Pimpri Chinchwad Education Trust's

PIMPRI CHINCHWAD COLLEGE OF ENGINEERING

SECTOR NO. 26, PRADHIKARAN, NIGDI, PUNE 411044

An Autonomous Institute Approved by AICTE and Affiliated to SPPU, Pune

DEPARTMENT OF COMPUTER ENGINEERING

Curriculum Structure and Syllabus
of
Honors in Cyber Security
(Regulations 2023)

Academic Year 2026-28

Institute Vision

To be one of the top 100 Engineering Institutes of India in coming five years by offering exemplarily Ethical, Sustainable and Value-Added Quality Education through a matching ecosystem for building successful careers.

Institute Mission

1. Serving the needs of the society at large through establishment of a state-of-art Engineering Institute.
2. Imparting right Attitude, Skills, Knowledge for self-sustenance through Quality Education.
3. Creating globally competent and Sensible engineers, researchers and entrepreneurs with an ability to think and act independently in demanding situations.

EOMS Policy

“We at PCCOE are committed to offer exemplarily Ethical, Sustainable and Value Added Quality Education to satisfy the applicable requirements, needs and expectations of the Students and Stakeholders.

We shall strive for technical development of students by creating globally competent and sensible engineers, researchers, and entrepreneurs through Quality Education.

We are committed for Institute’s social responsibilities and managing Intellectual property.

We shall achieve this by establishing and strengthening state-of-the-art Engineering Institute through continual improvement in effective implementation of Educational Organizations Management Systems (EOMS).”

	Pimpri Chinchwad Education Trust's **Pimpri Chinchwad College of Engineering**	
Course Approval Summary		

A) Board of study - Department of Computer Engineering

Sr. No.	Name of the Course	Course Code	Page number	Signature and stamp of BoS
1	Cyber Law and Cryptography	BCE25HN07	5	
2	Cryptography Laboratory	BCE25HN08	7	
3	Digital Forensics and VAPT	BCE26HN07	10	
4	Digital Forensics and VAPT Laboratory	BCE26HN08	12	
5	AI for Cyber Security	BCE27HN06	15	
7	Project	BCE28HN06	20	

Approved by Academic Council:

Chairman, Academic Council
Pimpri Chinchwad College of Engineering

Preface

Looking at Global Scenario to enhance the employability skills and impart deep knowledge in emerging/ multidisciplinary areas, an additional avenue is provided to passionate learners through the Minors and Honors Degree Scheme in academic structure.

For **Honors degree** program, student has to earn additional 20 credits in emerging area of one's own domain.

Objectives of Honors Degree

- To enable students to pursue allied academic interest in contemporary areas.
- To provide effective yet flexible options for students to achieve basic to intermediate level competence in the contemporary area.
- To enhance the employability skills with different combinations of competencies and flavors. To provide an academic mechanism for fulfilling demand of specialized areas from industries for higher order skill jobs.
- To provide a strong foundation to students aiming to pursue research/ higher studies in the contemporary field of study.

Preface of Honors in Cyber Security

Today's digital world increases the sophistication of threats to the cyber landscape coupled with the rapid increase in attempts to disrupt our critical systems and gain commercial and personal data. There is an ever-increasing demand for highly skilled cyber security graduates to defend individuals and organizations from various cybercrimes. The Cyber Security Honors Program is created to train the next generations of cyber security experts to develop reliable and lawful networks. Security, cryptography, cyber law, incident response, and digital forensics are just some of the topics that will be covered in this comprehensive program.

With a carefully designed curriculum that emphasizes practical experience, students working toward an honors degree in cyber security can acquire the analytical and investigative skills necessary to keep up with the ever-changing nature of cybersecurity threats. Department of Computer Engineering Cyber Security Honors Program teaches students to think critically about security in order to address complex problems, identify and counteract cyber threats, evaluate risks, and implement state-of-the-art security measures. Courses in Advanced Security and Digital Forensics, as well as Blockchain Architecture Design, are among those available through the Honors program. Through the course of study, students will acquire the broad range of knowledge, skills, abilities, and dispositions necessary for success as cybersecurity professionals in a variety of public and private sectors.

Objectives

This program aims to

1. Prepare responsible Cyber Security professionals by training them about cyber laws, Information security compliances, and ethical disclosures.
2. Apply security best practices to keep the system running as usual despite the existence of inherent risks.
3. Design, deploy, and assess a computational solution to the issue of securing software and systems.

