ANURAG UNIVERSITY

DEPARTMENT OF INFORMATION AND TECNOLOGY

HACK ATTACK – PROBLEM STATEMENTS

CYBERSECURITY

Guarding Your Digital World

Healthcare

1.Secure Data Exchange in Telemedicine:

During a virtual consultation, a patient's medical records and treatment plans are being transmitted between the doctor and the patient. Hackers target this communication to intercept sensitive health data. You need to design a secure, encrypted telemedicine system that ensures no unauthorized person can access or manipulate the information exchanged.

- **Scenario:** During a virtual consultation, a patient's medical records and treatment plans are exchanged between a doctor and a patient. Hackers attempt to intercept this data, which contains sensitive health information. The risk of exposure could lead to data breaches, identity theft, or fraudulent medical claims.

- **Solution:** Implement an end-to-end encrypted telemedicine system using advanced encryption protocols such as AES-256. Data integrity is maintained through digital signatures, while multi-factor authentication (MFA) ensures secure access to the system by both patients and healthcare providers.

- **Impact:** The secure system prevents unauthorized access, protecting patient confidentiality and trust. It mitigates the risk of data breaches, improves compliance with health data privacy laws like HIPAA, and ensures that medical advice and treatment plans remain tamper-proof, fostering trust in telemedicine solutions.

2.Multi-Layered Authentication for Medical Records Access:

A cybercriminal tries to access patient records using stolen credentials. The system only relies on basic username and password authentication, making it vulnerable. Your goal is to implement a multi-layered authentication process, involving biometric scans and dynamic access permissions, to secure sensitive medical information and prevent unauthorized access.

- **Scenario:** A cybercriminal obtains stolen credentials and attempts to access sensitive patient records. The current system uses basic username and password authentication, making it vulnerable to breaches. Once inside, the attacker could misuse the personal health information (PHI) without being detected, leading to privacy violations and data misuse.

- **Solution:** Implement a multi-layered authentication system combining biometric verification (such as fingerprint or facial recognition) with dynamic access permissions based on roles. This system limits access to only necessary information, ensuring even if credentials are stolen, unauthorized access is blocked at multiple points.

- **Impact:** This approach strengthens security by reducing the likelihood of breaches, protecting patient privacy, and ensuring that sensitive data remains accessible only to authorized personnel. It prevents identity theft, enhances trust in medical systems, and complies with stringent healthcare regulations like HIPAA.

Digital Education

1.End-to-End Encryption in Online Classrooms:

During a live virtual classroom session, a malicious actor infiltrates the platform and attempts to eavesdrop on private conversations between students and teachers. Your task is to design a secure, encrypted communication protocol that ensures all interactions remain confidential and immune to external attacks.

- **Scenario:** In a live online classroom, students and teachers exchange sensitive information, like personal data and academic progress. A malicious actor gains unauthorized access and tries to eavesdrop on these conversations, potentially stealing or altering confidential information. This compromises the integrity of the virtual learning environment and puts the participants' privacy at risk.

- **Solution:** Implement end-to-end encryption (E2EE) where all communication data is encrypted on the sender's side and decrypted only by the intended recipient. Secure key exchange mechanisms like Diff-Hellman can ensure encryption keys remain safe from external interference, safeguarding private interactions during online classes.

- **Impact:** With E2EE, confidential conversations between students and teachers are protected from unauthorized access, improving the security and privacy of virtual classrooms. This fosters a safer learning environment, boosting trust in online education platforms while complying with data protection regulations.

2.Phishing Prevention Training for Educators and Students:

A teacher receives a phishing email disguised as a message from the school's IT department, asking for their login credentials. Unaware of the threat, they almost fall for the scam. Your task is to create an interactive training program that educates both teachers and students on recognizing phishing attempts and responding to cybersecurity threats effectively.

- **Scenario:** A teacher receives an email claiming to be from the IT department, asking for login credentials. It looks legitimate, and the teacher is about to enter their details, unaware it's a phishing scam that could compromise the school's network.

- **Solution:** Create an interactive training program that teaches educators and students to spot phishing attempts. It includes examples, quizzes, and tips on reporting suspicious emails.

- **Impact:** The training raises awareness, reducing phishing risks. Both teachers and students become more vigilant, helping protect personal data and the school's systems.

Fintech

1.Real-Time Fraud Detection in Digital Payments:

A financial institution is experiencing a surge in fraudulent transactions across its digital payment platforms. Customers are unknowingly authorizing payments to malicious actors. You need to implement an AI-powered fraud detection system that identifies suspicious activity in real-time and halts transactions before any financial damage occurs.

- **Scenario:** A financial institution faces increasing fraudulent transactions on its digital payment platforms. Malicious actors exploit vulnerabilities, tricking customers into authorizing payments unknowingly. This has led to financial losses and damaged customer trust, prompting an urgent need for real-time fraud detection.

- **Solution**: Implementing an AI-powered fraud detection system that uses machine learning algorithms to analyse transaction patterns, flag anomalies, and block suspicious activities in real time. The system continuously learns from new threats, improving its detection accuracy over time.

- **Impact:** The solution minimizes fraudulent transactions, safeguarding both customers and the institution. Real-time detection reduces financial losses, enhances customer trust, and boosts the institution's reputation for secure payments. The system's scalability also ensures long-term protection against evolving threats.

2. Cybersecurity in Peer-to-Peer (P2P) Payment Systems:

A user of a popular P2P payment app becomes the victim of identity theft, with hackers gaining access to their account and transferring funds. You are tasked with creating advanced security protocols that prevent unauthorized access to P2P platforms, ensuring user identity is protected and transactions remain secure.

