사물인터넷융복합논문지 Vol. 10, No. 5, pp. 119-124, 2024 https://doi.org/10.20465/KIOTS.2024.10.5.119

이더리움 스마트컨트랙트 가스 제한 취약점 방지를 위한 Unified Random Forest 적용 실시간 탐지 기법

장수안[1], 이근호[2], 윤성현[3*]
[1]백석대학교 컴퓨터공학부 학생, [2,3]백석대학교 컴퓨터공학부 교수

A Scheme Real-Time Detection Technique using Unified Random Forest to prevent Ethereum Smart Contract Gas Limit Vulnerabilities

Su-An Jang[1], Keun-Ho Lee[2], Sung-Hyun Yun[3*]
[1]Undergraduate Student, Division of Computer Engineering, Baek-Seok University
[2,3]Professor, Division of Computer Engineering, Baek-Seok University

요 약 이더리움은 스마트컨트랙트를 활용하는 여러 암호화폐 중 하나로, 오늘날 대표적으로 잘 알려진 암호화폐이다. 스마트컨트랙트로 인해, 보안과 거래 속도, 투명성 및 신뢰성을 보장하며 블록체인 기술에서 안전한 암호화폐 거래가 가능하게 한다. 하지만, 스마트컨트랙트에서도 치명적인 취약점은 존재하며, 이를 억제하고 보완하기 위한 기술들이 개발되고 있다. 그중 이더리움 네트워크에서 발생하는 중요한 문제점 중 하나인 가스 제한(Gas Limit) 취약점이 존재한다. 가스 제한 취약점은 이더리움에서 스마트컨트랙트가 실행될 때 요구되는 수수료로 사용되지만, 이 가스 비용을 조작하여 계약 중단을 유도하거나, 최적화 방해, DoS 공격을 유발할 수 있다. 이를 통해 피해자의 가스만 소모하고, 네트워크 혼잡을 일으켜 피해를 준다. 본 논문에서는 Unified Random Forest 모델을 활용하여, 이더리움 네트워크에서 발생하는 트랜잭션 데이터를 실시간으로 탐지하여 가스 제한 취약점을 방지하는 기법을 제안하고자 한다. 해당 기법을 통해, 무분별한 가스 손실을 최소화하고, 비이상적인 트랜잭션을 탐지하여 사전에 가스 제한 취약점을 막을 수 있다.

주제어 : 스마트컨트랙트, 가스 제한 취약점, 실시간 탐지, Unified Random Forest

Abstract Ethereum is one of the many cryptocurrencies that use smart contracts, and it is a well-known cryptocurrency today. Due to smart contracts, security, transaction speed, transparency and reliability are guaranteed, and secure cryptocurrency transactions are possible in blockchain technology. However, there are fatal vulnerabilities in smart contracts, and technologies are being developed to suppress and supplement them. Among them, one of the important problems occurring in the Ethereum network, a vulnerability to gas limit, exists. A gas limit vulnerability is used as a fee required when a smart contract is executed in Ethereum, but it can manipulate this gas cost to induce contract suspension, interfere with optimization, and cause DoS attacks. This consumes only the victim's gas, causes network congestion, and damages. In this paper, we propose a technique to prevent gas limitation vulnerabilities by detecting transaction data occurring in the Ethereum network in real time. Through this technique, it is possible to minimize indiscriminate gas loss and prevent gas limitation vulnerabilities in advance by detecting abnormal transactions.

Key Words : Smart Contract, Gas Limit Vulnerabilities, Real-time detection, Unified Random Forest

*교신저자 : 윤성현(shcrpt@gmail.com)
접수일 2024년 09월 06일 수정일 2024년 09월 30일 심사완료일 2024년 10월 04일

1. 서론

블록체인의 기술이 발전하면서, 오늘날 디지털 화폐의 출현과 암호화폐가 일상에서 쉽게 접하고, 활용한다. 2015년 이더리움의 등장으로 스마트컨트랙트가 제공되면서 블록체인 발전에 가속화가 이루어졌다. 스마트컨트랙트는 이더리움 네트워크에서 작동하여 매우 높은 보안과 신뢰성을 보여주지만, 현재 스마트컨트랙트에 대한 취약점이 존재하고 OWASP TOP 10 Smart Contract에서 가스 제한 취약점(Gas Limit Vulnerabilities)이 9위에 위치한다[1].

