M. Tech Program in Cyber Security

TIFAC-Centre Of Relevance and Excellence (CORE) in Cyber Security

Cyber security is a very fast moving field. A program in security that aims to be on the forefront has to necessarily have a companion-advanced program that has a good balance between theoretical and practical aspects, analytical methods and system architectures, academic ideas and industry practices.

The Centre for Cyber Security was identified by TIFAC (Department of Science and Technology, Govt. of India) as a CORE in Cyber Security in September 2005. The TIFAC CORE gives significant thrust to the frontier areas of Cyber Security, including technology, practice, management, and policy issues. Research areas of the TIFAC CORE are organized into four broad categories, namely: Enterprise Wide Security, Data Center Security, Language-Based Security, and Hardware and Embedded Systems Security. These categories represent four horizontal layers of security in a typical information system /network that a practitioner would normally encounter in today’s industrial settings and corporate environments. CORE also focuses on theory and practice of authentication, authorization, and access control techniques.

This M. Tech program provides a good blend of theory and industrial practice; necessary theoretical background, insight into general and technical aspects of Cyber Security, analytical methods and management practices in the field of Cyber Security are the areas receiving detailed attention. It aims at moulding the student into an Information Security professional. Practicing industry professionals and enterprise experts with little or no knowledge in Cyber Security too can benefit from this program.
## CURRICULUM

### First Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16MA 608</td>
<td>FC</td>
<td>Mathematical Foundations for Cyber Security</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>16CY 602</td>
<td>FC</td>
<td>Concepts in System Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16CY 603</td>
<td>FC</td>
<td>Cryptography</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CY 611</td>
<td>SC</td>
<td>Internetworking- Protocols and Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16CY 612</td>
<td>SC</td>
<td>Data Mining and Machine Learning in Cyber Security</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16HU 601</td>
<td>HU</td>
<td>Cultural Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Credits 18**

* Non-Credit Course

### Second Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16CY 613</td>
<td>SC</td>
<td>Cyber Forensics</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 614</td>
<td>SC</td>
<td>Cryptographic Protocols and Standards</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16CY 604</td>
<td>FC</td>
<td>Secure Coding</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CY 615</td>
<td>SC</td>
<td>Cyber Security Lab</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective I</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective II</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16 EN 600</td>
<td></td>
<td>Technical Writing*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Credits 19**

* Non-Credit Course

### Third Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td></td>
<td>Elective III</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective IV</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 798</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>

**Credits 17**

### Fourth Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16CY 799</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>

**Credits 12**

**Total Credits: 66**
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16MA 608</td>
<td>Mathematical Foundations for Cyber Security</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>16CY 602</td>
<td>Concepts in System Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16CY 603</td>
<td>Cryptography</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CY 604</td>
<td>Secure Coding</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

### Subject Core

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16CY 611</td>
<td>Internetworking - Protocols and Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16CY 612</td>
<td>Data Mining and Machine Learning in Cyber Security</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CY 613</td>
<td>Cyber Forensics</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 614</td>
<td>Cryptographic Protocols and Standards</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16CY 615</td>
<td>Cyber Security Lab</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

### Electives

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16CY 701</td>
<td>Mobile &amp; Wireless Networking and Security</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 702</td>
<td>Language-Based Security</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 703</td>
<td>Network Security</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 704</td>
<td>Steganography and Obfuscation</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 705</td>
<td>Information Security and Risk Management</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16CY 706</td>
<td>HDL and Cryptographic Applications</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 707</td>
<td>Coding and Information Theory</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CY 708</td>
<td>Security in Cloud Computing</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CY 709</td>
<td>Design and Analysis of Algorithms</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CY 710</td>
<td>Formal Methods for Security</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 711</td>
<td>Secure Systems Engineering</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 712</td>
<td>Security in Internet of Things</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16CY 713</td>
<td>Android Security</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

### Project

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Courses</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16CY 798</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>16CY 799</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>

TEXT BOOKS/REFERENCES:


TEXT BOOKS/REFERENCES:

