Structure and Syllabi
for
Minor in Emerging Area
"Machine Learning for Cyber Security"

w. e. f. Academic Year 2024-2025
(2023 Pattern)

Dr. N. M. Ranjan BoS Chairman	Dr. Ram Joshi Dean of Academics	J.S.P.M.'s Rajarshi Shahu College of Engineering, Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33	Dr. Rakesh K. Jain Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Department of Information Technology
Minor in Emerging Area
Machine Learning for Cyber Security
Structure (Effective from 2024-25)

Course Code	Course	Teaching Scheme				Credit	Examination Scheme				Total Marks
		L	T	P	Hr	C	ISE	MSE	ESE	TW	
	S. Y. Sem IV										
ITH2201T	Foundations of Cyber Security	3	-	-	3	3	20	30	50	-	100
ITH2201L	Foundations of Cyber Security Laboratory	-	-	2	2	1	ISCE: 30		20	-	50
	T. Y. Sem V										
ITH3201T	Machine Learning and Cyber Security	3	-	-	3	3	20	30	50	-	100
ITH3201L	Machine Learning and Cyber Security Laboratory	-	-	2	2	1	ISCE: 30		20	-	50
	TY Sem VI										
ITH3202T	Machine Learning for Penetration Testing	3	1	-	3	4	20	30	50	-	100
	B.Tech. Sem VII										
ITH4201T	Software Security	3	-	-	3	3	20	30	50	-	100
ITH4202L	Mini Project	-	-	6	6	3	ISCE: 50		50	50	150
Total		**12**	**1**	**10**	**22**	**18**					**650**

Abbreviations:
L – Lecture, T – Tutorial, P – Practical, Hr – Hours, C – Credits, TuT – Tutorial, ISE – In Semester Evaluation, MSE – Mid Semester Evaluation, ESE – End Semester Evaluation

Notes:
Eligibility for admission to the UG Bachelor's Degree with Double Minor: Minimum CGPA/CPI of 7.5 or minimum 75% after second semester for UG Bachelor's Degree.

For Theory courses: There shall be MSE, ISE and ESE. The ESE is a separate head of passing. For Lab courses: There shall be continuous assessment (ISCE consists of ISE and MSE). The ESE is a separate head of passing.

Dr. N. M. Ranjan
BoS Chairman

Dr. Ram Joshi
Dean of Academics

J.S.P.M.'s Rajarshi Shahu College of Engineering, Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33

Dr. Rakesh K. Jain
Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Department of Information Technology
S.Y. Semester -IV
[ITH2201T]: Foundations of Cyber Security

Teaching Scheme:	Credits:	Examination Scheme:
TH : 03 Hours/Week	TH : 03	In Sem. Evaluation : 20 Marks Mid Sem. Exam : 30 Marks End Sem. Exam : 50 Marks Total Marks : 100 Marks

Course Prerequisites: Computer Networks

Course Objective:
To learn about the most basic aspects of cyber security, including the impact of cyber attacks and the most common cyber security roles.

Course Outcome:
After successful completion of the course, students will able to:
CO1: Learn security fundamentals, including common threats and tools to prevent attacks
CO2: Study basics of cryptography, such as public-key infrastructure
CO3: Implement some advanced topics, like penetration testing
CO4: Examine the cyber security job market
CO5: Analyze intrusion detection systems with a case study
CO6: Implement fundamental cryptography in a real practice

Course Contents

UNIT-I	Introduction to Security Trends	07 Hours
The Computer Security Problem - Targets and Attacks - Approaches to Computer Security - Ethics - Basic Security Terminology - Security Models		
UNIT-II	**Operational and Organizational Security**	**07 Hours**
Policies, Procedures, Standards, and Guidelines - Security Awareness and Training - Interoperability Agreements - The Security Perimeter - Physical Security - Environmental Issues - Wireless - Electromagnetic Eavesdropping - People—A Security Problem - People as a Security Tool		
UNIT-III	**Cryptography**	**07 Hours**
Cryptography in Practice - Historical Perspectives - Algorithms - Hashing Functions - Symmetric Encryption - Asymmetric Encryption - Quantum Cryptography- Cryptography Algorithm Use		
UNIT-IV	**Authentication and Remote Access**	**07 Hours**
User, Group, and Role Management - Password Policies - Single Sign-On - Security Controls and Permissions - Preventing Data Loss or Theft - The Remote Access Process - Remote Access Methods		

