EFFICIENT METHODS TO AVIOD SMART CONTRACT VULNERABILITIES USING BLOCKCHAIN

A project report submitted in partial fulfillment of the requirements for the award of the Degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

Submitted by

M. ANURADHA
Reg.No.17811A0531

N. S.S.S. AVANI
Regd.No.17811A0534

B. SIVANI
Regd.No.17811A0511

M. VENKATESH
Redg.No.17811A0529

S. VARA PRASAD
Regd.No.17811A0522

Under the guidance of

Mr. K. VARA PRASAD, M. Tech
Assistant professor

Department of Computer Science and Engineering

AVANTHI INSTITUTE OF ENGINEERING &TECHNOLOGY
(Approved by AICTE, New Delhi & Permanently affiliated to JNTU Kakinada)
(Accredited by NAAC, UGC & NBA, AICTE)
MAKAVARAPALEM, NARSIPATNAM,
VISAKHAPATNAM-531113
(2017-2021)

AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY
(Approved by AICTE, New Delhi & Permanently affiliated to JNTU Kakinada)
(Accredited by NAAC, UGC & NBA, AICTE)
MAKAVARAPALEM, NARSIPATNAM,
VISAKHAPATNAM-531113

CERTIFICATE

This is to certify that the project entitled "EFFICIENT METHODS TO AVOID SMART CONTRACT VULNERABILITIES USING BLOCKCHAIN" in partial fulfillment for the of degree of Bachelor of Technology in COMPUTER SCIENCE AND ENGINEERING, at AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, MAKAVARAPALEM, VISAKHAPATNAM is an bonafied work carried out by M. ANURADHA (17811A0531), N. S.S.S. AVANI (17811A0534), B. SIVANI (17811A0511), M. VENKATESH (17811A0529), S. VARA PRASAD (17811A0522) under the guidance and supervision during 2020-2021.

(K. VARA PRASAD)
Project Guide

(U. NANAJI)
Head of the Department

External Examiner

Scanned with CamScanner

ABSTRACT

Ethereum smart contracts are programs which will run inside public distributed network called block chain. These smart contracts are used to perform operation over ether i.e transfer. receiving across the blockchain, by public to manage their accounts. These smart contracts are immutable once deployed on blockchain. So, developers need to make sure that smart contracts are bug-free at the time of deployment. As we are developing supply chain management (SCM) for textile industry project, to protect the project from smart contract vulnerabilities. In this paper we have analyzed the Decentralized Autonomous organization i.e DAO attack, which takes the advantage of smart contract vulnerability. Some functions are exposed to access by external contracts. The attacker makes use of vulnerability in smart contract and he can implement code to recursively call the function to transfer the funds in to his own account. And also we analyzed Reentrancy attack, which also used by attacker to recursively call the contract to multiple transfers of funds to his own account. And finally we analyzed Underflow attack, which make use of vulnerability in smart contract while transferring ethers between the users without considering limitations of integers values.