## SEMESTER – III

## 21NB71 PROJECT WORK – I
**vide Automotive Engineering 21AE71**

## SEMESTER – IV

## 21NB81 PROJECT WORK – II
**Vide Automotive Engineering 21AE81**

## PROFESSIONAL ELECTIVE THEORY COURSES (Four to be opted)

## 21NB21 / 21NN38 INFORMATION SYSTEM SECURITY MANAGEMENT

**3 0 0 3**

**INTRODUCTION:** Information Security Overview, Threat and Attack Vectors, Types of Attacks, Common Vulnerabilities and Exposure (CVE), Security Attacks, Fundamentals of Information Security, Computer Security Concerns, Information Security Measures, NOS 9001. (11)

**FUNDAMENTALS AND DATA LEAKAGE:** Key Elements of Networks, Logical Elements of Networks, Critical Information Characteristics, Information States, Work Effectively with Colleagues (NOS 9002), Data Leakage and Statistics, Data Leakage Threats, Reducing the Risk of Data Loss, Key Performance Indicators (KPI), Database Security. (11)

**POLICIES, PROCEDURES AND AUDITS:** Information Security Policies – Necessity, Key Elements and Characteristics, Security Policy Implementation, Configuration, Security Standards - Guidelines and Frameworks, Case Study: Cyber Security Audit. (11)

**ROLES AND RESPONSIBILITIES:** Security Roles and Responsibilities, Accountability, Roles and Responsibilities of Information Security Management, Team Responding to Emergency Situation- Risk Analysis Process, Case Study: Popular Standard- ISO/IEC 27001 Information Security Management. (12)

**Total L: 45**

**REFERENCES:**

1. Michael E.Whilman and Herbert J.Mattord “Management of Information Security”, 6thEdition, Cengage, USA, 2018.
2. Douglas Landoll “Information Security Policies, Procedures, and Standards - A Practitioner's Reference”, CRC Press, USA, 2016.
3. Michael T. Goodrich and Roberto Tamassia, “Introduction to Computer Security”, Addison Wesley, Boston, 2011
4. Harold F. Tipton and Micki Krause , “Information Security Management Handbook”, 6th Edition ,CRC Press, USA, 2007.


## 21NB22 INFORMATION ETHICS AND CYBER LAWS

**3 0 0 3**

**ETHICS IN IT:** Definition - Ethics in the business world: Corporate social responsibility – Improving corporate ethics – Ethical work environment - Ethics in Information Technology domain -Ethical considerations in decision making - Software engineering code of ethics and practices: IEEE-CS –ACM Joint task force. (10)

**ETHICAL THEORIES :** Utilitarianism, Intrinsic and instrumental value, Acts Vs. rules, Critique of utilitarianism, Deontological theory, Rights, Rights and social contract theory, Virtue ethics, Analogical reasoning in computer ethics. (11)

**INTELLECTUAL PROPERTY:** Copyrights, Patents, Trade secrets - Ethics of IT organizations: Key ethical issues for organization - Contingent workers – Outsourcing – Whistle blowing – Green computing - Types of Professional relationships - Conflicting responsibilities. (12)

**CYBER LAWS:** Information privacy – Privacy laws, applications and court rulings, Key privacy and anonymity issues: Data breaches – Electronic discovery – Consumer profiling – Workplace monitoring – Advanced surveillance technology - Licensing – Selling software – Piracy - Federal laws for prosecuting computer attacks - Risk assessment. (12)

**Total L:45**

**REFERENCES:**

1. George Reynolds, “Ethics in Information Technology” 6th Edition, Thomson Asia Pvt. Ltd., Chennai, 2019.
2. Deborah G Johnson, “Computer Ethics”, Pearson Education, New Delhi, 2009.
3. Akash Kamal Mishra, “Cyber Laws in India- Fathoming your Lawful Perplex”, Xpress Publishing., Chennai, 2020.
4. Richard A. Spinello, “Cyber Ethics, Morality and Law in Cyber Space”, 5th Edition, Jones & Bartlett Learning., MA,

2020.
5. Caroline Whitback, “Ethics in Engineering Practice and Research”, Cambridge University Press, UK, 2011.
6. Penny Duquenoy, Simon Jones and Barry G Blundell, “Ethical, legal and professional issues in computing”, Middlesex University Press,UK, 2008.

## 21NB23 BLOCKCHAIN AND CRYPTOCURRENCIES

**3 0 0 3**

**INTRODUCTION:**Blockchain Cryptography, Distributed P2P Network, Blockchain Architecture, Generic Elements of Blockchain, Distributed Ledger Technology, Mining, Rewards, Types of Blockchain Systems, Benefits, Features and Limitations of Blockchain, Consensus Mechanism. (11)

**CRYPTOCURRENCIES:**Bitcoin: Blocks, Merkle Tree, Keys, Addresses and Wallets, Transactions, Hardness of Mining and Consensus, Anonymity, Forks, Double Spending, Bitcoin Network, Bitcoin Clients and APIs, Ripple and Stellar, Alternative Coins. (12)

**BLOCKCHAIN PLATFORMS:**Ethereum Framework: Components, Smart Contracts, Ethereum Development Environment – Development Tools and Frameworks, Hyperledger: Tools and Framework, Hyperledger Fabric – Architecture – Components, Plug and Play Feature, Deploying Parachains. (12)

