DEPARTMENT OF

INFORMATION AND TECNOLOGY

HACK ATTACK – PROBLEM STATEMENTS

BLOCKCHAIN

Empowering Trust, Securing the Future.

Healthcare

1. AI-Based Threat Detection in Healthcare Networks:

Design AI-driven systems to monitor and detect potential cyber threats in healthcare IT infrastructure, minimizing downtime and enhancing patient safety.

- **Scenario:** Healthcare networks are increasingly vulnerable to cyber threats due to the rise in connected medical devices and sensitive patient data. A potential attack could disrupt critical services, leading to compromised patient care and safety. For instance, a ransomware attack could lock healthcare providers out of patient records, delaying treatment and endangering lives.

- **Solution:** Implementing AI-based threat detection systems can continuously monitor network activity, using machine learning algorithms to identify and respond to anomalies in real-time. These systems can analyse patterns, detect unusual behaviour, and automatically mitigate threats, ensuring a robust security posture while maintaining uninterrupted access to patient data.

- **Impact:** The deployment of AI-driven threat detection in healthcare networks can significantly enhance patient safety by reducing downtime and ensuring data integrity. Proactive threat management minimizes the risk of breaches, leading to increased trust among patients and stakeholders. Ultimately, this contributes to improved healthcare delivery and operational efficiency, safeguarding sensitive information and ensuring seamless care.

2.Multi-Factor Authentication for Medical Staff:

Develop a multi-factor authentication system tailored for medical professionals, ensuring secure yet quick access to medical records in emergency situations.

- **Scenario:** In a busy hospital, medical staff often face emergencies where immediate access to patient records is crucial. However, relying solely on passwords can lead to delays or unauthorized access. A multi-factor authentication (MFA) system can enhance security while allowing swift entry during critical moments, ensuring that only authorized personnel can access sensitive medical information.

- **Solution:** Implement a multi-factor authentication system using biometrics (e.g., fingerprint or facial recognition) combined with time-sensitive one-time passwords (OTPs) sent to staff mobile devices. This approach ensures secure access while minimizing time delays, enabling medical professionals to retrieve vital patient data quickly and efficiently in emergencies.

- **Impact:** The introduction of MFA for medical staff significantly enhances data security, reducing the risk of unauthorized access to sensitive information. This system not only protects patient privacy but also fosters trust among patients and healthcare providers. By ensuring rapid access to medical records in emergencies, it ultimately contributes to improved patient outcomes and healthcare efficiency.

Digital Education 🎓

1.AI-Based Proctoring Security for Exams:

Create AI-driven proctoring systems that not only monitor but also detect and prevent cheating during online examinations, maintaining academic integrity.

- **Scenario:** In an online examination setting, students may be tempted to cheat by using unauthorized resources or collaborating with others. Traditional proctoring methods often fall short, leading to concerns about academic integrity and the value of the assessment. This scenario highlights the need for a more effective solution to ensure fairness and trust in the examination process.

- **Solution:** AI-driven proctoring systems utilize advanced algorithms to monitor student behaviour in real-time during online exams. These systems employ facial recognition, eye-tracking, and anomaly detection to identify suspicious activities, such as looking away from the screen or the presence of unauthorized materials. By automatically flagging potential violations, these solutions help educators maintain a secure and honest testing environment.

- **Impact:** Implementing AI-based proctoring can significantly enhance the integrity of online examinations, instilling greater confidence among educators and students alike. This technology reduces instances of cheating, promotes a level playing field, and ensures that academic achievements reflect genuine understanding. Ultimately, it helps uphold the value of educational credentials in a rapidly evolving digital landscape.

2. Blockchain for Academic Credential Verification:

Implement blockchain technology to securely store and verify academic credentials, preventing fraud and ensuring the integrity of educational qualifications.

- **Scenario:** In today's digital world, academic credential fraud is a growing concern, with many employers and educational institutions struggling to verify the authenticity of degrees and certificates. Graduates often face challenges in proving their qualifications, leading to distrust in academic institutions and complicating hiring processes.

