Design and Simulation of a Secure Enterprise IoT Network Using Cisco Packet Tracer with a Federated Learning-Based Secure Method.

H.M.G.G.Dammika Sumanadeera
（Reg. No.: MS24021098）

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

December 2025

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Pradeep Abeygunawardhana

Approved for MSc. Research Project:

MSc in IT Programme Co-ordinator, SLIIT

Approved for MSc:

Head of Graduate Studies, FoC, SLIIT

DECLARATION

This is to certify that the work is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Sign: 

H.M.G.G.Dammika Sumanadeera

Date: 05/01/2026

Design and Simulation of a Secure Enterprise IoT Network Using Cisco Packet Tracer with a Federated Learning-Based Secure Method.

H.M.G.G.Dammika Sumanadeera

MSc. in Information Technology

Supervisor: Prof. Pradeep Abeygunawardhana

December 2025

ABSTRACT

The rapid growth of the Internet of Things (IoT) in businesses has led to major security issues, with botnet attacks being a serious threat. Although Federated Learning (FL) provides a way to detect threats while preserving privacy, it is still vulnerable to data poisoning from harmful devices. Current blockchain solutions for securing FL are often too heavy on resources for widespread use in IoT. This paper offers a two-part integrated approach. First, an enterprise IoT network was designed and simulated securely using a prototype with Cisco Packet Tracer. Second, a new lightweight novel FL framework was developed that did not rely on blockchain, using the N-BaIoT dataset to protect against botnet attacks. The paper proposed Reputation-Weighted Coordinate Median with Update Validity Tests (RWCM+UVT) framework incorporates a reputation-based system, a robust aggregation algorithm, and an adaptive update validation gate. By simulating botnet attacks within this controlled environment, this paper demonstrates that the RWCM+UVT framework effectively identifies and mitigates the impact of malicious devices, achieving near-perfect detection accuracy without the prohibitive overhead of blockchain technology.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to the Sri Lanka Institute of Information Technology (SLIIT) for providing me with the opportunity and resources to carry out this research.

My sincere thanks go to Prof. Pradeep Abeygunawardhana, whose invaluable supervision, constructive feedback, and continuous encouragement guided me throughout the course of this project. His insightful advice, critical review of my ideas and writing, as well as his generous support through resources and academic freedom, were instrumental in the successful completion of this research.

I would also like to extend my appreciation to the guidance panel members for their valuable comments and support, to the MSc course coordination members for their guidance and assistance, and to SLIIT for fostering a collaborative and supportive academic environment that made this research possible.

TABLE OF CONTENTS

List of Figures

List of Tables