# Pokhara University
## Faculty of Science and Technology

Course No: CMP 641 (3 Credits) Full marks: 100
Course Title: **Blockchain Technology(Elective)** Pass marks: 60
Nature of the course: Theory Total Lectures: 45 hrs.
Level: Masters Program: MSc

## 1. Course Description

This course provides an in-depth introduction to Blockchain Technology, its foundational concepts, and real-world applications. Students will explore the underlying cryptographic principles, consensus algorithms, smart contracts, and blockchain protocols like Ethereum and Hyperledger. The course emphasizes knowledge enabling students to design, develop, and deploy decentralized applications (DApps). It also includes coverage of Web3 ecosystems, Non-Fungible Tokens (NFTs), Decentralized Finance (DeFi), and emerging governance models such as DAOs. Emphasis is placed on security, scalability, and legal frameworks, providing a holistic understanding of blockchain's impact across industries including finance, supply chain, healthcare, and governance.

## 2. General Objectives

- Understand the fundamental principles of blockchain technology.
- Analyze various blockchain consensus mechanisms and architectures.
- Develop smart contracts using platforms like Ethereum and Solidity.
- Explore real-world applications of blockchain in various sectors.
- Design and implement decentralized applications (DApps).
- Evaluate the scalability, security, and privacy aspects of blockchain.
- Understand the Web3 ecosystem including NFTs, DeFi, and DAOs.
- Examine regulatory, ethical, and governance considerations in blockchain adoption.

## 3. Methods of Instruction

Lectures with interactive discussion, Instructor-led demonstrations, Group assignments and project work, Guest lectures from industry experts, Case study analysis and Student presentations.

## 4. Contents in Detail

| Specific Objectives | Contents |
|---|---|
| - Define blockchain/DLT, characteristics, types, benefits, challenges, applications.<br><br>- Understand its foundational role. | **Unit 1: Introduction to Blockchain (6 hrs)**<br>1.1 Defining Blockchain, Blockchain Evolution<br><br>1.2 Distributed Ledger Technology (DLT), Generic Blockchain elements, Blockchain Header<br><br>1.3 Blockchain Characteristics, Blockchain Structure<br><br>1.4. Blockchain Applications in Health, Insurance, Media, Asset Management, Supply Chain, Food Safety, Banking, Government<br><br>1.5 Types of Blockchain (Public, Consortium & Private)<br><br>1.6 Blockchain Benefits, Obstacles & Challenges, Current Landscape and Future Trends |
| - Explain essential cryptography: encryption, hashing, signatures, Merkle Trees.<br><br>- Understand algorithms (RSA, ECC), ZKPs. | **Unit 2: Cryptography for Blockchain (5 hrs)**<br>2.1 Symmetric and Asymmetric Cryptography<br><br>2.2 Public and Private keys, DES, AES, RSA, ECC<br><br>2.3 Open SSL, Hash Function, Hash Pointer and Data Structure<br><br>2.4 Merkle Trees, Distributed Hash Table (DHTs), Digital Signature, Multisignature, Elliptic Curve Digital signature algorithm (ECDSA)<br><br>2.5 Zero Knowledge Proofs (ZKPs) |
| - Describe Bitcoin history, architecture, transactions, mining, security.<br><br>- Differentiate Bitcoin/altcoins, understand ICOs, SPV. | **Unit 3: Cryptocurrency Fundamentals (5 hrs)**<br>3.1 Bitcoin Definition, Bitcoin History, Bitcoin Block, Genesis Block, Token and ICO, Bitcoin Exchanges<br><br>3.2 Bitcoin Payment, Bitcoin Transactions, Script Parsing and Processing, Simplified Payment Verification (SPV)<br><br>3.3 Bitcoin Architecture, Bitcoin P2P Network, Bitcoin Address, Bitcoin Storage & Uses, Bitcoin Security, Wallet<br><br>3.4 Altcoins, Cryptocurrency Ecosystem, Relationship between Altcoins & Bitcoin |

