SRINIVAS UNIVERSITY
INSTITUTE OF ENGINEERING AND TECHNOLOGY
Department of CYBER SECURITY AND CYBER FORENSICS

GUIDE CONSENT FORM

B. Tech (CS&CF) – Major Project 2025-26

Name of the Guide	Prof. Vyshak R	**Department**	Cybersecurity
Mobile Number	93503 28819	**Email ID**	
Name of the Mentor (Industry) *	Prof.Vyshak R		
Name and Address of the Company *	Srinivas University, Mukka, Surathkal		
Mobile Number *	9350328819		
Email ID *			

***** *Mention NA if not applicable*

Student Information:

Register No.	Name of the Student	Mobile No.	Email ID
01SU22CF009	REGAN ELSTON TEMUDO	9371919768	regan.iet@srinivasuniversity.edu.in
01SU22CF010	SHASHANK M B	9113534166	shashankmb.iet@srinivasuniversity.edu.in
01SU22CF011	SHRAVAN KUMAR UK	8088593127	shravanuk.iet@srinivasuniversity.edu.in
01SU22CF015	VARAD MILIND BORADE	8779295486	varadb.iet@srinivasuniversity.edu.in

CampusNix

Abstract:

CampusNix is a secure, Ubuntu-based operating system designed specifically for conducting proctored academic examinations in a controlled environment. The system enforces strict lockdown measures on hardware, software, and network activity to prevent cheating. It integrates open-source security frameworks such as USBGuard for USB device control, AppArmor for application lockdown, and AdGuard Home for DNS-based content filtering. Clipboard functions and web browsers are disabled, ensuring students cannot copy, paste, or browse unauthorized content. Real-time monitoring is achieved using Veyon, allowing faculty to view student screens throughout the examination. Additionally, CampusNix features an automated file-backup and encryption system that safeguards deleted files for faculty review. Logs and backups are secured using AES-256 encryption to maintain confidentiality. By combining these modules, CampusNix establishes a zero-trust exam environment that is transparent, tamper-proof, and adaptable for academic institutions.

Project Overview:

CampusNix aims to create a hardened Linux-based operating system that guarantees exam integrity by locking down system resources during tests. The OS transforms ordinary computers into secure exam workstations where only authorized software and hardware are accessible. Through integrated monitoring, content filtering, and encryption mechanisms, it ensures a safe and fair testing environment. The project leverages open-source tools and frameworks to achieve robust system control without reliance on proprietary software, enabling universities to deploy it efficiently on a large scale.

Objectives:

Objective 1: Develop a secure Ubuntu-based operating system that enforces a strict lockdown during examination mode, restricting all unauthorized applications, USB devices, and network traffic.
Objective 2: Enable real-time monitoring of student desktops through faculty-controlled interfaces to detect and prevent suspicious activity.
Objective 3: Automate secure file backup and logging systems that preserve deleted files and audit data using AES-256 encryption.
Objective 4: Integrate DNS-level content filtering and clipboard blocking mechanisms to prevent data exfiltration or communication during exams.
Objective 5: Provide a modular, open-source, and easily deployable system adaptable for academic institutions conducting digital assessments.

Scope:

CampusNix focuses on providing a secure, controlled computing environment for students during computer-based or online exams. The system limits access to unauthorized devices, applications, and websites, while enabling faculty oversight. It operates solely within the exam environment and is intended for deployment in institutional labs or approved student devices. The project's scope does not include remote proctoring or securing non-exam applications.

Methodology:

The project is implemented using open-source components integrated within a customized Ubuntu distribution. USBGuard is employed for device authorization and USB control, while AppArmor and shell scripts enforce process-level restrictions. The Veyon framework enables instructor-side monitoring of student screens. Clipboard control is achieved by disabling X server clipboard access, and DNS-based filtering is implemented via AdGuard Home. Python scripts using pyudev monitor hardware events, and inotify-tools provide file event monitoring for backup and encryption using OpenSSL's AES-256 utility. The ISO image is built using Ubuntu live-build tools, and the overall system follows an Agile development process to iteratively test and refine lockdown mechanisms.

Expected Outcomes:

1. **Secure Exam Environment:** A fully operational Ubuntu-based OS image that automatically enforces lockdown features and prevents unauthorized access during examinations.
2. **Reduced Cheating Incidents:** Prevention of digital cheating through device, application, and network restrictions.
3. **Enhanced Monitoring:** Real-time faculty supervision using integrated Veyon modules.
4. **Data Protection:** Secure AES-256 encrypted backups of deleted files and logs to ensure academic integrity.
5. **Open-Source Deployment:** Availability of a transparent, customizable solution for institutions seeking affordable exam security systems.

Significance:

CampusNix addresses critical weaknesses in traditional online exam setups by integrating system-level security directly into the operating environment. It minimizes reliance on third-party browsers or software, ensuring exam integrity through OS-level control. This approach fosters trust between students and faculty by guaranteeing fairness and transparency. Additionally, it contributes to the field of educational cybersecurity by demonstrating how open-source tools can be unified to create robust, ethical, and scalable security solutions for academia.

Innovation:

- **Integrated Open-Source Frameworks:** Combines multiple open-source tools—USBGuard, Veyon, AdGuard Home, and OpenSSL—into a single secure operating system.
- **System-Level Security:** Moves beyond browser lockdowns by enforcing restrictions at the kernel and OS level.
- **Encrypted Data Handling:** Employs AES-256 encryption for logs and backups, ensuring complete data confidentiality.
- **Adaptive Design:** Modular and customizable, allowing institutions to modify configurations according to policy needs.
- **Real-Time Device Monitoring:** Uses Linux udev event detection to track and alert on hardware changes during exams.

Resources Required:

Hardware: Standard desktop computers, network routers/switches, storage servers for logs, and faculty systems for monitoring.
Software: Ubuntu Linux, USBGuard, AppArmor/SELinux, Veyon, AdGuard Home, OpenSSL, inotify-tools, Python (with pyudev and cryptography libraries), live-build tools for ISO generation.
Development Tools: Shell scripting, Python IDEs (VS Code, PyCharm), Git for version control, Docker for containerized testing, and cloud services for documentation and version management.
Data: System configuration files, security policies, exam session logs, and encrypted backups for validation testing.

References:

[1] USBGuard Project Documentation – https://usbguard.github.io/

[2] Safe Exam Browser Documentation – https://safeexambrowser.org/

[3] Gandraß et al., “Examuntu: A Secure and Portable Linux Distribution for E-Assessments.”

[4] Studies on Online Exam Security and Proctoring Systems.

[5] Veyon User Manual – https://veyon.io/

[6] inotify-tools Manual – https://github.com/inotify-tools/inotify-tools

[7] OpenSSL Documentation – https://www.openssl.org/docs/manmaster/man1/enc.html

[8] AdGuard Home Official Documentation – https://adguard.com/en/adguard-home/overview.html

[9] pyudev Documentation – https://pyudev.readthedocs.io/

Expected Outcome:

CampusNix is expected to significantly improve the reliability and fairness of computer-based examinations by providing a hardened operating system that enforces complete lockdown of unauthorized activity. It will reduce instances of digital malpractice, strengthen institutional integrity, and establish a new benchmark for open-source exam security platforms. Through real-time monitoring, encrypted audit trails, and transparent configuration, CampusNix ensures trust, accountability, and scalability across educational environments.

I have verified the abstract and recommending the student(s) for continuing the project.

Signature of the Guide with date