ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

("ವಿ ಟಿ ಯು ಅಧಿನಿಯಮ 1994"ರ ಅಡಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಿಂದ ಸ್ಥಾಪಿತವಾದ ರಾಜ್ಯ ವಿಶ್ವವಿದ್ಯಾಲಯ)

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

(State University of Government of Karnataka Established as per the VTU Act, 1994)

Phone : 0831-2498100 / 24054
Fax : 0831-2405467
Email : registrar@vtu.ac.in
Web : https://vtu.ac.in

Prof. B. E. Rangaswamy, **Ph.D**
REGISTRAR

REF: VTU/BGM/Circular 566/2024-25/ 560

Date: 13 MAY 2024

CIRCULAR

Sir,

Subject: **Updated** Syllabus of **BIC401-Element of Cyber Security and IoT** regarding…

Reference: Chairperson BOS in CSE/ISE VTU Belagavi's email dated 12.05.2024
The Hon'ble Vice-Chancellor's approval dated: 13.05.2024

This refers to the subject cited above, **BIC401-Element of Cyber Security and IoT**, the syllabus has been revised to meet the title, course/subject objective, and outcome. The updated syllabus is attached to this circular for teachers' and students' reference and use.

It is hereby requested that all principals of engineering colleges that offer the program CSE(IoT Cyber Security and Blockchain Technology) update the content of the circular to all concerned.

Encl: Updated syllabus copy of BIC401

Sd/-
REGISTRAR

To,
The Principals of Affiliated, Constituent Engineering Colleges under the ambit of the university

Copy to.

1. To the Hon'ble Vice-Chancellor through the secretary to VC, VTU Belagavi for information
2. The Chairperson BoS in CSE/ISE for UG programs of the university, VTU Belagavi
3. The Registrar (Evaluation) VTU Belagavi for information and needful
4. The Director, ITI SMU, VTU Belagavi for information and arrange for uploading the circular on the VTU web portal
5. The Special Officer QPDS for information and to follow the updated syllabus for question paper setting and ensure during the scrutiny
6. The Special Officer Academic Section for information

13/05/24

REGISTRAR

1315

Elements of Cyber Security and IoT		Semester	4
Course Code	BIC401	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	3
Examination type (SEE)	Theory		

Course objectives:

1. To gain basic knowledge of computer networks and cybersecurity terminologies.
2. To organize various attack techniques and exploitation in cyber security
3. To Learn various malicious code available to perform the attack.
4. To understand the fundamentals of IoT, Sensor Networks and smart objects.
5. To describe the characteristics of different IoT access technologies and application-based protocols for IoT.

Teaching-Learning Process

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
6. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.
7. Introduce Topics in manifold representations.
8. Show the different ways to solve the same problem with different circuits/logic and encourage the students to come up with their own creative ways to solve them.
9. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding
10. Use any of these methods: Chalk and board, Active Learning, Case Studies

Module-1 **8 hours**

Networking Basics: Computer Network: The Meaning, LAN vs. WAN, Network Infrastructure, Peer-to-Peer vs. Client-Server, Client-Server Network Architecture, Network Devices, Network Speeds, The OSI Model, Roles of Each One of the 7 Layers, The Network Administrator, Collision and Broadcast Domains.

Networking Hardware: Host Machines (Workstations and Computers), Network Adapter (Network Interface Card), Hub, Switch, Router, Modem.

IP Addressing: What is an IP address? What is the Function of an IP Address? Hexadecimal Number System, Default Gateway, Finding Your IP Address Manually, IP Address Configuration, DHCP, Default IP Address Classes.

Network and Security Concepts: Information Assurance Fundamentals, Basic Cryptography, Symmetric Encryption, Public Key Encryption, The Domain Name System (DNS), Firewalls.

Textbook 3 - Chapter 1, 2, 5 and Textbook 1 - Chapter 1.1 (1.1.1 - 1.1.6)

Module-2 **8 hours**

Attacker Techniques and Motivations: How Hackers Cover Their Tracks (Anti-forensics), Fraud Techniques, Threat Infrastructure.

Exploitation: Techniques to Gain a Foothold - Shellcode, Integer Overflow Vulnerabilities, Stack-Based Buffer Overflows, Format String Vulnerabilities, SQL Injection, Malicious PDF Files, Race Conditions, Web Exploit Tools, DoS Conditions, Brute Force and Dictionary Attacks.

Textbook 1 - Chapter 2: 2.1-2.3 (excluding 2.1.2), Chapter 3: 3.1

Module-3 **8 hours**

Exploitation (Contd..): Misdirection, Reconnaissance, and Disruption Methods.

Malicious Code: Self-Replicating Malicious Code, Evading Detection and Elevating Privileges, Stealing Information and Exploitation.

Textbook 1 - Chapter 3: 3.2, Chapter 4

Module-4 **8 hours**

Introduction to IoT: Genesis of IoT, IoT and Digitization, IoT Impact, Convergence of IT and OT, IoT challenges.

Smart Objects: Sensors, Actuators, Micro-Electro-Mechanical systems (MEMS), Smart Objects, Trends in smart objects. Sensor Networks.

Textbook 2 - Chapter 1, Chapter 3

Module-5 **8hours**

IoT Access Technologies: IEEE 802.15.4, IEEE 901.2a, IEEE 802.11ah, LoRaWAN.

IP as the IoT Network Layer: The business case for IP, the need for Optimization, optimizing IP for IoT.

Application Protocols for IoT: The transport Layer, IoT application transport methods, SCADA, CoAP, MQTT.

Textbook 2 - Chapter 4, Chapter 5, Chapter 6

Course outcome (Course Skill Set)

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

CO1: Explain the terminology and role of Cyber Security in computer networks.

CO2: Illustrate the various attack techniques and exploitation methods used by attacker.

CO3: Compare various malicious code available for the attacks.

CO4: Explain fundamentals of IoT and its challenges.

CO5: Classify different access technologies proposed for IoT.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods

of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by the University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module
4. Marks scored shall be proportionally reduced to 50 marks

Books

Text Books:

1. James Graham, Richard Howard and Ryan Olson, Cyber Security Essentials, CRC Press, 2011.
2. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", 1st Edition, Pearson Education (Cisco Press Indian Reprint). (ISBN: 978-9386873743).
3. Russell Scott, Computer Networking: Computer Networking for Beginners and Beginners Guide (All in One), 978-1652202806, 2019 (Publisher: Russell Scott, 2019).

References:

1. Anand Shinde, "Introduction to cyber security", ISBN 978-1-63781-642-4, Nationpress.com.
2. Charles J Brooks, Christopher Grow, Philip Craig, Donald Short , "Cybersecurity-Essentials"- 1st Edition, , Sybex Publications.
3. Sudip Misra, Anandarup Mukherjee, Arijit Roy, "Introduction to IoT", Cambridge University Press 2021

Web links and Video Lectures (e-Resources):

1. https://onlinecourses.nptel.ac.in/noc17_cs22/course
2. https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html
3. https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs31/

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Project Based Learning
- Case Study