# **Department of Computer Science Batch: [2025]**

**Proposal Form for Final Year Project**

**Title:**  
Antivirus: AI based Threat Detection

**Domain(s):**   
  
**Nature of Project (Select all that apply):**

Power Electronics

Machine Learning

Others:

Cybersecurity

* New Project
* Extension of Existing Project
* Industrial Collaboration
* Funded
* Collaboration with Other Departments / Academic Institutions

**Collaboration Name (if any):** [Name/N/A]

**Brief Outline:**

This project aims to develop a lightweight antivirus tool for Windows that operates entirely offline. It combines traditional signature-based malware detection with AI-assisted behavioural analysis to identify both known and suspicious threats. The tool allows users to scan directories, receive real-time alerts, and take action by quarantining or removing malicious files. Designed with modularity, transparency, and future extensibility in mind, the system serves as an open-source solution that addresses the limitations of commercial antivirus software while remaining accessible for learners and developers alike.

**Objectives:**

* To develop a lightweight and offline antivirus tool tailored for Windows systems.
* To implement signature-based scanning for detecting known malwares.
* To integrate an AI-assisted module for identifying suspicious files through behavioural patterns.
* To provide core threat response features such as user Real time alerts, quarantine, and secure removal.
* To ensure the system remains modular, transparent, and easily extensible for future enhancements.

**Scope:**

This project focuses on building a lightweight antivirus tool for Windows that operates entirely offline. The system includes core functionalities such as directory-based file scanning, signature-based malware detection, and AI-assisted behavioural analysis for suspicious files. It enables users to review, quarantine, or remove detected threats, and maintains detailed local logs for each scan. The project scope is limited to single-device usage with no cloud connectivity, prioritizing modularity, transparency, and foundational threat detection features.

**Proposed Methodology:**

The development will follow a modular, component-based approach. The system is divided into independent modules including File Scanner, Signature Matcher, AI Classifier, Logger, Real-Time Alert Manager, and Threat Handler (quarantine/removal). Development will begin with core file scanning and signature-based detection, followed by integration of a lightweight, AI model for behavioural analysis of suspicious files. The system will be implemented in C, tested on Windows, and designed to support future enhancements.

**Resources Involved:**

**Software & Tools:**

* GCC Compiler (MinGW)
* Visual Studio Code (development environment)
* Git (for version control)

**Libraries & Frameworks:**

* Standard C Library (libc, I/O, etc) – for memory, strings, file handling and directory traversal.
* OpenSSL – for hash compute.
* libcsv – for reading/writing CSV scan logs
* FANN – For light weight AI logic

**Human Resources:**

* Three team members collaboratively working on scanning, detection logic, AI integration, and reporting
* Supervisor (Review, Guidance)

**Hardware:**

* Standard PC/Laptop System (Windows)

**Final Outcomes / Deliverables:**

1. A fully functional offline antivirus tool for Windows with modular components
2. Signature-based detection system using hash, string, regex comparison
3. AI-assisted classification module for behavioral threat analysis
4. Logging system for scan results, alerts, and user actions (CSV format)
5. Quarantine and malware removal capabilities with user confirmation
6. Complete project documentation including use cases, diagrams, and source code

**Learning Outcomes:**

1. Practical experience in modular system design and malware detection techniques
2. Application of both signature-based and AI-assisted methods for real-world file analysis
3. Learned to manage file I/O, and directory traversal in C.
4. Understood how to log, alert, and safely manage potentially harmful files
5. Strengthened documentation, presentation, and software engineering practices

**Industrial Support (If any):**

[Details/N/A]

**FYDPD to Sustainable Development Goals (SDGs) Mapping**

|  |  |  |
| --- | --- | --- |
| SGDs | Mapping | Description |
| SDG 01. No poverty |  |  |
| SDG 02. Zero hunger |  |  |
| SDG 03. Good health and well-being |  |  |
| SDG 04. Quality education |  | Encourages open-source learning and hands-on application of cybersecurity. |
| SDG 05. Gender equality |  |  |
| SDG 06. Clean water and sanitation |  |  |
| SDG 07. Affordable and clean energy |  |  |
| SDG 08. Decent work and economic growth |  | Promotes practical digital skills and supports IT sector upskilling. |
| SDG 09. Industry, innovation, and infrastructure |  | Supports innovation in malware detection through AI-enhanced solutions. |
| SDG 10. Reduced inequalities |  |  |
| SDG 11. Sustainable cities and communities |  |  |
| SDG 12. Responsible consumption and production |  |  |
| SDG 13. Climate action |  |  |
| SDG 14. Life below water |  |  |
| SDG 15. Life on land |  |  |
| SDG 16. Peace, justice and strong institutions |  |  |
| SDG 17. Partnerships for the goals |  |  |