스마트컨트랙트 취약점을 보완할 다양한 솔루션들이 개발 및 제안되고 있지만, 가스 제한 취약점에 대한 실시간 탐지 방식은 아직 상용화되지 않은 상태이다. 이더리움 네트워크에서 매 순간 발생하는 다량의 거래 트랜잭션은 동시다발적으로 발생하기 때문에 각각의 트랜잭션에 대하여 일일이 취약점을 잡아내는 것은 쉽지 않다. 하지만, Unified Random Forest 모델을 활용하여 실시간 트랜잭션 탐지에 도움을 줄 수 있다.

Unified Random Forest는 다수의 랜덤 포레스트(Random Forest)를 결합한 앙상블 모델로, 단일 랜덤 포레스트에서 구성되는 Decision Tree가 Unified Random Forest에서는 하나의 랜덤 포레스트로 활용한다.

이는 이더리움 트랜잭션과 같은 복잡한 데이터셋에서도 우수한 성능을 발휘할 수 있고, 다량의 트랜잭션을 한 번에 처리할 수 있다. 트랜잭션에서 가스 제한 취약점을 유발하는 특징을 찾기 위해, 스마트컨트랙트에서 가스를 호출하는 함수의 발생 빈도, 할당된 가스의 평균값을 통한 비이상적인 가스 할당 등을 집중적으로 학습하여 탐지에 활용할 수 있다.

본 논문에서는 위와 같은 일련의 방식을 통해 Unified Random Forest를 활용한 이더리움 스마트컨트랙트에서 가스 제한 취약점 실시간 탐지 기법을 제안하고, 이에 대한 탐지 과정을 함께 제안하려 한다.

2. 관련연구

2.1 이더리움

이더리움은 2015년에 출현한 탈중앙화 블록체인 플랫폼으로, 스마트컨트랙트와 디앱(DApp)을 지원하는 특징이 있다. 하지만, 2016년 이더리움 네트워크에 만들어진 탈중앙화 자율 조직 DAO에서 발생한 보안 취약점으로 인해 해킹사고가 발생했고, 이더리움과 이더리움 클래식으로 나누어지는 분기점이 되었다[2].

이를 통해 스마트컨트랙트의 보안 중요성이 대두되었고, 해당 해킹사고에서 활용된 스마트컨트랙트 재진입 공격은 현재까지 치명적인 스마트컨트랙트 취약점으로 꼽히고 있다.

2022년 이더리움은 더 머지(The Merge) 업그레이드를 통해 거래 처리 속도 및 혼잡한 네트워크 환경에서 발생하는 가스 비용 문제점을 해결하는 것을 목표로 하였다. 기존 PoW 작업 증명 방식에서 PoS 지분 증명으로 합의 알고리즘을 전환하였고, 이를 통해 에너지 효율 및 확장성 문제를 개선하였다[3].

현재는 탈중앙화 금융(DeFi), 대체 불가능한 토큰(NFT)를 도입하여 더욱 확장하고 있다. 이더리움은 스마트컨트랙트, 더 머지, 탈중앙화 금융, NFT 등의 기술로 확장하며 빠르게 발전하고 있으며, 다양한 산업 분야에 응용하며 새로운 혁신을 이끌고 있다[4].

2.2 스마트컨트랙트

이더리움 스마트컨트랙트는 이더리움 네트워크에서 실행되는 자동화 계약 프로토콜이다. 이더리움 스마트컨트랙트는 솔리디티(Solidity) 프로그래밍 언어로 작성된 계약 코드로, 특정 조건이 충족될 때 자동으로 트랜잭션이 처리되는 구조를 갖는다. 탈중앙화된 성격으로 운영되어 블록체인에 저장되고, 배포된 스마트컨트랙트는 수정할 수 없는 변경 불가성 특징을 가지므로, 계약이 투명하게 유지된다. 또한, 스마트컨트랙트 코드는 블록체인에 기록되고 암호화되어 안전하게 처리되어 보안을 유지한다.

