 도 2 및 도 3에서 상술한 바와 같이 원본 스마트 컨트랙트(즉, 제1 원본 스마트 컨트랙트)에 대한 수정이 완료되면(즉, 종료 조건이 만족되면) 프로세서(130)는 또 다른 원본 스마트 컨트랙트(즉, 제2 원본 스마트 컨트랙트)를 대상으로 상술한 후보 패치 생성 및 검증 등을 수행할 수 있다. 이러한 경우 프로세서(130)는 제1 원본 스마트 컨트랙트에 대한 검증 및 수정에서 사용되었던 복수의 후보 패치들 및 각 후보 패치에 대한 안전성 점수를, 과거 수정 이력에 해당하는 지식 데이터로 저장할 수 있다. 다양한 실시예에서 원본 스마트 컨트랙트에 적용된 각 후보 패치에 대한 검증이 완료되면 프로세서(130)는 검증이 완료된 각 후보 패치 및 각 후보 패치에 대한 안전성 점수를 지식 데이터로서 저장할 수 있다.
- [0104] 이처럼, 복수의 원본 스마트 컨트랙트들에 대한 검증 및 수정이 수행될 때마다 지식 데이터가 획득되며, 이러한 지식 데이터는 추후 제2 통계 모델을 학습하기 위한 제2 학습 데이터로 이용될 수 있다. 하기에서는 도 7 내지 도 9를 참조하여 제2 통계 모델에 대한 학습 및 이용에 대해서 상세하게 설명하도록 한다.
- [0105] 도 7은 본 개시의 실시예에 따라 제2 통계 모델을 학습시키기 위한 제2 학습 데이터를 생성하는 방법을 설명하기 위한 예시도이다.
- [0106] 도 7을 참조하면, 프로세서(130)는 검증기(410)를 이용하여, S300에서 선택된 후보 스마트 컨트랙트(400)를 검증할 수 있다.
- [0107] 프로세서(130)는 검증 결과에 대한 보고서(즉, 검증 결과를 나타내는 취약점 보고서 및 퇴행 보고서)(420)를 획득하고, 획득된 검증 결과 보고서(420)를 이용하여 제1 학습 데이터(430)를 생성할 수 있다. 여기서, 제1 학습 데이터(430)는 각 후보 패치에 대한 특징 벡터 및 안전성 점수를 포함할 수 있다.
- [0108] 후보 스마트 컨트랙트(400)에 대한 검증이 완료되면 프로세서(130)는 새로운 후보 패치 및 새로운 후보 스마트 컨트랙트에 대한 검증을 수행할 수 있다. 이러한 경우 후보 스마트 컨트랙트(400)에 적용된 후보 패치의 안전성 점수는 지식 데이터(700)를 생성하기 위해 이용될 수 있다. 원본 스마트 컨트랙트에 적용된 복수의 후보 패치들 각각에 대한 검증이 완료되면 원본 스마트 컨트랙트에 적용되었던 모든 후보 패치 및 모든 후보 패치에 대한 안전성 점수는 지식 데이터(700)를 생성하기 위해 이용될 수 있다.
- [0109] 구체적으로, 프로세서(130)는 각 후보 패치를 추상화된 형태의 패치로 변환하여 추상화된 후보 패치를 생성할 수 있다. 프로세서(130)는 추상화된 후보 패치 및 후보 패치에 대한 안전성 점수를 포함하는 지식 데이터(700)

를 생성할 수 있다.

- [0110] 이후 프로세서(130)는 검증기(410)를 이용하여 새로운 원본 스마트 컨트랙트(즉, 제2 원본 스마트 컨트랙트)를 검증하여 검증 결과 보고서를 획득하고, 획득된 검증 결과 보고서에 기반하여 제2 원본 스마트 컨트랙트에 존재하는 적어도 하나의 취약점을 수정하기 위한 복수의 후보 패치들을 생성할 수 있다.
- [0111] 제2 원본 스마트 컨트랙트에 대한 수정을 가속화하기 위해 프로세서(130)는 지식 데이터(700)를 변환하여 제2 학습 데이터(710)를 생성하고, 생성된 제2 학습 데이터(710)를 이용하여 제2 통계 모델을 학습시킬 수 있다.
- [0112] 도 8은 본 개시의 실시예에 따라 제2 통계 모델을 학습시키기 위한 방법을 설명하기 위한 예시도이다.
- [0113] 도 8을 참조하면, 프로세서(130)는 도 7에서 설명한 제2 학습 데이터를 포함하는 제2 학습 데이터 세트(800)를 이용하여 제2 통계 모델(810)을 학습시킬 수 있다. 여기서, 제2 학습 데이터 세트(800)는 적어도 하나의 제2 학습 데이터를 포함하고, 각 제2 학습 데이터는 추상화된 과거 후보 패치에 대한 특징 벡터 및 과거 후보 패치에 대한 안전성 점수를 포함할 수 있다. 예를 들어, 프로세서(130)는 매개 변수화된 특징 인코딩 함수를 이용하여 추상화된 과거 후보 패치를 특징 벡터로 변환할 수 있다. 프로세서(130)는 제1 통계 모델(510)에서 설명한 바와 같이 지도 학습 알고리즘을 이용하여 제2 통계 모델(810)이 후보 패치에 대한 예상 안전성 점수를 산출하도록 학습할 수 있는데, 이러한 지도 학습 알고리즘은 선형 회귀 모델을 학습하기 위한 알고리즘일 수 있으나, 이에 한정되지 않는다.
- [0114] 정답 패치일 가능성이 높은 후보 패치가 적용된 후보 스마트 컨트랙트를 우선적으로 검증하기 위해 프로세서(130)는 제2 통계 모델을 이용하여 워크셋에 포함된 후보 패치들 중에서 정답 패치일 가능성이 높은 순서대로 적어도 하나의 후보 패치를 결정할 수 있다. 하기에서는 이러한 적어도 하나의 후보 패치를 결정하기 위해 하기의 도 9를 참조하여 설명하도록 한다.
- [0115] 도 9는 본 개시의 실시예에 따라 제2 통계 모델을 이용하여 적어도 하나의 정답 후보 패치를 결정하기 위한 방법의 일례를 설명하기 위한 흐름도이다.
- [0116] 도 9를 참조하면, 프로세서(130)는 제2 통계 모델을 이용하여 복수의 후보 패치들에 대한 예상 안전성 점수를 산출하고(S900), 산출된 예상 안전성 점수를 이용하여 복수의 후보 패치들에 대한 비용 점수를 산출한다(S910). 구체적으로, 프로세서(130)는 복수의 후보 패치들 각각에 대한 특징 벡터를 생성하고, 생성된 특징 벡터에 기반하여 후보 패치에 대한 예상 안전성 점수를 산출하도록 학습된 제2 통계 모델을 이용하여 각 후보 패치에 대한 예상 안전성 점수를 산출할 수 있다.
- [0117] 프로세서(130)는 산출된 예상 안전성 점수를 이용하여 비용 점수(cost(p))를 결정하기 위해 상술한 ' $\text{cost}(p) = -(\text{score}(p) - \text{penalty}(p))$ '와 같은 제2 비용 계산식을 이용할 수 있으나, 이에 한정되지 않는다.
- [0118] 다음으로, 프로세서(130)는 최소 비용 점수를 갖는 후보 패치에서 높은 비용 점수를 갖는 후보 패치 순으로 적어도 하나의 후보 패치를 결정한다(S920). 이와 같이 적어도 하나의 후보 패치가 적용된 후보 스마트 컨트랙트가 정답 스마트 컨트랙트일 가능성이 높은 순서대로 검증됨으로써, 수정 루프 동작에 대한 가속화가 이루어질 수 있다.
- [0119] 하기에서는 스마트 컨트랙트 취약점 수정 장치(100)의 동작을 의사코드로 표현한 도 10 내지 도 12를 참조하여 스마트 컨트랙트 취약점 수정 동작에 대해서 보다 상세하게 설명하도록 한다. 제시된 실시예에서 스마트 컨트랙트 취약점 수정 장치(100)의 프로세서(130)는 도 10 내지 도 12에서 표현된 의사코드가 구현된 프로그램 코드들을 판독하여 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정을 위한 데이터 처리를 수행할 수 있다.
- [0120] 도 10은 본 개시의 실시예에 따른 스마트 컨트랙트 취약점 수정 동작을 의사코드로 표현한 일례를 나타내는 예시도이다. 제시된 실시예에서는 복수의 스마트 컨트랙트들에 대한 검증 및 수정 루프 동작이 이루어진 경우를 가정하여 설명하도록 한다. 특히, 도 10의 라인 1 내지 라인 15는 스마트 컨트랙트에 대한 수정 알고리즘 동작으로 정의될 수 있다.
- [0121] 도 10을 참조하면, 라인 1에서 프로세서(130)는 검증기(Verify)를 호출하여 원본 스마트 컨트랙트( $s_0$ )를 검증한 후 검증 결과에 대한 취약점 보고서( $VR_0$ ) 및 퇴행 보고서( $RR_0$ )를 획득할 수 있다.
- [0122] 라인 2에서 프로세서(130)는 통계 모델들을 학습하기 위해 사용되는 변수들인 학습 데이터 세트( $D_{on}$ ) 및 지식 데