**APPLICATIONS**: Blockchain and Internet of Things (IoT), Blockchain for Payment, Blockchain for Enterprise, Case Study: Voting, Land Registry, Healthcare, Smart Appliances, Supply Chains. (10)

**Total L: 45**

**REFERENCES:**

1. Lorne Lantz and Daniel Cawrey, “Mastering Blockchain”, O'Reilly Media, Inc., California, 2020.
2. Andreas M. Antonopoulos, “Mastering Bitcoin: Programming the Open Blockchain”, 3rdEdition, Shroff Publishers and Distributors, Mumbai, 2018.
3. Chris Dannen, “Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners”, Apress, New York, 2018.
4. Gulshan Shrivastava, Dac-Nhuong Le, Kavita Sharma, “Cryptocurrencies and Blockchain Technology Applications”, Wiley-Scrivener, Massachusetts, 2020.

## 21NB24 CYBER WARFARE

**3 0 0 3**

**INTRODUCTION**: Cyber warfare, Cyber Threatscape, Cyberspace Battlefield, Cyber Doctrine - prevention, anticipation and detection. (9)

**CYBER WARRIOR:**Information Warfare, Defensive skill, Distributed denial of service attack, Ethical hacking, Offensive skill, PersonallyIdentifiable Information. (13)

**CYBER WEAPONS:**Logical weapons - Access and privilege escalation tool, Physical weapons - Electromagnetic attacks, Psychological Weapons - social engineering attack, Defense mechanisms. (11)

**CYBER WAR CAPABILITIES**: Operational aspects, Intelligence, planning and conduct of cyber-attack, Riots in Xinjiang and Chinese warfare, Asymmetrical threat in North Korea. (12)

**Total L: 45**

**REFERENCES:**

1. Jeffrey Carr, “Inside Cyber Warfare: Mapping the Cyber Underworld”, O'Reilly Media, USA, 2011.
2. Jason Andress and Steve Winterfeld, “Cyber Warfare Techniques, Tactics and Tools for Security Practitioners”, 2ndEdition, Syngress, USA, 2014.
3. Daniel Ventre, “Cyberwar and Information Warfare”, John Wiley & Sons.USA, 2012.
4. François Delerue, “Cyber Operations and International Law”, Cambridge University Press, USA, 2020.

## 21NB25 MOBILE SECURITY AND DEVICE FORENSICS

**3 0 0 3**

**INTRODUCTION TO MOBILE SECURITY:** Mobile computing technologies - Fundamentals of mobile computing - Mobile computing infrastructure, communications, devices, platforms, and applications – Cryptanalysis - Mobile Malware - Threat Scenarios - Mitigating Mobile Malware - Mobile Security Penetration Testing Tools. (9)

**MOBILE APPLICATION SECURITY**: Mobile Platform – Issues facing Mobile Devices – Apple iPhone – Google Android – Mobile Services – WAP and Mobile HTML Security – Bluetooth Security – SMS Security – Mobile Geolocation – Enterprise Security on Mobile OS. (12)

**DEVICE FORENSICS :** Introduction to Mobile Forensics - Mobile forensic challenges - Mobile phone evidence extraction process - Practical mobile forensic approaches - Mobile forensic tool leveling system - Data acquisition methods - Potential evidence stored on mobile phones - Good forensic practices – Android App Analysis and Overview of Forensic Tools (12)

**MOBILE DATA EXTRACTION**: Understanding Android model - Android security - Android Forensic Setup and Pre Data Extraction Techniques - Screen lock bypassing techniques - Android Data Extraction Techniques – Android & iOS Data Recovery Techniques (12)

**Total L: 45**

**REFERENCES:**


1. Himanshu Dwivedi, Chris Clark and David Thiel "Mobile Application Security", Mc Graw Hill, USA, 2015.
2. Nikoley Elenkov, "Android Security Internal: An In-depth Guide to Android's Security Architecture", No Starch Press, USA, 2015.
3. Eamon P. Doherty, "Device Forensics for Handheld Devices", Taylor & Franics Group, USA, 2013.
4. Noureddine Boudriga, "Security of Mobile Communications, Taylor & Franics Group, USA, 2010.


## 21NB26 DATA ANALYTICS FOR CYBER SECURITY

**3 0 0 3**

**INTRODUCTION:** Data Analytics Life Cycle: Data Ingestion – Data Processing and Cleaning - Visualization and Exploratory analysis - Classification - Clustering - Feature Extraction and Selection - Modeling - Model Selection and Fitting - Evaluation and Inference. Security Analytics, Basics of Security, Attacker and their Motivations , Security Goals: Confidentiality - Integrity - Availability - Authentication - Access Control - Accountability - Non-repudiation , Attacks and Impacts, Applications of Data Science to Security Challenges: Malware – Intrusions - Spam/Phishing - Credit Card Fraud - Denial of Service. (11)

**ANALYTICS TECHNOLOGY AND TOOLS:** Streaming Data Analytics - Map Reduce Framework - Hadoop, SPARK, Tools: Pig - Hive - Splunk - Sqoop - Flume, Open Source Databases: Hbase - MongoDB. - Neo4j. (12)