이더리움 스마트컨트랙트는 이더리움 가상 머신(EVM)에서 실행된다. 이는 블록체인 네트워크에서 독립적으로 실행할 수 있도록 하는 가상환경으로 이를 통해 배포, 계약, 실행이 이루어진다. 이와 같은 특성으로 이더리움 네트워크는 효율적인 공급망 관리와 신뢰성을 보여주고 있다[5-8].

2.3 가스 제한 취약점

먼저 이더리움 가스(Gas)는 이더리움 네트워크에서 트랜잭션이나 스마트컨트랙트를 실행하기 위해 사용되는 수수료로, 작업에 대한 비용을 의미한다.

가스는 이더리움의 암호화폐인 이더(Ether, ETH)로 지불되며, 네트워크에서 수행되는 작업의 복잡도, 혼잡

도에 따라 달라질 수 있고, 시장 수요에 맞춰 변동한다. 사용자는 트랜잭션을 우선적으로 처리하기 위해 더 높은 가스 가격을 설정할 수 있다. 또한, 이더리움은 PoS 지분 증명 합의 알고리즘을 사용하는데, 이때 참여한 검증자들이 트랜잭션을 처리한 대가로 가스를 보상받는 용도로 사용된다.

가스 한도(Gas Limit)는 트랜잭션이나 스마트컨트랙트가 사용하는 최대 가스양을 설정하는 값으로, 사용자 설정 가스 한도와 블록 가스 한도로 나눠진다. 사용자 설정 가스 한도는 사용자가 트랜잭션을 실행할 때 사용할 수 있는 최대 가스를 제한하며, 잘못된 가스 설정으로 인한 트랜잭션 실패와 피해를 막기 위해 사용된다. 블록 가스 한도는 이더리움 블록 하나에 포함될 수 있는 최대 가스양을 제한하여, 이더리움 네트워크가 지나치게 복잡한 트랜잭션으로 과부하 되는 것을 방지한다.

가스 제한 취약점은 주로 스마트컨트랙트가 예상치 못한 방식으로 동작하거나, 비정상적인 트랜잭션을 발생시키는 것을 유도하는 과정에서 발생하는 취약점이다. 복잡한 연산을 수행하는 스마트컨트랙트에서 트랜잭션이 실행하면서 가스 한도를 초과하면, 그 시점에서 트랜잭션은 실패하고, 사용된 가스는 소모된 상태로 남는다. 이 상황에서 사용자는 가스를 지불했지만, 트랜잭션은 처리되지 않아 가스만 소모한 상태가 된다.

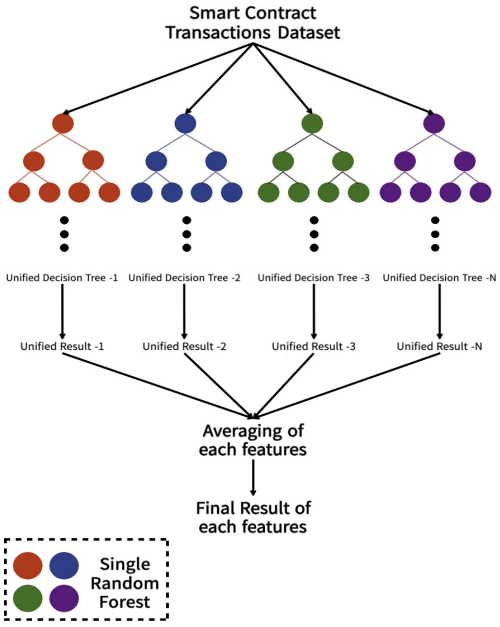
가스 제한 취약점으로 인해 공격자는 가스 한도를 악용하여 스마트컨트랙트가 정상적으로 작동하지 못하게 만들어 서비스 거부 공격을 일으킬 수 있다. 공격자가 매우 복잡한 트랜잭션을 발생하여 스마트컨트랙트가 해당 작업을 수행하도록 하고, 가스 한도를 초과하도록 설계된 데이터를 보내 블록체인 네트워크에 과부하를 주거나, 실행되지 못하게 유도할 수 있다. 이 과정에서 서비스 거부 공격을 이행할 수 있다.