이터 세트( $K_{on}$ ) 각각을 초기화( $\emptyset$ )할 수 있다.

- [0123] 라인 3에서 프로세서(130)는 현재의 수정 진행 상태를 추적하기 위해 사용되는 변수들인, 현재까지 패치 안전성과 패치 크기 측면에서 가장 우수한(즉, 비퇴행적이고, 탐지된 취약점의 수가 현재까지 최소이고, 적용된 후보 패치의 크기가 현재까지 최소인 조건들을 만족하는) 후보 스마트 컨트랙트들에 대한 집합(S), 해당 후보 스마트 컨트랙트들에서 탐지된 취약점의 수(n) 및 해당 후보 스마트 컨트랙트들에 적용된 패치의 크기(ps) 각각을 초기화( $\emptyset, |VR_0|, 0$ )할 수 있다. 프로세서(130)는 현재 시점에서 가장 우수한 수정된 스마트 컨트랙트를 결정하기 위해 이러한 변수들을 이용할 수 있다. 이러한 변수들은 후보 스마트 컨트랙트에 대한 검증 및 수정이 진행될 때마다 갱신될 수 있다.
- [0124] 라인 4에서 프로세서(130)는 원본 스마트 컨트랙트( $s_0$ ) 및 원본 스마트 컨트랙트( $s_0$ )에 대한 취약점 보고서( $VR_0$ )를 이용하여 패치 컴포넌트 집합(C)을 생성한다.
- [0125] 패치 컴포넌트 집합을 생성하기 위해서 프로세서(130)는 사전 설정된 복수의 수정 템플릿들을 이용할 수 있다. 수정 템플릿( $a \in A$ (수정 템플릿 집합))은 패치의 기본적인 단위이며, 패치 컴포넌트( $c \in C$ (패치 컴포넌트 집합))는 수정 템플릿들의 시퀀스로 이루어질 수 있다. 즉,  $c = a_1, \dots, a_n \in A^*$ 이고,  $C \subseteq A^*$ 일 수 있다. 예를 들어, 수정 템플릿은  $Insert(l, s)$ 을 포함할 수 있고,  $Insert(l, s)$ 은 라인(l)의 명령문(statement)의 바로 앞에 또 다른 명령문(s)를 삽입하는 템플릿을 의미할 수 있다. 또한, 수정 템플릿은  $Rep(l, e_1, e_2)$ 를 포함할 수 있는데,  $Rep(l, e_1, e_2)$ 는 라인(l)에서 표현식(expression)  $e_1$ 을  $e_2$ 로 교체하는 템플릿을 의미할 수 있다. 이러한 수정 템플릿의 디자인은 스마트 컨트랙트 취약점 수정 장치(100)의 수정 동작에서 지원하고자 하는 취약점 종류에 따라 달라지거나 확장될 수 있다.
- [0126] 패치 컴포넌트 집합(C)은  $Extract(s_0, VR_0)$ 의 출력으로 획득될 수 있다. 여기서, 프로세서(130)는  $Extract$  함수를 이용하여 취약점 보고서( $VR_0$ )에 기록된 취약점의 타입 및 위치를 참조하여 사전 설정된 수정 템플릿들로부터 원본 스마트 컨트랙트( $s_0$ )를 수정하기 위한 패치 컴포넌트들을 결정할 수 있다. 예를 들어, 라인(1)의 표현식  $a+b$ 에서 정수 오버플로우 버그가 발생함을 나타내는 ' $(l_0, -, l, a+b) \in VR_0$ '라는 알람이 탐지되었다고 가정한다. 이러한 경우 프로세서(130)는 사전 설정된 복수의 수정 템플릿들을 이용하여 ' $Insert(l, require(a+b >= a))$ '와 같은 패치 컴포넌트를 생성하고, 생성된 패치 컴포넌트(c)를 패치 컴포넌트 집합(C)에 포함시킬 수 있다.
- [0127] 라인 5에서 프로세서(130)는 패치 컴포넌트 집합(C)을 이용하여 초기 후보 패치를 생성하고, 생성된 초기 후보 패치를 원본 스마트 컨트랙트( $s_0$ )에 적용하여 후보 스마트 컨트랙트(s)를 생성한 후 워크셋(W)을 초기화할 수 있다. 여기서, 워크셋은 검증의 대상이자 수정을 위해 사용되는 후보 패치(p) 및 후보 스마트 컨트랙트(s)를 포함할 수 있다.
- [0128] 구체적으로, 프로세서(130)는  $Generate$  함수를 이용하여 패치 컴포넌트의 시퀀스로 이루어지는 후보 패치(p)를 생성하고, 생성된 후보 패치(p)를 원본 스마트 컨트랙트( $s_0$ )에 적용하여 후보 스마트 컨트랙트(s)를 생성할 수 있다. 라인 6 및 라인 12는 통계 모델의 학습에 관련되므로, 하기의 도 12를 참조하여 상세히 설명하도록 한다.
- [0129] 다음으로, 라인 7부터 라인 14까지는 상술한 수정 루프 동작을 의미할 수 있다. 다시 말해서, 라인 7부터 라인 14까지는 도 3의 S300 내지 S350을 구체화한 의사코드의 일레이다.
- [0130] 라인 8에서 프로세서(130)는 각 후보 패치에 대한 비용 점수( $cost(p)$ )를 산출하고, 산출된 비용 점수 중 최소 비용 점수( $\arg \min_{(s,p) \in W} cost(p)$ )를 갖는 후보 패치(p) 및 후보 스마트 컨트랙트(s)를 선택할 수 있다. 여기서, 비용 점수( $cost(p)$ )는 상술한 제1 비용 계산식을 이용하여 산출될 수 있다.
- [0131] 라인 9에서 프로세서(130)는 선택된 후보 패치(p) 및 후보 스마트 컨트랙트(s)를 워크셋(W)에서 삭제할 수 있다.
- [0132] 라인 10에서 프로세서(130)는 검증기(Verify)를 호출하여, 선택된 후보 스마트 컨트랙트(s)를 검증한 후 검증 결과에 대한 취약점 보고서(VR) 및 퇴행 보고서(RR)를 획득할 수 있다.