| | |
|---|---|
| - Analyze consensus mechanisms (PoW, PoS, BFT).<br><br>- Compare approaches, explain forks, evaluate security/scalability trade-offs. | **Unit 4: Consensus Mechanisms (5 hrs)**<br>4.1 Distributed Consensus<br><br>4.2 Byzantine Generals Problem, Byzantine Agreement, Byzantine Fault Tolerance (BFT), Lamport-Shostak-Pease BFT Algorithm<br><br>4.3 Proof of Work, Proof of Stake, Proof of Authority, Proof of Burn, Proof of Elapsed Time, Proof-of-X approaches<br><br>4.4 Virtual Mining, Mining Difficulty, SegWit and Forks (Hard and Soft) |
| - Define smart contracts, history, implications (DAOs).<br><br>- Learn design best practices, execution, failure modes, automation. | **Unit 5: Smart Contracts (5 hrs)**<br>5.1 Smart contract Definition, History of Smart Contract<br><br>5.2 Economic Concept of Contracts, Regulation and Legal Frameworks<br><br>5.3 DAO, Consensus Protocols and Inter-Contract Execution<br><br>5.4 Smart Contract Design, Smart Contract Best Practices, Smart Contract Failure and responses.<br><br>5.5 Solidity for Smart Contract Development |
| - Explore Ethereum: Ether, gas, structure, EVM, state, transactions.<br><br>- Identify tools/languages for DApp development. | **Unit 6: Ethereum Ecosystem & dApp Development (6 hrs)**<br>6.1 Introduction, Ethereum Blockchain: Currency, Forks, Gas, Ethereum Structure<br><br>6.2 Consensus Mechanism, World State, Transactions<br><br>6.3 Elements of Ethereum Blockchain: Ethereum Virtual Machine<br><br>6.4 Ethereum Environment, Precompiled Contracts, Ether, Messages, Accounts, Block, Mining<br><br>6.5 Ethereum testnets & dApp Development: tools, languages, compilers |
| - Analyze Hyperledger Fabric architecture/consensus.<br><br>- Understand components, | **Unit 7: Hyperledger Fabric and Permissioned Blockchain (7 hrs)**<br>7.1 Introduction, Hyperledger Architecture, Consensus Algorithm in Hyperledger, Hyperledger Node |

| | |
|---|---|
| flow, channels, identity, tools for enterprise chaincode. | 7.2 Hyperledger Fabric: Fabric Architecture, Transaction Flow in Fabric, Components of Fabric<br><br>7.3 Ordering Services, Channels in Fabric, Fabric Peer and Certificate Authority<br><br>7.4 Fabric Membership and Identity management, Hyperledger Fabric Network<br><br>7.5 Hyperledger Composer, Hyperledger Explorer, Hyperledger Caliper, Chaincode, Peers |
| - Explore Web3 stack, Layer 2, NFTs, DeFi, and interoperability.<br><br>- Assess legal, ethical, and sustainability issues in blockchain and decentralization. | **Unit 8: Web3, Emerging Technologies, and Socio-Ethical Aspects (6 hrs)**<br><br>8.1 Layer 2 solutions (Polygon, Optimism, zkRollups)<br><br>8.2 Introduction to Web3 stack: Wallets, IPFS, The Graph, NFTs, DeFi basics<br><br>8.3 Interoperability: Polkadot, Cosmos<br><br>8.4 Data privacy, GDPR, and blockchain<br><br>8.5 Environmental impact of mining<br><br>8.6 Regulatory landscape: Nepal and global overview, Ethical considerations of decentralization |

## 5. Case Studies

- Blockchain in Supply Chain (e.g., IBM Food Trust)
- DeFi platforms (e.g., Uniswap, Compound)
- Blockchain for identity and e-governance (e.g., Estonia's e-Residency)
- Blockchain in E-Governance and Voting Systems

## 6. Evaluation system

| **Evaluation Components** | **Weight (%)** | **Marks** |
|---|---|---|
| Internal Evaluation | | |
| Attendance & Class Participation | 10% | 6 |
| Assignments | 10% | 6 |
| Presentations/Quizzes | 10% | 6 |
| Internal Assessment | 50% | 30 |
| Practical and Case Studies | 20% | 12 |

| | | |
|---|---|---|
| Total Internal | | 60 |
| Semester-End Examination (Theory) | 100% | 40 |
| | **Total** | **100** |

## 6. Student Responsibilities

Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for the Semester-End Examinations. Students are advised to attend all the classes, formal exam, test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

## References:


1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
2. Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain (2nd ed.). O'Reilly Media.
3. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.
4. Singhal, B., Dhameja, G., & Panda, P. S. (2018). Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions. Apress.
5. Bashir, I. (2017). Mastering Blockchain: Master the Theoretical and Technical Foundations of Blockchain Technology and Explore Its Future (2nd ed.). Packt Publishing.
6. Antonopoulos, A. M., & Wood, G. (2018). Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media.