Learning Outcomes

Students, after completing this Honors course successfully, will be able to

1. Reflect critically on existing theoretical knowledge, ideas, and practice within computing and cyber security to address the research topic.
2. Realize legal and ethical principles to be adopted in the domain of security practices
3. Demonstrate an understanding of specialized knowledge in computing and cyber security, tools and techniques, and digital forensic lifecycle for proactive security.

INDEX

LIST OF ABBREVIATIONS IN CURRICULUM STRUCTURE

Sr. No.	Abbreviation	Expansion
1.	L	Lecture
2.	P	Practical
3.	T	Tutorial
4.	H	Hours
5.	CR	Credits
6.	FA1	Formative Assessment 1
7.	FA2	Formative Assessment 2
8.	SA	Summative Assessment
9.	TW	Term Work
10.	OR	Oral
11.	PR	Practical
12.	PROJ	Project

Curriculum Structure

Honors in Cyber Security

CURRICULUM STRUCTURE

Structure for Honors in Cyber Security (Computer Engineering)

Semester	Course code	Course Name	Teaching Scheme				CR	Evaluation Scheme						
			L	P	T	H		FA1	FA2	SA	TW	PR	OR	Total
V	BCE25HN07	Cyber Law and Cryptography	3	-	-	3	3	20	20	60	-	-	-	100
V	BCE25HN08	Cryptography Laboratory	-	4	-	4	2	-	-	-	50	-	-	50
VI	BCE26HN07	Digital Forensics and VAPT	3	-	-	3	3	20	20	60	-	-	-	100
VI	BCE26HN08	Digital Forensics and VAPT Laboratory	-	4	-	4	2	-	-	-	50	-	-	50
VII	BCE27HN06	AI for Cyber Security	2	4	-	6	4	10	10	30	50	-	-	100
VIII	BCE28HN06	Project	-	8	-	8	4	-	-	-	50	-	50	100
	Total		8	20	0	28	18	50	50	150	200	-	50	500

L-Lecture, **P**-Practical, **T**-Tutorial, **H**-Hours, **Cr**-Credits, **FA**-Formative Assessment, **SA**-Summative Assessment, **TW**-Term Work, **OR**-Oral, **PR**-Practical

Course Syllabus Semester – V

Honors in Cyber Security

Program:	B. Tech. (Computer) - Honors in Cyber Security					Semester: V	
Course:	Cyber Law and Cryptography					Code: BCE25HN07	
Credit	Teaching Scheme (Hrs./Week)			Evaluation Scheme and Marks			
	Lecture	Practical	Tutorial	FA		SA	Total
				FA1	FA2		
3	3	-	-	20	20	60	100

Prior Knowledge of:

1. Basic algorithm analysis
2. Complexity theory,
3. Elementary notions of logic
4. Set theory.

is essential.

Course Objectives:

1. To provide a detailed understanding of Cyber Crimes, Countermeasures and Cyber Laws, and Information Security Standard.
2. Analyze the legal perspectives and laws related to cybercrimes in the Indian context.
3. To provide the fundamental mathematical base for cryptographic algorithms
4. To provide in-depth knowledge of cryptography theories, algorithms, and systems.

Course Outcomes:

After learning the course, the students will be able to:

1. Comprehend how various cybercrime take place and evaluate the effect of cybercrime
2. Comprehend how cyber laws are effective against cybercrimes and design a system compliant with Information Security Standard
3. Apply the knowledge of Finite Fields for various algorithms of cryptography
4. Apply the knowledge of various identification schemes.
5. Evaluate the performance of different message digest and hash algorithms.
6. Analyze and model modern cryptography including problem statements and mathematical approaches.

Detailed Syllabus:

Unit	Description	Duration (H)
I	**Fundamentals of Cyber Crime:** Overview, nature, scope, and types of Cyber Crime; Comparison between traditional criminal techniques and cybercrime; Impact of cybercrime on E-Governance and E-commerce; Best Practices of cybercrime investigation Procedure for search and seizure for digital evidence. Tools and Methods of Cyber Crime: Phishing, Password Cracking, Keyloggers, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Identity Theft Case Study: Challenges in handling cybercrime from the perspective of Individuals and enterprises	08