- **Solution:** Implementing a blockchain-based system for academic credential verification allows educational institutions to securely store and issue digital credentials. Each degree or certificate is recorded on a tamper-proof blockchain, enabling employers and other institutions to easily verify credentials through a decentralized, transparent system, ensuring authenticity and preventing fraud.

- **Impact:** The use of blockchain for credential verification enhances trust between employers and graduates, streamlining the hiring process. It reduces administrative overhead for educational institutions while providing graduates with easily accessible, verifiable credentials. This innovation promotes accountability and integrity in education, ultimately fostering a more reliable and efficient job market.

Fintech

1.AI-Powered Real-Time Fraud Detection:

Create an AI-based system for real-time fraud detection in digital payments, ensuring secure transactions and preventing financial losses.

- **Scenario**: As online transactions surge, financial institutions face increasing challenges from fraudulent activities. Cybercriminals employ sophisticated techniques, resulting in substantial financial losses for both businesses and consumers. Manual fraud detection methods are slow and often ineffective, leading to a need for a more proactive approach to safeguard digital payment systems and maintain customer trust.

- **Solution:** An AI-powered real-time fraud detection system utilizes machine learning algorithms to analyze transaction patterns, identifying anomalies and flagging suspicious activities instantly. By integrating this system into payment gateways, it enhances security through continuous monitoring, ensuring rapid responses to potential fraud and reducing false positives with adaptive learning.

- **Impact:** The implementation of AI-driven fraud detection significantly decreases financial losses due to fraud, enhances customer trust, and streamlines transaction processes. Businesses benefit from improved security measures, leading to a safer digital payment environment. This proactive approach fosters a positive reputation, encouraging consumer adoption of digital transactions and driving growth in the e-commerce sector.

2. Blockchain for Cross-Border Payment Security:

Develop a blockchain solution to enhance the security of cross-border payments, reducing fraud risks and ensuring compliance with global financial regulations.

- **Scenario:** Cross-border payments often face challenges such as high transaction costs, lengthy processing times, and the risk of fraud. Traditional banking systems may lack transparency and can be vulnerable to cyberattacks, leaving individuals and businesses exposed to financial loss. Compliance with diverse global regulations adds another layer of complexity, hindering seamless international transactions.

- **Solution:** Implementing a blockchain-based platform for cross-border payments can provide a secure, transparent, and efficient alternative. By utilizing smart contracts and decentralized ledgers, transactions can be automated, reducing the potential for human error and fraud. The system can also ensure real-time compliance with financial regulations across different jurisdictions, enabling smoother international trade.

- **Impact:** This blockchain solution can significantly enhance the security of cross-border payments, fostering trust among users and reducing the risk of fraud. By lowering transaction costs and processing times, it can encourage more businesses to engage in international trade. Ultimately, this innovation promotes financial inclusion and accelerates economic growth by simplifying cross-border transactions.

Smart City Planning 

1.Securing Autonomous Vehicles in Smart Cities:

Develop cybersecurity protocols for autonomous vehicles, ensuring secure communication with smart city infrastructure and preventing malicious attacks on vehicle control systems.

- **Scenario:** In a smart city, autonomous vehicles rely on seamless communication with traffic lights, road sensors, and other infrastructure to navigate safely. However, malicious hackers could exploit vulnerabilities, intercepting data packets or sending false information, which may lead to accidents, traffic disruptions, or unauthorized access to vehicle control systems.
- **Solution:** Develop robust cybersecurity protocols using encryption, authentication, and intrusion detection systems for autonomous vehicles. Implement a secure vehicle-to-infrastructure (V2I) communication framework that includes regular software updates, secure coding practices, and real-time monitoring to identify and mitigate potential threats.
- **Impact:** By securing autonomous vehicles in smart cities, we enhance public safety, reduce the risk of accidents, and foster public trust in autonomous technology. This proactive approach not only safeguards individual vehicles but also contributes to the overall integrity of smart city infrastructure, promoting smoother traffic flow and efficient urban mobility.