Dr. N. M. Ranjan	Dr. Ram Joshi		Dr. Rakesh K. Jain
BoS Chairman	Dean of Academics		Director

J.S.P.M.'s Rajarshi Shahu College of Engineering, Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33

UNIT-V	Intrusion Detection Systems	07 Hours
History of Intrusion Detection Systems - IDS Overview - Network-Based IDSs - Host-Based IDSs Intrusion Prevention Systems - Honeypots and Honeynets – Tools		
UNIT-VI	**Network Security**	**07 Hours**
Principles of Network Security, Network Security Terminologies, Network Security and Data Availability, Components of Network Security, Network Security Policies.		

Text Books:

T1. W.A.Coklin, G.White, Principles of Computer Security: Fourth Edition, McGrawHill, 2016

T2. William Stallings, Cryptography and Network Security Principles and Practices, Seventh Edition,Pearson

Reference Books:

R1. Achyut S. Godbole, Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing, Tata McGraw-Hill Education, 2013

R2. AtulKahate, ―Cryptography and Network Security‖, Tata McGraw-Hill, 2003

MOOC Platform:

https://www.springboard.com/resources/learning-paths/cybersecurity-foundations/

Dr. N. M. Ranjan	Dr. Ram Joshi		Dr. Rakesh K. Jain
BoS Chairman	Dean of Academics		Director

J.S.P.M.'s Rajarshi Shahu College of Engineering Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Department of Information Technology

S.Y. Semester -IV

[ITH2201L]: Foundations of Cyber Security Laboratory

Teaching Scheme:	**Credits:**	**Examination Scheme:**
LAB: 02 Hours/Week	LAB: 01	ISCE: 30 Marks ESE: 20 Marks

Course Prerequisites: Computer Networks

Lab Objective:
To learn about the most basic aspects of cyber security, including the impact of cyber attacks and the most common cyber security roles.

Lab Outcome:
After successful completion of the course, students will able to:
LO1: Learn security fundamentals, including common threats and tools to prevent attacks
LO2: Study basics of cryptography, such as public-key infrastructure
LO3: Implement some advanced topics, like penetration testing
LO4: Examine the cyber security job market
LO5: Analyze intrusion detection systems with a case study
LO6: Implement fundamental cryptography in a real practice

Lab Contents

Guidelines for Assessment

Continuous assessment of laboratory work is to be done based on overall performance and lab practicals /assignments performance of student. Each lab practical/assignment assessment will assign grade/marks based on parameters with appropriate weightage. Suggested parameters for overall assessment as well as each lab assignment assessment include- timely completion, performance, innovation, efficient codes, punctuality and neatness.

List of Laboratory Assignments/Experiments

1	Study of the features of firewall in providing network security and to set Firewall Security in windows.
2	Implement Euclidean and Extended Euclidean algorithm to find out GCD and solve the inverse mod problem.
3	Installation of kali linux.
4	Create Virtual Machine using any of the cloud platform and analyze it.
5.	Implement network-based Intrusion Detection System
6	Implement RSA Algorithm

Dr. N. M. Ranjan **BoS Chairman**	**Dr. Ram Joshi** **Dean of Academics**	J.S.P.M.'s Rajarshi Shahu College of Engineering, Pune University I.D. No. PU/PN/Engg./173/(2001), Tathawade, Pune-33	**Dr. Rakesh K. Jain** **Director**

Text Books: T3. W.A.Coklin, G.White, Principles of Computer Security: Fourth Edition, McGrawHill, 2016 T2. William Stallings, Cryptography and Network Security Principles and Practices, Seventh Edition,Pearson
Reference Books: R1. Achyut S. Godbole, Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing, Tata McGraw-Hill Education, 2013 R2. AtulKahate, ―Cryptography and Network Security‖, Tata McGraw-Hill, 2003
MOOC Platform: https://www.springboard.com/resources/learning-paths/cybersecurity-foundations/