II	**Cyber Security Laws and Regulations:** Indian Law Perspective - IT Act (2000) and Personal Data Protection Bill (2019); Global-Regulation Perspective - GDPR, GLBA, HIPAA; **Cyber Laws and Compliance:** Different Aspects of Cyber Laws - Contractual aspects, Intellectual property aspect, Criminal Aspects; Legal framework for managing cyber security; Information Security Standards - SOX, NIST, ISO Case Study: Legal Procedure for GDPR violation	**07**
III	**Finite Fields:** Modular Arithmetic, congruence theorem, Algebraic structure, GF (2n) fields Euclidean theorem, Extended Euclidean theorem, Factorization, Fermat's theorem, Euler's theorem, Chinese remainder theorem, Discrete logarithms, Lagrange's method.	**08**
IV	**Advance Cryptosystems** **Asymmetric key Cryptosystems:** Rabin, El-Gamal, Knapsack**,** Elliptic Curve cryptosystem, Pairing-based Cryptography**,** Identity-Based and Attribute-Based cryptosystem**.** **Symmetric key Cryptosystems:** IDEA, Blowfish, CAST-128**.**	**07**
V	**Introduction to Cryptographic Hash Functions**: Fundamentals of MAC Protocols, HMAC, CMAC, CBC-MAC and PMAC, Design of Collision-Resistant Hash Functions, Popular Uses of Collision-Resistant Hash Functions, MD5, SHA-I, SHA-256. **Digital Signature schemes:** Elgamal, Schnorr signature schemes, ECDSA, CCA security for symmetric encryption. Case study: Multi-collision resistant hash function.	**08**
VI	**Cryptography in the age of quantum computers:** Grover's algorithm and symmetric cryptography, Shor's algorithm and public-key cryptography, Quantum key distribution, Quantum secret sharing, and multiparty computation, post-quantum cryptography. Case study: The DARPA Quantum Cryptography Network.	**07**
	Total	**45**

Text Books:

1. William Stallings**, "**Cryptography and Network Security: Principles and Practice", 6th Edition, Pearson Education, ISBN 13: 9781292158587
2. Forouzan, B.A., **"**Cryptography & Network Security" Tata McGraw-Hill Education, ISBN-13: 978-0070702080
3. Kahate, A.,"Cryptography, and Network Security". McGraw-Hill Higher Ed., ISBN-13: 9789353163303
4. Godbole, N., "Information Systems Security: Security Management, Metrics, Frameworks and Best Practices". 1st Ed. John Wiley & Sons India, ISBN: 9788126564057.

Reference Books:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", 20th Anniversary Edition, Wiley, ISBN: 978-1-119-09672-6.
1. Jeff Koseff , "3rd Edition, Cyber Security Law" Wiley ISBN: 9781119231509

Web references:

1. williamstallings.com/Extras/Security-Notes/
2. www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/
3. http://freevideolectures.com/Course/3027/Cryptography-and-Network-Security
4. http://cs.brown.edu/courses/csci1510/2013_lectures.html
5. NPTEL Course lectures links :- https://nptel.ac.in/courses/106/105/106105031/ (Modern cryptography, ECC and SHA)

Program:	B. Tech. (Computer) - Honors in Cyber Security			Semester:			V
Course:	Cryptography Laboratory			Code:			BCE25HN08
Credit	Teaching Scheme (Hrs./Week)			Evaluation Scheme			
	Lecture	Practical	Tutorial	TW	PR	OR	Total
2	-	4	-	50	-	-	50

Prior Knowledge of:

1. Basic algorithm analysis
2. Complexity theory
3. Elementary notions of logic
4. Set theory

is essential.

Course Objectives:

1. To explore the working principles of well-known attacks such as Buffer Overflow, SQL Injection and their countermeasures.
2. To explore the issues security issues in the network and resolve it.
3. To develop the ability to use modern cryptographic utilities to build programs for secure communication.

Course Outcomes:

After learning the course, the students will be able to:

1. Acquire background on well-known Cryptography Digital Signature Techniques
2. Apply various public key cryptography techniques
3. Apply finite field (mathematics) for achieving security
4. Apply security and privacy methods in development of modern applications and in organizations to protect resources and to prevent cyber crimes
5. Evaluate security mechanisms using rigorous approaches by digital signatures and Hash functions.
6. Develop awareness of latest trends and advances in security using quantum computing

Guidelines for Students:

- The laboratory assignments are to be submitted by students in the form of a journal.
- Journal consists of prologue, certificate, table of contents and handwritten write-up of each assignment (Title, Objectives, Problem Statement, Outcomes, Date of Completion, Assessment grade/marks and assessor's sign, Theory- Concept, algorithm, sample input and expected output, conclusion).
- Program codes with sample output of all performed assignments are to be submitted as softcopy.