16CY 603          CRYPTOGRAPHY            3-0-1-4

Shannon ciphers and perfect security, Computational ciphers and semantic security, Pseudorandom generators, Stream Ciphers: One time pad, Composing PRGs, Pseudorandom bit generators & Pseudorandom functions: provably secure pseudorandom generators, existence of pseudorandom generators. Pseudorandom functions and permutations (PRFs and PRPs), PRP under chosen plaintext attack and chosen ciphertext attack, usage of PRFs and PRPs in shared random function model and in modeling block ciphers. Construction of PRF, applications of PRFs: cryptographically strong hashing, private-key encryption. Symmetric encryption schemes: Block ciphers and modes of operation, indistinguishability under chosen plaintext and chosen ciphertext attack. One way and trapdoor functions, Discrete Logarithm functions, RSA functions. Publickey encryption: RSA, Rabin, Knapsack cryptosystems and ECC; polynomial indistinguishability, semantic security; probabilistic public key encryption. Message authentication & Digital signatures: designing MACs using PRFs, CBC MAC and its security, universal hash based MACs, MACing with Cryptographic hash functions,Authenticated encryption; trapdoor function model, Generic signature schemes, RSA, ElGamal and Rabin’s signature schemes, probabilistic signatures, signature scheme based on Claw-free trapdoor permutations, blind signatures, threshold signature schemes.

TEXT BOOKS/REFERENCES:

16CY 604          SECURE CODING            3-0-1-4


TEXTBOOKS / REFERENCES:

16CY 611 INTERNATIONAL - PROTOCOLS AND SECURITY 3-0-0-3


TEXT BOOKS/REFERENCES:

16CY 612 DATA MINING & MACHINE LEARNING IN CYBER SECURITY 3-0-1-4


**TEXT BOOKS/REFERENCES:**


**16CY 613 CYBER FORENSICS 2-0-1-3**


**TEXT BOOKS/REFERENCES:**

16CY 614  CRYPTOGRAPHIC PROTOCOLS AND STANDARDS  3-0-0-3


TEXT BOOKS/REFERENCES:

16CY 615  CYBER SECURITY LAB  0-0-3-3

1. Installing and exploiting security tools for protecting a network.
2. Implementation of cryptographic algorithm for building a secure communication network.
3. Analysis of malicious software in tampering with the operating system process list.
4. Exploiting the vulnerabilities in a LAN environment to launch attacks.
5. Usage of forensics tools in gathering information from communication devices and host machines.
6. Identifying and securing the systems from malicious software.
7. Performing a vulnerability assessment of Wireless devices and audit the same with penetration testing.
8. Analyze the source code and carry out a reverse engineering of binaries and executables.
9. Application of machine learning algorithms in intrusion detection dataset
10. Create, install, update, and disassemble android applications.

Some of the experiments makes use of Kali Linux distro & Metasploit Framework and other open source security tools. Latest version of these tools and distros are available in the Cyber Security Lab.

**Experiment No. 1: LAN based Network Security**
Set up a simple LAN as shown in Figure 1. M1-3 and S1-3 are machine which have Linux and Windows running.

![Network Switch](image)

**Figure 1: A Simple LAN environment**

1. Configure LAN-1 and LAN-2 as separate VLANs in the Network Switch.
   - Use inter VLAN ACL
2. Create a SPAN port in the Network switch and send the mirrored traffic to a promiscuous mode port for the purpose of IDS and other packet analysis. Practice port based and VLAN based mirroring.
3. Familiarize with 802.1x, Network Admission Control, Microsoft NAP, RADIUS protocol, RADIUS per port ACL

**Experiment No. 2: Network reconnaissance and Protection**
- Installing ‘iptable’ in Ubuntu VM to allow/block communication between VMs
  - Installing Email server and Web server in VMs. Usage of Firewall (iptable) in blocking/allowing a sub-network from accessing the servers
  - Configuring iptable to block Telnet inbound and outbound connections
2. Use ‘nmap’ tool to perform vertical and horizontal scanning for checking open and closed ports. Use nmap commands for performing the following experiments:
   - Use ping sweeping to determine which hosts are running
   - Check for vulnerable services available using TCP connect scans
   - Perform OS Fingerprinting to determine the OS of target machine
   - Choose different options under each category according to your creativity.
3. Invoke ‘p0f’ Passive OS Fingerprinting tool to perform the following
   - Operating system and service pack
   - Installed applications
   - Open ports available and services running in the machine
Experiment No. 3: Secure communication between hosts using, SSL-TLS, IPSec, and Secure Layer 2 VPNs.
Establish a Client-Client Secure communication protocol as shown in Figure 2.

