# MEPCO SCHLENK ENGINEERING COLLEGE, SIVAKASI

# C:\Users\Administrator\Downloads\Color 21.jpgINSTITUTION’S INNOVATION COUNCIL



**Student Projects Scheme (SPS)**

**SPS PROJECT PROPOSAL**

|  |  |  |  |
| --- | --- | --- | --- |
| **1.** | **Details of Applicants :** | | |
|  | **Student 1**  **Name:** Prabhu R | **Student 2**  **Name:** Vijesh Pethuram K |  | |
| **Dept:** Information Technology  **Year:** IV  **E-mail:** rprabhubarath\_bit25@mepcoeng.ac.in  **Mobile:** 8610562311 | **Dept:** Information Technology  **Year:** IV  **E-mail:** vijesh.moses\_bit25@mepcoeng.ac.in  **Mobile:** 8637480351 |  | |
| **2.** | **Details of the Guide :** | | |
|  | **Name:** Dr. T. Revathi  **Designation :** Senior Professor & Head  **Mobile No. :** 04562-235380  **E-mail:** trevathi@mepcoeng.ac.in | | |
| **3.** | **Project Title :**  **ENSEMBLE LEARNING BASED INTRUSION DETECTION SYSTEM FOR HEALTHCARE SECTOR** | | |
| **4.** | **Sector in which your Project proposal is to be Considered(Please tick the appropriate stream- Only one sector to be marked)** | | |
|  | Inter Disciplinary | | |
| **5.** | **Project Summary :**  The Ensemble-Based Intrusion Detection System for the Healthcare Sector is a sophisticated solution designed to address the increasing cybersecurity challenges faced by healthcare organizations. These institutions are prime targets for cyberattacks due to the sensitive nature of patient data and the critical infrastructure they operate. EIDS-HS combines multiple machine learning models into an ensemble approach, providing high accuracy in detecting threats while reducing false positives. It operates in real time, identifying malicious activities and responding swiftly with actions such as blocking harmful traffic and alerting authorities. The system ensures secure communication by encrypting all data exchanges and employs continuous learning to stay updated with evolving malware patterns and attack strategies. Its scalable design allows it to adapt to the needs of various healthcare setups, from small clinics to large hospitals. EIDS-HS not only protects sensitive data but also maintains operational continuity, ensuring that critical healthcare services remain unaffected by cyber threats. This comprehensive solution bridges the gap between the dynamic nature of modern cyberattacks and the pressing need for robust, real-time security in the healthcare industry. | | |
| **6.** | Project Details : | | |
|  | 1. **INTRODUCTION**   **a. Background**  The Ensemble-based Intrusion Detection System for the Healthcare Sector (EIDS-HS) uses cutting-edge machine learning approaches to combat the growing cybersecurity threats that healthcare organisations must contend with. Strong, flexible intrusion detection systems are now essential since healthcare systems are often the target of cyberattacks since patient data is so sensitive. EIDS-HS continuously refines its capabilities with newly gathered data by combining various machine learning models in an ensemble method to increase the accuracy and dependability of malware detection. The system not only identifies possible intrusions but also lessens the impact of attacks by combining secure communication protocols with proactive reaction methods, such as blocking bad IPs and notifying authorities. The goal of this project is to give healthcare organisations a flexible and safe way to protect their networks and patient information while maintaining operational continuity and confidentiality.   * 1. **b. Description of the problem**   Protecting its networks and systems from an increasing number of cyber threats is a major concern for the healthcare industry. Healthcare companies are particularly vulnerable to ransomware, phishing, and malware assaults because of the sensitive nature of patient data and the vital infrastructure found in hospitals. Unauthorised access to private medical data, interruption of necessary services, and significant financial and reputational harm to the organisations concerned are all possible outcomes of these assaults. Monitoring and safeguarding all entry points is made more difficult by the complexity of healthcare networks, which frequently include servers, cloud-based systems, and networked devices. The dynamic nature of cyber threats frequently outpaces the capabilities of current standard security measures, especially when it comes to sophisticated, targeted attacks. Furthermore, a lot of healthcare institutions lack the technology necessary for real-time danger identification and adaptive response. Advanced intrusion detection systems (IDS) that can constantly learn from new malware and attack patterns are therefore desperately needed in order to reduce risks by sending out precise and timely alerts. These solutions are essential for protecting patient safety, preventing data breaches, and preserving the integrity of hospital operations. The issue is made worse by the requirement for a solution that strikes a compromise between the efficiency and dependability needed in a hospital setting and good security.   * 1. **C. Brief Review of previous work**   Prior research in hospital network intrusion detection systems (IDS) has concentrated on improving the precision and effectiveness of identifying cyberthreats in medical settings, which are frequently the target of highly skilled attackers. Conventional IDS methods, like anomaly-based and signature-based detection, have proven inadequate in addressing emerging and changing threats. In order to improve detection skills, researchers have started looking at machine learning (ML) models. Cloud-based solutions provide benefits including scalability, real-time updates, and remote data access. Furthermore, several studies have combined capture engines and proxy servers to gather data in real time for improved threat detection. Despite these developments, a number of issues still exist, namely with regard to protecting privacy, securely transmitting sensitive medical data, and guaranteeing prompt intrusion detection in dynamic healthcare settings.   