DAYANANDA SAGAR UNIVERSITY

KUDLU GATE, BANGALORE – 560068

SCHOOL OF ENGINEERING

Bachelor of Technology
in
COMPUTER SCIENCE AND ENGINEERING

Project Phase I

Project Proposal
on

(AI/ML Based Hardware Security For Edge Devices In IOT)

By

Sourabh J Gor - ENG21CS0411
Sri Vishnavi Ananya Gollapalli - ENG21CS0414
N Rishi Rohan - ENG21CS0256
Tejas B – ENG21CS0446

Batch no - **97**

Under the supervision of
Mr. Vishwas D B, Prof, CSE

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,
SCHOOL OF ENGINEERING
DAYANANDA SAGAR UNIVERSITY,

(2024-2025)

Project Summary

With the rapid expansion of the Internet of Things (IoT) and the proliferation of interconnected devices, ensuring secure and efficient hardware-level security has become critical. Traditional software-based security approaches are increasingly inadequate in preventing hardware attacks, counterfeiting, and unauthorized access to IoT devices. This paper aims to address these challenges by implementing and evaluating Physical Unclonable Functions (PUFs), specifically Ring Oscillator (RO-PUF) and Arbiter PUF, for generating unique and secure hardware identifiers and encryption keys, while analyzing their effectiveness and efficiency in real-world IoT applications.

Verified By:

Guide Name: Prof. Vishwas D B

Date:

Signature:

1. Introduction

The Internet of Things (IoT) has revolutionized various industries, connecting millions of devices and creating smart environments. However, as IoT devices become widespread, they are increasingly susceptible to security threats such as unauthorized access, data breaches, and counterfeiting. Traditional software-based solutions are not sufficient to secure these low-power devices, necessitating a shift towards hardware-based security measures. Physical Unclonable Functions (PUFs) are emerging as an effective hardware security solution, providing unique device identification and encryption key generation based on intrinsic manufacturing variations. This paper explores the implementation and evaluation of PUFs, specifically Ring Oscillator (RO-PUF) and Arbiter PUF, to enhance security in IoT devices.

2. Problem Definition

As IoT devices become integral in various applications, their security remains a critical concern. Current software-based security techniques are vulnerable to attacks such as side-channel attacks and physical tampering, compromising data integrity and device authentication. Additionally, counterfeit and cloned devices pose significant risks, undermining supply chain integrity and intellectual property rights. The challenge is to develop a secure, efficient, and unclonable hardware-based solution that can provide robust security for IoT devices without significantly increasing power consumption or cost.

3. Objectives

- To design and implement a hardware-based security mechanism using PUFs to generate unique and secure identifiers for IoT devices.
- To evaluate and compare two types of PUFs, namely Ring Oscillator (RO-PUF) and Arbiter PUF, in terms of their security, performance, and efficiency.
- To demonstrate how PUFs can be used to protect against counterfeiting, cloning, and unauthorized access in IoT applications.
- To analyze the reliability, uniqueness, and unpredictability of PUF outputs under varying environmental conditions such as temperature and voltage variations.

4. Scope of the project

- The project focuses on developing hardware security mechanisms suitable for IoT devices, emphasizing the implementation and evaluation of PUFs.
- The scope includes designing PUF circuits, generating challenge-response pairs (CRPs), and testing the performance of PUFs in providing secure hardware-based identifiers.
- The analysis covers key parameters such as uniqueness, reliability, and unpredictability of the PUFs.
- The project does not delve into software security techniques or integration with larger software security frameworks, as it focuses solely on hardware-level security for IoT devices.

5. Functional Requirements

- The system must be capable of generating unique hardware-based identifiers for each IoT device using PUFs.
- The PUFs should produce different outputs for each device to ensure uniqueness.
- The PUFs should generate consistent outputs for the same device when the same challenge is applied, ensuring reliability.
- The system must support cryptographic operations, such as generating encryption keys based on PUF outputs.
- The system should provide countermeasures against cloning and counterfeiting of IoT devices.

6. Non-Functional Requirements

- Scalability: The hardware security mechanism should be scalable to accommodate a wide range of IoT devices with varying power and resource constraints.
- Energy Efficiency: The PUF implementation must consume minimal power to be suitable for low-power IoT devices.
- Reliability: The system should perform consistently under different environmental conditions, including variations in temperature and voltage.
- Security: The generated identifiers and keys must be highly secure, ensuring that they cannot be predicted or cloned by attackers.
- Ease of Integration: The hardware design should be compatible with various IoT platforms for seamless integration.

7. Software/System Requirements

- Hardware Design Software: Xilinx Vivado (or any suitable tool) for designing and simulating PUF circuits.
- Development Environment: Tools supporting Hardware Description Languages (HDLs) like VHDL or Verilog for PUF design.
- Testing and Evaluation Tools: Simulation software for verifying the reliability, uniqueness, and unpredictability of PUF designs.
- Operating Environment: The system should be tested and deployed in environments representative of real-world IoT applications, such as home automation, industrial monitoring, and smart cities.