NFCM Technicals

1. Introduction to NFCM

The National Financial Cybersecurity Mission (NFCM) aims to strengthen the digital financial infrastructure by promoting awareness, cybersecurity hygiene, and resilience against digital threats. This mission supports initiatives that secure financial platforms, build trust among citizens, and encourage safe financial behavior in the digital economy.

2. Key Technical Areas

- Digital Payment Security (e.g., UPI, QR code authentication, tokenization)
- Phishing & Scam Detection Algorithms
- Multi-factor Authentication (MFA) and Biometric Security
- Secure Digital Identity (eKYC, Aadhaar masking)
- Data Encryption and Secure Communication Protocols
- AI & ML in Fraud Detection and Risk Scoring
- Cyber Incident Reporting & Response Frameworks
- Financial Threat Intelligence Sharing (Banks, NBFCs, FinTechs)

3. NFCM Implementation Strategies

- Establishing cyber literacy programs for citizens and financial institutions. - Creating sector-specific cyber risk frameworks and simulation exercises. - Integrating AI agents in financial platforms for secure transaction guidance. - Collaborating with CERT-In, RBI, and NPCI to share threat intelligence.

4. Tools and Technologies Used

- IBM Watsonx and Granite for AI-powered financial advisory
- SIEM (Security Information and Event Management) tools
- UEBA (User and Entity Behavior Analytics) systems
- Blockchain-based identity validation solutions
- Vector Databases for threat pattern retrieval

5. Expected Outcomes

- Enhanced digital trust and financial inclusion. - Reduced fraud rates in digital transactions. - Empowered citizens with cybersecurity awareness. - Strengthened public-private collaboration in securing financial systems.