1. **DESCRIPTION OF THE PROPOSAL**    1. **Objectives of the project**   The objectives of the proposed Ensemble Intrusion Detection System for Healthcare Systems are as follows:  **1. Develop a Secure Intrusion Detection Framework**:  Design and implement a robust intrusion detection system for healthcare networks that ensures the security and privacy of sensitive medical data while detecting potential cyber threats in real-time.  **2. Utilize Ensemble Machine Learning Models**:  Leverage an ensemble machine learning approach to improve the accuracy of intrusion detection, by combining multiple models to enhance prediction capabilities and reduce false positives in identifying malicious activities.  **3. Enable Continuous Learning and Adaptation**:  Establish a system that can continuously gather new malware samples through the deployment of proxy servers and capture engines, and send them to the cloud server for real-time model updates and fine-tuning.  **4. Ensure Secure Communication**:  Implement secure communication protocols between the hospital servers, proxy servers, and cloud servers, ensuring that all data exchanges are encrypted, and preventing unauthorized access or tampering.  **5. Alert Hospital Authorities**:  Develop an alert mechanism within the system that notifies hospital authorities immediately upon detection of an intrusion, enabling swift action to mitigate potential damage.  **6. Provide Real-Time Malware Detection and Response**:  Enable the system to detect and respond to malware attacks in real time, blocking harmful traffic, and providing automatic responses such as blocking IP addresses or ports associated with malicious activities.  **7. Support Scalability and Flexibility**:  Ensure that the proposed system is scalable and flexible enough to be deployed in various healthcare settings, from small clinics to large hospitals, without compromising on performance or security.   * 1. **Methodology detailing stepwise activities and sub-activities:**   The methodology for the Ensemble Intrusion Detection System for Healthcare Systems is structured in a series of phases, each encompassing specific activities and sub-activities. These steps ensure a comprehensive, secure, and efficient implementation of the system. The phases are outlined as follows: **1. System Design and Architecture** **1.1 Requirement Analysis:** Define the system scope, focusing on the types of cyber threats to be detected, the hospital network architecture, and the components involved.  **1.2 Architecture Design:** Design the system architecture, detailing the interactions between hospital servers, proxy servers, cloud servers, and capture engines. Choose the ensemble machine learning models and detection strategies for enhanced performance. **2. Data Collection and Preprocessing** **2.1 Data Collection:** Deploy proxy servers and capture network traffic, including potential malware and attack data, from various sources in the hospital network.  **2.2 Data Preprocessing:** Cleanse the collected data by removing irrelevant information. Normalize and extract relevant features to ensure the data is ready for machine learning analysis. **3. Intrusion Detection System Development** **3.1 Capture Engine Development:** Develop capture engines to monitor and analyse network traffic in real-time, filtering the data before sending it to cloud servers for analysis.  **3.2 Ensemble Model Development:** Train multiple machine learning models on the preprocessed data, then combine them into an ensemble model to improve accuracy and reduce false positives in intrusion detection.  **3.3 Real-Time Malware Detection:** Implement a real-time detection system that classifies network activities and generates alerts for suspected malicious behaviour, ensuring prompt response to security threats. **4. System Integration and Testing** **4.1 Component Integration:** Integrate all system components—capture engines, cloud servers, proxy servers, and the ensemble model—into a cohesive solution.  **4.2 Functional Testing:** Test the system's ability to detect various intrusions and ensure the accuracy of alerts and detection mechanisms.  **4.3 Security Testing:** Conduct security tests to assess the system's resilience against common attacks such as session hijacking, impersonation, and unauthorized access. **5. Formal Security Verification** **5.1 Scyther Tool Verification:** Use the Scyther tool to formally verify the security of EIDS-HS. Define essential claims and run simulations to check for vulnerabilities like replay and impersonation attacks.  **5.2 Security Analysis:** Review the verification results and address any identified vulnerabilities or weaknesses in the system design. **6. Continuous Learning and Maintenance** **6.1 Continuous Model Updating:** Establish a process for regularly updating the ensemble model with new malware samples and threat intelligence to keep the system adaptive and responsive to emerging threats.  **6.2 Ongoing Maintenance and Monitoring:** Continuously monitor system performance, conduct regular updates, and ensure that any emerging vulnerabilities are addressed promptly.   1. **WORK PLAN**   **a. Phase-wise plan of action:**  **Before Implementation:**   1. **Requirement Analysis (Nov 15 - Dec 5, 2024)**    * Identify specific cybersecurity threats facing healthcare networks.    * Conduct a thorough analysis of the hospital network architecture.    * Define the scope, objectives, and requirements of the Intrusion Detection System. 