SEMESTER -II

CTMTAIDS SII P1: Advanced Machine Learning for Cyber Security and Forensics

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To focus on recent advances in deep learning with neural networks.
2. To apply the concepts of machine learning for forensic investigation.
3. To understand a range of machine learning algorithms along with their strengths and weaknesses for computer forensics.
4. To understand and apply advanced machine learning algorithms to particular scenarios such phishing and spam filtering.
5. To identify machine learning methods to use and apply them rigorously in order to solve cyber security problems.

UNIT –I

Introduction to Machine Learning, Examples of Machine Learning applications Learning associations, Classification, Regression, Unsupervised Learning, Reinforcement Learning. Supervised learning- Input representation, Hypothesis class, Version space.

UNIT -II

Advanced machine learning topics: Bayesian modelling and Gaussian processes, randomized methods, Bayesian neural networks, approximate inference. Deep learning: regularization, convolutional neural networks, recurrent neural networks, variational autoencoders, generative models, applications.

UNIT -III

Applications of machine learning in natural language processing: recurrent neural networks, backpropagation through time, long short term memory, attention

networks, memory networks, neural Turing machines, machine translation, question answering, speech recognition, syntactic and semantic parsing.

UNIT -IV

Introduction to Internet architecture, measuring Internet traffic behavior and anomaly detection, Live Demonstration: Analyze internet network traffic using unsupervised learning techniques, Applications of machine learning to network security, Supervised learning examples: Spam filtering, phishing, Unsupervised learning examples: Anomaly detection

UNIT -V

Fairness, Transparency, and Explainability in cybersecurity ML models, Privacy definitions and how to actualize privacy for cybersecurity applications in industry, Externalities and implications of errors in ML models for cybersecurity.

Reference Books: -

1. Kevin P. Murphy. Machine Learning: A Probabilistic Perspective. MIT Press 2012
2. Ian Goodfellow, Yoshua Bengio and Aaron Courville. Deep Learning. MIT Press 2016
3. A Primer on neural networks for natural language processing, by Yaov Goldbeg.
4. R. G. Cowell, A. P. Dawid, S. L. Lauritzen and D. J. Spiegelhalter. "Probabilistic Networks and Expert Systems". Springer-Verlag. 1999.
5. M. I. Jordan (ed). "Learning in Graphical Models". MIT Press. 1998. Collection of papers. These appear collated here.
6. J. Pearl. "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference." Morgan Kaufmann. 1988.
7. Graphical models by Lauritzen, Oxford science publications
8. F. V. Jensen. "Bayesian Networks and Decision Graphs". Springer. 2001.
9. Neural Networks and Deep Learning by Michael Nilson

CTMTAIDS SII P2: Mobile Security and Forensics

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand the architecture of the mobile devices operating systems like Android.
2. To understand the security concepts of the mobile devices and its OS.
3. To learn the android application security testing and auditing.

UNIT –I

Introduction to Android, Android's Architecture, Android Run Time, Android Application Framework, Introduction to Android Application component, Sandboxing, Android application inter-process communication, Application permission, Android boot process, Android partitions, File systems.

UNIT – II

Configuration of lab using Santoku or Kali Linux or Mobexler or Android Studio or GenY motion, ADB commands, Configuration vulnerable application, Open GApps Project, need of ARM Translator, Mobile application security pen-testing strategy, Android application vulnerability exploitation : Insecure login, hard core issues, insecure data storage issue, input validation issues, access control issues, content provider leakage, path traversal Client-side injection attacks or other latest vulnerability or latest OWASP top 10 vulnerabilities.

UNIT – III

Reverse engineering using APK Tool, JADX, JD-GUI, Hex Dump, Dex Dump, Reversing and Auditing Android Apps: Android application teardown and secure source code review.

UNIT-IV

Security auditing using Drozer, MobSF (Mobile Security Framework): Static and Dynamic Analysis, Android application security vulnerability assessment using

QARK, Android dynamic instrumentation using Frida and Objection framework. Introduction to Xposed is a framework.