![Figure 2: Secure Communication](image)

The goal of this experiment is to use all the encryption protocols, SSL-TLS, IPSec, and Secure Layer 2 VPNs between the hosts. The student is expected to learn which applications and data can be encrypted using respective modes.

The Client machines (Client-1 and Client-2) and Admin machine are installed in different VMs. All the three machines are interconnected through a network switch with different IP addresses. The Admin runs a program that generates 2048 bit RSA public and private key for a Client that wants to communicate. Admin generates 2048 bit RSA public and private key for Client-1 and Client-2. The private keys are distributed to client machines and public keys are stored in a structure in the admin machine. When Client-1 wants to send message to Client-2, it encrypts the messages with public key of Client-2. The message is decrypted by Client-2 with its private key. Similar communication pattern from Client-2 to Client-1 need to be maintained.

Manually capture the traffic between the hosts to ensure the proper working of the encryption. Construct an asynchronous communication between Client-1 and Client-2. Run a Wireshark/TCPdump at the SPAN/Promiscuous port of the network switch and identify the communication between the communicating entities (Admin, Client-1, and Client-2).

Experiment No. 4: LAN based insider attacks
Make use of Ettercap/arpspoof tool to perform ARP Cache Poisoning based attacks in a LAN environment:
1. Perform Denial of Service (DoS) attacks using ARP Cache Poisoning attacks
2. Perform DNS Spoofing attack using ARP Cache Poisoning attacks
3. Perform Password stealing (over plaintext) using ARP Cache Poisoning attacks

Invoke ‘sslstrip tool’ for stealing password from any machine that is connected in a LAN by stripping the https connection.
For all the above attacks, observe the ARP cache table, CAM table, etc., before and after the attack. Run Wireshark and observe the traffic patterns before and after the attack.

Experiment No. 5: Malware & Attack evasion Techniques
Consider the following tasks:
1) Enlist the processes, installed programs, dump the LM hashes, etc. from the Win XP machine
2) Does ‘client.exe’ enlisted in the process list? If, write a procedure/program to hide the process (client.exe) from process table list?
3) Set Firewall rules in Windows machine to block communication between the two VMs.

**Experiment No. 6: Password cracking & Recovery Lab**
Explore password cracker tool ‘John the Ripper’ to crack the passwords in /etc/shadow file. Generate your own shadow files and crack the password.

Explore the usage of ‘chnptw’ tool from Kali Linux OS by booting from a Live CD or USB. Explore the possibility of resetting/bypassing the administrator password of Windows 7 user. Install Kon-Boot on USB/CD/DVD to bypass password checking procedure in Windows machine.
Use GPGPU, Rainbow Tables and CFG to crack password
Familiarize with SNORT and SURICATA. Send network packets to both the IDS and see the results

**Experiment No. 7: Wireless security Lab**
Perform a VA/PT on your local Wi-Fi network and try automated attacks with NetStumbler and Kismet to gather information wireless network and try attacks like CowPatty and Aircrack. Further execute aircrack-ng to simulate attacks 802.11 WEP and WPA-PSK keys for auditing wireless networks and performing airodump, aircrack, airmon, airbase, aireplay and airtun using Kali 2.0 (Sana) Linux. Attempt a Wi-Fi sniffing to gather location data which can be used to identify device parameters of wireless communication devices.

**Experiment No. 8: Reverse Engineering Lab**
Use Metasploit (open-source exploit framework) to write and test your own exploit into any PC/Site with existing payloads using Virtual Machines in Ubuntu Host and Windows XP Virtual disk. These traces should be executed in OllyDbg step by step, and debug the protocols every single command, laidback with registers and flags, with buffer information. Also debug standalone DLL’s like MessageBox and wsprintf. Use IDA Pro (evaluate a limited version of the disassembler) to examine a protected and obfuscated sample executable. (.NET Reflector can be used to search through, the class hierarchies of .NET assemblies, even without any source code).
Perform static and dynamic code auditing.
Experiment No. 9: Security Data Analytics Lab

Download KDD CUP’99 dataset (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html). Separate the datasets into two class dataset such as normal-dos, normal-probe, normal-u2r, and normal-r2l. Any of the toolkits such as R, Weka, RapidMiner, Matlab, etc., can be used.