Guidelines for Laboratory /TW Assessment:

- Continuous assessment of laboratory work is done based on the overall performance and laboratory performance of students.
- Each laboratory assignment assessment should assign grade/marks based on the parameters with appropriate weightage.
- Suggested parameters for overall assessment as well as each laboratory assignment assessment includes- performance, timely completion, innovation, efficiency, punctuality, and neatness.

Guidelines for Laboratory Conduction

- Operating System: 64-bit Open-source Linux or its derivative.
- Programming Tools: Open-Source C, C++, JAVA and PYTHON.
- All assignments are compulsory to perform.

Assignment No.	Suggested List of Assignments
1	Given a piece of code with buffer-overflow vulnerability, gain the root privilege by exploiting this vulnerability
2	Demonstrate SQL Injection using SQL Map
3	Demonstrate Cross-site Scripting attack.
4	Demonstrate password cracking using Cain and Abel and John the Ripper tools.
5	Write a program to solve a system of linear congruence by applying the Chinese Remainder Theorem
6	Write a program to implement the MD5/SHA-1 algorithm.
7	Write a program to implement Rabin Cryptosystem.
8	Write a program to implement Knapsack Cryptosystem
9	Write a program to illustrate El-Gamal digital signature.
10	Write a program to illustrate Elliptic curve digital signature algorithm.
11	Write a program to illustrate Schnorr digital signature schemes.
12	Implement shor's public key cryptography algorithm.

Reference Books:

1. William Stallings**,** Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, ISBN13: 9781292158587
2. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education, ISBN-13: 978-0070702080
3. Kahate, A**.** Cryptography, and Network Security. McGraw-Hill Higher Ed., ISBN-13: 9789353163303
4. Godbole, N., Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. 1st Ed.John Wiley & Sons India, ISBN: 9788126564057.
5. Riggs, C., Network Perimeter Security: Building Defence In-Depth, AUERBACH, USA, eISBN: 9780429211577.

Web references:

1. NPTEL Course lectures links:

   https://nptel.ac.in/courses/106/105/106105031/ (Modern cryptography, ECC and SHA)

Course Syllabus Semester – VI
Honors in Cyber Security

Program:	B. Tech.(Computer) - Honors in Cyber Security			Semester:			VI
Course:	Digital Forensics and VAPT			Code:			BCE26HN07
Credit	Teaching Scheme (Hrs./Week)			Evaluation Scheme and Marks			
	Lecture	Practical	Tutorial	FA		SA	Total
				FA1	FA2		
3	3	-	-	20	20	60	100

Prior Knowledge of:
1. Cryptography
2. System Security

is essential.

Course Objectives:

This course aims at enabling students:
1. Understand the fundamental concepts and principles of cybersecurity, digital forensics, and system security.
2. Analyze common cyber threats, vulnerabilities, and security mechanisms used to protect information systems.
3. Learn the methodologies for digital evidence collection, preservation, and forensic investigation.
4. Understand vulnerability assessment and penetration testing approaches for evaluating system and network security.

Course Outcomes:

After learning the course, the students will be able to:
1. Apply forensic techniques to recover and analyze digital evidence from storage media and file systems.
2. Analyze disk and memory artifacts to identify malicious activity, reconstruct events, and extract actionable forensic evidence.
3. Analyze disk and memory artifacts to identify malicious activity, reconstruct events, and extract actionable forensic evidence.
4. Apply vulnerability scanning and assessment methods to identify, prioritize, and mitigate security weaknesses.
5. Evaluate penetration testing workflows and overall system and network security posture.

Detailed Syllabus:

Unit	Description	Duration (H)
I	**Advanced Digital Evidence and Artifact Recovery:** Introduction to digital forensics, purpose and scope of forensic investigation; types of digital evidence and forensic lifecycle; chain of custody and proper evidence handling; overview of common file systems (FAT, NTFS, EXT) and their structures; disk imaging and cloning techniques; deleted file recovery and metadata extraction; timestamp analysis and artifact identification from installed applications and user activity; hands-on exercises on recovering files from disk images and verifying integrity of recovered evidence.	9
II	**Disk and Memory Forensics:** Overview of memory forensics and volatile data; memory acquisition techniques and RAM dumps; analyzing running processes, handles, and loaded modules; identifying malware artifacts in memory; process and network connection analysis; pagefile and swap	9