Dr. N. M. Ranjan **BoS Chairman**	**Dr. Ram Joshi** **Dean of Academics**	J.S.P.M.'s Rajarshi Shahu College of Engineering Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33	**Dr. Rakesh K. Jain** **Director**

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Department of Information Technology

T.Y. Semester -V

[ITH3201T]: Machine Learning and Cyber Security

Teaching Scheme:	Credit	Examination Scheme:
TH: - 03Hours/Week	TH:03	In Sem. Evaluation:20 Marks Mid Sem. Exam: 30 Mark End Sem. Exam : 50 Marks

Course Prerequisites: Fundamentals of Cyber Security

Course Objective:

1. To study how machine learning can help in securing data.
2. To learn how machine learning has contributed to the success of filters
3. To understand quick way to detect anomalies
4. To conduct malware analysis by extracting used information from computer binaries
5. To examine how attackers exploit consumer-facing websites and app functionality
6. To translate your machine learning algorithms from the lab to production

Course Outcome:

After successful completion of the course, students will able to:

CO1: Learn different machine learning algorithms to secure information
CO2: Implement filtering methods using machine learning techniques
CO3: Analyze different methods of detecting anomalies.
CO4: Perform malware analysis using information
CO5: Visualize the attacks on consumer websites
CO6: Model machine learning based model to create a production system

Course Contents

UNIT-I	Convergence of Machine Learning and Cyber Security	06 Hours
Cyber Threat Landscape,The Cyber Attacker's Economy, Overview of Machine Learning, Real-World Uses of Machine Learning in Security, Spam Fighting: An Iterative Approach		
UNIT-II	**Anomaly Detection**	**07 Hours**
Anomaly Detection Versus Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods, Feature Engineering for Anomaly Detection, Anomaly Detection with Data and Algorithms, Challenges of Using Machine Learning in Anomaly Detection		
UNIT-III	**Malware Analysis**	**07 Hours**
Understanding Malware, Feature Generation, From Features to Classification, Live malware analysis, dead malware analysis, Android Malware Analysis		

Dr. N. M. Ranjan BoS Chairman	Dr. Ram Joshi Dean of Academics	J.S.P.M.'s Rajarshi Shahu College of Engineering Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33	Dr. Rakesh K. Jain Director

UNIT-IV	Network Traffic Analysis	07 Hours
Theory of Network Defense, Machine Learning and Network Security, Building a Predictive Model to Classify Network Attacks		
UNIT-V	**Protecting the Consumer Web**	**07 Hours**
Monetizing the Consumer Web, Types of Abuse and the Data That Can Stop Them, Supervised Learning for Abuse Problems, Clustering Abuse		
UNIT-VI	**Production Systems**	**07 Hours**
Defining Machine Learning System Maturity and Scalability, Data Quality, Model Quality, Performance, Maintainability, Monitoring and Alerting, Security and Reliability		

Text Books:

T1. Clarence Chio, David Freeman **"**Machine Learning and Security**",** O'Reilly Media, Inc.ISBN: 9781491979907

T2. SumeetDua, Xian Du. "Data Mining and Machine Learning in Cybersecurity", CRC Press, ISBN:978-1439839423

Reference Books:

R1. Learning Nessus for Penetration Testing, by Himanshu Kumar

R2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2ed

R3. Mastering Modern Web Penetration Testing by Prakhar Prasad

Dr. N. M. Ranjan
BoS Chairman

Dr. Ram Joshi
Dean of Academics

J.S.P.M.'s Rajarshi Shahu College of Engineering Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33.

Dr. Rakesh K. Jain
Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to SavitribaiPhule Pune University, Pune)

Department of Information Technology

T.Y. Semester -V

[ITH3201L]: Machine Learning and Cyber Security Laboratory

Teaching Scheme:	**Credits:**	**Examination Scheme:**
LAB: 02 Hours/Week	LAB: 01	ISCE: 30 Marks ESE: 20 Marks

Course Prerequisites: Fundamentals of Cyber Security

Lab Objective:

1. To study how machine learning can help in securing data.
2. To learn how machine learning has contributed to the success of filters
3. To understand quick way to detect anomalies
4. To conduct malware analysis by extracting used information from computer binaries
5. To examine how attackers exploit consumer-facing websites and app functionality
6. To translate your machine learning algorithms from the lab to production

Lab Outcome:

After successful completion of the course, students will able to:

LO1: Learn different machine learning algorithms to secure information
LO2: Implement filtering methods using machine learning techniques
LO3: Analyze different methods of detecting anomalies.
LO4: Perform malware analysis using information
LO5: Visualize the attacks on consumer websites
LO6: Model machine learning based model to create a production system

Lab Contents

Guidelines for Assessment

Continuous assessment of laboratory work is to be done based on overall performance and lab practicals /assignments performance of student. Each lab practical/assignment assessment will assign grade/marks based on parameters with appropriate weightage. Suggested parameters for overall assessment as well as each lab assignment assessment include- timely completion, performance, innovation, efficient codes, punctuality and neatness.

List of Laboratory Assignments/Experiments

1	Use of any supervised learning algorithm for securing information.
2	Anomaly detection using supervised learning algorithm.
3	Study and implement intrusion detection system using SVM
4	Live malware analysis using unsupervised learning algorithm
5.	Study and implement clustering abuse.

Dr. N. M. Ranjan
BoS Chairman

Dr. Ram Joshi
Dean of Academics

J.S.P.M.'s Rajarshi Shahu College of Engineering Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33

Dr. Rakesh K. Jain
Director

6	Develop a machine learning model and deploy it as a web service

Text Books:

T1: Clarence Chio, David Freeman "Machine Learning and Security", O'Reilly Media, Inc.ISBN: 9781491979907

T2: SumeetDua, Xian Du. "Data Mining and Machine Learning in Cybersecurity", CRC Press, ISBN:978-1439839423

Reference Books:

R4. Learning Nessus for Penetration Testing, by Himanshu Kumar

R5. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2ed

R3: Mastering Modern Web Penetration Testing by Prakhar Prasad

Dr. N. M. Ranjan	Dr. Ram Joshi		Dr. Rakesh K. Jain
BoS Chairman	Dean of Academics		Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to SavitribaiPhule Pune University, Pune)

Department of Information Technology

T.Y. Semester -VI

[ITH3202T]: Machine Learning for Penetration Testing

Teaching Scheme:	Credit	Examination Scheme:
TH: - 3 Hours/Week	TH:03	In Sem. Evaluation:20 Marks Mid Sem. Exam: 30 Marks End Sem. Exam : 50 Marks

Course Prerequisites: Fundamentals of Cyber Security

Course Objective:

1. To understand basics of machine learning and the algorithms used to build robust systems.
2. To know how security products leverage machine learning
3. To identify machine learning development environments and Python libraries
4. To understand machine learning techniques for detection of phishing, botnet, etc.
5. To analyze best practices for Machine Learning and Feature Engineering

Course Outcome:

After successful completion of the course, students will able to:

CO1: Demonstrate the use of machine learning algorithms for penetration testing
CO2: Apply machine learning methods to detect phishing attacks
CO3: Apply machine learning methods for botnet detection
CO4: Identify the steps to detect advanced persistent threats
CO5: To implement machine learning based applications to detect Intrusion Detection Systems
CO6: To use best practices for machine learning to solve real examples

Course Contents

UNIT-I	Introduction to Machine Learning in Penetration Testing	07 Hours
Introduction, technical requirements, machine learning development environment and python libraries, ML in penetration testing- promises and challenges		
UNIT-II	**Phishing Domain Detection**	**07 Hours**
Introduction, social engineering overview, Steps of social engineering penetration testing, Building real-time phishing attack detectors using different machine learning models		
UNIT-III	**Botnet Detection with Machine Learning**	**07Hours**
Overview of Botnet, technical requirement, building a botnet detector model with multiple machine learning techniques, how to build a Twitter bot detector – a case study		
UNIT-IV	**Detecting Advanced Persistent Threats**	**07 Hours**

Dr. N. M. Ranjan	Dr. Ram Joshi		Dr. Rakesh K. Jain
BoS Chairman	Dean of Academics		Director

J.S.P.M.'s Rajarshi Shahu College of Engineering, Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33