1. Apply Correlation based Feature Selection Algorithms (FSA) in order to derive the subset of features that represent the dataset. What is the gain in applying FSA? Is there any change in detection rate with and without applying FSA? How the execution time/model building time varies with and without applying FSA?
2. Apply Multilayer Perceptron Classification algorithm and calculate the metrics such as detection rate, false alarm rate, ROC value, F-measure for each class. Also, vary the parameters such as momentum and learning rate and calculate the metrics.
3. Apply Simple k-Means Clustering algorithm and calculate the metrics such as detection rate, false alarm rate, ROC value, F-measure for each class. Also, vary the parameters such as Euclidean and Manhattan distances and calculate the metrics.
4. Apply RIPPER algorithm (rule based classifier) to formulate the rules extracted from the dataset. Determine the number of rules extracted and enumerate each rule.

Devise a procedure/mechanism in building a dataset for the following:
1. Network Intrusion Detection system dataset
2. Host Intrusion Detection system dataset
3. Malware dataset
4. Botnet dataset
5. Spam email, Web browsing, Net flow data, firewall logs, Anomilize Tools, DNS records

Refer: http://www.unb.ca/research/iscx/dataset/index.html
Systematically generate the dataset involving each of the four identified modules – Experimental set up, Data collection, Feature construction and Class labeling.

Experiment No. 10: Mobile & Smart Phone Security Lab

Familiarize with mobile .apk files, Create your own android app, Find vulnerable app in play store, Perform forensics analysis on the app and document the inferences.

16CY 701 MOBILE AND WIRELESS NETWORKING AND SECURITY 2-0-1-3

TEXT BOOKS/REFERENCES:


16CY 702 LANGUAGE-BASED SECURITY 2-0-1-3

General purpose languages, Domain Specific languages, Abstract Syntax Tree, Axiomatic semantics of programming languages, Assertions, Tree patterns expressing security properties using discrete structures and Logic, Examining AST using ASTLOG, Querying AST objects using QL, Semmle QL Tool, Insight into Analysis and Verification of concurrent programs and cryptographic protocols written in C, Insight into Code analysis and Program Transformation using Spoon for Java. Software engineering practices for development of high assurance code - Model Checking, Program Analysis techniques for analyzing software – Static analysis, Dynamic analysis, Taint analysis, Program slicing.

TEXT BOOKS/REFERENCES:


16CY 703 NETWORK SECURITY 2-0-1-3

Techniques for network intrusion detection: signature-based and anomaly-based detection, Snort, Firewalls-packet filters and stateful firewalls, application-aware firewalls, proxies, NAT, Virtual Private Networks-tunneling, IPSEC VPNs, L2TP, PPP, PPTP, denial of service (DoS) and distributed denial-of-service (DDoS) attacks, detection and reaction, worm and virus propagation, tracing the source of attacks, traffic analysis, techniques for hiding the source or destination of network traffic, secure routing protocols, protocol scrubbing and advanced techniques for reacting to network attacks. HTTP authentication, SSL/TLS, Kerberos, secure DNS, Email spam and its solutions, broadcast security, secure multicasting.

TEXT BOOKS/REFERENCES:


16CY 704  STEGANOGRAPHY AND OBFUSCATION  2-0-1-3


TEXTBOOKS/ REFERENCES:


16CY 705  INFORMATION SECURITY AND RISK MANAGEMENT  3-0-0-3

Information Risk Management, Relationships among different security components - threat agent, vulnerability, risk, asset, exposure and safeguards. Governance models such as COSO and CobiT, ISO 27000 series of standards for setting up security programs, risk analysis and management, policies, standards, baselines, guidelines and procedures as applied to Security Management program, Information strategy objectives, Security awareness and training. Security Architecture and Design – review of architectural frameworks (such as Zachman and SABSA), concepts of Security Models (such as Bell-LaPadula, Biba and Brewer-Nash), vulnerabilities and threats to information systems (such as traditional on-premise systems, web based multi-tiered applications, distributed systems and cloud based services), application of countermeasures to mitigate against those threats and security products evaluation. Business Continuity and Disaster Recovery- Business Continuity Management concepts, Business Impact Analysis, BC/DR Strategy development, backup and offsite...
facilities and types of drills and tests. An introduction to Operational Security and Physical Security aspects.

