

FACULTY OF COMPUTER SCIENCE & INFORMATION COMPUTING TECHNOLOGY

DEPARTMENT OF INFORMATION COMPUTING TECHNOLOGY

PROJECT PROPOSAL

**RANSOMWARE DETECTION AND**

**PREVENTION SYSTEM**

SEE YONG JUN

2290017-DCS

Report submitted in partial fulfilment of the requirements for

DIPLOMA IN COMPUTER SCIENCE

MAY 2024

TABLE OF CONTENTS

[**ABSTRACT** 2](#_Toc168835875)

[1.0 INTRODUCTION 3](#_Toc168835876)

[2.0 PROBLEM STATEMENT 4](#_Toc168835877)

[3.0 OBJECTIVES 5](#_Toc168835878)

[4.0 SCOPE 5](#_Toc168835879)

[5.0 JUSTIFICATION 5](#_Toc168835880)

[6.0 METHODOLOGY 5](#_Toc168835881)

[7.0 TIMELINE 6](#_Toc168835882)

[8.0 REFERENCES 7](#_Toc168835883)

# **ABSTRACT**

Information security is seriously threatened by the increase in ransomware attacks, which makes the creation of strong detection and prevention systems necessary. The goal of this research is to use advanced monitoring techniques and machine learning to develop an efficient system for ransomware detection and prevention. Python is used in the VS Code environment to construct the system, which uses file monitoring tools and APIs (such Windows' pywin32) to keep track of questionable activity. Utilizing machine learning tools such as TensorFlow and Scikit-learn, prediction models that can recognize ransomware activity are constructed. The system interfaces with backup software and APIs for automated data backup and recovery in order to guarantee data protection. Additionally, a web-based alerting dashboard is implemented using Flask/Django to provide real-time notifications and management of potential threats. This comprehensive approach aims to mitigate the risks associated with ransomware attacks, ensuring the integrity and availability of critical data.

# 1.0 INTRODUCTION

In recent years, ransomware attacks have become one of the most common and destructive types of cyberthreats. Malicious software is used in these attacks to encrypt victims' data, making them unreadable until a ransom is paid. Effective detection and prevention measures are critically needed, as evidenced by the attacks' growing sophistication and frequency.

The goal of this project is to create a thorough system for detecting and preventing ransomware in order to guard against the devastating effects of these kinds of online threats. The suggested system offers a multi-layered protection mechanism by utilizing a mix of file monitoring tools, backup solutions, and machine learning algorithms.

The main development tool is Python, a strong and flexible programming language, and the project is being worked on in the Visual Studio Code (VS Code) environment. File system activity is constantly monitored by file monitoring programs and APIs, such Windows' pywin32, to identify any unusual behavior suggestive of ransomware. Models that can precisely recognize ransomware patterns and behaviors are created and trained using machine learning frameworks, such as TensorFlow and Scikit-learn.

The solution connects with backup software and APIs to further improve data security by enabling automated data backup and recovery in the case of an attack. Furthermore, Flask/Django is used to create a web-based alerting dashboard that offers real-time warnings and facilitates effective management and threat response.

The goal of this research is to develop a strong and efficient ransomware detection and prevention system by integrating various technologies and approaches. Protecting vital data from the constantly changing threat landscape while maintaining its availability and integrity is the ultimate objective.

# 2.0 PROBLEM STATEMENT

Ransomware attacks have become a formidable and escalating threat, jeopardizing the integrity, confidentiality, and availability of digital data across diverse sectors. These attacks typically involve the encryption of files by malicious software, demanding a ransom for the decryption key. The escalating sophistication and widespread impact of ransomware highlight the critical need for advanced detection and prevention strategies.

Traditional antivirus and security solutions often struggle to promptly detect and mitigate ransomware attacks due to their dependence on signature-based detection methods, which fall short against novel and evolving threats. The lack of real-time monitoring and rapid response capabilities further exacerbates systems' vulnerability to ransomware.

The primary challenge lies in creating a system that can detect ransomware activity at its nascent stage and prevent substantial damage. This necessitates a solution that not only monitors file system activities but also utilizes advanced machine learning techniques to identify suspicious behavior patterns indicative of ransomware. Additionally, there is a need for a robust backup and recovery system to restore data in the event of an attack, minimizing downtime and data loss.