**STATISTICS AND DATA MINING:** Probability Theory: Bayes theorem - Binomial Distribution - Poisson Distribution - Geometric, Continuous, Uniform, Exponential, Normal and Chi Square Distribution. Unsupervised Learning - K-Means Clustering - Malware Detection - Hierarchical Clustering - Malware Clustering. Supervised Learning - Naïve Bayes - Logistic Regression - Decision Trees and Random Forest - Support Vector Machines – Phishing URL Detection - Intrusion Detection - Botnet Detection. (11)

**TEXT MINING AND NATURAL LANGUAGE PROCESSING**: Tokenization - Pre-processing - Bag-Of-Words - Vector space model - Latent Semantic Indexing – Embedding - Sentiment Analysis. Natural Language Processing - Text pre-processing - Feature Engineering on Text Data - Corpus-based Analysis - Email Spam Detection - Phishing Email Detection. (11)

**Total L: 45**

**REFERENCES:**


1. Rakesh M. Verma and David J. Marchette, "Cybersecurity Analytics", CRC Press, USA, 2019.
2. Mehedy Masud, Latifur Khan and Bhavani Thuraisingham, "Data Mining Tools for Malware Detection", CRC press, USA, 2016.
3. Tony Thomas, Athira P. Vijayaraghavan and Sabu Emmanuel, "Machine Learning Approaches in Cyber Security Analytics", Springer Singapore, 2019.
4. Drew Conway and John White, "Machine Learning for Email", O'Reilly Media, USA, 2011.
5. Sumeet Dua and Xian Du, "Data Mining and Machine Learning in Cybersecurity", CRC Press, USA, 2011.
6. EMC Education Services, "Data Science and Big data Analytics: Discovering, Analyzing, Visualizing and Preserving Data", Wiley, USA, 2015.


## 21NB27 ADVANCED PERSISTENT THREAT

**3 0 0 3**

**INTRODUCTION:**Threat – Current Landscape - Proactive vs. Reactive Security, Cyber Cancer, Characteristics of APT, APT vs. Traditional Threat, Stages of APT, Assessing the Risk of APT, Cyber Kill Chain. (10)

**APT HACKER ATTACK PHASES:** AHM Components, Core Steps: Reconnaissance - Enumeration - Exploitation - Maintaining Access - Clean Up - Progression - Exfiltration, Reconnaissance Data: Technical - Non Technical, Social Engineering Tactics, Spear-Phishing Methods, Remote Targeting: Client Hacking, Spear Phishing, Physical Infiltration, Physical Social Engineering, Defeating Physical Security Controls. (13)

**DEFENSE MECHANISM FOR APT:** Security Management for APT Threats, Security Technology Measures, Managing an APT Incident, Conducting APT Controls Review, Advanced Dissecting Techniques, Application Crashing Monitoring, Behavior-Based Analysis, Implementing Proactive Security and Reputational Ranking, Implementing Adaptive Security. (12)

**ADVANCED ATTACKS AND TOOLS:** APT Attacks: Stuxnet – Duqu – Flame - Iran Certificate Attack - Equation Group and Grayfish, APT Attack Simulators: CALDERA - Infection Monkey - Flightsim. (10)

**Total L: 45**

**REFERENCES:**


1. Tyler Wrightson, “Advanced Persistent Threat Hacking: The Art and Science of Hacking any Organization”, McGraw Hill, New Delhi, 2015.
2. Eric Cole, “Advanced Persistent Threat”, Syngress, USA, 2013.
3. Ira Winkler and Araceli Treu Gomes, “Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies”, Syngress, USA, 2016.
4. Charles P Pfleeger and Shari Lawrence Pfleeger, “Analyzing Computer Security: A Threat, Vulnerability, Countermeasure Approach”, Pearson Education, New Delhi, 2014.


## 21NB28 PATTERN RECOGNITION

**3 0 0 3**

**REPRESENTATION**: Introduction to pattern recognition, Pattern representation, Segmentation and Grouping, Feature extraction, Analysis, Feature selection, Applications of pattern recognition. (7)

**CLASSIFICATION TECHNIQUES:** Nearest neighbor algorithm, Variants of the NN algorithm, Use of the nearest neighbour algorithm, Branch and bound algorithm, Data reduction, Prototype selection - Bayes Classifier: Introduction, Continuous features, Minimum error rate classification, Classifiers, Discriminant functions and decision surfaces, Normal density and its discriminate function, Discrete features, Estimation of probabilities. (15)

**HIDDEN MARKOV MODELS**: Markov models for Classification, Hidden Markov models: HMM parameters - Learning HMMs, Classification using HMMs, Speech Recognition, Biological Analysis. (8)

**UNSUPERVISED LEARNING AND CLUSTERING:** Mixture Densities and Identifiability, Maximum Likelihood Estimates, Application to Normal Mixtures, Unsupervised Bayesian Learning - Clustering: Partitional clustering, Hierarchical Algorithms-Divisive clustering - Agglomerative clustering, Clustering large data sets. (15)

**Total L:45**

**REFERENCES:**


1. Murty MN and Devi VS, “Introduction to pattern recognition and machine learning”, World Scientific press, Singapore, 2015.
2. Homenda W and Pedrycz W, “Pattern Recognition: A Quality of Data Perspective”, John Wiley & Sons, New York, 2018.
3. Duda, Richard O, Peter E. Hart, and David G. Stork, “Pattern classification”, John Wiley & Sons, New York, 2012.
4. Bhardwaj A and Verma P.,“Textbook on Pattern Recognition”, Alpha Science International, Ltd, UK, 2015.