UNIT-V

Traffic Analysis for Android Devices, Android traffic interception, Ways to analyse Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception, other ways to intercept SSL traffic.

Reference Books

1. Android Security Internals: An In-Depth Guide to Android's Security Architecture by Nikolay Elenkov, No Starch Press Publication (2015).
2. Android Hacker's Handbook by Joshua J. Drake, Zach Lanier, Georg Wicherski, Pau Oliva Fora, Stephen A. Ridley, Collin Mulliner, Wiley Publication (2014).
3. Learning Pentesting for Android Devices by Aditya Gupta, Packt Publication (2014).
4. Android Apps Security Mitigate Hacking Attacks and Security Breaches by Sheran Gunasekera, Apress Publication (2020).
5. The Mobile Application Hacker's Handbook by Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, Wiley Publication (2015).

CTMTAIDS SII P3: Natural Language Processing

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To learn the concept of scripting for cyber security.
2. To learn Python basics for scripting.
3. To learn PowerShell scripting for information security concept.
4. To learn bash scripting for cyber security related task.
5. To learn the concept related secure development and threat hunting.

UNIT – I

Origins and challenges of NLP, Language Modelling, Grammar-based LM, Statistical LM, Regular Expressions, Finite-State Automata, English Morphology, Transducers for lexicon and rules, Tokenization, Detecting and Correcting Spelling Errors, Minimum Edit Distance

UNIT – II

Unsmoothed N-grams, Evaluating N-grams, Smoothing, Interpolation and Backoff Word Classes, Part-of-Speech Tagging, Rule-based, Stochastic and Transformation-based tagging, Issues in PoS tagging, Hidden Markov and Maximum Entropy models.

UNIT – III

Context-Free Grammars, Grammar rules for English, Treebanks, Normal Forms for grammar, Dependency Grammar, Syntactic Parsing, Ambiguity, Dynamic Programming parsing, Shallow parsing, Probabilistic CFG, Probabilistic CYK, Probabilistic Lexicalized CFGs, Feature structures, Unification of feature structures.

UNIT – IV

Requirements for representation, First-Order Logic, Description Logics, Syntax-Driven Semantic analysis, Semantic attachments, Word Senses, Relations

between Senses, Thematic Roles, selectional restrictions, Word Sense Disambiguation, WSD using Supervised, Dictionary and Thesaurus, Bootstrapping methods, Word Similarity using Thesaurus and Distributional methods.

UNIT – V

Discourse segmentation, Coherence, Reference Phenomena, Anaphora Resolution using Hobbs and Centering Algorithm, Coreference Resolution, Resources: Porter Stemmer, Lemmatizer, Penn Treebank, Brill's Tagger, WordNet, PropBank, FrameNet, Brown Corpus, British National Corpus (BNC).

Reference Books:-

1. Daniel Jurafsky, James H. Martin Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics and Speech, Pearson Publication, 2014.
2. Steven Bird, Ewan Klein and Edward Loper, Natural Language Processing with Python, First Edition, O_Reilly Media, 2009.
3. Breck Baldwin, Language Processing with Java and LingPipe Cookbook, Atlantic Publisher, 2015.
4. Richard M Reese, Natural Language Processing with Java‖, O_Reilly Media, 2015.
5. Nitin Indurkhya and Fred J. Damerau, Handbook of Natural Language Processing, Second Edition, Chapman and Hall/CRC Press, 2010.
6. Tanveer Siddiqui, U.S. Tiwary, Natural Language Processing and Information Retrieval‖, Oxford University Press, 2008.

CTMTAIDS SII P4: Intelligent Systems and Security

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To give an overview of the concepts and practical examples in the development, feasibility and sustainability of smart cities across the world.
2. To understand the application areas of IOT.
3. To realize the revolution of internet in mobile devices, cloud and sensor networks.
4. To understand building blocks of Internet of Things and characteristics.

UNIT – I

Internet of Things Vision, IoT examples, IoT Applications, Security, Privacy and Trust, Device Level Energy Issues, IoT Related Standardization, Recommendations on Research Topics, SMART Objects Smart objects, Wired Cables, hubs, Wireless RFID, WiFi, Bluetooth, Different functional building blocks of IOT architecture.