**FYDPD to Complex Computing Problem (CCP) Mapping**

|  |  |  |
| --- | --- | --- |
| **CCP Attribute** | **Mapped WP** | **How Addressed in FYDPD** |
| Depth of knowledge required | WP1 | Requires understanding of malware behaviour, hashing, string or regex algorithms, C system calls, and safe file handling. |
| Range of conflicting requirements | WP2 | Balances accuracy, performance, offline operation, usability, and system safety. |
| Depth of analysis required | WP3 | Involves detailed implementation of pattern matching, file classification. |
| Familiarity of issues | WP4 | Tackles challenges in malware detection and limitations of free antivirus solutions. |
| Extent of applicable codes | WP5 | Implemented in C using file I/O, directory traversal, and secure memory handling. |
| Stakeholder involvement & conflicting requirements | WP6 | Addresses user expectations (simplicity, reliability) and aligns with academic guidance and feedback. |
| Interdependence (many sub-parts) | WP7 | Combines multiple modules: scanner, matcher, classifier, logger, alert, quarantine, and removal logic. |

**Gantt Chart**

**Year:** 2025 to 2026

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Week** | **Task** | **Start Date** | **End Date** | **Duration** |
| Week 1 | Initial Setup & Literature Review | 2025-10-13 | 2025-10-19 | 7 Days |
| Week 2 | Scanner Module Development | 2025-10-20 | 2025-10-26 | 7 Days |
| Week 3 | Signature-Based Pattern Matching | 2025-10-27 | 2025-11-02 | 7 Days |
| Week 4 | Signature Database & Updater | 2025-11-03 | 2025-11-09 | 7 Days |
| Week 5 | AI Setup & Dataset Preparation | 2025-11-10 | 2025-11-16 | 7 Days |
| Week 6 | AI Model Training & Evaluation | 2025-11-17 | 2025-11-23 | 7 Days |
| Week 7 | AI Integration & Testing | 2025-11-24 | 2025-11-30 | 7 Days |
| Week 8 | Logging Mechanism Implementation | 2025-12-01 | 2025-12-07 | 7 Days |
| Week 9 | Real-Time Scanning Feature | 2025-12-08 | 2025-12-14 | 7 Days |
| Week 10 | Quarantine & Removal Feature | 2025-12-15 | 2025-12-21 | 7 Days |
| Week 11 | GUI Design & Prototyping | 2025-12-22 | 2025-12-28 | 7 Days |
| Week 12 | GUI Implementation & Integration | 2025-12-29 | 2026-01-04 | 7 Days |
| Week 13 | Testing & Debugging Phase | 2026-01-05 | 2026-01-11 | 7 Days |
| Week 14 | Prototype Finalization & Submission | 2026-01-12 | 2026-01-18 | 7 Days |

**Details of Project Team**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Name of Student** | **IU Reg. No.** | **CGPA** | **Signature** |
| 1 | Muhammad Usman | IU05-0122-0303 | 3.02 |  |
| 3 | Syed Muhammad Daniyal | IU05-0122-0497 | 2.4 |  |
| 2 | Bin Yameen | IU05-0122-0468 | 2.03 |  |

**Details of Supervisor(s) / Industrial Advisor**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Name** | **Designation & Department** | **Contact No.** | **Signature** |
| Supervisor | Dr. Muhammad Naveed | Faculty Member | (+92) 333 2422649 |  |

# **For Office Use Only**

☐ Proposal Approved   ☐ Not Approved   ☐ Returned for Clarification / Modification

**Comments (if any):**

**Project Serial No.:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Name** | **Signature** |
| FYDP Coordinator |  |
| Chairperson |  |
| Associate Dean/Dean |  |