COURSE TITLE	**INTRODUCTION TO FINTECH AND SECURITY**
COURSE CODE	**01CC0708**
COURSE CREDITS	**3**

Objective:

1 This course provides an introduction to the dynamic world of Financial Technology (FinTech) and examines the critical security challenges and considerations inherent in this rapidly evolving domain. Students will gain an understanding of key FinTech areas such as digital payments, blockchain, and alternative finance, while simultaneously exploring the unique security risks, threats, and regulatory requirements that shape the industry. The course emphasizes the importance of building security into FinTech solutions from the ground up and covers essential security measures, compliance standards, and emerging trends at the intersection of finance and technology.

Course Outcomes: After completion of this course, student will be able to:

1 Apply fundamental concepts of FinTech, including digital payments, alternative finance, and the FinTech ecosystem, to analyze real-world financial technology applications

2 Analyze core FinTech technologies such as blockchain, APIs, cloud computing, and AI/ML, with a focus on their security implications and associated risks.

3 Analyze various security threats in FinTech, including data breaches, financial fraud, cyberattacks, insider threats, and third-party risks, to determine their impact on financial systems.

4 Evaluate security measures and controls in FinTech, including authentication mechanisms, cryptographic techniques, fraud detection systems, and secure software development practices

5 Design and develop secure FinTech solutions by integrating regulatory requirements, compliance standards, and emerging security technologies to address future challenges.

Pre-requisite of course: Basic understanding of core financial concepts (e.g., transactions, payments, lending). Familiarity with fundamental information technology concepts. Basic understanding of cybersecurity concepts (e.g., threats, data breaches)

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
1	**Introduction to FinTech** FinTech (Financial Technology) definition, scope of FinTech, historical evolution of FinTech,, Digital Payments (mobile payments, online transfers), Alternative Finance (P2P lending, crowdfunding), Wealth Management (robo-advisors), InsurTech, RegTech, FinTech ecosystem (startups, incumbent financial institutions, technology providers, regulators), drivers of FinTech innovation and adoption	5
2	**Core FinTech Technologies and Security Implications** Digital Payment Technologies (payment gateways, mobile wallets, contactless payments – how security is integrated and challenged), Blockchain and Distributed Ledger Technology (DLT) (fundamentals of blockchain relevant to finance, security properties (immutability, transparency), potential vulnerabilities in implementation), Application Programming Interfaces (APIs) in FinTech (Open Banking) (role of APIs, security risks (API vulnerabilities, data exposure), security best practices for FinTech APIs), Cloud Computing in FinTech (benefits, security concerns specific to financial data in the cloud, compliance in cloud environments), Artificial Intelligence (AI) and Machine Learning (ML) in FinTech (brief introduction to applications like fraud detection, credit scoring)	8
3	**Security Risks and Threats in FinTech** Data Breaches in FinTech (types of sensitive data handled, common causes, consequences),, Financial Fraud (payment fraud (card-not-present fraud, account takeover), identity theft and synthetic identity fraud, loan fraud), Cyberattacks Targeting FinTech (DDoS attacks on payment platforms malware targeting financial data, phishing and social engineering specific to financial services),, Insider Threats in FinTech (misuse of privileged access, data theft by employees), Third-Party and Supply Chain Risks in the FinTech Ecosystem	6
4	**Security Measures and Controls in FinTech** Authentication and Access Control in FinTech (strong authentication methods (MFA, biometrics), adaptive authentication, identity verification (KYC/AML integration)),, Cryptography in FinTech (encryption for data at rest and in transit (TLS/SSL), secure key management considerations),, Fraud Detection and Prevention Techniques (rule-based systems, machine learning for fraud detection, behavioral analytics, transaction monitoring), Secure Software Development Practices for FinTech Applications (secure coding standards, security testing (SAST, DAST, Penetration Testing) in a FinTech context), Physical Security Considerations for FinTech Infrastructure	8