2. **Data Collection Setup (Dec 5 - Dec 8, 2024)**    * Deploy proxy servers within the healthcare network to capture traffic data.    * Ensure data sources include potential malware and threat information. 3. **Data Preprocessing (Dec 9 - Dec 12, 2024)**    * Clean and normalize the collected data.    * Extract relevant features to prepare the data for machine learning analysis. 4. **Capture Engine Development (Dec 12 - Dec 22, 2024)**    * Develop engines to monitor and capture network traffic in real-time.    * Set up filtering mechanisms to ensure only relevant data is sent to cloud servers. 5. **Ensemble Model Development (Dec 23 - Jan 5, 2025)**    * Train multiple machine learning models on preprocessed data.    * Integrate these models into an ensemble to improve accuracy and reduce false positives. 6. **Integration of Components (Jan 6 - Jan 12, 2025)**    * Integrate capture engines, cloud servers, and the ensemble model into a unified system. 7. **Security Verification with Scyther Tool (Jan 12 - Jan 27, 2025)**    * Use the Scyther tool for formal security verification.    * Simulate attacks to ensure resilience against common threats.   **After Implementation:**   1. **Deployment in Healthcare Systems (Jan 28 - Feb 3, 2025)**    * Deploy the system in various healthcare environments.    * Ensure smooth integration with existing network infrastructure. 2. **Continuous Learning Setup (Feb 4 - Feb 10, 2025)**    * Implement mechanisms for continuous model updates with new threat data.    * Set up processes to ensure the system can adapt to emerging threats. 3. **System Performance Evaluation (Feb 10 - Feb 15, 2025)**    * Evaluate system accuracy, response time, and scalability in real-world conditions.    * Gather feedback from stakeholders and fine-tune the system as necessary.   **b. Milestones:**   1. Requirement Analysis Completion – Dec 5, 2024 2. Data Collection Setup Completion – Dec 8, 2024 3. Data Preprocessing Completion – Dec 12, 2024 4. Capture Engine Development Completion – Dec 22, 2024 5. Ensemble Model Development Completion – Jan 5, 2025 6. Component Integration Completion – Jan 12, 2025 7. Security Verification with Scyther Completion – Jan 27, 2025 8. System Deployment in Healthcare Environments – Feb 3, 2025 9. Continuous Learning Mechanism Setup Completion – Feb 10, 2025 10. System Performance Evaluation Completion – Feb 15, 2025   **c. GANTT chart:**       1. **BUDGET DETAILS**   **a. Equipment**   1. Servers/Cloud Infrastructure: Azure. 2. Arduino UNO Board 3. ESP32 4. TMP36 or LM35 5. Heart Rate (Pulse) Sensor   **b. Consumables**   1. Breadboards 2. Jumper Wires 3. Connectors and Header Pins 4. **EXPECTED OUTCOMES**   **a. Quantify output in measurable parameters:**  **1. Anomaly Detection Rate**  The percentage of total anomalies or threats that the system successfully detects out of the total potential threats. We expect high detection rates for all types of attacks (e.g., DDoS, unauthorized access attempts).  **2. Accuracy:**  The percentage of correctly classified instances (both normal and anomalous data). High accuracy means the system can accurately differentiate between normal and anomalous traffic without making mistakes.  **3. Detection Time:**  The time taken by the system to detect and respond to an intrusion or anomaly in real-time. We need to minimize detection time to ensure real-time monitoring and timely responses.  **b. Suggest Post Project Activities**  **1. System Maintenance:**  Regular updates, bug fixes, and version control are necessary to keep the system secure, functional, and up-to-date with emerging threats. Monitoring system components for issues and ensuring security patches are applied helps to maintain reliability.  **2. Performance Monitoring:**  Ongoing tracking of the system’s real-time performance, including network traffic, anomaly detection, false positives/negatives, and response times, is essential for maintaining system health and ensuring it adapts to the growing needs of healthcare environments.  **3. Incident Response:**  Developing and refining an incident response plan helps manage and mitigate security breaches. Post-incident reviews are critical to identify weaknesses and adjust procedures, ensuring the system becomes more resilient to future attacks.  **4. System Scaling and Expansion**  As healthcare environments grow, expanding the system’s deployment and scaling the hardware and software infrastructure ensures the system can handle increased traffic and new devices. Integration with other security solutions enhances the overall defense. | | |
|  |  | | |

**DECLARATION**

**Project Title: ENSEMBLE LEARNING BASED INTRUSION DETECTION SYSTEM FOR HEALTHCARE SECTOR**

**Declaration by the student(s):**

We, **PRABHU R and VIJESH PETHURAM K**, of the **DEPARTMENT OF INFORMATION TECHNOLOGY**, hereby declare that we shall undertake the SPS project strictly in accordance with the provisions specified in the project proposal and we shall submit bi-monthly reports about the progress of the work and final report on completion of the project on time.

Date:

Place: **Signature of the student(s)**

--------------------------------------------------------------------------------------------------------------------------------------

**Recommendation by guide:**

I, Dr. T. Revathi, of the **DEPARTMENT OF INFORMATION TECHNOLOGY,** recommend the above SPS project, which is to be carried out under my supervision. I shall arrange to submit the final report on completion of the project on time and I will mentor the students throughout their endeavours.

|  |  |
| --- | --- |
| Forwarded | Recommended |
| **Signature of the HOD** | **Signature of the guide** |
|  | |
| **APPROVED**  **PRINCIPAL** | |