UNIT – II

HTTP basics, HTTP architecture, Adding HTTP support to the actuator, CoAP basics, CoAP protocol architecture, MQTT Protocol, Publishing and subscribing, Xamp basics, Xamp protocol architecture.

UNIT – III

Smart Cities: Distributed Intelligence and Central Planning on the Interplay between Humans and Smart Devices, Theoretical Tools, Intelligence Artificial Intelligence (Machine Intelligence), Information Dynamics, Synergetic, Information Dynamics and Allometry in Smart Cities.

UNIT – IV

Leveraging Smart City Projects for Benefitting Citizens: The Role of ICTs Smart

City and ICT: Using Technologies to Improve the Citizens Quality of Life, Smart City Goals: The Impact on Citizens Well-Being and Quality of Life, Critical Dimensions: Urbanization, Local Climate Change, and Energy Poverty, Environmental Issues: The Role of Local and Global Climate Change.

UNIT – V

Understanding the risks, Modes of attack, Tools for achieving security, need for interoperability, Security and privacy issues in smart devices, data breach and identity theft, case study on alexa, google nest etc.

Reference Books: -

1. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems by Dr. Ovidiu Vermesan and Dr. Peter Friess
2. Learning Internet of Things by Peter Waher
3. Internet of Things (A Hands-on Approach) by Vijay Madisetti and Arshdeep Bahga
4. Rethinking the Internet of Things: A Scalable Approach to Connecting Everything by Francis DaCosta
5. Getting Started with the Internet of Things by Cuno Pfister

CTMTAIDS SII P5: Program Elective

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

List of Program Elective		
Sr. No.	Subject Code	Subject Name
1	CTMTAIDS SII P5 EL1	Blockchain Security and Investigation
2	CTMTAIDS SII P5 EL2	Malware Analysis and Reverse Engineering
3	CTMTAIDS SII P5 EL3	Deep and Reinforcement Learning Techniques
4	CTMTAIDS SII P5 EL4	Cloud Intelligence and Forensics
5	CTMTAIDS SII P5 EL5	Social Network Analysis and Threat Intelligence
6	CTMTAIDS SII P5 EL6	Big Data Analytics

CTMTAIDS SII P5 EL1: Blockchain Security and Investigation

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand concept of Blockchain.
2. To learn various use-cases of Blockchain.
3. To understand fundamental of Blockchain security.
4. To learn various Blockchain security techniques.

UNIT–I

Introduction, Cryptography, Hash Function, Hash Pointers and One-Way Functions, Digital Signatures – ECDSA, Memory Hard Algorithm, Zero Knowledge Proof, Distributed Database, Two General Problem, Byzantine General Problem and Fault Tolerance, Introduction to Quantum Computing and How it will break existing methods

UNIT-II

Introduction, Advantages over Conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain Application, Soft and Hard Fork, Private and Public Blockchain

UNIT–III

Nakamoto Consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy Utilization, Alternate Smart Contract Construction

UNIT–IV

History, Distributed Ledger, Bitcoin Protocols – Mining Strategy and Rewards, Ethereum Construction, Gas Limit, DAO, Smart Contract, GHOST,

Vulnerabilities, Attacks, Sidechain, Name coin, Case Study related to – Naïve Blockchain Construction, Play with Go-Ethereum, Application using Blockchain

UNIT-V

Stakeholders, Roots of Bitcoin, Legal Aspects-Cryptocurrency Exchange, Black Market and Global Economy, Applications: Internet of Things, Medical Record Management System, Domain Name Service and Future of Blockchain, Case study related to Mining Puzzles

Reference Books: -

1. Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction, Princeton University Press, 2016 by Arvind Marayan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder.
2. Bitcoin and Blockchain Security by Elli Androulaki and Ghassan Karame
3. Blockchain Cybersecurity, Trust and Privacy by Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo
4. Blockchain for Cyber Security and Privacy: Architectures, Challenges and Applications by Mamoun Alazab, Yassine Maleh, Mohammad Shojafar, Imed Romdhani
5. The Truth Machine: The Blockchain and the Future of Everything by Michael Casey and Paul Vigna
6. Blockchain for Distributed Systems Security by Laurent L. Njilla, Charles Kamhoua and Sachin Shetty
7. Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
8. The Age of Cryptocurrency by Paul Vigna and Michael Casey
9. The Basics of Bitcoins and Blockchains by Antony Lewis
10. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