**Pokhara University**
**Faculty of Science and Technology**

Course Code.:CMP 642
Course title: **Cryptography (Elective)**
Nature of the course: Theory/Tutorial/Practical
Year: 2025

Full marks: 100
Pass marks: 45
Time per period: 1 hour
Total periods: 45
Level: Master
Program: ME
Computer/MSC

## 1. Course Description

This course is designed to establish the theoretical foundations and practical implementations of modern cryptography with an emphasis on advanced concepts. It builds on introductory cryptography, delving deeper into symmetric and asymmetric cryptographic primitives, cryptographic hash functions, message authentication, number theory, and post-quantum cryptographic schemes. Moreover, the course aims to foster a comprehensive understanding of cryptographic security models and the ability to rigorously analyze protocols for confidentiality, integrity, and authenticity in real-world systems.

## 2. General Objectives

: The course is designed with the following general objectives:

- To make students competent in symmetric and asymmetric cryptographic primitives.
- To make the students competent in the principles of provable security and cryptographic hardness assumptions.
- Familiarize the formal model of cryptographic construction.
- To be able to implement cryptographic schemes (e.g., RSA, El Gamal, HMAC) in lab environments.
- To make the students competent in post-quantum cryptographic candidates (e.g., lattice-based NTRU, hash-based signatures).
- Enable students to apply cryptography to secure protocols (SSL/TLS, IPsec).

## 3. Methods of Instruction

- Lectures with slides and blackboard explanations

- Interactive tutorial discussions and problem-solving sessions
- Hands-on practical labs involving cryptographic programming
- Student-led presentations on advanced topics
- Assignments and project-based learning

## 4. Contents in detail with specific objectives

| Specific Objectives | Contents |
|---|---|
| - Define computational security and secure encryption schemes, including CPA and CCA security.<br><br>-Differentiate concrete and asymptotic security.<br>- Prove security via reductionist arguments. | **Unit 1: Private-Key Encryption (7 hrs)**<br>1.1 Computational Security : Concrete and Asymptotic Approach<br>1.2 Computationally Secure Encryption<br>1.3 Constructing Secure Encryption Schemes, Pseudorandom Generators<br>1.4 Proofs by Reduction<br>1.5 Stronger Security Notions: Chosen-Plaintext Attacks and CPA-Security<br>1.6 Constructing CPA-Secure Encryption Schemes<br>1.6.1 Pseudorandom Functions, CPA-Secure Encryption from Pseudorandom functions<br>1.7 Chosen-Ciphertext Attacks |
| - Formalize integrity vs. Secrecy.<br>- Design CBC-MAC and analyze its security.<br>- Implement authenticated encryption<br>- Interpret message integrity and authenticity using MACs. | **Unit 2: Message Authentication Codes (6 hours)**<br>2.1 Message Integrity, Secrecy vs. Integrity, and Encryption vs. Message Authentication<br>2.2 Message Authentication Codes<br>2.3 Constructing Secure Message Authentication Codes: A Fixed-Length MAC, Domain Extension for MACs<br>2.4 CBC-MAC: The Basic Construction<br>2.5 Authenticated Encryption<br>2.5.1 Generic Constructions<br>2.5.2 Secure Communication Sessions |