- **Scenario:** A user of a widely used P2P payment app falls victim to identity theft, leading to hackers gaining access to their account. They exploit security loopholes to transfer funds without authorization. The breach not only compromises financial data but also erodes the user's trust in the platform, highlighting the vulnerability of digital payment systems.

- **Solution:** Implement multi-factor authentication (MFA), biometric verification, end-to-end encryption, and behavioural analytics to detect suspicious activity. Integrating AI-powered fraud detection systems can prevent unauthorized access while securing user data and transactions.

- **Impact:** These protocols would significantly reduce identity theft and unauthorized access, bolstering trust in the platform. Enhanced security ensures safe financial transactions, encouraging more users to adopt P2P services. Financial institutions will also experience fewer fraud cases, protecting both their reputation and users' assets.

Smart City Planning

1. IOT Security in Smart City Infrastructure:

A cybercriminal gains access to a city's to IOT-enabled traffic management system, causing chaos by manipulating traffic lights. You are responsible for creating a comprehensive cybersecurity solution that secures all IOT devices in the city, from traffic systems to public utilities, preventing malicious actors from compromising critical infrastructure.

- **Scenario:** In a bustling smart city, a cybercriminal infiltrates the IOT-enabled traffic management system, disrupting traffic by manipulating signals, causing accidents, gridlock, and public safety hazards. The city's entire infrastructure, including utilities, relies on interconnected IOT devices, making it vulnerable to further attacks.

- **Solution:** Implement a multi-layered security approach, including network segmentations, encryption of data transmission, device authentication, and AI-powered anomaly detection. Regular updates, secure boot processes, and intrusion detection systems should also be deployed to safeguard all IOT devices.

- **Impact**: The solution ensures the continuous and secure operation of IOT infrastructure, reducing the risk of cyberattacks and protecting public safety. By enhancing the resilience of critical systems, it fosters trust in smart city technologies, improving urban efficiency and safety.

2. AI-Driven Cyber Threat Detection in Smart Cities:

The water supply system of a smart city is targeted by cybercriminals aiming to disrupt services. You need to implement AI-powered monitoring systems that detect unusual activities in real-time, helping city authorities neutralize threats before they affect citizens.

- **Scenario:** A smart city's water supply system, critical for public well-being, faces a cyberattack where criminals attempt to disrupt services. With digital control systems managing operations, any breach could result in water contamination, service outages, or damage to infrastructure, affecting thousands of residents. Timely detection is essential to prevent large-scale disruption.

- **Solution:** Implement an AI-driven monitoring system that continuously analyse network traffic, water distribution patterns, and operational data. Machine learning algorithms identify anomalies and suspicious behaviour triggering real-time alerts. Automated responses can neutralize threats by isolating affected systems and alerting authorities for further action.

- **Impact:** AI-powered detection can safeguard essential services, minimizing risks of water contamination, outages, and infrastructural damage. Real-time threat mitigation ensures continuity, enhances public safety, and strengthens the resilience of smart city infrastructure against future cyber threats.

Agri Innovate

1. IOT Security in Precision Agriculture:

In a farm that relies on IOT-enabled devices for crop monitoring and automated irrigation, a hacker tries to alter sensor data to disrupt farming decisions. Your challenge is to create a cybersecurity framework that ensures the integrity of sensor data and prevents unauthorized access.

- **Scenario:** In a precision agriculture farm, IOT devices continuously monitor soil moisture, temperature, and crop health. A hacker infiltrates the system, manipulating sensor data to indicate ideal conditions for irrigation, leading to overwatering. This results in crop damage and financial loss, as the farm's automated systems make decisions based on compromised data, jeopardizing the entire harvest.

- **Solution:** Implement a robust cybersecurity framework comprising multi-factor authentication, encrypted data transmission, and anomaly detection algorithms. Regularly update IOT device firmware and conduct vulnerability assessments to identify and rectify security gaps. Establish a response plan to mitigate damage from potential breaches and ensure data integrity through block chain technology for sensor data verification.

- **Impact:** By securing IOT devices in precision agriculture, the framework enhances trust in sensor data, leading to informed decision-making. This protection minimizes crop loss, optimizes resource use, and maximizes yield, ultimately improving farm profitability. A resilient system fosters stakeholder confidence and encourages further adoption of IOT technologies in agriculture, driving innovation and sustainability.

2. Cybersecurity for Agricultural Drones:

A farm relies on drones for monitoring crop health, but hackers attempt to hijack these drones, causing them to malfunction. Your task is to design a secure communication protocol that protects these drones from interference and ensures the safe transmission of data.

- **Scenario:** A farm uses drones to monitor crop health, providing critical insights for optimizing yield. Hackers target these drones, attempting to hijack their control systems and disrupt operations. This creates risks of data breaches, loss of drone functionality, and damage to crops, severely impacting farm productivity.

- **Solution:** Design a secure communication protocol with end-to-end encryption, mutual authentication, and real-time anomaly detection. By employing encrypted channels and digital signatures, it prevents unauthorized access, ensuring that only authenticated users can control and receive data from the drones.

- **Impact:** The secure protocol protects drones from hijacking, ensuring uninterrupted operations and safeguarding critical agricultural data. This strengthens farm productivity, improves decision-making through reliable crop monitoring, and enhances overall security in agriculture-tech, reducing risks of cyberattacks.