또한, 비효율적인 가스 소모를 진행할 경우, 트랜잭션 가스 비용이 과도하게 높아진다. 공격자가 스마트컨트랙트에 반복적인 연산이나 무작위 조건문 실행, 데이터 저장 및 읽기 작업의 반복 등을 통해 사용자에게 지나치게 높은 가스 비용을 부담하게 하는 문제를 일으킬 수 있다[9-12].

2.4 Unified Random Forest

단일 랜덤 포레스트는 여러 개의 결정 트리(Decision Trees)를 조합하여 사용한다. 랜덤 포레스트는 높은 정확도와 과적합 방지, 다량의 데이터를 처리할 수 있다는 장점이 존재하지만, 이더리움 트랜잭션과 같이 다량의 데이터에서 특징을 추출하여 예측값을 도출하는 과정에서 일반적인 랜덤 포레스트로 처리하기에 상당한 무리가 있다고 생각한다. 하루 평균 발생하는 이더리움 트랜잭션 수는 평균 1백만 건에 해당하는데, 이를 단일 랜덤 포레스트로 실시간 학습 및 처리를 진행하는 것은 매우 많은 리소스와 시간을 소모하기 때문이다. 또한, 이더리움 트랜잭션에서 가스를 할당하는 특정 함수들만 특정하여 진행하기에 단일 랜덤 포레스트를 사용하여 처리하는 것은 어렵다. 따라서, 기존 랜덤 포레스트의 장점을 가져감과 동시에, 이더리움 스마트컨트랙트에서 효율적인 실시간 탐지를 위해 Unified Random Forest를 활용한다.

본 논문에서는 다수의 단일 랜덤 포레스트를 앙상블 모델로 하여 Unified Random Forest를 활용하려고 한다. 단일 랜덤 포레스트가 Unified Random Forest에서 하나의 결정트리로 활용하고, 이 과정에서 배깅(Bagging) 방식을 적용하여 과적합 방지와 성능 향상을 유도할 수 있다[13-15].



[Fig. 1] Unified Random Forest structure and procseeing

위 [Fig.1] 그림과 같이 Unified Random Forest 구조를 통해 효율적인 스마트컨트랙트 트랜잭션 실시간 탐지를 가능하게 한다.

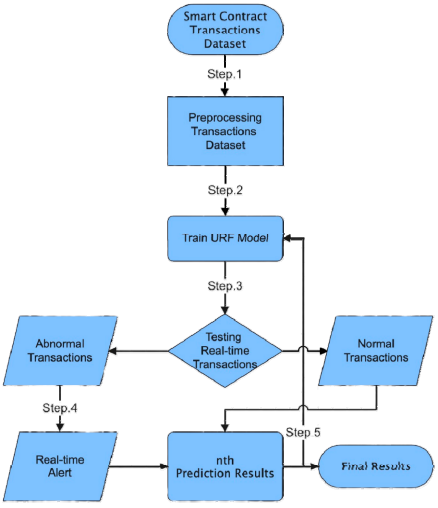
단일 랜덤 포레스트와 구조는 유사하지만, 각 노드에 하나의 랜덤 포레스트가 들어가 Unified Decision Tree를 이룬다. N개의 Unified Decision Tree들이 모

여 N개의 Unified Result를 도출하고, 이를 각각의 특징별 평균을 계산한다.