| | |
|---|---|
| -Construct cryptographic hash functions.<br>- Prove collision resistance of Merkle-Damgård.<br>- Implement HMAC and Merkle trees.<br>- Analyze the random oracle model. | **Unit 3: Hash Functions and Applications (6 hrs.)**<br>3.1 Collision Resistance and Weaker Notions of Security<br>3.2 Domain Extension: The Merkle–Damgard Transform<br>3.3 Message Authentication using Hash Functions, Hash-and-MAC<br>3.4 Generic Attacks on Hash Functions: Birthday Attacks for Finding Collisions and Small-Space Birthday Attacks<br>3.5 The Random-Oracle Model<br>3.5.1 Soundness of Random-Oracle Methodology<br>3.6 Additional Applications of Hash Functions: Fingerprinting and Deduplication, Merkle Trees, Password Hashing and Key Derivation . |
| - Apply modular arithmetic to RSA/DH.<br>- Generate safe primes for cryptographic use.1<br>- Formalize hardness assumptions (Factoring, DLOG) | **Unit 4: Number Theory and Cryptographic Hardness Assumptions (6 hours)**<br>4.1 Preliminaries and Basic Group Theory: Primes and Divisibility, Modular Arithmetic, Groups, The Group Z_N*<br>4.2 Primes, Factoring, and RSA: Generating Random Primes, The Factoring Assumption, and The RSA Assumption<br>4.3 Cryptographic Assumptions in Cyclic Groups: Cyclic Groups and Generators<br>4.4 The Discrete-Logarithm/Diffie–Hellman Assumptions<br>4.5 Elliptic Curve Arithmetic |
| - Interpret secure constructions of public-key encryption schemes.<br>- Contrast CPA/CCA-security in hybrid encryption.<br>- Implement El Gamal and RSA<br>- Analyze KEM/DEM paradigms. | **Unit 5: Public-Key Encryption (6 hours)**<br>5.1 Public-Key Encryption : Security against Chosen-Plaintext Attacks, and Security against Chosen-Ciphertext Attacks<br>5.2 Hybrid Encryption and the KEM/DEM Paradigm : CPA-Security and CCA-Security<br>5.3 CDH/DDH-Based Encryption<br>5.3.1 El Gamal Encryption<br>5.3.2 DDH-Based Key Encapsulation<br>5.4 RSA Encryption<br>5. 5 Elliptic Curve Cryptography |

| | |
|---|---|
| -Interpret security protocols and standards on the internet.<br><br>-Configure TLS/SSL for secure channels.<br><br>-Deploy PGP/SMIME for email security. | **Unit 6 : Network and Internet security (6 Hrs)**<br><br>6.1 Web Security Issues<br><br>6.2 Secure Sockets Layer (SSL) Security<br><br>6.3 Transport Layer Security (TLS)<br>6.4. HTTPS<br>6.5 Secure Shell (SSH)<br>6.6. Electronic mail security: Pretty Good Privacy (PGP) and S/MIME<br>6.7 IP Security Overview: Applications and Benefits of IPsec |
| - Interpret quantum-resilient cryptographic primitives (lattice based, code based, multivariate based and hash based)<br><br>- Compare lattice-based (NTRU, LWE) and hash-based signatures.<br><br>- Implement NTRU and McEliece .<br><br>- Analyse various Multivariate scheme | **Unit 7: Post-Quantum Cryptography (8 Hrs)**<br><br>7.1 Overview of post-quantum Cryptography<br>7.2 Lattice-based Cryptography<br>7.2.1 NTRU<br>7.2.2 Lattices and the Security of NTRU<br>7.2.3 Learning With Errors<br>7.3 Code-based Cryptography: the McEliece Cryptosystem<br>7.4. Multivariate Cryptography: Hidden Field Equations, The Oil and Vinegar Signature Scheme<br>7.5 Hash-based Signature Schemes : Lamport Signature Scheme and an overview of Winternitz Signature Scheme |

## 5. List of Tutorials

The following tutorial activities of 16 hours per group of maximum 24 students should be conducted to cover all the required contents of this course.

| S.N. | Tutorials |
|---|---|
| 1 | Symmetric encryption security proofs (reduction-based) |
| 2 | Constructing PRFs and their applications |
| 3 | CPA vs CCA: construction and examples |

| | |
|---|---|
| 4 | MAC construction and collision resistance exercises |
| 5 | CBC-MAC case study |
| 6<br>7 | HMAC implementation and security analysis<br>Birthday problem and hash collisions |
| 8<br>9 | Hash-based MAC implementation<br>Group theory refresher for cryptography |
| 10 | RSA key generation and vulnerabilities |
| 11 | ElGamal implementation and hybrid encryption |
| 12 | Exploring TLS handshake protocol |
| 13<br>14 | Secure email protocols simulation<br>Lattice-based cryptography : NTRU exercises |
| 15 | Code-based cryptosystem example: McEliece |
| 16 | Construct a toy examples of Oil and Vinegar Signature |
| 17 | Lamport Signature Scheme exercises |

