# EFFECTIVENESS OF CURRENT LINUX OS SECURITY MECHANISMS AGAINST RANSOMWARE ACTIVITIES

**J.A Nipuna Sandes Perera**

A dissertation submitted in partial fulfilment of the requirements for the
Master of Science degree in Cyber Security and Forensics

**Department of Computing**
**Informatics Institute of Technology, Sri Lanka**
**in Collaboration with**
**University of Westminster, UK**

**2021**

# Abstract

This project is primarily aimed at examining whether the existing Linux security mechanisms are adequate to mitigate or minimize the impact of ransomware activities. Linux is one of the main operating systems that is used to run the product workloads of various small to large business applications. Ransomware makers have now significantly increased their targeting of Linux-based operating systems. This is a very problematic situation affecting cybersecurity mechanisms. It has therefore become impossible to rely solely on peripheral security mechanisms. When those security mechanisms are bypassed, ransomware can have some space to infiltrate the operating system and carry out destructive activities internally. This thesis describes the procedure for exploring the effectiveness of existing security mechanisms in Linux against ransomware activity to prevent such spaces.

In order to find out whether the existing security mechanisms in Linux are effective against ransomware activities, first researched the literature to gather information, developed a questionnaire based on that information and sent it to the domain experts and the industry experts to gather their opinions and suggestions. Based on all the information gathered in the above-mentioned steps, several experiments were designed and carried out using a POC ransomware and a well-known Linux operating system. Based on all the facts collected via the above-mentioned strategies, the final result was described. Entire followed procedures and collected facts related to this work can be found in this thesis.

**Keywords: -** Linux, Ransomware, Linux Security Mechanisms, Linux Ransomware, Operating system security, Linux server hardening