## 21NB29 DESIGN AND ANALYSIS OF SECURITY PROTOCOLS

**3 0 0 3**

**MATHEMATICAL FOUNDATIONS:** Probability and Information Theory, Computational Complexity: Deterministic Polynomial Time, Probabilistic Polynomial Time, Non-deterministic Polynomial Time, Algebraic and Number Theory Foundations. (9)

**CRYPTOGRAPHIC TECHNIQUES, SECURITY NOTIONS AND DEFINITIONS**: Zero-knowledge Proof, Semantic Security, Provable Security: Standard Model, Group Model, Random Oracle Model, Unconditional Security, Security Properties, Cryptographic Techniques: Symmetric and Asymmetric Techniques - Data Integrity Techniques. (14)

**MODELING AUTHENTICATION PROTOCOLS:** Authentication Types and Techniques, Modeling Authentication Protocol: EKE - PAKE - SSH - SSL/TLS, Typical Attacks and Vulnerabilities. (8)

**ANALYSIS OF SECURITY PROTOCOLS:** Formal Methods: Formal Specification of Protocols, Formal Proof of Security: Computational Model, Symbolic Manipulation View: Theorem Proving – Protocol and Adversary Models, Formal Analysis Techniques: Model Checking, NRL Protocol Analyzer, CSP Approach, FDR, Formal Analysis Tools: Murphi, AVISPA, Hermes, PRISM, ProVerif, Scyther, Limitations of Formal Analysis. (14)

**Total L:45**

**REFERENCES:**


1. Hans Delfs and Helmut Knebl, “Introduction to Cryptography”, Springer-Verlag, Berlin, 2015.
2. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Pearson Education, New Delhi, 2013.
3. Ling Dong and Kefei Chen, “Cryptographic Protocol”, Springer, Beijing, 2012.
4. Peter Ryan and Steve A. Schneider, “Modelling & Analysis of Security Protocols”, Addison-Wesley, New York, 2001.
5. Giampaolo Bella, “Formal Correctness of Security Protocols”, Springer, New York, 2007.

## 21NB30 CYBER SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

**3 0 0 3**

**INFORMATION SECURITY**: Foundations of Information Security, Security Mindset, Information Systems Strategy, Strategic Planning, Value of IT, Implementing IT Portfolio, Policies. (10)

**GOVERNANCE OF IT:** Governance of Enterprise IT – Good Practices for Governance of Enterprise IT - Frameworks – Audit Role in Governance of Enterprise IT – Information Security Governance. (11)

**MANAGEMENT OF IT**: Information Security Management – IS Management System – IS Management Roles and Responsibilities – Classification of Information Assets – IS Control Design – System Access Permissions – Privacy Principles and Role of IS Auditors. Compliance: Definition, Need, Requirements, Cost and solution. (12)

**AUDITING NETWORK INFRASTRUCTURE:** Auditing Remote Access – Auditing Internet points of Presence – Network Penetration tests – Full Network Assessment – Development & Authorization of Network changes – Unauthorized changes- Risk Management Process. (12)

**Total L: 45**

**REFERENCES:**


1. Michael Whitman and Herbert Mattord, “Management of Information Security”, Cengage Learning, USA, 2017.
2. Jason Andress and Steven Winterfeld, “The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice”, Elsevier, USA,2014.
3. Mark S Merkow , Jim Breithaupt, “Information Security: Principles and Practice”, Pearson Education Inc.., New Delhi, 2014.
4. Charles P. Pfleeger and Sari Lawrence Pfleeger, “Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach”, Pearson Education, New Delhi,2012.
5. Michael E Whitman, Herbert J Mattord, “Principles of Information Security”, Cengage Learning, USA, 2014.


## 21NB31 HUMAN COMPUTER INTERACTION

**3 0 0 3**

**INTRODUCTION:** Overview of HCI, Mental models, Cognitive architecture, Task loading and stress, Human error identification. (9)

**INPUT TECHNOLOGIES**: Sensor and recognition-based input, Haptic interfaces- Non speech auditory output- Network based interactions Visual design principles, Intercultural user interface designs -Conversational speech interface, Multimodal interface adaptive interfaces and agents. (12)

**DATA GATHERING, ANALYSIS AND PRESENTATION:** Key issues, Data recording, Interviews, Questionnaires, Observation, Choosing and combining Techniques, Qualitative and quantitative, Simple quantitative analysis, Tools, Theoretical frameworks. Design rules, Standards and Guidelines, Golden rules and heuristics patterns, Elements of windowing systems. (12)

**EVALUATION FRAMEWORK:** Goals of evaluation –Types of evaluation –Evaluation case studies: A framework to guide evaluation –Usability testing –Conducting experiments, Field studies –Inspections-Heuristic evaluation and walkthroughs, Collaboration and communication, Dialog Analysis and design , Human factors and society. (12)