	file examination; timeline reconstruction from memory; extraction and analysis of forensic artifacts.	
III	**Log and Network Forensics:** Collection and analysis of system, application, and security logs; correlation of events across multiple sources; identification of anomalies and suspicious activities; intrusion detection evidence analysis; network traffic capture and packet analysis; monitoring and interpreting network protocols; tracing attacks and reconstructing attack timelines; forensic investigation of network-based incidents and evidence preservation.	**9**
IV	**Vulnerability Assessment Techniques:** Vulnerability scanning and enumeration; CVE mapping and exploitability analysis; system and application misconfiguration assessment; threat modeling and attack surface evaluation; automated and manual assessment methods; risk scoring, prioritization, and remediation strategy; interpretation of vulnerability reports for security audit and compliance.	**9**
V	**Penetration Testing and Exploitation:** Reconnaissance and information gathering; enumeration of hosts, services, and users; vulnerability validation and exploitation workflow; privilege escalation techniques; post-exploitation analysis; attack chain reconstruction; reporting and documentation of exploited vulnerabilities; evaluation of system and network security posture.	**9**
	Self-Study: Anti-Forensics Techniques and Detection, Fileless Malware Detection in Memory, Encrypted Traffic Analysis (TLS Fingerprinting), Zero-Day Vulnerabilities and Responsible Disclosure, Living-off-the-Land (LotL) Attack Techniques:	***5**
	Total (not including *)	**45**

Text Books:

1. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, 2018, Cengage Learning, ISBN 9781337568944
2. The Hacker Playbook 3: Practical Guide to Penetration Testing, Peter Kim, 2018, CreateSpace Independent Publishing, ISBN 9781980901759

Reference Books:

1. 1. Digital Forensics and Incident Response, Gerard Johansen, 2019, Packt Publishing, ISBN 9781788830680
2. 2. Hands-On Penetration Testing on a Budget, Sagar Rahalkar, 2020, Packt Publishing, ISBN 9781838649462 ISBN: 9780071798693

E-resources:

1 https://onlinecourses.nptel.ac.in/noc24_cs94/preview
2. https://onlinecourses.nptel.ac.in/noc22_cs83/preview
3. https://nptel.ac.in/courses/106104189

Program:	B. Tech. (Computer) - Honors in Cyber Security			Semester:			VI
Course:	Digital Forensics and VAPT Lab			Code:			BCE26HN08
Credit	Teaching Scheme (Hrs./Week)			Evaluation Scheme and Marks			
	Lecture	Practical	Tutorial	TW	OR	PR	Total
2	-	4	-	50	-	-	50

Prior Knowledge of:
1. Cryptography
2. Network security

is essential.

Course Objectives:

This course aims:
1. To provide hands-on experience with digital forensic tools for acquisition, recovery, and analysis of digital evidence.
2. Develop practical skills for analyzing disk, memory, and network artifacts to investigate security incidents.
3. To enable students to perform vulnerability scanning and basic penetration testing using industry-relevant security tools.
4. To train students in documenting forensic findings and security assessment results in a structured technical report.

Course Outcomes:

After learning the course, the students will be able to:
1. Apply digital forensic techniques to acquire and analyze evidence from storage media and file systems.
2. Analyze disk and memory artifacts to identify malicious activity and reconstruct system events.
3. Use forensic tools to investigate incidents and extract relevant digital evidence.
4. Perform vulnerability scanning to identify and prioritize security weaknesses.
5. Evaluate penetration testing results to assess system and network security posture.

Guidelines for Students:

- The laboratory course provides hands-on exposure to cybersecurity, digital forensics, vulnerability assessment, and penetration testing techniques. Students are required to perform the prescribed experiments using appropriate tools and document the procedure, observations, and results systematically in the laboratory journal.
- Each laboratory assignment should include **Title, objectives, a brief theory/concept, tools or a dataset used, a procedure, observations/results, and a conclusion**. Relevant outputs, screenshots, or evidence generated during the experiment should be properly recorded.
- Students must strictly follow ethical practices and perform all experiments only within the designated laboratory environment.

Guidelines for Laboratory/Term Work Conduction and Assessment:

- Continuous assessment of laboratory work is done based on overall performance and Laboratory performance of students.
- Each Laboratory assignment assessment should assign grade/marks based on parameters with appropriate weightage.
- Suggested parameters for overall assessment as well as each Laboratory assignment assessment include- timely completion, performance, innovation, efficiency, punctuality, and neatness.