TEXT BOOKS / REFERENCES:

16CY 706 HDL AND CRYPTOGRAPHIC APPLICATIONS 2-0-1-3

Introduction to Verilog: structure, constructs, and conventions; Modeling at Gate level, Data flow level, Behavior level, and switch level. Design, simulation, and synthesis of digital circuits, modules, and systems. Functions, tasks, User defined primitives, Compiler directives. Queues, PLAs, and FSMs. FPGAs – blocks inside, their features and use. IDE and its use. FPGA based design realizations. Design of finite field arithmetic operations. Representative designs with AES, ECC and Hash Algorithms.

TEXT BOOKS/REFERENCES:

16CY 707 CODING AND INFORMATION THEORY 3-0-1-4

Information, Entropy, Discrete memoryless source, Source coding – Shannon-Fano coding, Huffman coding, Lempel-Ziv and arithmetic codes, Rate distortion theory, Optimum Quantizer Design; Discrete memoryless channel, Mutual information, channel capacity, Shannon limit; Error control codes – Linear block codes, Error detection and correction, Hamming codes, Reed Muller codes, Golay codes, Cyclic codes, Binary BCH codes, Reed Solomon codes, Decoding algorithms, Trellis representation of codes, Convolution codes and its applications, Viterbi algorithm and decoding.

TEXT BOOKS/REFERENCES:

**16CY 708 SECURITY IN CLOUD COMPUTING 3-0-1-4**

The trade-offs and differences among cloud offerings such as SaaS, PaaS and IaaS. Key-value stores and their trade-offs against transactional SQL stores. Implementations of classic key-value stores such as Big Table & Dynamo. The use of consensus in distributed systems and its implementation in Paxos and Raft. MapReduce and other parallel processing frameworks. Server and network virtualization. Security in the cloud---infrastructure and data. Significant hands-on project experience with a chosen cloud computing framework. Privacy, Side Channel Attack, Insider attack on cloud computing. SAS-70 Certificates HIPAA, Public and Private cloud, Key Management problem for cloud. Homomorphic and Searchable Encryption.

**TEXT BOOKS/REFERENCES:**


**16CY 709 DESIGN AND ANALYSIS OF ALGORITHMS 3-0-1-4**


**TEXT BOOKS/REFERENCES:**

**16CY 710 FORMAL METHODS FOR SECURITY  2-0-1-3**

Formal Methods – propositional and predicate logic, and theorem-proving; fixed-points and their role in program analysis and model-checking; verification of sequential programs using weakest preconditions and inductive methods, and verification concurrent and reactive programs/systems using model-checking and propositional temporal logic (CTL and LTL); application of static and dynamic program analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols; information flow and taint analysis for security of web applications; pi-calculus for formal modelling of mobile systems and their security. SPIN, PVS, and Isabelle tools.

**TEXT BOOKS/REFERENCES:**

**16CY 711 SECURE SYSTEMS ENGINEERING  2-0-1-3**

Information flow and vulnerability model to build security into life cycle phase of software (and hardware) components. Threat and vulnerability analysis into architecture and design process, access-controlled and clean environment to build software, target environment hardening and secure application deployment. Introduction to hardware security – Physical and side channel attacks and its countermeasures, tamper resistance. Secure operational processes - roles and access policies for development. Practical aspects of cryptography - usable crypto algorithms and key life cycle management, mobile computing. Balancing security and usability – developing authentication mechanisms, secure browsing, social media and data sharing. Countermeasures for possible social engineering attacks in design. Secure interactive design. Usable PKI. Privacy issues in Human Computer Interaction. Security Economics: Risk assessment and selection of appropriate countermeasures with
cost-benefit trade-offs.

TEXT BOOKS/REFERENCES:

16CY 712 SECURITY IN INTERNET OF THINGS 2-0-1-3


TEXT BOOKS/REFERENCES:

16CY 713 ANDROID SECURITY 2-0-1-3


TEXT BOOKS/REFERENCES: