Project registration form

Course: BSc (Hons) in Cyber Security & Digital Forensics (TOP UP) – Kingston University (UK) – ESOFT Metro Campus

Student Name: Wanni Arachchige Nayana Anjana Shakthi Monarawila
Esoft ID Number: E175022

Project Title: AI-Powered Ransomware Early Detection System

Overview: (350 words max)

Ransomware has become one of the most serious online threats that can impact people, companies, and governmental organizations globally. It encrypts victims' data and demands ransom payments to unlock it, frequently leading to large losses in terms of money and reputation. Attackers are constantly changing their methods to avoid detection, therefore traditional antivirus software and signature-based protection solutions are insufficient in identifying newly created or altered ransomware strains. This drawback emphasizes how urgently an intelligent, proactive detection system that can spot possible ransomware activity before encryption starts is needed.

In order to solve this issue, the AI-Powered Ransomware Early Detection System project integrates machine learning (ML) and artificial intelligence (AI) technologies to anticipate and stop ransomware assaults in real time. To find anomalies that point to ransomware activity, the system will examine network traffic data, file activity patterns, and system behavior. This system will use dynamic behaviour analysis instead of static signatures, which will make it more resistant to polymorphic and zero-day assaults than traditional detection techniques.

The idea is to train machine learning models like Random Forest or Neural Networks using data from both real-world system operations and ransomware attack simulations. Features such as file encryption rates, system call frequency, and unusual resource utilization will be used by these models to learn to differentiate between malicious and legitimate activities. To avoid data loss, the system will immediately stop questionable processes or send out notifications

when it has been taught to monitor events in real time.

By providing quicker, more precise, and more flexible ransomware detection, this study seeks to illustrate how AI can improve cybersecurity defenses. Finally, by offering a novel approach to proactive cyber threat avoidance, the system will help to enhance digital safety in both personal computers and business networks.

Aims and Objectives: (About 100 words)

Aim

To develop an AI-powered early detection system capable of identifying and preventing ransomware attacks before encryption begins.

Objectives

- To analyze current limitations in ransomware detection techniques.
- To collect and preprocess datasets of ransomware and normal behavior.
- To design and train a machine learning model for ransomware detection.
- To evaluate the model's accuracy, precision, and detection speed.
- To implement a real-time alert or auto-prevention mechanism using AI.

Supervisor's Name: . M. S. Ranawake

(continues overleaf)

Member of staff only

The above project topic is approved and I agree to supervise this project.

…….. ……..

Supervisor's Signature *Date*

Remarks :