2.Public Wi-Fi Security in Smart Cities:

Design a cybersecurity solution that secures public Wi-Fi networks in smart cities, providing safe internet access while protecting users from cyber threats.

- **Scenario:** In a smart city, public Wi-Fi networks are widely available in parks, cafes, and transportation hubs, allowing residents and visitors to access the internet easily. However, this convenience comes with significant risks, such as data interception, malware distribution, and unauthorized access to personal information. Cybercriminals exploit

these vulnerabilities, putting users' sensitive data at risk and undermining trust in smart city initiatives.

- **Solution:** Implement a comprehensive cybersecurity solution featuring end-to-end encryption, secure login protocols (e.g., WPA3), and a robust firewall to protect public Wi-Fi networks. Additionally, deploy a network monitoring system that detects and mitigates suspicious activities in real time. User education programs on safe browsing practices and the importance of using VPNs can further enhance security and instil user confidence.

- **Impact:** This solution significantly reduces the risk of cyber threats in public Wi-Fi networks, promoting user trust and encouraging more people to utilize these services. By providing secure internet access, smart cities can enhance community engagement, drive economic growth, and foster a safer digital environment, ultimately improving the quality of life for residents and visitors alike.

Agri Innovate

1.Blockchain for Agricultural Supply Chain Security:

Develop a blockchain-based solution to secure the agricultural supply chain, ensuring transparency and preventing fraud in transactions between farmers, suppliers, and consumers.

- **Scenario:** In the agricultural sector, farmers face challenges with transparency and trust in their supply chains. Fraudulent activities, such as misrepresentation of product origins and quantities, lead to financial losses and reduced consumer confidence. Farmers, suppliers, and consumers often lack real-time information

about product quality, origin, and transaction history, making it difficult to ensure fair practices and traceability.

- **Solution:** Implementing a blockchain-based solution can enhance security and transparency in the agricultural supply chain. By recording every transaction on a decentralized ledger, all stakeholders—farmers, suppliers, and consumers—can access immutable records of product origin, quality, and movement. Smart contracts can automate and enforce agreements, reducing the risk of fraud and ensuring compliance with regulations while providing real-time data to all parties involved.

- **Impact:** This blockchain solution can significantly improve trust among stakeholders in the agricultural supply chain, leading to increased consumer confidence and higher sales for farmers. Enhanced traceability allows for quicker responses to quality issues, reducing waste and losses. Ultimately, this system can promote fairer pricing, boost agricultural productivity, and encourage sustainable practices, benefiting the entire ecosystem.

2. IoT Security for Smart Farming:

Create a secure framework for IoT devices used in precision agriculture, preventing unauthorized access to farming data and ensuring reliable operation of automated systems.

- **Scenario:** In a smart farming environment, IoT devices monitor soil conditions, crop health, and weather patterns, enabling precision agriculture. However, unauthorized access to these devices can lead to data manipulation or disruption of automated systems, resulting in crop loss and financial setbacks for farmers. As cyber threats increase, the need for a secure framework to protect sensitive farming data and ensure operational reliability becomes paramount.

- **Solution:** Implement a secure framework that includes strong authentication mechanisms, data encryption, and regular security updates for IoT devices. Utilize blockchain technology to create an immutable ledger for data transactions, ensuring transparency and accountability. Establish network segmentation to isolate critical

systems from less secure devices and deploy intrusion detection systems to monitor and respond to potential threats in real-time.

- **Impact:** The proposed security framework enhances the resilience of smart farming operations against cyber threats, safeguarding sensitive data and maintaining the integrity of automated systems. This leads to increased trust among farmers in IoT technologies, enabling more widespread adoption and investment in precision agriculture. Ultimately, it enhances productivity, reduces losses, and promotes sustainable farming practices, contributing to food security and environmental sustainability.