- [0133] 라인 11에서 프로세서(130)는 라인 3에서 설명한 수정 진행 상태를 결정하기 위한 변수들( $S, n, ps$ )을 갱신할 수 있다. 이에 대해서, 도 11을 참조하여 상세하게 설명하도록 한다.
- [0134] 도 11은 본 개시의 실시예에 따른 수정 진행 상태를 결정하기 위한 변수들을 갱신하는 동작을 의사코드로 표현한 일례를 나타내는 예시도이다.
- [0135] 도 11을 참조하면, 라인 1은 현재 후보 패치 및 현재 후보 스마트 컨트랙트( $p, s$ )에 대한 검증 결과( $VR, RR$ )에 기반하여 수정 진행 상태를 결정하기 위한 변수들( $S, n, ps$ )을 갱신하는 절차를 나타낸다. 여기서, 현재 후보 패치 및 현재 후보 스마트 컨트랙트는 라인 10에서 검증기를 통해 검증이 이루어진 후보 스마트 컨트랙트 및 해당 후보 스마트 컨트랙트에 적용된 후보 패치를 의미할 수 있다.
- [0136] 라인 2에서, 도 10의 라인 10에서 획득된 퇴행 보고서( $RR$ )와 도 10의 라인 1에서 획득된 퇴행 보고서( $RR_0$ )가 일치하고( $RR=RR_0$ )(즉, 비퇴행적이고), 도 10의 라인 10에서 탐지된 알람의 수( $|VR|$ )가, 안전성과 패치 크기 측면에서 가장 우수한(즉, 비퇴행적이고, 현재까지 탐지된 취약점의 수 중 최소 값을 가지고, 현재까지 적용된 패치의 크기 중 최소 크기를 가지는) 후보 스마트 컨트랙트에서 탐지된 취약점의 수( $n$ ) 미만이면( $|VR|<n$ ) 라인 3에서 프로세서(130)는 현재 후보 스마트 컨트랙트를 새로운 가장 우수한 스마트 컨트랙트로 결정하고, 수정 진행 상태를 결정하기 위한 변수들( $S, n, ps$ )을 갱신할 수 있다. 구체적으로, 현재 시점에서 가장 우수한 후보 스마트 컨트랙트에 대한 집합( $S$ )은 현재 후보 스마트 컨트랙트( $s$ )(즉, 라인 2에서 새롭게 결정된, 가장 우수한 후보 스마트 컨트랙트)만 포함되도록 갱신되고, 안전성과 패치 크기 측면에서 가장 우수한 후보 스마트 컨트랙트에서 탐지된 취약점의 수( $n$ )는 도 10의 라인 10에서 탐지된 현재 후보 스마트 컨트랙트( $s$ )에 대한 취약점의 수( $|VR|$ )로 갱신되며, 안전성과 패치 크기 측면에서 가장 우수한 후보 스마트 컨트랙트에 적용된 패치의 크기( $ps$ )는 현재 후보 스마트 컨트랙트에 적용된 후보 패치의 크기( $|p|$ )로 갱신될 수 있다.
- [0137] 라인 4에서 도 10의 라인 10에서 획득된 퇴행 보고서( $RR$ )와 도 10의 라인 1에서 획득된 퇴행 보고서( $RR_0$ )가 일치하고( $RR=RR_0$ ), 도 10의 라인 10에서 탐지된 알람의 수( $|VR|$ )가 안전성과 패치 크기 측면에서 가장 우수한 후보 스마트 컨트랙트에서 탐지된 알람의 수( $n$ )와 일치하며( $|VR|=n$ ), 현재 후보 패치의 크기( $|p|$ )가 안전성과 패치 크기 측면에서 가장 우수한 후보 스마트 컨트랙트에 적용된 패치의 크기( $ps$ )와 일치하면( $|p|=ps$ ) 라인 5에서 프로세서(130)는 현재 후보 스마트 컨트랙트가 새로운, 가장 우수한 스마트 컨트랙트에 해당한다고 결정하고, 수정 진행 상태를 결정하기 위한 변수들 중 가장 우수한 후보 스마트 컨트랙트들의 집합( $S$ )을 갱신할 수 있다. 예를 들어, 가장 우수한 후보 스마트 컨트랙트에 대한 집합( $S$ )에는 현재 후보 스마트 컨트랙트( $s$ )(즉, 라인 4에서 새롭게 결정된, 가장 우수한 후보 스마트 컨트랙트)가 포함될 수 있다.
- [0138] 라인 6에서 도 10의 라인 10에서 획득된 퇴행 보고서( $RR$ )와 도 10의 라인 1에서 획득된 퇴행 보고서( $RR_0$ )가 일치하고( $RR=RR_0$ ), 도 10의 라인 10에서 탐지된 알람의 수( $|VR|$ )가 안전성과 패치 크기 측면에서 가장 우수한 후보 스마트 컨트랙트에서 탐지된 알람의 수( $n$ )와 일치하며( $|VR|=n$ ), 현재 후보 패치의 크기( $|p|$ )가 안전성과 패치 크기 측면에서 가장 우수한 후보 스마트 컨트랙트에 적용된 패치의 크기( $ps$ ) 미만이면( $|p|<ps$ ) 라인 7에서 프로세서(130)는 현재 후보 스마트 컨트랙트( $s$ )가 더 간단한 후보 패치가 적용된 새로운 가장 우수한 후보 스마트 컨트랙트에 해당한다고 결정하고, 수정 진행 상태를 결정하기 위한 변수들 중, 가장 우수한 후보 스마트 컨트랙트에 대한 집합( $S$ ) 및 가장 우수한 후보 스마트 컨트랙트에 적용된 패치의 크기( $ps$ )를 갱신할 수 있다. 예를 들어, 가장 우수한 후보 스마트 컨트랙트에 대한 집합( $S$ )은 현재 후보 스마트 컨트랙트( $s$ )만 포함되도록 갱신되고, 안전성과 패치 크기 측면에서 가장 우수한 후보 스마트 컨트랙트에 적용된 패치의 크기( $ps$ )는 현재 후보 스마트 컨트랙트에 적용된 후보 패치의 크기로 갱신될 수 있다.
- [0139] 다시 도 10을 참조하면, 라인 13에서 프로세서(130)는 라인 4에서 산출된 패치 컴포넌트 집합( $C$ )과 원본 컨트랙트( $s_0$ )를 이용하여 새로운 후보 패치 및 새로운 후보 스마트 컨트랙트를 생성하고, 생성된 새로운 후보 패치 및 새로운 후보 스마트 컨트랙트를 위크셋( $W$ )에 포함시킬 수 있다. 여기서, 새로운 후보 패치 및 새로운 후보 스마트 컨트랙트는 하나 이상을 의미할 수 있다.
- [0140] 새로운 후보 패치( $p \cdot c$ ) 및 새로운 후보 스마트 컨트랙트( $s$ )는  $Generate(C, s_0, p)$ 의 출력으로 획득될 수 있다 ( $\{(s, p \cdot c) \mid c \in C, \neg \text{unuseful}(p \cdot c)\}$ ). 구체적으로, 프로세서(130)는  $Generate$  함수를 이용하여 현재 후보 패치( $p$ )에 패치 컴포넌트( $c$ )를 이어 붙여서 새로운 후보 패치( $p \cdot c$ )를 획득하고, 원본 스마트 컨트랙트( $s_0$ )에 새로

운 후보 패치( $P \cdot C$ )를 적용하여 새로운 후보 스마트 컨트랙트(s)를 획득할 수 있다. 나아가, 프로세서(130)는 생성된 새로운 후보 패치들 중 유용하지 않을 가능성이 높은 후보 패치들을 제외시키기 위해 unuseful과 같은 술어(predicate)를 이용할 수 있다. 예를 들어,  $l_1=l_2$ ,  $s_1=s_2$ 이고, 후보 패치  $p = \text{Insert}(l_1, s_1) \cdot \text{Insert}(l_2, s_2)$ 가 존재하는 경우 unuseful(p)는 참(true)을 반환함으로써, 프로세서(130)는 후보 패치 p가 유용하지 않을 가능성이 높은 후보 패치로 결정하여 제외시킬 수 있다.

[0141] 라인 14에서 프로세서(130)는 워크셋(W)이, 공집합이 될 때까지 또는 사전 설정된 타임아웃에 도달할 때까지 등의 종료 조건을 만족할 때까지 라인 7에서 라인 14까지의 동작을 반복 수행할 수 있다. 다양한 실시예에서 프로세서(130)는 정답 스마트 컨트랙트가 발견될 때까지 또는 수정 루프 동작을 수행하는 횟수가 사전 설정된 임계 횟수에 도달할 때까지 등의 종료 조건을 만족할 때까지 라인 7에서 라인 14까지의 동작을 반복 수행할 수도 있다.