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
5	**Regulatory Landscape, Compliance, and Future of FinTech Security** Key Regulations and Standards (overview of relevant regulations (e.g., GDPR, CCPA for data privacy),, financial industry standards (e.g., PCI DSS for card payments)), Know Your Customer (KYC) and Anti-Money Laundering (AML) Compliance (the role of technology (RegTech) in meeting these requirements), Regulatory Sandboxes and their impact on security practices, Emerging Security Threats (risks from advanced AI attacks, potential impact of quantum computing on current cryptography), Future Trends in FinTech Security (AI for enhanced security, decentralized finance (DeFi) security challenges, privacy-enhancing technologies)	5
Total Hours		**32**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Research and Present on a FinTech Area: Students research a specific FinTech area (e.g., InsurTech, Robo-advisors) and present on its basic functionality and inherent security considerations.	2
2	**Practical 2** Explore Security Features of a Mobile Payment App: Examine the security features and settings available in a popular mobile payment or banking application.	2
3	**Practical 3** Using a Tool to Inspect Website Security: Use a browser's developer tools or an online scanner to analyze the SSL/TLS configuration and security headers of a public FinTech website.	2
4	**Practical 4** Using a Tool to Inspect Website Security: Use a browser's developer tools or an online scanner to analyze the SSL/TLS configuration and security headers of a public FinTech website.	2
5	**Practical 5** Simulating a Secure Authentication Flow: Design and document the steps of a secure multi-factor authentication process for a hypothetical FinTech application.	2
6	**Practical 6** Researching KYC/AML Requirements: Research the basic KYC/AML compliance requirements for opening an account with a specific type of FinTech service (e.g., a cryptocurrency exchange or a P2P lending platform).	2
7	**Practical 7** Analyzing the Security Risks of Open APIs: Given a simple diagram of two systems interacting via an API in a FinTech context, identify potential security risks.	2

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
8	**Practical 8** Exploring Blockchain Explorer: Use a public blockchain explorer (e.g., for Bitcoin or Ethereum) to understand the transparency and immutability of transactions (without engaging in any transactions).	2
9	**Practical 9** Investigating Fraud Detection Techniques: Research and describe the working principles of a specific fraud detection technique used in FinTech (e.g., transaction monitoring, behavioral analytics).	2
10	**Practical 10** Mini-Project: Proposing Security Controls: For a hypothetical simple FinTech product (e.g., a basic budgeting app with user accounts), identify potential threats and propose appropriate security controls and design considerations.	2
Total Hours		**20**

Textbook :

1 Cybersecurity Challenges in FinTech: Assessing Threats and Mitigation Strategies for Financial Institutions": A comprehensive review of cybersecurity challenges and mitigation strategies in the FinTech sector, Dr. Uma Maheswari S Dr. Gargi Chaudhary Francis Manna Mr. Vivek Pandurang Khalane Dr. E. Muthukumar, Educational Administration: Theory and Practice, 2024

References:

1 "The Human Factor in FinTech: Tips for Improving Data Security": Discusses the importance of human elements in cybersecurity and offers practical tips., "The Human Factor in FinTech: Tips for Improving Data Security": Discusses the importance of human elements in cybersecurity and offers practical tips., Sumsub Editorial Team, Sumsub, 2023

2 "FinTech Security: How to Protect Your FinTech App": Provides a checklist and best practices for securing FinTech applications., "FinTech Security: How to Protect Your FinTech App": Provides a checklist and best practices for securing FinTech applications., DashDevs Editorial Team, DashDevs, 2023

Suggested Theory Distribution:

The suggested theory distribution as per Bloom’s taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery

Remember / Knowledge	Understand	Apply	Analyze	Evaluate	Higher order Thinking / Creative
0.00	6.00	28.00	23.00	29.00	14.00

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Instructional Method:

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1. FinTech Security and Regulation (RegTech
2. FinTech Risk Management Course

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)