CTMTAIDS SII P5 EL2: Malware Analysis and Reverse Engineering

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		Total
					Internal Exams					University Exams		University Exams (LPW)		
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To learn the various malware types.
2. To learn the internals of executable files.
3. To learn various malware analysis techniques.
4. To learn the signature creation for malware detection.
5. To learn the reverse engineering of malware.

UNIT – I

Malware Definition and Types, Malware Analysis, Forensic Importance of Malware Analysis, Introduction to different analysis techniques, Malware Behavior, Setting up malware analysis laboratory. Static Analysis: Hashing, Finding Strings, Decoding Obfuscated Strings Using FLOSS, PE Files Headers and Sections, PE View, Linked Libraries and Functions, Dependency Walker, CFF Explorer, Resource Hacker, Malware signature and Clam AV Virus Signature, YARA Signatures, Dynamic Analysis: Sandboxes, Running and Monitoring a Malware, ProcessMonitor, Process Explorer, RegShot, faking a network, Using Wireshark for Packet Analysis.

UNIT – II

Introduction to x86 Assembly and CPU registers, Overview of the Stack, IDA Pro with its functions and features, Understanding of C code construct in Assembly, Analyzing Malicious Windows Programs, Live Memory Analysis using Volatility.

UNIT – III

Difference between Source level v/s Assembly level debugger, Kernel mode v/s

User mode debugger, Debugger common features, Breakpoints, Exceptions, Modification of Program Execution, Working with OllyDbg and Immunity Debugger, Kernel Debugging with WinDBG

UNIT – IV

Common behavior of the malwares, Process Injection, Process Replacement, Hook Injection, Data Encoding, Anti- Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, Packers and Unpacking.

UNIT - V

Introduction to Linux Malwares, Linux Binary architecture, Analysis of Linux Malware, Android Architecture, Android Permissions, Types of Android Malware, Analysis and Reverse Engineering of android malware.

Reference Books: -

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig.
2. Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware by Monappa K A (2018)
3. Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks by Alexey Kleymenov, Amr Thabet (2019)
4. Malware Analysis Cookbook: Tools and Techniques for Fighting Malicious Code by Matthew Richard, Blake Hartstein, Michael Hale Ligh, Steven Adair.
5. Practical Reverse Engineering: X86, X64, ARM, Windows Kernel, Reversing Tools, and Obfuscation by Alexandre Gazet, Bruce Dang, and Elias Bachaalany
6. The IDA Pro Book: The unofficial guide to the world’s most popular disassembler by Chris Eagle
7. Android Malware and Analysis by Tim Strazzere, Manu Quintans, Jose Andre Morales, Shane Hartman, Ken Dunham
8. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux and Mac Memory by Michael Hale Ligh, Andrew Case, Jamie Levy and Aaron Walters
9. Malware Forensics: Investigating and Analyzing Malicious Code by James M. Aquilina, Eoghan Casey, Cameron H. Malin
10. Sockets, Shellcode, Porting and Coding: Reverse Engineering Exploit and Tool Coding for Security Professionals by James C. Foster and Mike

CTMTAIDS SII P5 EL3: Deep and Reinforcement Learning Techniques

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand the fundamental principles and techniques in deep and reinforcement learning.
2. To understand applications of deep and reinforcement learning.
3. To understand the context of neural networks and deep learning.
4. To apply deep learning techniques for attack threat modeling.

UNIT – I

Introduction- Historical Trends in Deep Learning, Machine Learning Basics, History of Reinforcement Learning, Elements of Reinforcement Learning, Limitations and Scope.

