BACHELOR'S DEGREE PROGRAMME

B.Tech.

Computer Science and Engineering with Specialization in Internet of Things and Cyber Security including Blockchain Technology

Academic Curricula

2024-2028

SCHOOLOFCOMPUTERENGINEERING

KALINGAINSTITUTEOF INDUSTRIAL TECHNOLOGY
BHUBANESWAR – 751024

ODISHA,INDIA

Programme Specific Outcome (PSO)

- Design and develop intelligent automated systems applying mathematical, analytical, programming and operational skills to solve real world problems.
- Apply different security techniques, software tools to conduct experiments, interpret data and to solve complex problems.
- Implement engineering solutions for the benefit of society by the use of intelligent techniques.

Guideline and Notes to obtain the Specialization

A student has to follow the B.Tech Computer Science curricula. To get the specialization the student has to take the following as the professional electives in the respective semester from the basket.

PE: Professional Elective				
Sl.No	**CourseCode**	**Course Title**	**Pre-requisites**	**Credits**
PE I		Any one Subject from PE- I Basket of CSE Syllabus.		3
PE II	CS30031	Privacy and Security in IoT	-	3
PE III	CS30014	Principle of Cryptography		3
PE IV	CS40015	Industrial IoT		3
PE V	CS40012	Block chain		3

Course Title	Privacy and Security in IoT
CourseCode (Credit)	CS30031 (L-T-P-Cr: 3-0-0-3)
Pre-requisites	

Course Objectives:

- To impart knowledge on the state-of-the-art methodologies and Security in Internet of Things (IoT).
- To understand the Privacy Preservation and Trust Models in Internet of Things (IoT).
- To study the Internet of Things (IoT) Security protocols and Security framework.

CourseContents:

UNIT I

Security in IoT

IoT security: Vulnerabilities, Attacks and Countermeasures - Security Engineering for IoT development - IoT security lifecycle.

UNIT II

Network Robustness and Malware Propagation Control in IoT

Network Robustness - Fusion Based Defense Scheme - Sequential Defense Scheme - Location Certificate Based Scheme - Sybil node detection scheme - Formal Modeling and Verification -Sybil Attack Detection in Vehicular Networks - Performance evaluation of various Malware Dynamics Models - Analysis of Attack Vectors on Smart Home Systems.

UNIT III

Blockchain Technology in IoT

Technical Aspects - Integrated Platforms for IoT Enablement - Intersections between IoT and Distributed Ledger - Testing at scale of IoT Blockchain Applications - Access Control Framework for Security and Privacy of IoT - Blockchain Applications in Healthcare.

UNIT IV

Privacy Preservation in IoT

Privacy Preservation Data Dissemination: Network Model, Threat Model – Problem formulation and definition - Baseline data dissemination - Spatial

Privacy Graph based data dissemination -Experiment Validation - Smart building concept-Privacy Threats in Smart Building - Privacy Preserving Approaches in Smart Building - Smart Meter Privacy Preserving Approaches.

UNIT V

Privacy Protection in IoT

Lightweight and Robust Schemes for Privacy Protection in IoT Applications: One Time Mask Scheme, One Time Permutation Scheme - Mobile Wireless Body Sensor Network - Participatory Sensing.

UNIT VI

Trust Models for IoT

Trust Model Concepts - Public Key Infrastructures Architecture Components - Public Key Certificate Formats - Design Considerations for Digital Certificates - Public Key Reference Infrastructure for the IoT - Authentication in IoT - Computational Security for IoT.

UNIT VII

Security Protocols for IoT Access Networks

Time Based Secure Key Generation -Security Access Algorithm: Unidirectional, Bidirectional Transmission - Cognitive Security - IoT Security Framework - Secure IoT Layers – Secure Communication Links in IoT - Secure Resource Management, Secure IoT Databases.

Course Outcome:

At the end of this course, student will be able to:

- Identify different Internet of Things technologies and their applications.
- Assess the need for Privacy and security model for the Internet of Things.
- Explore various Trust Model for IoT and customize real time data for IoT applications.
- Design security framework and solve IoT security issues

Text Book(s)

1. Hu, Fei. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, 2016, 1st edition, CRC Press, USA.

Reference Books

1. Russell, Brian and Drew Van Duren. Practical Internet of Things Security, 2016,1st edition, PACKT Publishing Ltd, UK

2. Kim, S., Deka, G. C., & Zhang, P. (2019). Role of blockchain technology in IoT applications. Academic Press.
3. Whitehouse O Security of things: An Implementers' guide to cyber-security for internet of things devices and beyond, 2014, 1st edition, NCC Group, UK.

