Hackathon Date : Nov 16, 2024
Duration : 24 Hours
Theme : AI/ML for Cybersecurity

To foster interest and encourage students to explore the applications of AI/ML in cybersecurity, we are organizing a hackathon where students of PES University across RR and EC campus will compete to showcase their skills and creativity This hackathon focuses on leveraging AI/ML to address some of the most pressing challenges in cybersecurity. Participants will be encouraged to create innovative solutions across various tracks that highlight different aspects of cybersecurity.

Selection Criteria : The team needs to implement a solution in at least one of the Tracks and meet a minimum of one objective.

Track I: Dark Patterns on E-commerce Websites

- **Overview**: Dark patterns are deceptive tactics on e-commerce sites designed to influence users into making choices they might not otherwise make. Examples include hidden fees, forced account creation, and hard-to-find opt-outs. This track challenges teams to leverage AI/ML to detect, analyze, and counteract dark patterns, enhancing transparency and protecting user rights.
- **Objectives**:
    - **Automated Detection of PII in Documents**: Develop an AI tool to scan e-commerce websites, identifying instances where personal information is collected without adequate disclosure or consent.
    - **Detection of Manipulative Tactics**: Build an ML model to detect deceptive UI elements, focusing on patterns that influence users toward unwanted actions.
    - **Behavioral Analysis of User Response**: Use AI to analyze user behavior in response to dark patterns, identifying which manipulative designs are most effective and which users find most deceptive.
    - **Adversarial Testing for Dark Patterns**: Develop adversarial models that simulate common dark patterns. Use these to test the resilience of detection systems against evolving manipulative tactics.
    - **Counteractive Mechanisms**: Create a browser extension or plugin that provides real-time alerts or recommendations to users encountering dark patterns, enabling them to make informed decisions.

Track II: Dark Web Monitoring

- **Overview**: The dark web is a marketplace for illicit activities, often including data sales, hacking tools, and cyberattack planning. Monitoring dark web activity helps preempt cybersecurity threats but poses ethical and privacy challenges. This track focuses on creating AI/ML solutions that monitor these activities while preserving user privacy and ensuring ethical practices.

- **Objectives**:
    - **Privacy-Preserving Monitoring**: Implement methods like differential privacy to monitor dark web forums and marketplaces, ensuring sensitive data is handled ethically.
    - **Sentiment and Content Analysis**: Develop tools to analyze dark web conversations to identify emerging threats, with a focus on user sentiments, discussion topics, and cyber threat-related jargon.
    - **Threat Attribution Models**: Design models that can attribute suspicious activities to probable sources or threat actors, providing insights on the origin and affiliations of these threats.
    - **Automated Threat Intelligence Gathering**: Build a solution that gathers and correlates threat intelligence from various dark web sources, integrating findings with known security databases.

Track III: Forensic Investigations

- **Overview**: Digital forensics involves the secure collection, preservation, and analysis of digital evidence post-incident. This track centers on creating tools that automate and enhance forensic investigations, making them faster and more accurate in identifying suspicious activities and reconstructing incident timelines.
- **Objectives**:
    - **AI-Enhanced Evidence Validation**: Create tools that automatically validate digital evidence, ensuring that any tampering or alteration is detected and that data integrity is maintained throughout the investigative process.
    - **Anomaly Detection in Logs**: Build models to analyze logs for anomalies that may indicate unauthorized access or suspicious activities, supporting faster threat detection.
    - **Simulating Cyber Incidents for Tool Testing**: Develop controlled cyber incident scenarios to test forensic tools in realistic conditions, assessing robustness and accuracy.
    - **Forensic Timeline Reconstruction**: Design AI tools to reconstruct the timeline of suspicious activities, helping investigators trace and visualize the actions of malicious actors.

Track IV: Real-Time Feed of Cyber Incidents

- **Overview**: Real-time awareness of cyber incidents is essential for effective threat response. This track focuses on building tools that provide live feeds of cyber incidents, integrating predictive insights and visualizations to help organizations understand and respond to global threats.
- **Objectives**:
    - **Real-Time Incident Detection**: Create an AI/ML system that monitors various data sources to detect and report cyber incidents as they occur.

    - **Predictive Incident Analysis**: Develop models that analyze past trends to predict potential cyber incidents, helping organizations anticipate and mitigate attacks proactively.
    - **Real-Time Incident Visualization**: Build visualization dashboards to represent real-time cyber threats, with features like heatmaps, time-lapse displays, or industry-specific threat landscapes.
    - **Incident Prioritization**: Design a system that prioritizes incidents based on their potential impact, allowing organizations to focus on the most critical threats.

Track V: Open Innovation for AI/ML in Cybersecurity

- **Overview**: This open innovation track encourages tackling cybersecurity issues with creative, unconventional approaches to AI/ML. Solutions may include areas such as explainable AI (XAI) and human-AI collaboration, inspiring novel applications in cybersecurity.
- **Objectives**:
    - **Focus on Explainable AI (XAI)**: Create transparent and interpretable models that help cybersecurity professionals understand the decision-making process of AI-driven tools.
    - **AI-Augmented Human Collaboration**: Develop solutions that enable AI systems to work alongside human analysts, enhancing their ability to detect and respond to threats with prioritization, real-time alerting, and decision support.
    - **Novel Applications in Cybersecurity**: Propose innovative uses of AI/ML, such as automating routine security tasks, generating personalized threat assessments, or exploring new analytics in cybersecurity.