## 6. Practical Work: Implementation in SageMath, Python or any Other languages

| S.N. | Practical Works |
|---|---|
| 1 | Implement a stream cipher using a PRG |
| 2 | Simulate a block cipher and apply ECB/CBC modes |
| 3 | Design and test a CPA-secure encryption using a PRF |
| 4 | Implement CBC-MAC and analyze its behavior |

| | |
|---|---|
| 5 | RSA encryption/decryption tool with key generation |
| 6 | ElGamal encryption and decryption module |
| 7 | SSL/TLS protocol implementation in Python/Java |
| 8 | Secure email simulation using PGP |
| 9 | Implement NTRU encryption/decryption in Python/Sage |
| 10 | Implement McEliece Cryptosystem in Python/Sage |
| 11 | Implement Multivariate bases schemes in Python/Sage |

## 7. Evaluation system and students' responsibilities

**Internal Evaluation**

In addition to the formal end-semester exam(s), the internal (formative) evaluation of a student may consist of quizzes, assignments, lab reports, projects, class participation and presentation etc. The tabular presentation of the internal evaluation is as follows. The components may differ according to the nature of the subjects.

| **Internal Evaluation** | **Weight** | **Marks** | **External Evaluation** | **Marks** |
|---|---|---|---|---|
| **Theory** | | 30 | | |
| Attendance & Class Participation | 10% | | | |
| Assignments | 20% | | | |
| Presentations/Quizzes | 10% | | | |
| Internal Assessment | 60% | | | |
| **Practical** | | 20 | | |
| Attendance & Class Participation | 20% | | | |
| Lab Report/Project Report | 30% | | Semester-End examination | 50 |
| Practical Exam/Project Work | 30% | | | |

| | | | | |
|---|---|---|---|---|
| Viva | 20% | | | |
| Total Internal | | 50 | | |
| Full Marks: 50 + 50 = 100 | | | | |

**Student requirements**:
Each student must secure at least 45% marks in internal evaluation with 80% attendance in the class in order to appear in the semester-end examination. Failing to get such a score will be equated with NOT QUALIFIED (NQ) and the student will not be eligible to appear in the End- Semester examinations. Students are advised to attend all the classes and complete all the assignments within the specified time period. Failure of a student to attend a formal exam, quiz, test, etc. won't qualify him/her for re-exam. ***Students are required to complete all the requirements defined for the completion of the course***

## 8. Prescribed Books and References


1. Cryptography Theory and Practice , Douglas R. Stinson, Maura B. Paterson, CRC Press.
2. Introduction to Modern Cryptography, Jonathan Katz,Yehuda Lindell McGraw Hill.
3. A Graduate Course in Applied Cryptography, Dan Boneh and Victor Shoup, Stanford University.

**Pokhara University**
**Faculty of Science and Technology**

Course No.: CMP 644 Full marks: 100

Course title: Information System Audit (Elective) Pass marks: 60

Nature of the course: Theory Total Lectures: 45 hrs.

Level: Masters Program: ME CE/MSc CS

## 1. Course Description

The Information System Audit course for graduate students provides an in-depth understanding of auditing principles, methodologies, and best practices for assessing the security, integrity, and compliance of information systems. The course covers risk assessment, control frameworks, IT governance, regulatory compliance, and emerging threats in cybersecurity. Students will gain hands-on experience in auditing IT infrastructure, applications, and processes through case studies and practical exercises. This course covers different concepts of Information Systems Auditing including basics, hardware and software security issues, information systems audit and conducting IS audit, risk-based systems audit, business continuity and disaster, auditing in the ICT environment, and security testing.

## 2. General Objectives

- To develop a foundational understanding of information systems auditing principles, processes, and methodologies.
- To explore risk-based auditing approaches within ICT environments.
- To examine the role of Governance, Risk, and Compliance (GRC) in information systems auditing.
- To understand the importance of business continuity and disaster recovery in audit planning.
- To gain familiarity with security testing tools, vulnerability assessment, and penetration testing techniques.
- To analyze emerging trends and challenges in the field of information systems auditing.