Suggested Tools to be Used:

1. **Operating System:** 64-bit Open-source Linux or its derivative (e.g., Kali Linux, Ubuntu)
2. **Security and Forensic Tools:** Burp Suite, OWASP ZAP, Autopsy, Wireshark, and other relevant tools as required.

Assignment No.	Suggested List of Assignments

1	Recover deleted and hidden files from disk images and analyze metadata to reconstruct user and system activity
2	Investigate file system structures, timestamps, and log artifacts using Autopsy to track potential tampering or malicious behavior
3	Capture RAM dumps with LiME and analyze running processes and loaded modules using Volatility to detect suspicious or unauthorized activity
4	Extract malware artifacts from memory dumps using Volatility and Rekall, reconstruct sequence of events, and identify malware behavior patterns
5	Collect and correlate Windows/Linux system and application logs using ELK stack or Graylog to detect anomalies and potential intrusions
6	Analyze network traffic captures using Wireshark and tcpdump to identify abnormal communication patterns and potential attack attempts
7	Perform vulnerability scanning of lab systems and applications using OpenVAS or Nessus, map discovered vulnerabilities to CVE records, and assess exploitability
8	Evaluate server and application configurations using Lynis or Nmap scripts to identify misconfigurations, weak points, and security gaps
9	Map penetration testing workflow for a target web application using Metasploit framework and OWASP ZAP, identify potential attack vectors, and analyze exploitation paths conceptually
10	Integrate findings from forensic analysis and vulnerability assessment using combined reports from Autopsy, Volatility, and OpenVAS to evaluate overall system and network security posture and recommend mitigation strategies

Text Books:

1. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, 2018, Cengage Learning, ISBN 9781337568944
2. The Hacker Playbook 3: Practical Guide to Penetration Testing, Peter Kim, 2018, CreateSpace Independent Publishing, ISBN 9781980901759

Reference Books:

1. Digital Forensics and Incident Response, Gerard Johansen, 2019, Packt Publishing, ISBN 9781788830680
2. Hands-On Penetration Testing on a Budget, Sagar Rahalkar, 2020, Packt Publishing, ISBN 9781838649462

E-resources:

1. https://www.autopsy.com/support/
2. https://www.volatilityfoundation.org/
3. https://portswigger.net/burp/documentation

Course Syllabus Semester – VII
Honors in Cyber Security

Program:	B.Tech.(Computer) - Honors in Cyber Security					Semester: VII				
Course:	AI for Cyber Security					Code: BCE27HN06				
Credit	Teaching Scheme (Hrs./Week)			Evaluation Scheme						
	Lecture	Practical	Tutorial	FA		SA	TW	OR	PR	Total
				FA1	FA2					
4	2	4	-	10	10	30	50			100

Prior Knowledge of :
1. Digital Forensics
2. VAPT Techniques
3. Machine Learning Concepts

is essential.

Course Objectives:
This course aims at enabling students:
1. understand the application of AI and machine learning techniques in cybersecurity.
2. analyze malware, spam, and cyber attack patterns using AI-based methods.
3. explore AI-driven approaches for fraud detection and authentication.
4. understand AI techniques for intrusion detection and anomaly detection.

Course Outcomes:
After learning the course, the students will be able to:
1. Apply AI and machine learning techniques to analyze cyber security threats and vulnerabilities in real-world systems.
2. Analyze malware behaviour, attack and spam patterns using AI-based detection methods
3. Evaluate AI-driven approaches for fraud detection, authentication mechanisms, and security analytics.
4. Analyze network behaviour for intrusion detection and anomaly detection using AI techniques.

Guidelines for Laboratory/Term Work Assessment:

1. Continuous assessment will be based on the student's performance in implementing AI-based cybersecurity techniques during laboratory sessions. Evaluation should consider parameters such as correct application of machine learning methods for threat detection, data preprocessing and feature extraction, interpretation of security analytics results, timely completion of assignments, and quality of documentation.
2. The Mini Project should be evaluated based on problem identification in cybersecurity, appropriate dataset selection (e.g., malware, network traffic, or phishing datasets), implementation of AI/ML models, evaluation using metrics such as accuracy, precision, recall, and F1-score, and clarity of the final report and presentation.

