Topic 4

1. **Title:** ***Framework Model for Identifying, detecting and Report for Cyber Security on Bhuvan Portal***
2. **Description**: The organization of technologies, procedures, and methods designed to protect networks, devices, programs, and data from attack, damage, malware, viruses, hacking, data theft, or unauthorized access is referred to as cyber security. The primary goal of cyber security is to protect the confidentiality of all organizational data from both external and internal threats, as well as disruptions caused by natural disasters. Bhuvan is accessed by the users across the world and is prone to cyber-attacks. There are many state-of-art security devices and solutions implemented to tackle the attacks. However, it is imperative to utilize AI/ ML models to analyze the patterns and Behavior Analysis of the logs collected by the Network Security Devices and to automate / alert mechanisms to report the system / network administrators in near- real – time basis.
3. **Objectives**:
    a. To implement AI/ ML based security analysis model for finding the behaviors of the cyber attacker and to analyze the user traffic who are accessing Bhuvan Geo- Portal.
    b. The framework / model Should Identify, Protect, Detect, Respond, and Recover from the cyber security attacks.
4. **Expected Outcomes:**
    a. Develop a Framework/ Model for analyzing security patterns on the fire wall logs collected.
    b. Model / Framework should include anomaly detection, pattern recognition of user access and report from the logs collected.
5. **Relevant data and steps to get the data from Bhuvan/ other sources:**
    a. Server and Firewall logs- old data.
    b. Traffic patterns – bandwidth utilization
6. **Steps to be followed for achieving the objectives:**
    a. Packet Sniffing or Network Traffic Analysis is the process of tracking all incoming and outcoming traffic, network traffic, and availability using packet sniffers. Packet sniffers are used for comparing real-time networks and past data for detecting anomalies and potential vulnerabilities.
    b. Monitor the information contained in the packets or the intended source and destination of the packets.
    c. Process the system/ traffic logs and detect the users that are flagged.
    d. Analyze the data packets transferred over the network
    e. Analyze the user access pattern and develop a model to automatically detect.
    f. Generate a report after analyzing the packets
    g. Develop software for detecting any data breach or ensuring the safety of the packet transfer process.
7. **Evaluation:**
    a. The Model will be tested using the sample logs from NRSC/ Bhuvan systems.
    b. The accuracy of the model in identifying the malicious users will be evaluated.
    c. The reporting mechanism will be evaluated through mail alerts and dashboard integration