ADVANCING RANSOMWARE DETECTION SYSTEM USING MACHINE LEARNING

G.A.A.I.S De Silva
Reg. No: MS24034036

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

(CYBER SECURITY)

September 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.

_____

Dr. Harinda Fernando

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is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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: …….....

GAAIS DE SILVA

Date: ……04/11/2025……..

ABSTRACT

G.A.A.I.S De Silva

MSc. in Information Technology Cyebr Security

Supervisor: Dr. Harinda Fernando

December 2025

Ransomware attacks pose a significant and evolving threat to data security and operational integrity, necessitating advanced detection mechanisms. This project aims to develop an effective ransomware detection system leveraging machine learning techniques, specifically Recurrent Neural Networks (RNN) and auto encoders, to analyze network traffic for anomalies indicative of ransomware activity. Utilizing the UNSW-NB15 datasets, we undertook extensive data preprocessing, including handling missing values and normalizing features, to prepare the datasets for training. The model employs Long Short-Term Memory (LSTM) layers to capture temporal dependencies and patterns within the network traffic data. The training and validation processes focused on normal traffic data to establish a baseline for detecting deviations caused by ransomware. Our results demonstrate high accuracy in distinguishing between normal and ransomware-infected traffic, with a clear ability to identify potential threats in real-time. This innovative approach showcases the potential of RNN-based auto encoders in enhancing cyber security measures. The conclusion emphasizes the system's effectiveness in providing early warnings of ransomware attacks, thereby significantly aiding in the protection of valuable data assets and maintaining operational continuity.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to my research supervisor, **Dr. Harinda Fernando**, for her invaluable guidance, patience, and support throughout my research journey. Her expertise and insightful feedback have been instrumental in shaping this work.

I am also grateful to the **Sri Lankan Institute of Information Technology** for providing me with the necessary resources to carry out my research.

TABLE OF CONTENTS

List of Figures

List of Tables