**Total L: 45**

**REFERENCES:**


1. Jan Noyes and Chris Baber, “User Centered Design of Systems”, Springer, Germany, 2013.
2. Alan Dix, Janet Finlay, Gregory D Abowd and Russell Beale, “Human Computer Interaction”, Pearson, New Delhi, 2012.
3. John Helen Sharp, Yvanno Rogers and Jenny preece, “Interaction Design: Beyond Human Computer Interaction”, Wiley, USA,2011.
4. Ben Shneiderman, “Designing the User Interfaces Strategies for Effective Human Computer Interaction”, Pearson, New Delhi,2009


## 21NB32 NETWORK SECURITY

**3 0 0 3**

**NETWORK SECURITY:** Threats in networks, Network security controls, Intruders, Intrusion detection, Password management, Malicious software, Firewalls: Need – Characteristics – Types - Firewall basing - Firewall location and configurations. (11)

**AUTHENTICATION AND IP SECURITY:** Authentication systems, Authentication of people, Security handshake pitfalls, Strong password protocols, IP security overview, IP security policy, Encapsulating Security Payload, Combining security associations, Internet key exchange, Cryptographic suites, Integrated Windows Authentication, Single Sign On. (11)

**ELECTRONIC MAIL SECURITY:** Web security considerations, Secure Socket Layer, Transport Layer Security, HTTPS, Secure Shell, Store and forward, Establishing keys, Privacy, Source authentication, Message integrity, Non-Repudiation, Proof of submission and delivery, Pretty Good Privacy, Secure/Multipurpose Internet Mail Extension. (11)

**WIRELESS NETWORK SECURITY:** IEEE 802.11i wireless LAN security, Wireless Application Protocol, Wireless Transport Layer Security. Advanced Protocols: Zero knowledge proofs, Blind signatures, Identity based public key cryptography, Oblivious transfer, Digital certified mail, Simultaneous exchange of secrets, Security of Emerging Technology. (12)

**Total L: 45**

**REFERENCES:**


1. Alfred J Menezes, Paul C Van Oorschot and Scott A Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton,2010.
2. Bernard Menezes, "Network Security and Cryptography", Cengage Learning, New Delhi, 2011.
3. Chalie Kaufman, Radia Perlman and Mike Speciner, "Network Security: Private Communication in a Public World", Pearson Education, New Delhi, 2007.
4. Wenbo Mao, "Modern Cryptography", Pearson Education, New Delhi, 2013.


## 21NB33 OPERATING SYSTEM HARDENING

**3 0 0 3**

**PROCESS AND MEMORY MANAGEMENT:** Introduction, Operating System Structures – Simple, Layered, Kernel, Microkernel - Operations – Services, Process management: Process concept - Interprocess communication - CPU scheduling algorithms – Deadlocks, Memory management: Paging - Page replacement algorithms. (11)

**STORAGE MANAGEMENT:** Disk structure, Disk scheduling algorithms, File concept, Access methods, File system structure, File system implementation, Allocation methods, Free space management. (11)

**PROTECTION AND SECURITY:** Protection: Goals – Principles – Domain - Access matrix - Access control - Revocation of access rights - Capability-based systems, Kernel patch protection, Security: Program threats - System and network threats - User authentication - Security defenses Implementation - Firewalling to protect systems and networks, OS security patches. CASE STUDY: Linux system. (12)

**TRUSTED OPERATING SYSTEMS:** Trusted system, Security policies, Models of security, Design elements, Security features, Kernelized Design, Virtualization, Layered Design, Assurance: Flaws-Methods- Evaluation. (11)

**Total L: 45**

**REFERENCES:**


1. Silberschatz A, Galvin P and Gagne G, "Operating Systems Concepts", John Wiley and Sons, New York, 2018.
2. William Stallings, "Operating Systems: Internals and Design Principles", Pearson Education, New Delhi, 2018.
3. Deitel H M, "Operating System", Pearson Education, New Delhi, 2011.
4. Charles P Pfleeger and Shari Lawrence Pfleeger, "Security in Computing", Prentice Hall, New Delhi, 2018.
5. Michael Palmer, "Guide to Operating Systems Security", Cengage Learning, New Delhi, 2011.


## 21NB34 CYBER SECURITY FOR IOT AND EDGE COMPUTING

**3 0 0 3**

**CRYPTOGRAPHIC FUNDAMENTALS FOR IOT AND EDGE:** Introduction, Vulnerabilities, Attacks and Counter Measures, Security Engineering for IoT Development, IoT security life cycle, Cryptographic fundamentals for IoT Security Engineering.(11)

**SECURITY PROTOCOLS FOR IOT AND EDGE :** Infrastructure, IPv6, LowPAN, Identification, Electronic Product Code, uCode, Transport, Bluetooth, LPWAN, Data, MQTT, CoAP, Multi-layer Frameworks: Alljoyn -IoTivity. (11)

**IOT EDGE TO CLOUD ARCHITECTURE:** Identity lifecycle, Authentication credentials, IoT IAM infrastructure, Authorization with Publish Subscribe schemes, Access Control, Cloud and Fog Topologies, Open stack cloud architecture, Edge X. (12)

**PRIVACY PRESERVATION AND TRUST MODELS FOR IOT:** Concerns in data dissemination, Lightweight and robust schemes for Privacy protection, Trust and Trust models for IoT, Self-organizing Thing, Preventing unauthorized access. (11)

**Total L: 45**

**REFERENCES:**


1. Madhusanka Liyanage, An Braeken, Pardeep Kumar and Mika Ylianttila, "IoT Security: Advances in Authentication", John Wiley & Sons Ltd, 2019.
2. Fei Hu, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations", CRC Press, 2016.
3. Jie Wu and Wei Chang, "Fog/Edge Computing For Security, Privacy, and Applications", Springer International Publishing, 2020.
4. Shancang Li and Li Da Xu, "Securing the Internet of Things", Elsevier, USA, 2017.

## 21NB35 CLOUD SECURITY

**3 0 0 3**

**INTRODUCTION:** Characteristics – Architectural influences – Delivery models – Deployment models – Benefits – Data centers - Security objectives – CIA triad – Security services – Security design principles – Secure cloud software testing, Case study: Amazon AWS – Open Stack. (11)

**SECURITY ARCHITECTURE AND RISKS**: Overview – General issues – Trusted cloud computing – Execution environment – Micro architecture - Identity management and access control – Autonomic Security, Risk Management: Risk analysis – Trust Models – Privacy and compliance risks - Risk management framework, Metrics, API security, Data security, Cloud Security Alliance (CSA) - Certificate of Cloud Security Knowledge (CCSK). (11)

**CLOUD INFRASTRUCTURE AND VULNERABILITIES:** Virtualization –Types, Virtual machine provisioning and manageability, Virtual machine migration – VM migration attack, Cloud storage device: Cloud storage levels, Network storage interfaces, Database storage interfaces, Operational planning, Threat expectations – Threat Agents – Cloud security threats: Threats to infrastructure and data, Cloud service provider risk - Cyber security case studies: Energy– Healthcare– Banking – Military. (11)

**DESIGN PATTERNS:** Security patterns – Trusted platform – Geo tagging – VM platform encryption – Secure cloud interfaces – Resource access control – Cloud data breach protection – Permanent data loss protection – In-transit cloud data encryption – Denial-of-Service protection – Traffic Hijacking protection – Federated cloud authentication – Independent cloud auditing. (12)

**Total L: 45**

**REFERENCES:**


1 Melvin B Greer and Kevin L Jackson, “Practical Cloud Security: A Cross Industry View”,CRC Press, Boca Raton, 2017.
2. Ronald L Krutz and Russel Dean Vines, “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”, Wiley India, New Delhi, 2016.
3. Rajkumar Buyya, James Broberg and Andrzej Goscinski, “Cloud Computing: Principles and Paradigms”, Wiley India, New Jersey, 2016.
4. John R. Vacca, “Cloud Computing Security: Foundations and Challenges”, CRC Press, New York, 2017.
5. John W Rittinghouse and James F Ransome, “Cloud Computing: Implementation, Management and Security”, CRC Press, Boca Raton, 2017.
6. Thomas Erl, Robert Cope and Amin Naserpour, “Cloud Computing Design Patterns”, Prentice Hall, New York, 2015.


## 21NB36 CYBER PHYSICAL SYSTEMS

**3 0 0 3**

**CYBER PHYSICAL SYSTEM CONCEPTS:** Design challenges-Mobile cyber physical systems - Design principles - Physical system controls- Modeling Issues - Unmanned Aerial Vehicle Communications. (11)

**SENSOR BASED CYBER PHYSICAL SYSTEMS:** Wireless Sensor and Actuator Networks for Cyber Physical Systems-Applications-Community Sensing-Wireless Embedded/Implanted Micro Systems-Architecture and Security - Application of Machine Learning in monitoring physical activity. (12)

**INDUSTRIAL CONTROL SYSTEMS:** Energy efficient building Cyber Physical System for Smart Grid Applications-Cyber Physical System for transportation applications-Video communications in cyber physical systems. (11)

**MODELING CYBER PHYSICAL SYSTEMS:** Synchronous model, Asynchronous model, Dynamic systems, Timed model, Real Time scheduling, Hybrid system. (11)

**Total L: 45**

### References:


1. Fei Hu, “Cyber-Physical Systems: Integrated Computing and Engineering Design”, CRC Press, London, 2013.
2. Rajeev Alur, “Principles of Cyber Physical Systems”, MIT Press, London, 2015.
3. Houbing Song, **.Danda B**Rawat and **Physical Systems: Foundations, Principles and -Cyber“Sabina Jeschke, ,“Applications**
Elsevier Inc, CA, USA, 2017.
4. Danda B. Rawat, **Joel J.P.C. Rodrigues and Physical-Cyber“Ivan Stojmenovic,** Systems: From Theory to Practice“, CRC
Press, London, 2016


## 21NB37 DATA VISUALIZATION

**3 0 0 3**

**INTRODUCTION:**The Visualization Process - Scatter plot, Data Foundation - Types of Data - Visualization stages - Semiology of Graphical Symbols - The Eight Visual Variables - Experimental Semiotics based on Perception Gibson‘s Affordance theory – A Model of Perceptual Processing, Introduction to Tableau , RStudio. (11)

