SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107 An Autonomous Institution Accredited by NBA – AICTE and Accredited by NAAC
UGC wit'A' Grade Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING IOT Including CS&BCT
COURSE NAME : DISTRIBUTED LEDGER TECHNOLOGY

TOPIC: Preventing Cybercrime Through Blockchain

Introduction to Blockchain and Cybercrime Prevention

Cybercrime is a growing threat, targeting sensitive data, digital assets, and infrastructure. Blockchain offers a powerful way to fight cybercrime through decentralization, transparency, and immutability. Unlike traditional systems that can be hacked through a central point, blockchain has no single point of failure, making it harder for attackers to manipulate or steal information.

Securing Data with Immutability and Transparency

Blockchain ensures that once data is written, it cannot be altered or deleted. This immutability protects records from tampering and fake entries.

- All transactions are time-stamped and traceable, making it easy to detect suspicious activities.
- Organizations can use blockchain to store logs, documents, and user access histories, ensuring no one can modify them in secret.
- This transparency acts as a deterrent to internal and external cyber attackers.

Decentralization Reduces Attack Surface

Traditional systems often store sensitive data in centralized databases, which are prime targets for hackers.

- Blockchain distributes data across a network of nodes, making it almost impossible for a single attack to compromise the system.
- Even if one node is compromised, the rest of the network continues to function safely, preserving data integrity.
- This makes blockchain a strong foundation for securing critical infrastructure, such as finance, healthcare, and government services.

Real-World Use Cases in Cybercrime Prevention

Blockchain is already being used in several areas to reduce cybercrime:

- Identity Management: Prevent identity theft by using blockchain for secure, verifiable digital identities.
- IoT Security: Secure smart devices using blockchain-based authentication, preventing unauthorized access.
- Supply Chain Authentication: Protect products from counterfeit by verifying each step of the supply chain on the blockchain.
- Anti-Phishing Systems: Blockchain-based DNS systems make it harder for attackers to spoof websites and trick users.