UNIT – II

Deep Networks, Deep Feedforward Networks, Examples, Gradient-based Learning, Hidden Units, Architecture Design, Back-propagation and other differentiation algorithms, Regularization for Deep Learning, Optimization for training deep models, Challenges, Basic algorithms for parameter initialization, Algorithms with adaptive learning rates, Approximate second-order methods, Optimization strategies and Meta-Algorithms.

UNIT – III

Convolution Networks, Operation, Motivation, Pooling, Variants of the Basic Convolution Function, Efficient Convolution Algorithms, Random or Unsupervised Features, Sequence Modeling, Recurrent and Recursive Nets, Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder, Sequence-to-Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks, Applications.

UNIT – IV

Tabular Solution Methods, Multi-armed Bandits, Dynamic Programming, Monte Carlo Methods, Temporal-Difference Learning, -n-step Bootstrapping.

UNIT – V

Approximate Solution Methods, On-policy Prediction with Approximation, On-policy Control with Approximation –Off.

Reference Books: -

1. Ian Goodfellow, YoshuaBengio, and Aaron Courville, "Deep Learning" MIT Press, 2016.
2. Richard S. Sutton and Andrew G. Barto,"Reinforcement Learning: An Introduction" second edition, MIT Press.
3. Cosma Rohilla Shalizi, Advanced Data Analysis from an Elementary Point of View, 2015.
4. Deng and Yu, Deep Learning: Methods and Applications, Now Publishers, 2013.

CTMTAIDS SII P5 EL4: Cloud Intelligence and Forensics

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand forensic data available in the cloud.
2. To implement best practices in cloud logging for DFIR.
3. To learn how to leverage Microsoft Azure, AWS and Google Cloud Platform resources to gather evidence.
4. To understand what logs Microsoft 365 and Google Workspace have available for analysts to review.
5. To learn how to move your forensic processes to the cloud for faster data processing.

UNIT – I

Introduction to cloud computing, characteristic of cloud computing, cloud computing models: Service model and deployment model, cloud services and technologies, research challenges, cloud computing reference architecture, network recruitment for cloud computing. Cloud Computing Security Baseline: Overview of computer security, vulnerabilities and attacks, privacy and security in cloud storage services, privacy and security in multi clouds, cloud accountability, Understanding the Threats, Classification and countermeasures: Infrastructure and host threats, service provider threats, generic threats, threat assessment.

UNIT – II

Creating a Safe Environment, Access control, The CIA model :Confidentiality, Integrity, Availability, A real-world example, The principles of security: The Principle of Insecurity, The Principle of Least Privilege, The Principle of Separation of Duties, The Principle of Internal Security, Data Center security: Select a good place, Implement a castle-like structure, Secure your authorization points, Defend your employees, Defend all your support systems, Keep a low profile, Server security: The importance of logs, Where to store the logs?,

Evaluate what to log, Evaluate the number of logs, The people aspect of security: Simple forgetfulness, Shortcuts, Human error, Lack of information, Social engineering, Evil actions under threats, Evil actions for personal advantage.

UNIT – III

The Open Systems Interconnection model: Layer 1 – the Physical layer, Layer 2 – the Data link layer, Address Resolution Protocol (ARP) spoofing, MAC flooding and Content Addressable Memory table overflow attack, Dynamic Host Configuration Protocol (DHCP) starvation attack, Cisco Discovery Protocol (CDP) attacks, Spanning Tree Protocol (STP) attacks, Virtual LAN (VLAN) attacks, Layer 3 – the Network layer, Layer 4 – the Transport layer, Layer 5 – the Session layer, Layer 6 – the Presentation layer, Layer 7 – the Application layer, TCP/IP, Architecting secure networks, Different uses means different network, The importance of firewall, IDS, and IPS, Firewall, Intrusion detection system (IDS), Intrusion prevention system (IPS), Generic Routing Encapsulation (GRE), VXLAN, Flat network versus VLAN versus GRE in OpenStack Quantum, Design a secure network for your OpenStack deployment, The networking resource policy engine, Virtual Private Network as a Service (VPNaaS)