각각의 특징에는 스마트컨트랙트 트랜잭션에서 가스를 담당하는 함수들의 호출 빈도, 수정 빈도 등이 포함된다. 최종 결정 값은 이 특징들을 모두 고려하여 하나의 트랜잭션에서 발생하는 가스 함수들의 이상치를 판별한다.

3. Unified Random Forest를 활용한 가스 제한 취약점 탐지 과정

본 논문에서 제안하는 이더리움 스마트컨트랙트 가스 제한 취약점 실시간 탐지 과정은 다음과 같다.



[Fig. 2] Ethereum Smart Contract Gas Limitation Vulnerability Real-time detection algorithm using Unified Random Forest

다음은 [Fig. 2] 그림의 단계별 과정에 관해 설명한다.

Step.1 이더리움 스마트컨트랙트 트랜잭션 데이터셋을 수집하여, 트랜잭션에서 발생하는 스마트 컨트랙트 가스 함수 호출 빈도수, 가스 할당 한도, 가스 사용량 등의 특징을 추출하고, 전처리를 진행한다.

Step.2 전처리가 완료된 트랜잭션 데이터셋을 Unified Random Forest에서 학습을 진행한다. 이를 통해 다량의 트랜잭션 중에서 가스 한도 초과가 발생한 특정 트랜잭션을 파악하고, 이에 대한 패턴, 특징, 구조를 학습한다.

Step.3 학습된 Unified Random Forest 모델에 실시간 트랜잭션 데이터를 적용하여, 가스 사용량 예측값을 도출하고 초과 여부를 판별한다. 이때, 정상적 범주의 가스 한도인 경우와 비정상적 범주의 가스 한도를 판단하여 예측 결과값을 도출한다.

Step.4 실시간 예측값을 바탕으로 가스 한도 초과 가능성을 감지할 경우, 거래를 진행하고 있는 사용자에게 실시간 경고 메시지를 부여한다.

Step.5 실시간 예측값을 Unified Random Forest의 Unified 결정트리에 다시 데이터로 사용하여, 반복 학습을 진행하고 Unified Random Forest의 성능을 향상하게 시킨다.

이와 같은 다섯 단계를 통해 실시간 이더리움 스마트컨트랙트 트랜잭션에 대한 가스 제한 취약점을 탐지하고, 이를 사용자에게 즉각적으로 알릴 수 있다. 또한, 지속해서 실시간 트랜잭션 데이터를 Unified Random Forest에 학습 데이터로 다시 활용하면서, 데이터를 누적하며 학습함으로써 양과 질을 모두 챙길 수 있는 장점이 있다. 게다가, 이러한 반복 학습을 통해 Unified Random Forest의 성능은 증진하고, 과적합은 방지하며 오류를 최소화할 수 있다.

4. 결론

본 논문에서는 다수의 단일 랜덤 포레스트를 앙상블한 Unified Random Forest를 활용하여, 스마트컨트렉트에서 발생하는 가스 제한 취약점을 실시간으로 탐지하는 기법을 제안한다.

해당 기법을 통해 이더리움 스마트컨트랙트 트랜잭션에서 가스 제한 취약점으로 무분별한 사용자들의 가스 소모 피해를 방지하고, 이더리움 블록체인 네트워크의 혼잡도를 감소시킬 수 있다고 기대한다.

또한, 가스 제한 취약점을 탐지할 시, 해당 트랜잭션 거래자 혹은 사용자에게 즉시 해당 정보를 알리고, 이더리움 네트워크에 반영하여 해당 취약점에 대한 지속적인 예의 주시 및 피드백을 통해 사후 대응과 관리를 이행할 수 있다고 판단한다.

추후 심도 있는 추가 연구를 통해, 본 논문에서 제시한 기법에서 존재할 수 있는 실시간 트랜잭션 처리 과정에서의 결함점 및 하이퍼 파라미터 설정 등에 대하여 보완하고, 알고리즘 및 구동 과정의 고도화 작업을 이행할 것이다. 이더리움 테스트넷, 로컬 가상 네트워크 등을 활

용하여, 실제 이더리움 네트워크에서 해당 기법이 어떻게 작용하고, 처리되는지에 대하여 심화한 검증을 진행할 계획이다.