[0142] 라인 14에서 종료 조건이 만족되면, 라인 15에서 프로세서(130)는 수정된 스마트 컨트랙트의 집합(S) 및 지식 데이터 세트( $K_{on}$ )를 출력할 수 있다. 여기서, 수정된 스마트 컨트랙트의 집합(S)은 워크셋(W)이 공집합이 될 때까지, 사전 설정된 타임아웃에 도달할 때까지, 정답 스마트 컨트랙트가 발견될 때까지 또는 수정 루프 동작을 수행하는 횟수가 사전 설정된 횟수에 도달할 때까지 등의 종료 조건을 만족하는 시점에서의 가장 우수한(즉, 비퇴행적이고, 수정된 후보 스마트 컨트랙트들 중에서 탐지된 취약점의 수가 현재까지 최소이고, 적용된 후보 패치의 크기가 현재까지 최소인 조건들을 만족하는) 후보 스마트 컨트랙트들의 집합을 의미할 수 있다. 다양한 실시예에서 프로세서(130)는 정답 스마트 컨트랙트가 발견되면 사전 설정된 타임아웃에 도달하지 않더라도 수정 루프 동작을 종료할 수 있다.

[0143] 상세한 스마트 컨트랙트 취약점 수정 동작을 가속화하기 위해 프로세서(130)는 제1 및 제2 통계 모델들을 이용할 수 있다. 이를 위해 프로세서(130)는 도 10의 라인 12에서 제1 통계 모델( $M_{on}$ )을 학습시키기 위해 사용되는 제1 학습 데이터 세트( $D_{on}$ )에 기반하여 제1 통계 모델( $M_{on}$ )을 학습시키고, 도 10의 라인 6에서 제2 통계 모델( $M_{off}$ )을 학습시키기 위해 사용되는 사전 지식 데이터 세트( $K_{off}$ )를 획득할 수 있다. 제1 통계 모델( $M_{on}$ )을 학습시키는 과정에 대해서 하기의 도 12를 이용하여 상세하게 설명하도록 한다.

[0144] 도 12는 본 개시의 실시예에 통계 모델을 학습하기 위해 사용되는 데이터 및 통계 모델을 획득하기 위한 동작을 의사코드로 표현한 일례를 나타내는 예시도이다.

[0145] 도 12를 참조하면, 라인 1에서 프로세서(130)는 제1 통계 모델( $M_{on}$ )을 학습시키기 위해 사용되는 제1 학습 데이터(d)를 생성하고, 생성된 제1 학습 데이터(d)를 제1 학습 데이터 세트( $D_{on}$ )에 포함시킬 수 있다. 여기서, 제1 학습 데이터 세트( $D_{on}$ )는 제1 통계 모델( $M_{on}$ )을 학습시키기 위해 사용되는 제1 학습 데이터의 집합을 의미할 수 있다.

[0146] 구체적으로, 프로세서(130)는 현재 후보 패치(p) 및 현재 후보 패치가 적용된 후보 스마트 컨트랙트(s)에 대한 검증 결과(VR, RR)에 기반하여 제1 통계 모델( $M_{on}$ )을 학습시키기 위한 제1 학습 데이터( $d \in D_{on}$ )를 생성할 수 있다.

[0147] 이와 같이 생성된 제1 학습 데이터(d)는 현재 후보 패치(p)에 대한 특징 벡터( $\langle i_1, \dots, i_n \rangle \in \{0, 1\}^n$ ) 및 현재 후보 패치에 대한 안전성 점수(score)를 포함할 수 있다.

[0148] 먼저, 현재 후보 패치(p)에 대한 특징 벡터를 획득하기 위해 패치 컴포넌트 집합( $C=\{c_1, \dots, c_n\}$ )이 존재하고, 각 패치 컴포넌트( $c_1, \dots, c_n$ )가 고유 식별자( $i \in [1, n]$ )를 가진다고 가정한다. 프로세서(130)는 패치 컴포넌트 집합(C)으로 매개 변수화된 특징 인코딩(feature encoding) 함수( $F_c$ )를 이용하여 현재 후보 패치(p)를 특징 벡터로 변환할 수 있다. 이로 인해 생성된 특징 벡터( $F_c(p)$ )는  $F_c(p) = \langle F'_{c_1}(p), \dots, F'_{c_n}(p) \rangle$ 와 같이 표현될 수 있다. 여기서,  $F'_{c_n}$ 는 후보 패치( $p = c_{x_1} \dots c_{x_m} (x_1, \dots, x_m \in [1, n])$ )가 i번째 패치 컴포넌트  $c_i$ 를 포함하는지 확인하는 술어를 의미할 수 있다.

[0149] 후보 패치(p)가 i번째 패치 컴포넌트  $c_i$ 를 포함하는지 확인하기 위한  $F'_{ci}(p)$ 는,  $F'_{ci}(p) = \text{if } c_i \in \{c_{x_k} \mid k \in [1, m]\} \text{ then } 1 \text{ else } 0$  '와 같은 수식으로 표현될 수 있다. 이러한 특징 인코딩 방식은 기계 학습 기반의 프로그램 축소(program debloating) 방법에서 활용된 기존의 인코딩 방식(Effective Program Debloating via Reinforcement Learning [ACM CCS '18])을 바탕으로 고안된 것이나, 이에 한정되지 않는다.

[0150] 다음으로, 안전성 점수를 획득하기 위해 프로세서(130)는 다음의 <수학식 1>을 이용할 수 있다.

**수학식 1**

$$Q(p, VR_0, VR, RR_0, RR) = \begin{cases} \frac{|VR_0| - |VR| - \gamma * |p|}{|VR_0|} & \text{if } RR = RR_0 \text{ and } |VR| \leq |VR_0| \\ -(1 + |p|) & \text{if } RR \neq RR_0 \text{ or } |VR| > |VR_0|. \end{cases}$$

[0152] 여기서, 후보 패치(p)에 대한 안전성 점수는 원본 스마트 컨트랙트 대비 후보 스마트 컨트랙트의 알람 감소율을 의미할 수 있다.

[0153] 구체적으로, 후보 패치(p)가 적용된 후보 스마트 컨트랙트가 비퇴행적( $RR=RR_0$ )이고, 후보 스마트 컨트랙트가 원본 스마트 컨트랙트보다 더 안전하거나 동일하게 안전한 경우( $|VR| \leq |VR_0|$ ) 프로세서(130)는

$\frac{|VR_0| - |VR| - \gamma * |p|}{|VR_0|}$  '의 계산식을 이용하여 안전성 점수를 산출할 수 있다. 다시 말해서, 프로세서(130)는 감소된 알람 수( $|VR_0| - |VR|$ )에서 조정된(scaled) 패치 크기( $\gamma * |p|$ )만큼 감소시킨 결과를 원본 스마트 컨트랙트의 알람 수( $|VR_0|$ )로 나눈 값을 안전성 점수로 산출할 수 있다. 패치 크기가 더 큰 경우 올바르게 못하거나 불필요한 패치 컴포넌트를 포함할 가능성이 높을 수 있으므로, 원본 스마트 컨트랙트와 후보 스마트 컨트랙트의 알람 수가 동등하더라도 더 작은 크기의 패치가 더 바람직하다고 판단될 수 있다.

[0154] 후보 패치(p)가 적용된 후보 스마트 컨트랙트가 퇴행적( $RR \neq RR_0$ )이고, 원본 스마트 컨트랙트가 후보 스마트 컨트랙트보다 더 안전한 경우( $|VR| > |VR_0|$ ) 프로세서(130)는  $-(1 + |p|)$  '의 계산식을 이용하여 해당 후보 패치에 대해 낮은, 음의 안전성 점수를 부여할 수 있다.

[0155] 라인 2에서 프로세서(130)는 이와 같이 생성된 제1 학습 데이터 세트( $D_{on}$ )에 기반하여 제1 통계 모델( $M_{on}$ )을 학습시킬 수 있다. 예를 들어, 프로세서(130)는 후보 패치(p)에 대한 특징 벡터에 기반하여 후보 패치(p)에 대한 안전성 점수를 산출하도록 제1 통계 모델( $M_{on}$ )을 학습시킬 수 있다.

[0156] 라인 3에서 프로세서(130)는 새로운 지식 데이터(k)를 생성하고, 생성된 지식 데이터(k)를 지식 데이터 세트( $K_{on}$ )에 포함시킬 수 있다. 여기서, 지식 데이터(k)는 후보 패치(p)를 추상화한 형태의 패치( $\hat{p}$ )와 해당 후보 패치(p)의 안전성 점수(safety score)를 포함할 수 있다.

[0157] 구체적으로, 프로세서(130)는 추상화 함수( $\alpha$ )를 이용하여 후보 패치( $p = c_{x_1} \cdots c_{x_m} \mid x_1 \cdots x_m \in [1, n], n = |C|$ )를 추상화된 형태의 패치( $\hat{p} (= \alpha(p))$ )로 변환시킬 수 있다. 일반적으로, 패치에는 새로운 스마트 컨트랙트에 곧바로 적용되기 어려운 특정 코드에만 존재하는 정보(예: 라인 숫자, 변수 이름 등)를 포함하므로, 패치의 특정 정보를 추상화함으로써, 패치가 성공적으로 새로운 스마트 컨트랙트에 적용될 수 있다.

[0158] 여기서, 추상화 함수( $\alpha$ )는  $\alpha(p) = \alpha'(c_{x_1}) \cdots \alpha'(c_{x_m})$  '와 같이 정의될 수 있으며,  $\alpha'$ 는 후보 패치(p)를 이루는 패치 컴포넌트( $c = a_1, \dots, a_n$ )를 추상화된 형태의 패치 컴포넌트로 변환하는 함수를 의미할 수 있다. 여기서, 패치 컴포넌트의 추상화 함수( $\alpha'$ )는 라인 숫자와 같이 위치에 대한 정보를 함수 레벨 특징(function-level feature)으로 추상화하고, 명령문/표현식에 대한 정보를 명령문/표현식 내의 변수 타입들로 추상화하는

함수 일 수 있으나, 이에 한정되지 않는다.

[0159] 예를 들어, 하나의 수정 템플릿(Insert, Rep)만으로 이루어진 패치 컴포넌트에 대하여 해당 패치 컴포넌트에 대한 추상화 함수( $\alpha'$ )는 '와 같이 정의될 수 있다.

$$\alpha'(c) = \begin{cases} \widehat{\text{Insert}}(H(f_l), T_s(s')) & \text{if } c = \text{Insert}(l, s') \\ \widehat{\text{Rep}}(H(f_l), T_e(e_1), Op(e_1), T_e(e_2), Op(e_2)) & \text{if } c = \text{Rep}(l, e_1, e_2) \\ \dots & \dots \end{cases}$$

[0160] 여기서,  $\widehat{\text{Insert}}$ 는  $\text{Insert}(l, s')$ 에 대한 추상화된 패치 컴포넌트를 생성하기 위한 생성자(constructor)를 의미하고,  $\widehat{\text{Rep}}$ 는  $\text{Rep}(l, e_1, e_2)$ 에 대한 추상화된 패치 컴포넌트를 생성하기 위한 생성자를 의미할 수 있다. 또한,  $T_s(s')$ 는 명령문  $s'$ 에 등장하는 전역 변수 타입들의 집합을 의미하고,  $Op(e)$ 는  $e$ 에 등장하는 이항 연산자(binary operator)들의 집합을 의미할 수 있다.

[0161] 또한,  $H(f)$ 는 함수( $f$ )에 대한 특징을 변환하도록,  $H(f) = (D(f), U(f), P(f), L(f), E(f), X(f))$  '와 같이 정의될 수 있다.

[0162] 여기서,  $D(f)$ 와  $U(f)$ 는 함수( $f$ )의 할당문(assignment)에서 정의되고 분기문의 조건 표현식에서 사용된 전역 변수 타입들의 집합을 변환하고,  $P(f)$ ,  $L(f)$ ,  $E(f)$ ,  $X(f)$ 는 확인하고자 하는 내용이 참일 경우 '1'을, 거짓일 경우 '0'을 반환하는 술어(predicate)들일 수 있다. 구체적으로,  $P(f)$ 는 함수( $f$ )가 솔리디티 프로그램 언어에서 사전에 정의된 payable 수정자(또는 함수 변경자)를 포함하는지를 확인하는 술어를 의미하고,  $L(f)$ 는 함수( $f$ )가 루프(loop)를 포함하는지를 확인하는 술어를 의미하고,  $E(f)$ 는 함수( $f$ )가 이더(ether)를 송금하는 명령문을 포함하는지를 확인하는 술어를 의미하며,  $X(f)$ 는 함수( $f$ )가 스마트 컨트랙트를 비활성화시키는 명령문(예: selfdestruct)를 포함하는지를 확인하는 술어를 의미할 수 있다.

[0163] 이와 같이 생성되는 지식 데이터 세트( $K_{on}$ )는 새로운 원본 스마트 컨트랙트에 대한 검증 및 수정 동작이 수행되면 제2 통계 모델( $M_{off}$ )을 학습시키기 위한 제2 학습 데이터 세트( $D_{off}$ )를 획득하기 위해 후술하는 바와 같이 활용될 수 있다.

[0164] 다시 도 10를 참조하면, 프로세서(130)는 도 10의 라인 6에서 과거 수정 이력들이 통합된 사전 지식 데이터 세트(unified prior knowledge data set)( $K_{off}$ )를 생성하고, 생성된 사전 지식 데이터 세트( $K_{off}$ )에 기반하여 제2 통계 모델( $M_{off}$ )을 학습시킬 수 있다. 여기서, 과거 수정 이력들은 과거에 수행된 수정 알고리즘 동작(즉, 과거의 후보 패치가 적용된 후보 스마트 컨트랙트에 대한 수정 루프 동작 또는 과거 원본 스마트 컨트랙트를 각각에 대하여 수행된 검증 및 수정 동작)에 대한 결과들(즉, 지식 데이터 세트)을 포함할 수 있으며, 이러한 결과들은 과거에 적용된 복수의 추상화된 후보 패치들 및 각 후보 패치에 대한 안전성 점수 등을 포함할 수 있으나, 이에 한정되지 않는다.

[0165] 구체적으로, 프로세서(130)는 사전 지식 데이터 세트( $K_{off}$ )를 제2 학습 데이터 세트( $D_{off}$ )로 변환할 수 있다. 여기서, 제2 학습 데이터 세트( $D_{off}$ )는,  $D_{off} = \{(< i_1, \dots, i_n >, score) \mid (\hat{p}, score) \in K_{off}\}$  '와 같이 정의될 수 있다.

[0166] 제2 학습 데이터 세트( $D_{off}$ )를 생성하기 위해 프로세서(130)는 패치 컴포넌트 집합( $C$ )으로 매개 변수화된 특징 인코딩 함수( $G_c$ )를 이용하여 추상화된 후보 패치( $\hat{p}$ )에 대한 특징 벡터( $< i_1, \dots, i_n > \in \{0, 1\}^n$ )를 생성할 수 있다(즉,  $< i_1, \dots, i_n > = G_C(\hat{p})$ ).

[0167] 이러한 특징 인코딩 함수( $G_c$ )는,  $G_C(p) = < G'_{c_1}(p), \dots, G'_{c_n}(p) >$  '와 같이 정의될 수 있다. 여기서,  $G'_{c_i}$ 는 추상화된 패치( $\hat{p} = \hat{c}_{x_1} \dots \hat{c}_{x_m} \quad (x_1, \dots, x_m \in [1, n])$ )가  $i$ 번째 패치 컴포넌트( $c_i (i \in [1, n])$ )의 추상화된

결과를 포함하는지를 확인하는 술어를 의미할 수 있다.

[0168] 추상화된 후보 패치( $\hat{p}$ )가 패치 컴포넌트  $c_i$ 의 추상화된 결과를 포함하는지 확인하기 위한  $G_{c_i}(\hat{p})$ 는  $G_{c_i}(\hat{p}) = \text{if } \alpha'(c_i) \in \{\hat{c}_{x_k} \mid k \in [1, m]\} \text{ then } 1 \text{ else } 0$ 와 같은 수식으로 표현될 수 있다.

[0169] 프로세서(130)는 이와 같이 추상화된 후보 패치( $\hat{p}$ )에 대한 특징 벡터 및 해당 후보 패치(p)에 대한 과거 안전성 점수(즉, 사전 지식 데이터 세트( $K_{off}$ )에 기록된 안전성 점수)를 포함하는 제2 학습 데이터 세트( $D_{off}$ )를 생성하고, 생성된 제2 학습 데이터 세트( $D_{off}$ )에 기반하여 제2 통계 모델( $M_{off}$ )을 학습시킬 수 있다. 예를 들어, 프로세서(130)는 추상화된 후보 패치( $\hat{p}$ )에 대한 특징 벡터에 기반하여 후보 패치(p)에 대한 과거 안전성 점수를 산출하도록 제2 통계 모델( $M_{off}$ )을 학습시킬 수 있다.

[0170] 프로세서(130)는 이와 같이 학습된 제1 통계 모델( $M_{on}$ ) 또는 제2 통계 모델( $M_{off}$ )을 이용하여 정답 패치일 가능성이 높은 후보 패치들을 결정하고, 결정된 후보 패치들을 원본 스마트 컨트랙트에 적용하여 획득한 후보 스마트 컨트랙트에 대한 수정 루프 동작을 우선적으로 수행함으로써, 스마트 컨트랙트 취약점 수정 동작을 가속화할 수 있다.

[0171] 이에 대해서 구체적으로, 도 10의 라인 8에서 프로세서(130)는 상술한 제2 비용 계산식을 이용하여 각 후보 패치에 대한 비용 점수(cost(p))를 산출할 수 있다.

[0172] 각 후보 패치에 대한 비용 점수(cost(p))를 산출하기 위해서 프로세서(130)는 후보 패치(p)에 대한 예상 안전성 점수를 산출하는데, 예상 안전성 점수(score(p))는

$$\text{score}(p) = \begin{cases} M_{off}(FC(p)) & \text{if } M_{off} \neq \perp \\ -|p| & \text{if } M_{off} = \perp \text{ and } \exists e \in E. e \notin \{v \mid (v, -) \in D_{on}\} \\ M_{on}(FC(p)) & \text{if } M_{off} = \perp \text{ and } \forall e \in E. e \in \{v \mid (v, -) \in D_{on}\} \end{cases}$$

와 같이 정의될 수 있다.

[0173] 여기서, E는  $n(=|C|)$ 차원에서 가능한 모든 원핫(one-hot) 벡터들의 집합  $(E = \{i \mid i \in \{0, 1\}^n, i = \langle i_1, \dots, i_n \rangle, \sum_{j=1}^n i_j = 1\})$ 을 의미하고, e는 원핫 벡터를 의미할 수 있다.

[0174] 먼저, 사전 지식 데이터 세트에 기반하여 사전 학습된 제2 통계 모델( $M_{off}$ )이 존재하는 경우(**if**  $M_{off} \neq \perp$ )(즉, 첫번째 케이스)에 대해서 설명하도록 한다. 사전 학습된 제2 통계 모델( $M_{off}$ )이 존재한다는 것은 제2 통계 모델( $M_{off}$ )을 학습시킬 수 있는 사전 지식 데이터 세트가 존재하고, 사전 지식 데이터 세트에 기반하여 제2 통계 모델( $M_{off}$ )이 사전 학습되었다는 것으로 이해될 수 있다. 이러한 경우 프로세서(130)는 각 후보 패치에 대한 특징 벡터( $FC(p)$ )를 입력으로 각 후보 패치에 대한 예상 안전성 점수를 출력하도록 학습된 제2 통계 모델( $M_{off}$ )을 이용하여 각 후보 패치에 대한 예상 안전성 점수를 산출할 수 있다.

[0175] 다음으로, 제2 통계 모델( $M_{off}$ )을 학습시킬 수 있는 사전 지식 데이터 세트가 존재하지 않거나 후술할 제2 통계 모델( $M_{off}$ )의 무효화 절차에 의해 제2 통계 모델( $M_{off}$ )이 존재하지 않고, 단일 패치 컴포넌트로 구성된 후보 패치들 중 일부 후보 패치에 대한 안전성 점수가 결정되지 않은 경우(**if**  $M_{off} = \perp$  and  $\exists e \in E. e \notin \{v \mid (v, -) \in D_{on}\}$ )(즉, 두번째 케이스)에 대해서 설명하도록 한다. 단일 패치 컴포넌트로 구성된 후보 패치들 중 일부 후보 패치에 대한 안전성 점수가 결정되지 않았다는 것은 제1 통계 모델( $M_{on}$ )을 학습시키기 위한 학습 데이터 세트가 충분히 수집되지 않아 학습된 제1 통계 모델( $M_{on}$ )의 예측 능력이 부족할 가능성이 높은 상태인 것으로 이해될 수 있다. 이러한 경우 프로세서(130)는 각 후보 패치에 대한 패치 크기에 대한 음수 값( $-|p|$ )을 각 후보 패치에 대한 예상 안전성 점수로서 획득할 수 있다(즉, 두번째 케이스).

[0176] 다음으로, 제2 통계 모델( $M_{off}$ )이 존재하지 않고, 단일 패치 컴포넌트로 구성된, 모든 후보 패치에 대한 안전성

점수가 결정된 경우( $\text{if } M_{off} = \perp \text{ and } \forall e \in E. e \in \{v \mid (v, -) \in D_{on}\}$ )(세번째 케이스)에 대해서 설명하도록 한다. 단일 패치 컴포넌트로 구성된, 모든 후보 패치에 대한 안전성 점수가 결정되었다는 것은 제1 통계 모델( $M_{on}$ )을 학습시키기 위한 학습 데이터 세트가 충분히 수집되어 학습된 제1 통계 모델( $M_{on}$ )의 예측 능력이 안정적인 가능성이 높은 상태인 것으로 이해될 수 있다. 이러한 경우 프로세서(130)는 제1 통계 모델( $M_{on}$ )을 이용하여 각 후보 패치에 대한 예상 안전성 점수를 산출할 수 있다.

[0177] 이와 같이 예상 안전성 점수가 산출되면 프로세서(130)는 각 후보 패치에 대하여 산출된 예상 안전성 점수에서 각 후보 패치에 대한 패널티 점수를 감소시킨 값의 음수 값을 각 후보 패치에 대한 비용 점수로 산출할 수 있다. 프로세서(130)는 각 후보 패치에 대해 산출된 비용 점수가 가장 낮은 후보 패치에서 높은 후보 패치 순으로 상술한 수정 루프 동작을 수행할 수 있다.

[0178] 이와 같이 정답 스마트 컨트랙트일 가능성이 높은 후보 스마트 컨트랙트에 대하여 우선적으로 수정 루프 동작이 수행되므로, 스마트 컨트랙트 취약점 수정을 신속하고 효율적으로 수행할 수 있다.

[0179] 다양한 실시예에서 현재 수행 중인 수정 알고리즘 동작에서의 스마트 컨트랙트가 이전 수정 알고리즘 동작에서의 스마트 컨트랙트들과 다른 특성을 가진 경우 제2 통계 모델은 정답 스마트 컨트랙트를 발견하는데 도움이 되지 않는 후보 패치가 우선적으로 탐색되도록 오동작 될 수 있다. 수정 알고리즘 동작을 안정적으로 수행하기 위해 프로세서(130)는 사전 설정된 제한 조건이 만족되면 제2 통계 모델의 이용을 제한할 수 있다. 여기서, 사전 설정된 제한 조건은 현재 후보 패치에 대하여 산출된 안전성 점수가 음수 값을 갖는 경우(score<0), 또는 수정 루프 동작이 사전 설정된 임계 횟수(x, x는 자연수)를 반복할 때까지 정답 스마트 컨트랙트가 발견되지 않은 경우를 포함할 수 있다.

[0180] 제2 통계 모델의 이용이 제한되는 경우 프로세서(130)는 제1 학습 데이터 세트( $D_{on}$ )를 갱신할 수 있다. 예를 들어, 제1 학습 데이터 세트( $D_{on}$ )는 특징 벡터의 합이 1인 제1 학습 데이터만을 포함하도록,  $\{(<i_1, \dots, i_n>, score) \mid (<i_1, \dots, i_n>, score) \in D_{on}, \sum_{j=1}^n i_j = 1\}$ 와 같이 갱신될 수 있다.

[0181] 제2 통계 모델을 이용하는 동안 획득된 제1 학습 데이터 중 단일 패치 컴포넌트가 아닌 복수 개의 패치 컴포넌트로 이루어진 후보 패치에 기반하여 획득된 제1 학습 데이터를 이용하여 제1 통계 모델( $M_{on}$ )이 학습되는 경우, 제2 통계 모델을 이용하지 않고 획득된 제1 학습 데이터를 이용하여 학습한 제1 통계 모델( $M_{on}$ )만큼의 예측 능력이 보장되지 않을 수 있다. 이에, 제2 통계 모델을 이용하지 않고 획득된 제1 학습 데이터를 이용하여 학습한 제1 통계 모델( $M_{on}$ )만큼의 예측 능력을 보장하기 위해, 프로세서(130)는 갱신된 제1 학습 데이터 세트( $D_{on}$ )를 이용하여 제1 통계 모델( $M_{on}$ )을 재학습시킬 수 있다.

[0182] 이를 통해, 본 개시의 스마트 컨트랙트 취약점 수정 장치는 스마트 컨트랙트 취약점 수정을 신속하고 정확하게 수행할 수 있다.

[0183] 도 13은 본 개시의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도이다.

[0184] 본 개시가 일반적으로 컴퓨팅 장치에 의해 구현될 수 있는 것으로 전술되었지만, 당업자라면 본 개시가 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어 및/또는 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로써 구현될 수 있다는 것을 잘 알 것이다.

[0185] 일반적으로, 프로그램 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드(handheld) 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.

[0186] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘 다에 위치할 수 있다.

[0187] 컴퓨터는 통상적으로 다양한 컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체는 그 어떤

것이든지 컴퓨터 판독가능 매체가 될 수 있고, 이러한 컴퓨터 판독가능 매체는 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다. 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.

[0188] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.

[0189] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.

[0190] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇 가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.

[0191] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA) -이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 새시(도시 생략) 내에서 외장형 용도로 구성될 수 있음-, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘 다를 포함한다.

[0192] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 zip 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.

[0193] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.

[0194] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통

해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.

[0195] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.

[0196] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 컴퓨팅 디바이스 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원거리 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.

[0197] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 컴퓨팅 디바이스에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0198] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순히 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0199] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a, b, g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

[0200] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 정보 및 신호들이 임의의 다양한 상이한 기술들 및 기법들을 이용하여 표현될 수 있다는 것을 이해할 것이다. 예를 들어, 위의 설명에서 참조될 수 있는 데이터, 지시들, 명령들, 정보, 신호들, 비트들, 심볼들 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 입자들, 광학장들 또는 입자들, 또는 이들의 임의의 결합에 의해 표현될 수 있다.

[0201] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 소프트웨어로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에

대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

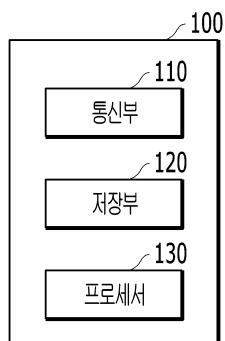
[0202] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조 물품(article)으로 구현될 수 있다. 용어 제조 물품은 임의의 컴퓨터-판독가능 저장장치로부터 액세스 가능한 컴퓨터 프로그램, 캐리어, 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트립, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 또한, 여기서 제시되는 다양한 저장 매체는 정보를 저장하기 위한 하나 이상의 장치 및/또는 다른 기계-판독가능한 매체를 포함한다.

[0203] 제시된 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조는 예시적인 접근들의 일례임을 이해하도록 한다. 설계 우선순위들에 기반하여, 본 개시의 범위 내에서 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조가 재배열될 수 있다는 것을 이해하도록 한다. 첨부된 방법 청구항들은 샘플 순서로 다양한 단계들의 엘리먼트들을 제공하지만 제시된 특정한 순서 또는 계층 구조에 한정되는 것을 의미하지는 않는다.

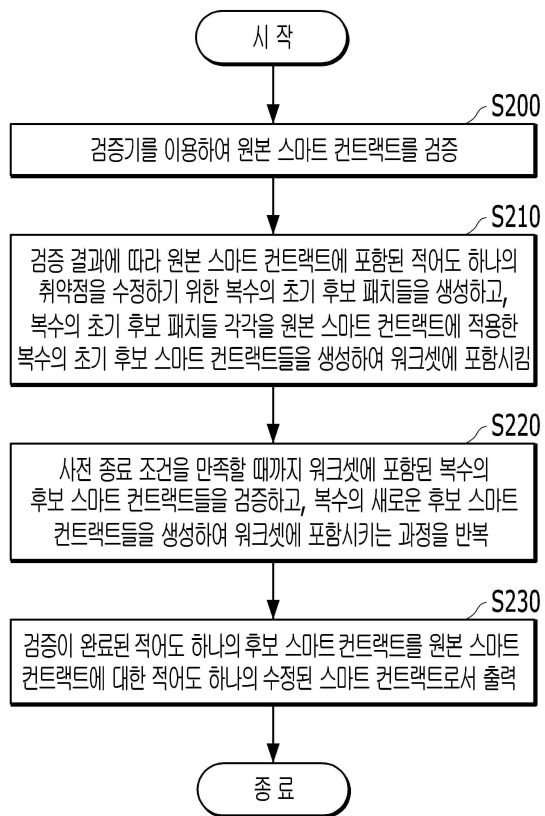
[0204] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

## 도면

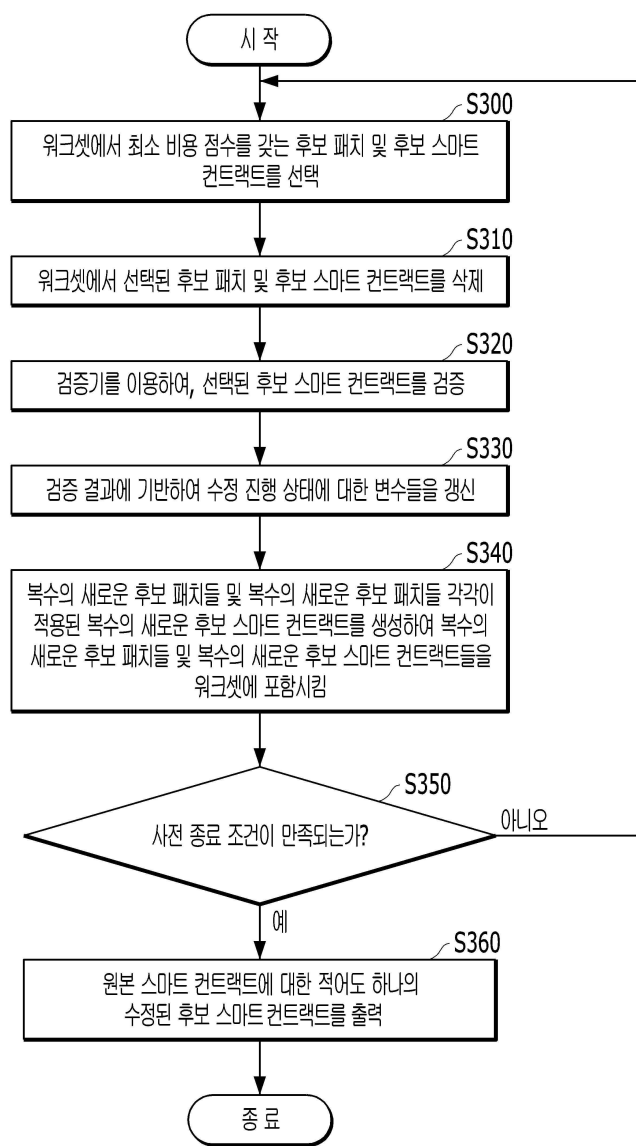
### 도면1



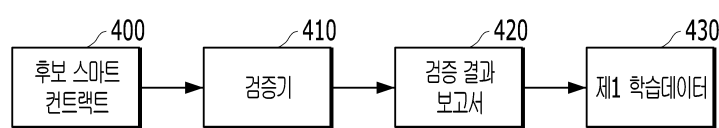
도면2



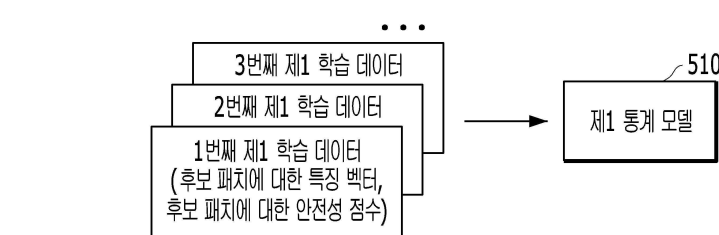
도면3



도면4

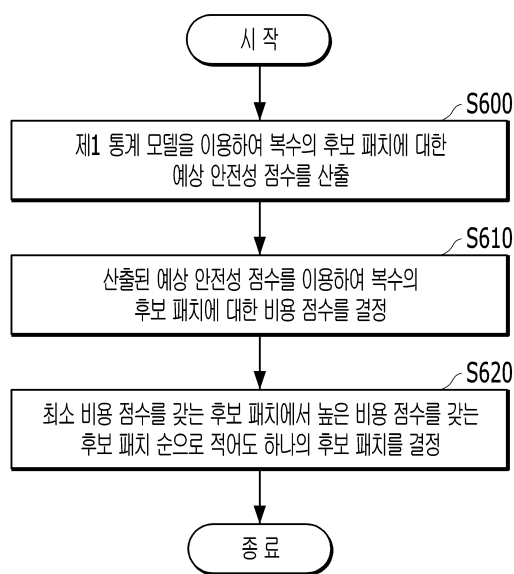


도면5

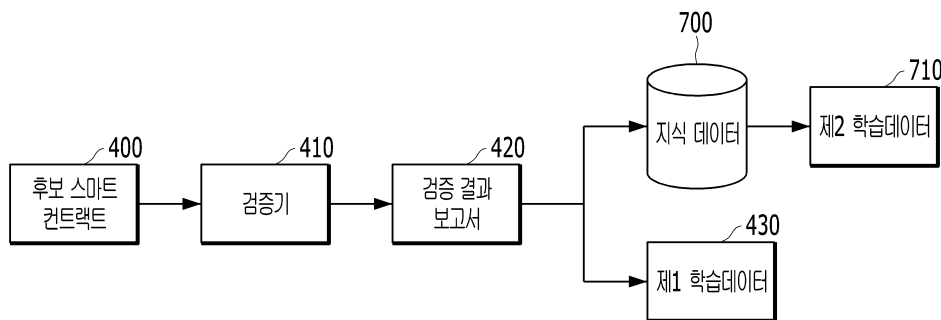


적어도 하나의 제1 학습 데이터를 포함하는 제1 학습 데이터 세트(500)

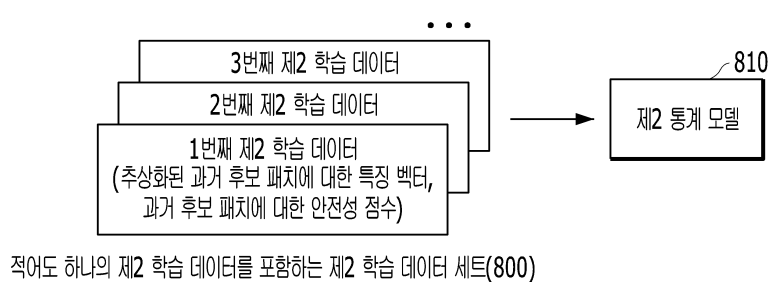
도면6



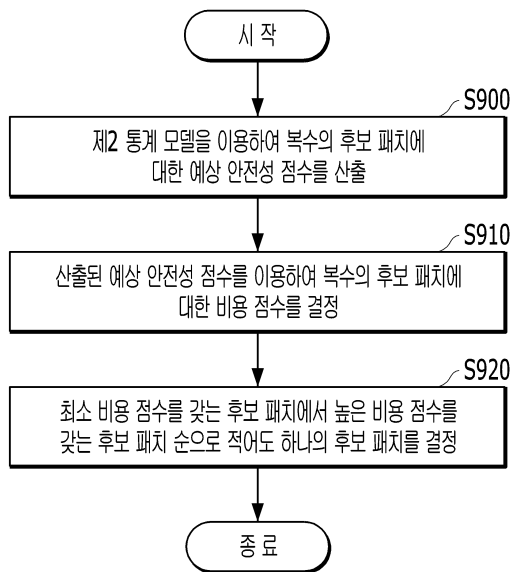
도면7



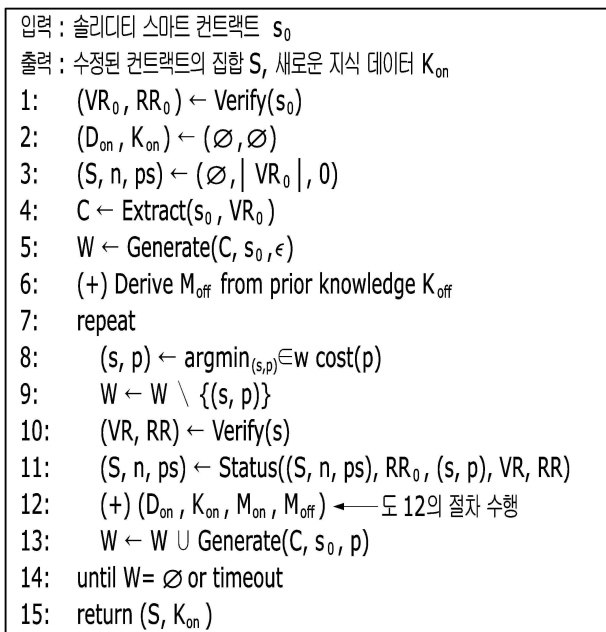
도면8



도면9



도면10



도면11

입력 :  $((S, n, ps), RR_0, (s, p), VR, RR)$   
 출력 : 갱신 가능성 있는  $(S, n, ps)$   
 1: procedure Status( $(S, n, ps), RR_0, (s, p), VR, RR$ )  
 2: if  $RR=RR_0 \wedge |VR| < n$  then  
 3:    $(S, n, ps) \leftarrow (\{s\}, |VR|, |p|)$   
 4: else if  $RR=RR_0 \wedge |VR| = n \wedge |p| = ps$  then  
 5:    $S \leftarrow S \cup \{s\}$   
 6: else if  $RR=RR_0 \wedge |VR| = n \wedge |p| < ps$  then  
 7:    $(S, ps) \leftarrow (\{s\}, |p|)$   
 8: return  $(S, n, ps)$

도면12

입력 : 패치 컴포넌트 집합 C, 검증 결과  $(VR_0, VR, RR_0, RR)$ , 후보 패치 p, 학습  
 관련 데이터  $(D_{on}, K_{on}, M_{on}, M_{off})$   
 출력 :  $(D_{on}, K_{on}, M_{on}, M_{off})$   
 1:  $D_{on} \leftarrow D_{on} \cup \{d\}$  where  $d = (F_c(p), Q(p, VR_0, VR, RR_0, RR))$   
 2: Derive  $M_{on}$  from  $D_{on}$   
 3:  $K_{on} \leftarrow K_{on} \cup \{k\}$  where  $k = (\alpha(p), Q(p, VR_0, RR_0, RR))$   
 4: If  $M_{off}$  is unlikely to be helpful, assign  $\perp$  to  $M_{off}$  and refine  $D_{on}, M_{on}$   
 5: return  $(D_{on}, K_{on}, M_{on}, M_{off})$

도면13