This project aims to address these challenges by developing a comprehensive ransomware detection and prevention system. The system will be developed using Python, incorporating file monitoring tools/APIs such as pywin32 for continuous surveillance. Machine learning libraries like Scikit-learn and TensorFlow will be employed to create predictive models capable of identifying ransomware activities. An integrated backup solution will ensure data protection and recovery, while a Flask/Django-based alerting dashboard will provide real-time threat notifications and management capabilities.

# 3.0 OBJECTIVES

1. Develop a system to monitor and analyze file activities.
2. Implement behavioral analysis to detect ransomware patterns.
3. Provide real-time alerts and response mechanisms.
4. Integrate backup and recovery solutions to mitigate the impact of attacks.

# 4.0 SCOPE

In order to guarantee real-time threat identification and automated data recovery, the project scope entails building a thorough ransomware detection and prevention system using Python, machine learning models, and file monitoring tools. In order to assure successful deployment and maintenance, a web-based dashboard will also offer real-time alerts and system management capabilities. This dashboard will be backed by comprehensive testing, documentation, and user training.

# 5.0 JUSTIFICATION

The increasing frequency and sophistication of ransomware attacks pose a significant threat to organizations, causing substantial financial losses, data breaches, and operational disruptions. Traditional security measures, primarily reliant on signature-based detection, often fail to identify and mitigate these evolving threats effectively. This project aims to address these shortcomings by integrating advanced machine learning techniques and real-time file monitoring to provide a proactive and robust defense against ransomware. By ensuring early detection and automated data recovery, the project seeks to minimize the impact of ransomware attacks, safeguard critical data, and enhance overall cybersecurity resilience, thus justifying the need for a comprehensive and modern approach to ransomware protection.

# 6.0 METHODOLOGY

|  |  |
| --- | --- |
| **Methodology** | **Descriptions** |
| Design System | Plan how the system works, including how will they interact. |
| Choose Tools | Select which software used to develop the system. |
| Develop Detection Methods | Create ways to identify ransomware, like using machine learning to recognize suspicious behavior. |
| Integrate Monitoring Tools | Implement tools to monitoring changes of ransomware activities. |
| Implement Backup | Set up a system to back up important files to protect them from ransomware attacks. |
| Create Alert System | Build a way to alert users if ransomware is detected, like a dashboard that shows warnings. |
| Testing | Test thoroughly whether system works as expected in different situations. |
| Deployment | Deploy in a real case environment. |
| Maintenance and Update | Collect feedback, then improve system and ensure is up to date. |
| Monitoring and Improvement | Monitor how the system works and make it better over time. |

# 7.0 TIMELINE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Weeks / Milestones | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| Project Planning and Requirements Gathering | **✓** | **✓** |  |  |  |  |  |  |  |  |  |  |  |  |
| Design Architecture and Choose Technologies |  |  | **✓** | **✓** |  |  |  |  |  |  |  |  |  |  |
| Develop Detection Algorithms and Integrate Monitoring Tools |  |  |  |  | **✓** | **✓** |  |  |  |  |  |  |  |  |
| Implement Backup Mechanism and Create Alerting Dashboard |  |  |  |  |  |  | **✓** | **✓** |  |  |  |  |  |  |
| Testing and Debugging |  |  |  |  |  |  |  |  | **✓** | **✓** |  |  |  |  |
| Deployment |  |  |  |  |  |  |  |  |  |  | **✓** | **✓** |  |  |
| Maintenance and Monitoring |  |  |  |  |  |  |  |  |  |  |  |  | **✓** | **✓** |

# 8.0 REFERENCES

1. Sophos. (2021). \*The state of ransomware 2021\*. Retrieved from https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

2. Verizon. (2022). \*2022 data breach investigations report\*. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

3. Gartner. (2020). Gartner forecasts worldwide security and risk management spending to grow 6.4% in 2020. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-06-03-gartner-forecasts-worldwide-security-and-risk-managem

4. McAfee. (2020). \*McAfee Labs threats report: August 2020\*. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2020.pdf

5. IBM. (2021). \*Cost of a data breach report 2021\*. Retrieved from https://www.ibm.com/security/data-breach