UNIT – IV

Securing the OpenStack Identification and Authentication System and Its Dashboard dentification versus authentication versus authorization, Identification, Authentication, something you know, something you have, something you are, the multifactor authentication, Authorization: Mandatory Access Control, Discretionary Access Control, Role-based Access Control, Lattice- based Access Control, Session management, Federated identity, Configuring OpenStack Keystone to use Apache

UNIT – V

Different storage types, Object storage, Block storage, File storage, Comparison between storage solutions, Security, Backends : Ceph, Gluster FS, The Logical Volume Manager, The Network File System, Sheepdog, Swift, Z File System (ZFS), Security, Securing OpenStack Swift, Hiding information, Securing ports, Securing the Hypervisor :Various types of virtualization, Full virtualization, Paravirtualization, Partial virtualization, Comparison of virtualization levels, Hypervisors: Kernel-based Virtual machine, Xen, VMware ESXi, Hyper-V, BareMetal, Containers, Docker, Linux Containers, Criteria for choosing a hypervisor : Team expertise, Product or project maturity, Certifications and attestations, Features and performance, Hardware concerns, Hypervisor memory optimization, Additional security features, Hardening the hardware management:

Physical hardware – PCI passthrough, Virtual hardware with Quick Emulator, sVirt – SELinux and virtualization, Hardening the host operative system, Cloud Forensics, Cloud Forensic Frameworks, Digital Forensic Investigation and Cloud Computing, Dimensions of cloud forensics, cloud crime, challenges cloud forensics, usages of cloud forensics, Cloud forensics tools.

Reference Books: -

1. OpenStack Cloud Security Paperback by Alessandro Locati Fabio, PacktPub
2. Cloud Storage Forensics 1st Edition by Darren Quick , Ben Martini , Raymond Choo Syngress
3. Cybercrime and Cloud Forensics: Applications for Investigation Processes Keyun Ruan (University College Dublin, Ireland)
4. Cloud Computing Security: Foundations and Challenges edited by John R. Vacca, CRC Press.
5. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, John Wiley and Sons

CTMTAIDS SII P5 EL5: Social Network Analysis and Threat Intelligence

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. Students will learn social media working concepts.
2. Students will learn social media based online data investigations and analysis.
3. Students will learn the intelligence gathering concepts from open source available data.

UNIT – I

Fundamentals of Social Networking, Social Networking viral, why social networking is popular, Psychology and Sociology for Online Media, Concepts of Geospatial Information System, How Facebook works?

UNIT – II

Graph Theory and Social Networks, Markets and Strategic Interactions in Networks, Information Networks and the World Wide Web, Network Dynamics: Population and Structural Models, Legal aspects of Privacy in India, Institutions and Aggregate Behavior, Social Media and its impact on Business, Politics, Law and Revolutions, Legal Responsibilities for Social Networking.

UNIT – III

Intelligence gathering, People searching, OSINT, Deep Web, Defamatory content analysis, Multimedia forensics over Social Networking, Emerging Trends in Social Networks

UNIT – IV

Introduction: hacking on Twitter data Micro formats: semantic Markup and common sense collide, Twitter: friends, followers, and set wise operations,

Twitter: the tweet, LinkedIn: clustering your professional network for fun (and profit?), cosine similarity, and collocations, Facebook: the hacker's outlook.

UNIT – V

Twitter GPS and Account Data, Hidden Social Network Content, Cell Phone Owner Information, Hidden, Photo GPS and Metadata, Deleted Websites and Posts, Website Owner Information, Alias Social Network Profiles, Additional User Accounts, Sensitive Documents and Photos, Live Streaming Social Content, Videos Uploaded by Location, Newspaper Archives and Scans, Social Content by Location, Text Transcripts of Videos, Historical Satellite Imagery, Duplicate Copies of Photos, Public Government Records, Document Metadata, Voter Registration Records, Facebook Wall Posts