Guidelines for Laboratory/Tutorial Conduction

1. Laboratory sessions should focus on the application of Artificial Intelligence and Machine Learning techniques to cybersecurity problems such as malware classification, phishing/spam detection, anomaly detection in network traffic, and user authentication analysis.
2. Students should perform experiments involving dataset preprocessing, feature extraction, model training, and evaluation of AI-based threat detection models, and analyze their effectiveness in identifying cyber attacks and abnormal system behaviour

using tools such as Python, Scikit-learn, and Jupyter Notebook.

Tools to be used:

Open-source tools and platforms are preferred for implementation. Students may use tools such as Python, Jupyter Notebook / Google Colab, and machine learning libraries like Scikit-learn, TensorFlow, and Keras for developing and evaluating AI-based cybersecurity solutions.

Detailed Syllabus:

Unit	Description	Duration (H)
I	**Introduction to AI for Cyber Security** Overview of AI in Cyber Security, Evolution from Expert Systems to AI-based Security Systems, Cyber Threat Landscape – Attacks, Vulnerabilities, Malware, Trojans, Security Data Sources – Logs, Network Traffic, Threat Intelligence Feeds, Feature Extraction from Security Data, Machine Learning Workflow for Security Analytics, AI Development using Jupyter Notebooks.	7
II	**Malware and Malicious Behaviour Detection** Malware Analysis and Classification, Signature-based and Behaviour-based Malware Detection, Supervised and Unsupervised Learning for Malware Detection, Decision Trees for Malicious Event Detection, Behaviour Profiling and Clustering of Malicious Activities, Phishing Detection using Machine Learning, Spam Detection using Natural Language Processing Techniques.	8
III	**AI Applications in Threat Detection** Email Spam Detection using Machine Learning, Image Spam Detection using Support Vector Machines, Natural Language Processing for Phishing and Spam Analysis, Fraud Detection using Machine Learning Models, Account Reputation Scoring and Abuse Detection, Keystroke Dynamics for User Authentication, Facial Recognition for Biometric Authentication.	7
IV	**Network Anomaly Detection and Adversarial ML** Network Traffic Behaviour Modelling, Time Series Analysis for Security Monitoring, Reconnaissance Attack Detection, Network Anomaly Detection Techniques, Machine Learning based Intrusion Detection Systems, Deep Learning for Intrusion Detection, Adversarial Attacks on Machine Learning Models, Model Poisoning, Black-box and White-box Attacks.	8
	Self- Study: Explainable AI for Security, Federated Learning in Cyber Security, Reinforcement Learning for Cyber Defense, Insider Threat Detection using AI, Security of AI Systems, AI for IoT Security.	*5
	Total (not including *)	45

Suggested Lab Assignments

1. Apply AI-based techniques to classify common cyber security threats (malware, trojans, phishing, vulnerabilities) using a given dataset or case examples.
2. Apply feature extraction and preprocessing techniques on system log datasets/threat intelligence datasets (or any other datasets as discussed with the instructor) to prepare data for AI-based threat detection
3. Apply supervised learning techniques to classify malware samples using a malware feature dataset.
4. Analyze patterns of malicious activities using clustering or classification models on a malware behaviour dataset.

5. Evaluate the performance of different machine learning or NLP-based models for email spam or phishing detection using an email dataset by comparing metrics such as accuracy, precision, recall, and F1-score.
6. Evaluate AI-based authentication methods using keystroke dynamics or biometric datasets by comparing their performance in detecting abnormal user behaviour using appropriate evaluation metrics.
7. Analyze network traffic datasets to identify anomalous patterns associated with cyber attacks using AI-based anomaly detection techniques.
8. Analyze adversarial attack techniques such as model poisoning, black-box, and white-box attacks and assess their impact on AI-based intrusion detection systems.
9 Mini Project

Text Books:

1. A. Hands-on Machine Learning for Cyber Security by Soma Halder, ISBN139781788992282
2. Machine Learning and Security by David Freeman, Clarence Chio Publisher: O'Reilly Media, Inc. Release Date: February 2018 ISBN: 9781491979891
3. Alessandro Parisi (2019). *Hands-On Artificial Intelligence for Cybersecurity*. Packt Publishing.