REFERENCES

[1] OWASP Foundation. OWASP Smart Contract Top 10. OWASP. Available online: https://owasp.org/www-project-smart-contract-top-10/

[2] J. -P. Schmitten, G. Augart and S. Hüsig, "Decentralized Blockchain Governance and Transaction Costs in Digital Transformation: The Case of the DAO Revisited," 2023 Portland International Conference on Management of Engineering and Technology (PICMET), Monterrey, Mexico, pp. 1-14, 2023.

[3] Ethereum Foundation. Ethereum Merge. Available online: https://ethereum.org/en/roadmap/merge/

[4] W. Chan and A. Olmsted, "Ethereum transaction graph analysis," 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, pp. 498-500, 2017.

[5] L. S. H. Colin, P. M. Mohan, J. Pan and P. L. K. Keong, "An Integrated Smart Contract Vulnerability Detection Tool Using Multi-Layer Perceptron on Real-Time Solidity Smart Contracts," in IEEE Access, vol. 12, pp. 23549-23567, 2024..

[6] D. He, Z. Deng, Y. Zhang, S. Chan, Y. Cheng and N. Guizani, "Smart Contract Vulnerability Analysis and Security Audit," in IEEE Network, vol. 34, no. 5, pp. 276-282, September/October 2020.

[7] R. Xie et al., "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System," in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 44-50, June 2020.

[8] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019.

[9] K. Kaur, S. Tomar and M. Tripathi, "Gas Fee Reduction by Detecting Loop Fusible Patterns in Ethereum Smart Contract," 2022 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Gandhinagar, Gujarat, India, pp. 458-463, 2022.

[10] B. D. Perera, N. S. W. Arachchige, M. K. N. T., M. P. S. Randunu, L. Rupasinghe and C. Liyanapathirana, "Optimizing Gas Fees for Cost-Effective E-voting Smart Contracts on the Ethereum Blockchain," 2023 5th International Conference on Advancements in Computing (ICAC), Colombo, Sri Lanka, pp. 7-11, 2023.

[11] F. Liu, X. Wang, Z. Li, J. Xu and Y. Gao, "Effective GasPrice Prediction for Carrying Out Economical Ethereum Transaction," 2019 6th International Conference on Dependable Systems and Their Applications (DSA), Harbin, China, pp. 329-334, 2020.

[12] A. M. Fajge, S. Goswami, A. Srivastava and R. Halder, "Wait or Reset Gas Price?: A Machine Learning-based Prediction Model for Ethereum Transactions' Waiting Time," 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, pp. 1153-1160, 2021.

[13] D. Jim Solomon Raja, R. Sriranjani, P. Arulmozhi and N. Hemavathi, "Unified Random Forest and Hybrid Bat Optimization Based Man-in-the-Middle Attack Detection in Advanced Metering Infrastructure," in IEEE Transactions on Instrumentation and Measurement, vol. 73, Art no. 2523812, pp. 1-12, 2024.

[14] D. Banerjee, N. Sharma, R. Chauhan, M. Singh and K. S. Gill, "Smart Disease Detection: Unifying CNNs and Random Forests for Accurate Pear Leaf Classification," 2024 3rd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2024.

[15] S. A. Roseline, A. D. Sasisri, S. Geetha and C. Balasubramanian, "Towards Efficient Malware Detection and Classification using Multilayered Random Forest Ensemble Technique," 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, pp. 1-6, 2019.

장 수 안(Su-An Jang) [준회원]

■ 2023년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
취약점 분석, 디지털 포렌식, 융합보안, 블록체인

이 근 호(Keun-Ho Lee) [종신회원]

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 기술전략팀 과장
- 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
융합보안, 블록체인, 개인정보보호, 이동통신 보안

윤 성 현(Sung-Hyun Yun) [종신회원]

- 1997년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 2002년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
블록체인 보안, 바이오메트릭 인증, DRM