Course Title	**PrinciplesofCryptography**
CourseCode (Credit)	**IT40009 (L-T-P-Cr: 3-0-0-3)**

CourseObjectives:

- Togainknowledgeaboutthe mathematicsofthecryptographicalgorithms
- Togetaninsightintotheworkingof differentexistingcryptographicalgorithms
- Tolearnaboutkeyexchangeprotocolsand attacksonsuch protocols
- Tointroducethefundamentalconceptsofhashfunctionsanddigitalsignatures
- Tolearnhowtousecryptographicalgorithmsinsecurity

CourseContents:

UNIT I

MathematicalFoundations:

NumberTheory:Fermat'stheorem,Cauchy'stheorem,Chineseremaindertheorem, Primalitytestingalgorithm, Euclid'salgorithmforintegers, quadraticresidues, Legendresymbol,Jacobisymbol.*

UNIT II

Classical Cryptosystems:

Cryptographyandcryptanalysis,ClassicalCryptography,differenttypeofattack: CMA,CPA,CCA,Shannonperfectsecrecy,OTP,Pseudorandombitgenerators, streamciphersandRC4.*

UNIT III

Symmetric Key Ciphers:

Blockciphers:Modesofoperation,DESanditsvariants,finitefields(2^n),AES,linear anddifferentialcryptanalysis.*

UNIT IV

Asymmetric Key Ciphers:

One-way function, Trapdoorone-way function, Public key cryptography, RSA cryptosystem, Diffie-Hellmankeyexchangealgorithm,ElGamalCryptosystem.*

UNIT V

Message Authentication:

Cryptographic hash functions, secure hash algorithm, Message authentication, digital signature, RSAdigitalsignature.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Identify the relevance of number theory, group, ring, finite fields and modular arithmetic in various contexts of Cryptography

CO2:Assess use of symmetric crypto system, public key crypto system and digital signature scheme

CO3: Design and implement cryptographic protocols

CO4: Discuss the security of cryptographic algorithms

CO5: Evaluate the security of a protocol based on security metrics

CO6: Justify the usage of security principles and digital signatures for any application

Textbooks:

1. Stinson.D.,"Cryptography: Theory and Practice", Third Edition, Chapman&Hall/CRC,2012.
2. Douglas Robert Stinson, Maura Paterson. "Cryptography: Theory and Practice", Fourth Edition, Chapman&Hall/CRC,2012.

ReferenceBooks:

1. W.Mao,"ModernCryptography:Theory&Practice",PearsonEducation,2010.
2. William.Stallings,"CryptographyandNetworkSecurityPrinciplesandpractice",SeventhEdition,PearsonEducation,2013.

Course Title	**Industrial IoT**
CourseCode(Credit)	**CS 40015 (L-T-P-Cr: 3-0-0-3)**

Course Objectives

- To provide students with a good depth of knowledge of Designing Industrial IOT Systems for various applications.

Course Contents:

UNIT – I

Introduction To Industrial Internet and Use-Cases: Industrial Internet- Key IIoT Technologies- Innovation and the IIoT -Key Opportunities and Benefits -

The Digital and Human Workforce - Logistics and the Industrial Internet- IOT Innovations in Retail.

UNIT – II

The Technical and Business Innovators of The Industrial Internet: Cyber Physical Systems (CPS), – IP Mobility – Network Virtualization - SDN (Software Defined Networks)- The Cloud and Fog – Role of Big Data in IIOT - Role of Machine learning and AI in IIOT

UNIT – III

IIOT Reference Architecture: Industrial Internet Architecture Framework (IIAF) -Industrial Internet Viewpoints -. Architectural Topology: The Three-Tier Topology- Key System Characteristics- Data Management- Advanced data analytics.

UNIT – IV

Protocols for Industrial Internet Systems: Legacy Industrial Protocols - Modern Communication Protocols-Proximity Network Communication Protocols- Wireless Communication Technologies- Gateways: industrial gateways - CoAP (Constrained Application Protocol)- NFC.

UNIT – V

Middleware Software Patterns and IIOT Platforms: Publish/Subscribe Pattern: MQTT, XMPP, AMQP, DDS- Middleware Architecture- SigFox-LoRaWAN Augmented reality- Real-World Smart Factories, Application of IIOT: Case study: Health monitoring, IoT smart city, Smart irrigation, Robot surveillance.