Reference Books:

1. Anthony D. Joseph et al. (2019). *Adversarial Machine Learning*. Cambridge University Press.

E-resources:

1. CICIDS2017 Dataset – https://www.unb.ca/cic/datasets/ids-2017.html
2. CVE Vulnerability Dataset – https://cve.mitre.org/data/downloads/index.htmlM
3. Microsoft Malware Classification Dataset – https://www.kaggle.com/c/malware-classification/data
4. Malimg Malware Image Dataset – https://www.kaggle.com/datasets/amauricio/malimg-dataset
5. SpamAssassin Public Email Dataset – https://spamassassin.apache.org/publiccorpus/
6. Phishing Websites Dataset – https://www.kaggle.com/datasets/uciml/phishing-websites-dataset
7. NSL-KDD Intrusion Detection Dataset – https://www.unb.ca/cic/datasets/nsl.html
8. UNSW-NB15 Dataset – https://research.unsw.edu.au/projects/unsw-nb15-dataset

Course Syllabus

Semester – VIII

Honors in Cyber Security

Program:	B. Tech.(Computer) - Honors in Cyber Security			Semester:			VIII
Course:	Project			Code:			BCE28HN06
Credit	Teaching Scheme (Hrs./Week)			Evaluation Scheme			
	Lecture	Practical	Tutorial	TW	PR	OR	Total
4	-	10	-	50	-	50	100

Prior knowledge of
Software Engineering, Engineering Mathematics, Cyber Security,
is essential

Course Objectives:
This course aims to: enable students::
1. To understand the Cyber Security Project Development Process.
2. To develop problem-solving skills by following the Software Development Life Cycle (SDLC) and focusing on secure development practices.
3. To review literature for cybersecurity project work from appropriate sources such as books, standards, manuals, research journals, and other credible sources, thereby enhancing analytical skills.
4. To design and implement real-world cybersecurity applications and solutions using appropriate tools, platforms, and security frameworks.
5. To validate and evaluate the security, performance, and effectiveness of the implemented solution.
6. To prepare good quality technical reports based on the selected project statement.

Course Outcomes:
After learning the course, the students will be able to:
1. Analyze the literature for various techniques and applications to find the gap and feasible solution.
2. Design real world applications considering emerging areas in technology.
3. Develop an application by considering actual requirements and social, environmental, ethical and legal issues
4. Test and evaluate the model results to develop a probable solution.
5. Prepare good-quality technical reports and present it effectively.

Guidelines for Project:

The objective of the Cyber Security Project is to develop and implement innovative or practical security solutions using knowledge acquired during the course. Final-year undergraduate students will work in groups to study feasibility, plan the project, analyze existing systems, explore relevant cybersecurity tools and technologies, and apply modern testing practices. The project culminates in the design and development of a functional model (software, hardware, or both) with appropriate security mechanisms and interfaces as an executable solution.

Project Guide:
- Each project activity must be supervised by a faculty member of the concerned department. This faculty member is termed as a Project Guide.
- Project guide shall help students to finalize (or identify) the project statement and suggest the objectives / methodology through brainstorming. The project team is required to regularly appraise the project guide about the progress and seek his/her guidance.
- Project guides must monitor the weekly progress being carried out by the project groups
- The project guide shall ensure the completion of all the project related activities as per the requirement of review.
- Project guide shall motivate and facilitate the students to write patent, copyright, research funding proposal and paper publications for the overall development of the student.

Project Activities:
Students are expected to perform the following activities –
1. Review of Recent Literature and Gap Identification
2. Requirement Analysis and Feasibility Study
3. Defining the Problem Statement and Objectives
4. Identifying the Project Implementation Requirements
5. Formulation of Methodology and Mathematical Modeling
6. Project Implementation
7. Testing and Deployment
8. Results Analysis and Validation

9. Research Paper Publication/IPR Filing if any
10. Report Writing

Project Report:
While preparing the project report, students should:

- Follow a standard structure (Abstract to Conclusion)
- Clearly define the cybersecurity problem and objectives
- Describe design, implementation, and security mechanisms
- Present results with analysis and validation/testing
- Document findings clearly with proper references

Research Outcome:

Based on the project results and conclusions, students are recommended to generate the research outcomes in terms of Research Publication, Patents, and Copyrights. This has to be done in consultation with project guides. Guides will decide the appropriateness of the results and converting those into research outcomes.

Vision and Mission of Computer Department

Department Vision

To be a premier Computer Engineering Department by achieving excellence in Academics and Research for creating globally competent and ethical professionals.

Department Mission

M1: To develop technologically competent and self-sustained professionals through contemporary curriculum.

M2: To nurture innovative thinking and collaborative research, making a positive impact on society.

M3: To provide state-of-the art computing environment and learning opportunities through Center of Excellence.

M4: To foster leadership skills and ethics with holistic development.