**Name : ankit**

**College : SISTC(Sydney) Australia**

**2. Project Title: Ransomware Detection and Response System**

**Objective:**

Create a ransomware detection and response system that monitors file changes on a system and identifies early signs of ransomware activity, such as mass file encryption. The system should alert the user and take immediate action to limit damage (e.g., isolate the infected machine).

**Key Features:**

1. **File System Monitoring:**
   * Monitor the file system in real-time for suspicious activity such as rapid encryption of files, file renaming, or deletion patterns typical of ransomware.
   * Use algorithms to detect anomalous changes to file extensions, content, or structure.
2. **Ransomware Behavior Analysis:**
   * Implement behavior-based detection methods that track processes attempting to modify or encrypt multiple files within a short time frame.
   * Detect ransomware indicators like creation of ransom notes or abnormal CPU usage spikes related to encryption.
3. **Alert and Response Mechanism:**
   * Immediately alert the user when suspicious file changes are detected.
   * Implement automatic response mechanisms such as isolating the affected machine from the network, halting the process causing the damage, or creating backups of unencrypted files.
4. **Backup and Restore Functionality:**
   * Automatically create regular backups of important files to prevent loss in the event of a ransomware attack.
   * Implement a recovery feature that can restore unencrypted files after detecting ransomware.
5. **Visualization Dashboard:**
   * Create a dashboard to show real-time file activity, suspicious events, and ransomware detection status.
   * Display logs of file changes and alerts to help users understand which files were affected and what actions were taken.

**Tech Stack:**

* **Programming Language**: Python (for file system monitoring, anomaly detection, and response automation)

**Libraries**:

* + **Watchdog**: For file system monitoring in real time.
  + **PyCryptodome**: For ransomware simulation (optional) and encryption detection.
  + **Matplotlib or Plotly**: For visualization and dashboard creation.
* **Optional Tools**: ELK Stack (Elasticsearch, Logstash, Kibana) for advanced monitoring and visualization.

**Expected Deliverables:**

* A real-time ransomware detection system capable of identifying and responding to ransomware activities before significant damage is done.
* A detailed report explaining detection methods, behavior analysis, and recovery mechanisms.
* (Optional) A simulation of ransomware to demonstrate the system’s effectiveness in a controlled environment.

**Challenges:**

* Ensuring quick detection of ransomware before it encrypts a significant portion of files.
* Balancing between detecting actual ransomware and avoiding false positives from legitimate file changes.
* Implementing fast recovery mechanisms without risking the loss of critical data.

**Summary of Project Ideas:**

1. **Blockchain-Based Secure Voting System**:
   * Focuses on creating a secure, tamper-proof voting system using blockchain technology.
   * Involves cryptography, decentralized systems, and secure identity management.
2. **Ransomware Detection and Response System**:
   * Focuses on real-time monitoring of file system activities to detect and respond to ransomware attacks.
   * Involves file system analysis, behavior-based detection, and automatic response mechanisms.