## 3. Methods of Instruction

Lecture, Discussion, Readings, Case Studies and Group Workshops

**4. Contents in Detail.**

| Specific Objectives | Contents |
|---|---|
| Acquire knowledge of the fundamental concept of Information System Audit and IT Audit Frameworks with emphasis on widely known standards such as ISO 27001, NIST, COBIT, CIS, MITRE and C2M2 | **Unit 1: Overview of Systems Audit (8 Hrs.)**<br>1.1 Information Systems Audit and Information Systems Auditor<br>1.2 Legal Requirements of an Information Systems Audit<br>1.3 Systems Environment and Information Systems Audit<br>1.4 Information Systems Assets and Classification of Controls<br>1.5 Information Systems Audit Coverage<br>1.6 Government and Regulatory Frameworks<br>1.7 IT Audit Framework, ISO 27001, NIST Cyber Security Framework, COBIT, CIS, MITRE, C2M2 |
| Gain the key concept of Hardware and Software Security Issues during Information System Audit | **Unit 2: Hardware and Software Security Issues (8 Hrs.)**<br>2.1 Hardware Security Objective<br>2.2 Peripheral Devices and Storage Media<br>2.3 Authentication Devices<br>2.4 Hardware Acquisition, Hardware Maintenance and Management of Obsolescence<br>2.5 Disposal of Equipment; Problem Management; Change Management<br>2.6 Network and Communication Issues.<br>2.7 Overview of Types of Software; Elements of Software Security<br>2.8 Control Issues during Installation and Maintenance<br>2.9 Licensing Issues, ICT Procurement Practices |
| Acquire the idea of Information System Audit Requirements in terms of Information System Control, Logs and Evidence Collection | **Unit 3: Information Systems Audit Requirements (8 Hrs.)**<br>3.1 Information Systems Control Objectives; Information Systems Audit Objectives;<br>3.2 System Effectiveness and Efficiency<br>3.3 Information Systems Abuse<br>3.4 Asset Safeguarding Objective and Process<br>3.5 Evidence Collection and Evaluation<br>3.6 Logs and Audit Trails as Evidence<br>3.7 IT Audit Standard and Regulatory Requirements |
| Gain the concept Information System Auditing | **Unit 4: Conducting an Information Systems Audit (10 Hrs.)**<br>4.1 Audit Program and Audit Plan<br>4.2 Audit Procedures and Approaches<br>4.3 System Understanding and Review<br>4.4 Compliance Reviews and Tests<br>4.5 Substantive Reviews and Tests<br>4.6 Audit Tools and Techniques<br>4.7 Sampling Techniques |

| | |
|---|---|
| | 4.8 Audit Questionnaire; Audit Documentation; Audit Report<br>4.9 Auditing Approaches; Sample Audit Work-Planning Memo<br>4.10 Sample Audit Work Process Flow<br>4.11 Conducting a Risk-Based Information Systems Audit<br>4.12 Risk Assessment and Risk Management Strategy. |
| Acquire knowledge of Business continuity and Disaster Recovery Plan during Information System Audit | **Unit 5: Business Continuity and Disaster Recovery Plan (6 Hrs.)**<br>5.1 Business Continuity and Disaster Recovery Process<br>5.2 Business Impact Analysis; Incident Response Plan<br>5.3 Disaster Recovery Plan<br>5.4 Types of Disaster Recovery Plans<br>5.5 Emergency Preparedness Audit Checklist<br>5.6 Business Continuity Strategies<br>5.7 Business Resumption Plan Audit Checklist<br>5.8 Recovery Procedures Testing Checklist; Plan Maintenance Checklist. |
| Apply the concept of VAPT, Cloud Computing Audits and Emerging Concepts | **Unit 6: Security Testing and Cloud Computing Audit (5 Hrs.)**<br>6.1 Cybersecurity<br>6.2 Vulnerability Assessment and Penetration Testing (VAPT)<br>6.3 Secured Software Development Testing,<br>6.4 Open Web Application Security Project<br>6.5 Security Testing Tools<br>6.6 Cloud Audit Considerations<br>6.7 Emerging Concepts in Information System Audit |

**5. Group Workshops**

The Group workshop should cover the following works:

| SN | Group Workshops |
|---|---|
| 1. | Information Security Gap Assessment through ISO 27001 |
| 2. | Cybersecurity Maturity Assessment through NIST Cybersecurity Framework |
| 3. | Develop IS Audit Terms of Reference |
| 4. | Develop the detailed Proposal for Conducting an Information System Audit |
| 5. | Conduct Information System Audit and Reporting |
| 6. | IT Governance Audit through Control Objectives for Related Technologies |
| 7. | Conducting Risk Assessment |