**SPATIAL, TIME ORIENTED DATA:** One-Dimension - Two-Dimension – Three Dimensional Data - Dynamic Data - Combining Techniques, Multivariate Data: Point-Based - Line Based - Region-Based Techniques, Characterizing and Visualizing Time-Oriented Data. (12)

**TREES, GRAPHS AND NETWORKS:** Displaying Hierarchical Structures – Arbitrary Graphs/Networks, Text and Document Visualization - Vector Space Model - Single Document -Document Collection Visualization. (11)

**RESEARCH DIRECTIONS:**Steps in designing Visualizations – Problems in designing effective Visualizations, Issues of Data – Cognition - Perception and Reasoning -System Design – Evaluation - Applications. (11)

**Total L: 45**

**REFERENCES**


1. Claus O. Wilke, “Fundamentals Of Data Visualization: A Primer On Making Informative And Compelling Figures”, O'Reilly Media, California, 2019.
2. Matthew Ward, Grinstein G and Keim D, “Interactive Data Visualization: Foundations, Techniques, And Applications”, 2nd Edition, CRC Press, Florida, 2015.
3. Healy K., “Data visualization: a practical introduction”, Princeton University Press, New Jersey, 2018.
4. Chang W. R, “Graphics cookbook: practical recipes for visualizing data”, O'Reilly Media, California, 2018.


## 21NB38 SOFTWARE CRASH ANALYSIS AND DISASTER RECOVERY

**3 0 0 3**

**SOFTWARE SECURITY AND VULNERABILITY ANALYSIS**: Security Incident, Disclosure Processes, Attack Surfaces and Attack Vectors, Reasons Behind Security Mistakes, Proactive Security, Security Requirements, Fuzzing Overview, Purpose of Vulnerability Analysis, Basic Bug Categories, Bug Hunting Techniques, Defenses. (10)

**THREAT ANALYSIS AND RISK-BASED TESTING:** Threat Trees, Threat Databases, Ad-Hoc Threat Analysis. Transition to Proactive Security - Cost of Patch Deployment. Defect Metrics and Security, Expected Defect Count Metrics, Vulnerability Risk Metrics, Interface Coverage Metrics, Input Space Coverage Metrics, Code Coverage Metrics, Process Metrics. (11)

**FUZZING METHODS AND TARGET MONITORING: PARADIGM SPLIT**: Random or Deterministic Fuzzing, Source of Fuzz Data, Fuzzing Vectors, Intelligent Fuzzing, Intelligent Versus Dumb Fuzzers, Fuzzer Classification via Interface. Target Monitoring - Methods of Monitoring, Virtualization, Fuzzing case study. (12)

**WINDOWS & LINUX EXPLOIT DEVELOPMENT AND DISASTER RECOVERY:** Stack based Overflows, Shellcode Injection (PE infection), Kernel Exploitation, Advanced Heap Spray techniques. Linux Exploit Development - Linux Format String Exploitation, Linux Shell code development. Disaster Recovery - Understanding Disaster Recovery, Bootstrapping the Disaster Recovery Plan Effort, Planning for various Disaster Scenarios. (12)

**Total L: 45**

**REFERENCES:**


1. Ari Takanen et al, “Fuzzing for Software Security Testing and Quality Assurance”, Artech House, UK, 2018.
2. Klaus Schmidt, “High Availability and Disaster Recovery Concepts, Design, Implementation”, Springer, Germany, 2010.
3. Michael Sutton et. al., “Fuzzing: Brute Force Vulnerability Discovery,” Addison-Wesley, UK, 2007.
4. Peter H. Gregory, “IT Disaster Recovery Planning For Dummies”, Wiley, Germany, 2007.


## 21NB39 DATA PRIVACY AND PROTECTION

**3 0 0 3**

**INTRODUCTION**: Introduction to data privacy, Methods of protecting data, Importance of balancing data privacy and utility, Introduction to anonymization design principles, Nature of data in the enterprise, Multidimensional data anonymization: Classification of privacy preserving methods, classification of data in multidimensional dataset, Group based anonymization, Complex data structures: privacy preserving graph data, time series data, longitudinal data, and transaction data, Threats to data structures and anonymization techniques. (12)

**PRIVACY PRESERVING DATA MINING AND REGULATIONS:** Data Mining: Key functional areas of multidimensional data, Synthetic data generation: Synthetic data and their use, privacy and utility in synthetic data, safety of synthetic data, Privacy regulations: UK data protection act, federal act of data protection of Switzerland, payment card industry data security standard, health insurance portability and accountability act (HIPAA), anonymization design checklist. Differential Privacy, Case Study: Privacy in Recommender System and location information (11)

**DATA PROTECTION**: Introduction, model for information, data and storage, importance of data protection in enterprise, data loss and business risk, connectivity: the risk multiplier, business continuity: the importance of data, the changing face of data protection, overview of storage technology: storage I/O basics, I/O stack, direct attached storage, network attached storage, storage area network, backup and restore: designing storage systems for backup and recovery, recovery from disaster: restoring data, design consideration for remote copy, Case Study: Bingham McCutchen, PdMain. (11)