Reference Books

1. Social Network Analysis: Methods and Applications by Katherine Faust and Stanley Wasserman
2. Social network analysis by John Scott
3. Models and Methods in Social Network Analysis by Stanley Wasserman, Peter J. Carrington, John Scott
4. The SAGE Handbook of Social Network Analysis by John Scott, Peter J. Carrington
5. Analysing Social Networks by Jeffrey C. Johnson, Martin G Everett, and Stephen Borgatti
6. Social Network Analysis: Methods and Examples by Franziska B. Keller, Lu Zheng, and Song Yang
7. Social Network Analysis by David Knoke and Song Yang
8. The Development of Social Network Analysis by Linton Freeman
9. Advances in Social Network Analysis: Research in the Social and Behavioural Sciences by Joseph Galaskiewicz, Stanley Wasserman
10. Understanding Social Networks: Theories, Concepts, and Findings by Charles Kadushin

CTMTAIDS SII P5 EL6: Big Data Analytics

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand Big Data and its analytics in the real world.
2. To analyze the Big Data framework like Hadoop and NOSQL to efficiently store and process Big Data to generate analytics.
3. To design of Algorithms to solve Data Intensive Problems using Map Reduce Paradigm.
4. To design and Implementation of Big Data Analytics using pig and spark to solve data intensive problems and to generate analytics.
5. To implement Big Data Activities using Hive.

UNIT – I

Introduction to Big Data, Types of Digital Data, Characteristics of Data Evolution of Big Data, Definition of Big Data, Challenges with Big Data, 3Vs of Big Data, Non-Definitional traits of Big Data, Business Intelligence vs. Big Data, Data warehouse and Hadoop environment, Coexistence.

UNIT – II

Big Data Analytics, Classification of analytics, Data Science, Terminologies in Big Data, CAP Theorem, BASE Concept, NoSQL, Types of Databases, Advantages, NewSQL, SQL vs. NOSQL vs NewSQL, Introduction to Hadoop, Features, Advantages, Versions, Overview of Hadoop Eco systems, Hadoop distributions, Hadoop vs. SQL, RDBMS vs. Hadoop, Hadoop Components, Architecture, HDFS, Map Reduce, Mapper, Reducer, Combiner, Partitioner, Searching, Sorting, Compression, Hadoop 2 (YARN), Architecture, Interacting with Hadoop Eco systems.

UNIT – III

No SQL databases, Mongo DB: Introduction, Features, Data types, Mongo DB

Query language, CRUD operations, Arrays, Functions: Count, Sort, Limit, Skip, Aggregate, Map Reduce. Cursors, Indexes, Mongo Import, Mongo Export. Cassandra: Introduction, Features, Data types, CQLSH, Key spaces, CRUD operations, Collections, Counter, TTL, alter commands, Import and Export, Querying System tables.

UNIT – IV

Hadoop Eco systems: Hive, Architecture, data type, File format, HQL, SerDe, User defined functions, Pig: Features, Anatomy, Pig on Hadoop, Pig Philosophy, Pig Latin overview, Data types, Running pig, Execution modes of Pig, HDFS commands, Relational operators, Eval Functions, Complex data type, Piggy Bank, User defined Functions, Parameter substitution, Diagnostic operator.

UNIT – V

Jasper Report, Introduction, Connecting to Mongo DB, Connecting to Cassandra, Introduction to Machine learning, Linear Regression, Clustering, Collaborative filtering, Association rule mining, Decision tree.

Reference Books: -

1. Seema Acharya, Subhashini Chellappan, “Big Data and Analytics”, Wiley Publication, 2015.
2. Judith Hurwitz, Alan Nugent, Dr. Fern Halper, Marcia Kaufman, “Big Data for Dummies”, John Wiley and Sons, Inc., 2013.
3. Tom White, “Hadoop: The Definitive Guide”, O’Reilly Publications, 2011.
4. Kyle Banker, “Mongo DB in Action”, Manning Publications Company, 2012.
5. Russell Bradberry, Eric Blow, “Practical Cassandra A developers Approach”, Pearson Education, 2014.

CTMTAIDS SII L1: Advanced Machine Learning for Cyber Security and Forensics Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
					Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.

CTMTAIDS SII L2: Mobile Security and Forensics Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
					Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.

CTMTAIDS SII L3: Natural Language Processing Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.

CTMTAIDS SII L4: Intelligent Systems and Security Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.

CTMTAIDS SII L5: Program Elective Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.