6. **Evaluation system and Students' Responsibilities**

**Internal Evaluation**

The internal evaluation of a student may consist of assignments, attendance, internal assessment and group workshop. The internal evaluation scheme for this course is as follows:

| **Internal Evaluation** | **Weight** | **Marks** | **External Evaluation** | **Marks** |
|---|---|---|---|---|
| **Theory** | | | Semester-End examination | 40 |
| Attendance & Class Participation | 10% | 6 | | |
| Assignments | 10% | 6 | | |
| Presentations/Quizzes | 20% | 12 | | |
| Internal Assessment | 40% | 24 | | |
| Group Workshops | 20% | 12 | | |
| **Total Internal** | | 60 | | |
| Full Marks: 60 + 40 = 100 | | | | |

**Student Responsibilities**:

Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for the Semester-End Examinations. Students are advised to attend all the classes, formal exam, test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

**7. Prescribed Books and References**

**References**:


1. Hall, J. A. (2020). *Information Technology Auditing and Assurance* (5th ed.). Cengage Learning
2. Moeller, R. (2022). *IT Audit, Control, and Security* (3rd ed.). Wiley.
3. ISACA. (2024). *CISA Review Manual.* ISACA.
4. ISACA. (2022). *COBIT 2019 Framework: Governance and Management of Enterprise IT.* ISACA
5. Veena Hingarh and Arif Ahmed (2013), *Understanding and Conducting Information Systems Auditing*, Wiley
6. Jack J. Champlain (2003), *Auditing Information Systems*, 2nd Edition, Wiley
7. Richard Cascarino (2007), *Auditor's Guide to Information Systems Auditing*, Wiley
8. ISACA Journals
9. ISACA IT Audit Frameworks
10. NIST Special Publications
11. COBIT, CIS Frameworks, MITRE, C2M2

**Pokhara University**
**Faculty of Science and Technology**

Course No.: CMP 644 Full marks: 100

Course Title: Digital Ecosystem (Elective) Pass marks: 60

Nature of the course: Theory Total Lectures: 45 hrs.

Level: Masters Program: ME CE/MSc CS

## 1. Course Description:

This course explores the comprehensive concept of digital ecosystems, covering their evolution, theoretical foundations, architecture, governance models, enabling technologies, sector-specific applications, and emerging trends. Students engage with real-world examples and practical assignments to understand and apply digital ecosystem strategies effectively.

## 2. General Objectives:

This course aims to equip students with an in-depth understanding of digital ecosystems, their components, management practices, and strategic implications, enabling students to apply ecosystem thinking effectively across business, governmental, and societal contexts.

## 3 .Methods of Instruction:

The course employs interactive lectures, class discussions, group assignments, case studies, and presentations. Students will conduct research on various topics, prepare reports, and engage in practical design and analytical exercises.

## 4. Contents in Detail.

| **Specific Objective** | **Unit 1: Introduction to Digital Ecosystems (4 hrs)** | |
|---|---|---|
| Define digital ecosystems and identify their key characteristics | ● Definition and Key Characteristics | |
| | ● Evolution from Traditional Ecosystems to Digital Ecosystems | |
| | ● Components: Platform, Participants, Data, and Value | |
| | ● Real-world Examples (e.g., Amazon, Google, Alibaba, Smart Cities) | |
| | ● Overview of Nepal's digital journey (Digital Nepal Framework) | |