**SECURITY AND INFORMATION LIFECYCLE MANAGEMENT** – Basic Security Concepts, Storage system security: DAS and SAN security, internal and external vectors, RISK, security practices for storage, secure fibre channel protocols: FC-SP and FCAP. Information Lifecycle Management (ILM): information assurance and data protection, unstructured and structured data, importance of context, determining and managing information context, location and information perimeter, the information lifecycle, changing value of information, automating ILM. (11)

**Total L: 45**

**REFERENCES:**


1. Nataraj Venkataramanan, Ashwin Shriram, "Data Privacy Principles and Practice", CRC Press, 2017.
2. Tianqing Zhu, Gang Li, Wanlei Zhou, Philip S. Yu, "Differential Privacy and Applications", 1st edn, Springer International Publishing, 2017..
3. Tom Petrocelli, "Data Protection and Information Lifecycle Management", Pearson, 2006.
4. David F.Ferraiolo, D.Richard Kuhn, Ramaswamy Chandramouli, "Role-Based Access Control", 2nd edn, Artech House, 2007.


## 21NB40 E-COMMERCE SECURITY

**3 0 0 3**

**INTRODUCTION**: Value chain and E-commerce, E-Commerce business models, E-Commerce Versus Traditional Commerce, Major categories, Advantages and disadvantages, Business-to-Consumer E-Commerce cycle, Models of Business-to-Business E-Commerce, Wireless and Voice-based E-Commerce. (9)

**SECURE WEB FRAMEWORK:** Architecture of WWW, Cryptography basics, Cryptography and the web, Understanding SSL and TLS, Digital Identification: Passwords – Biometrics - Digital Signatures - Digital Certificates – CAs - PKI. (12)

**PRIVACY AND SECURITY ISSUES:** Threats in E-commerce, Understanding privacy, Log files, Cookies, Privacy-Protecting techniques, Blocking ads and crushing cookies, Anonymous browsing, Backups and Anti-theft, Web server security, Securing Web Application, Deploying SSL server certificates, Blockchain-enabled E-commerce (13)

**ELECTRONIC PAYMENTS:** The SET protocol, Payment Gateway, certificate, digital Tokens, Smart card, credit card, magnetic strip card, E-Checks, Electronic wallets, Credit/Debit card-based EPS, online Banking. EDI Application in business, E-Commerce Law, Forms of Agreement, Government policies and Agenda, Intellectual property and Actionable content. (11)

**Total L: 45**

**REFERENCES**:


1. Hossein Bidgoli, "Electronic Commerce: Principles and Practice", Academic Press, USA, 2002.
2. Andrew Hoffman, "Web Application Security: Exploitation and Countermeasures for Modern Web Application", O'Reilly, USA, 2020.
3. Kenneth C.Laudon and Carol Guercio Traver, "E-Commerce", 10th Edition, Pearson, UK, 2016.
4. Dave Chaffey, 2nd Edition, ,"commerce Management-Digital Business and E"Bird and Tanya Hemphill -David Edmundson Pearson, UK, 2019


## OPEN ELECTIVES THEORY COURSE

## 21NB91 / 21NN91 COMPUTATIONAL FINANCE

**3 0 0 3**

**RETURNS AND PORTFOLIO OPTIMIZATION:** Compute Risk and Returns – How to measure drawdown in stock returns? – How to measure deviations from normality? – Estimating Value at Risk – How to construct Efficient Frontier using Quadprog – Fund Separation Theorem and Capital Market Line – How to construct Max Sharpe Ratio Portfolio- The limits of Portfolio diversification (11)

**PORTFOLIO INSURANCE STRATEGIES AND DYNAMIC ALLOCATION**: Constant proportion portfolio insurance (CPPI) – Designing and Calibrating CPPI strategies – Liability Driven Investing (LDI) – Performance-Seeking Portfolio and Liability-Hedging Portfolio (PSP/LHP) – Naïve Risk and Dynamic Risk Budgeting (11)

**FACTOR INVESTING MODELS:** CAPM and Introduction to factor models – Fama-French Models – Factor benchmarks and Style analysis – Difference in cap-weighted benchmarks and smart-weighted benchmarks – How to estimate the covariance matrix ?– How to use factor models to calculate expected returns? – Univariate time series Models (Autoregressive and Moving Average Models) – ARIMA – Forecasting Macro fundamentals – Volatility Models – ARCH & GARCH – Black-Litterman and Risk Parity Portfolios (11)

**MACHINE LEARNING ALGORITHMS AND APPLICATIONS IN FINANCE**: Supervised and Unsupervised Learning methods– Penalized Regression Techniques: Lasso, Ridge, and Elastic Net – Estimation of factor models with machine learning techniques – Graphical network analysis – Credit risk modelling using logistic/beta regression – Regime Switching Models – Forecasting investment models and Prediction of crash regime (12)

**Total L: 45**

**REFERENCES:**


1. Dixon, Halperin, Paul Bilokon , “Machine Learning in Finance: From Theory to Practice “, 1st edition Springer, ISBN-13: 978-3030410674,2020
2. Cerný, A. (2009). Mathematical techniques in finance: tools for incomplete markets. Princeton University Press, New Jercy.
3. Antoine Savine and Leif Andersen, “Modern Computational Finance: AAD and Parallel Simulations”,Wiley, 2018
4. Argimiro Arratia, “Computational Finance: An Introductory Course with R”, Atlantis Press, spain 2014.