Course Outcomes:

CO1: Identify the Key opportunities and benefits in Industrial IoT
CO2: Apply virtual network to demonstrate the use of Cloud in Industrial IoT
CO3: Analyze industrial IoT Three tier topology and data management system
CO4: Summarize Legacy Industrial and Modern Communication Protocols
CO5: Describe Middleware Architecture, LoRaWAN- and Augmented reality

TEXT BOOKS:

1. Gilchrist, Alasdair, “Industry 4.0 The Industrial Internet of Things”, Apress, 2017.

REFERENCE BOOKS:

1. Sabina Jeschke, Christian Brecher, Houbing Song, Danda B. Rawat “Industrial Internet of Things: Cyber manufacturing Systems” (Springer), 2017.
2. Zaigham Mahmood, “The Internet of Things in the Industrial Sector: Security and Device connectivity, smart environments and Industry 4.0 (Springer), 2019.
3. Industrial IoT Challenges, Design Principles, Applications, and Security by Ismail Butun (editor)
4. Vijay Madisetti and Arshdeep Bahga, “Internet of Things (A Hands-on-Approach)”, 1st Edition, VPT, 2014.
5. Michahelles, “Architecting the Internet of Things”, ISBN 978-3- 642-19156-5 e-ISBN 978-3-642- 19157-2, Springer
6. Francis daCosta, “Rethinking the Internet of Things: A Scalable Approach to Connecting Everything”, 1st Edition, Apress Publications, 20132 Cuno Pfister, Getting Started with the Internet of Things, O ‟Reilly Media, 2011, ISBN: 978-1-4493-9357-1

Course Title	**Block Chain**
CourseCode (Credit)	**CS40012 (L- T- P-Cr: 3-0-0-3)**

Course Objectives

- To understand the design principles Block Chain
- To describe differences between proof-of-work and proof-of-stake consensus
- To understand building a distributed application
- To understand Bitcoin's consensus mechanism

Course Contents:

Unit I

Blockchain Fundamentals:

Fundamental of Blockchain Technology and its Importance, Electronic Systems and Trust, Distributed Versus Centralized Versus Decentralized, Bitcoin

Predecessors, DigiCash, E-Gold, Cryptographic hash functions, Properties of a hash function-Hash pointer and Merkle tree, digital signatures, B-Money, Evolution of the Blockchain Technology, Storing Data in a Chain of Blocks, Compelling Components, Achieving Consensus

Unit II

Cryptocurrency Fundamentals:

Basic cryptocurrency system, Public and Private Keys in Cryptocurrency Systems, The UTXO Model, Transactions, Signing and Validating Transactions, Bitcoin Transaction Security, Wallet Types: Custodial Versus Noncustodial, Lightweight wallets, Hierarchical deterministic wallets, Permissioned and Permissionless Consensus, Proof-of-Work, Proof-of-Stake, Proof of Burn, Proof of Elapsed Time, Bitcoin Miner, Mining Difficulty

Unit III

Distributed Consensus:

Permissioned Blockchain: Design issues for Permissioned blockchains, Execute contracts, State machine replication, Overview of Consensus models for permissioned blockchain- Distributed consensus in closed environment, Paxos, RAFT Consensus Algorithm, Practical Byzantine Fault Tolerance (PBFT), Lamport-Shostak-Pease BFT Algorithm.

Unit IV

Forks and Altchains:

Understanding Forks, Contentious Hard Forks, The Bitcoin Cash Fork, Altcoins, Litecoin, Privacy-Focused Crypto currencies, Segregated witness, Validation and Analysis of Smart Contracts, Evolution of Ethereum, The Ethereum Classic Fork, Comparison among Bitcoin, Ethereum, Stellar, Monero, ZCash, Quorum and Hyperledger fabric. Enterprise, Healthcare and transportation application of Blockchain

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Explain the design principles of Bitcoin and Ethereum.

CO2: List and describe differences between proof-of-work and proof-of-stake consensus.

CO3: Interact with a blockchain system by sending and reading transactions

CO4: Design, build and deploy a distributed application.

CO5: Apply the concept of Bitcoin's consensus mechanism and the interaction between Bitcoin and Altcoins

CO6: Familiarize with Ethereum, smart contracts and related technologies, and solidity language

Textbooks:

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
2. Lorne Lantz & Daniel Cawrey, Mastering Blockchain Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications, O'REILLY Publications

Reference Books:

1. Bina Ramamurthy, Blockchain in Action, MANNING Publication.
2. Bikramaditya Singhal, Gautam Dhameja, and PriyansuSekhra Panda, Beginning Blockchain, Apress Publication.
3. Draft version of "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, "Block chain Technology: Crypto currency and Applications", World Scientific, 2020.
4. Josh Thompson, "Blockchain: The Block chain for Beginnings, Guild to Block chain Technology and Block chain Programming', Create Space Independent Publishing Platform, 2017.