| | | |
|---|---|---|
| | **Unit 2: Theoretical Foundations (5 hrs)** | |
| Apply theoretical concepts to analyze digital ecosystems | ● Introduction to Ecosystem Theory (Complex Systems Theory, Platform Theory, Network Effects Theory, Co-Evolution Theory, Innovation Ecosystem Theory) | |
| | **Unit 3: Architecture and Design of Digital Ecosystems (6 hrs)** | |
| Analyze open versus closed ecosystem architectures | ● Layers: Physical, Application, Service, and Business Layers | |
| | ● Open vs Closed Ecosystems | |
| | ● API Economy and Interoperability | |
| | ● Data Flow and Integration in Ecosystems | |
| | **Unit 4: Governance and Management (5 hrs)** | |
| Assess governance implications in managing digital ecosystems | ● Ecosystem Governance Models (Centralized Governance Model, Decentralized Governance Model, Hybrid Governance Model) | |
| | ● Platform Leadership and Orchestration | |
| | ● Trust, Security, and Privacy Issues | |
| | **Unit 5: Technologies Enabling Digital Ecosystems (6 hrs)** | |
| | ● Internet of Things (IoT) and Edge Computing | |
| Evaluate how emerging technologies support ecosystem functionalities | ● Artificial Intelligence and Machine Learning (Application of AI in Digital Ecosystem) | |
| | ● Blockchain and Decentralization | |
| | ● Cloud Computing and Microservices | |
| | **Unit 6: Digital Ecosystems in Different Sectors (6 hrs)** | |
| Identify strategic advantages of digital ecosystems in various sectors | ● E-commerce and Retail Ecosystems | |
| | ● Health and Smart City Ecosystems | |
| | ● Education Ecosystems (MOOCs, EdTech) | |
| | ● Tourism and Hospitality Ecosystems | |
| | ● Industrial and Manufacturing Ecosystems (Industry 4.0) | |
| | **Unit 7: Business Models and Strategy (5 hrs)** | |
| Apply ecosystem mapping and strategic positioning tools | ● Platform Business Models (Transaction Platform Model, Advertising Platform Model, Data-Driven Platform Model, Product-as-a-Service) Platform Model, Social Platform Model) | |
| | ● Ecosystem Mapping and Strategic Positioning | |
| | ● Metrics for Ecosystem Health and Success | |
| | ● Case Studies of Failures and Successes (e.g., Nokia, Uber, Tesla, Panasonic, KODAK) | |
| | **Unit 8: Emerging Trends and Future Directions (4 hrs)** | |
| Evaluate the impact of emerging trends on future digital ecosystems | ● Metaverse and Immersive Ecosystems | |
| | ● Ecosystemization of AI | |
| | ● Sustainable Digital Ecosystems (Green IT) | |

| | | |
|---|---|---|
| | ● Digital Twin Ecosystems | |
| | ● Research Frontiers and Open Challenges | |
| | **Practical Component / Assignments:** | |
| | ● **Case Study Analysis**: Choose a real-world domain digital ecosystem (e.g.: health, education, governance, fintech) | |
| | ● **Ecosystem Design Project**: Design a digital ecosystem for a sector (e.g., agriculture, tourism, finance). | |
| | ● **Research Paper / White Paper**: Investigate a current trend (e.g., DAOs in ecosystems, platform monopolies). | |
| | ● **Group Presentation**: Emerging Technologies Shaping Future Ecosystems | |

5. **Evaluation system and Students' Responsibilities**

**Internal Evaluation**

The internal evaluation of a student may consist of assignments, attendance, internal assessment and group workshop. The internal evaluation scheme for this course is as follows:

| **Internal Evaluation** | **Weight** | **Marks** | **External Evaluation** | **Marks** |
|---|---|---|---|---|
| **Theory** | | | Semester-End examination | 40 |
| Attendance & Class Participation | 10% | 6 | | |
| Assignments | 10% | 6 | | |
| Presentations/Quizzes | 20% | 12 | | |
| Internal Assessment | 40% | 24 | | |
| Group Workshops | 20% | 12 | | |
| **Total Internal** | | 60 | | |
| Full Marks: 60 + 40 = 100 | | | | |

**6. Student Responsibilities**:

Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for the Semester-End

Examinations. Students are advised to attend all the classes, formal exam, test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

## 7. Prescribed Books and References

**Textbooks:**


- Parker, G. G., Van Alstyne, M. W., &Choudary, S. P. (2016). Platform revolution: How networked markets are transforming the economy and how to make them work for you. W. W. Norton & Company.
- Cusumano, M. A., Gawer, A., &Yoffie, D. B. (2019). The business of platforms: Strategy in the age of digital competition, innovation, and power. Harper Business.
- Corallo, A., Passiante, G., &Prencipe, A. (2007). Digital business ecosystems. Edward Elgar Publishing.


**Reference Books:**


- Tiwana, A. (2013). Platform ecosystems: Aligning architecture, governance, and strategy. Morgan Kaufmann.
- Adner, R. (2012). The wide lens: What successful innovators see that others miss. Portfolio Penguin.
- Easley, D., & Kleinberg, J. (2010). Networks, crowds, and markets: Reasoning about a highly connected world. Cambridge University Press.