Introduction, threats and risk analysis, Threat-hunting methodology, Threat hunting with the ELK Stack		
UNIT-V	**Evading Intrusion Detection Systems**	**07 Hours**
Introduction, technical requirements, Adversarial machine learning algorithms, Evading intrusion detection systems with adversarial network systems		
UNIT-VI	**Best Practices for Machine Learning and Feature Engineering**	**07Hours**
Introduction, Feature engineering in machine learning, Feature selection algorithms, Best practices for machine learning		

Text Books:

1. ChihebChebbi, "Mastering Machine Learning for Penetration Testing", Packt, ISBN9781788997409
2. Learning Nessus for Penetration Testing, by Himanshu Kumar,
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition.
4. Mastering Modern Web Penetration Testing by Prakhar Prasad
5. Rtfm: Red Team Field Manual by Ben Clark

Reference Books:

R1. "Practical Malware Analysis" by Michael Sikorski and Andrew Honig
R2. "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition by Reverend Bill Blunden
R3. "Rootkits: Subverting the Windows Kernel" by Jamie Butler and Greg Hoglund
R4. "Practical Reverse Engineering" by Dang, Gazet, Bachaalany

Dr. N. M. Ranjan **BoS Chairman**	**Dr. Ram Joshi** **Dean of Academics**	J.S.P.M.'s Rajarshi Shahu College of Engineering, Pune University I.D. No. PU/PN/Engg./173/(2001), Tathawade, Pune-33	**Dr. Rakesh K. Jain** **Director**

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

B. Tech (Department of Information Technology)
B.Tech. Semester –VII
[ITH4201T]: Software Security

Teaching Scheme:	Credit	Examination Scheme:
TH: - 3Hours/Week	TH:3	In Sem. Evaluation:20 Marks Mid Sem. Exam: 30 Marks End Sem. Exam: 50 Marks

Course Prerequisites: Fundamentals of Cyber Security

Course Objective:
To explore the foundations of software security including important software vulnerabilities and attacks and important software vulnerabilities, including advanced testing and program analysis techniques.

Course Outcome:
After successful completion of the course, students will able to:
CO1: Study fundamentals of software security
CO2: Learn important software vulnerabilities and attacks
CO3: Understand software vulnerabilities
CO4: Design defenses that prevent or mitigate attacks
CO5: Implement techniques that can be used to strengthen the security of software systems at each phase of the development cycle
CO6: Test and verify that software is secure

Course Contents

UNIT-I	Security a software Issue	06 Hours
introduction, the problem, Software Assurance and Software Security, Threats to software security, Sources of software insecurity, Benefits of Detecting Software Security What Makes Software Secure: Properties of Secure Software, Influencing the security properties of software, Asserting and specifying the desired security properties?		
UNIT-II	**Requirements Engineering for secure software**	**07 Hours**
Introduction, the SQUARE process Model, Requirements elicitation and prioritization		
UNIT-III	**Secure Software Architecture and Design**	**07 Hours**
Introduction, software security practices for architecture and design: architectural risk analysis, software security knowledge for architecture and design: security principles, security guidelines and attack patterns Secure coding and Testing: Code analysis, Software Security testing, Security testing considerations throughput the SDLC		
UNIT-IV	**Security and Complexity**	**07 Hours**
System Assembly Challenges: introduction, security failures, functional and attacker perspectives for security analysis, system complexity drivers and security		
UNIT-V	**Governance and Managing for More Secure Software**	**07 Hours**

Dr. N. M. Ranjan	Dr. Ram Joshi		Dr. Rakesh K. Jain
BoS Chairman	Dean of Academics		Director

J.S.P.M.'s Rajarshi Shahu College of Engineering, Pune University I.D. No. PU/PN/Engg./173/(2001) Tathawade, Pune-33

Governance and security, Adopting an enterprise software security framework, How much security is enough?, Security and project management, Maturity of Practice		
UNIT-VI	**Case Studies of Software Security**	**07 Hours**
A case study in open source software security and privacy,Java Card Security Testing, A Case Study of Software Security Test Based on Defects Threat Tree Modeling		
Text Books: T1. Software Security Engineering: Julia H. Allen, Pearson Education		
Reference Books: R1. Developing Secure Software: Jason Grembi, Cengage Learning R2. Software Security: Richard Sinn, Cengage Learning		
MOOC Platform: **https://www.coursera.org/learn/software-security**		

Dr. N. M. Ranjan
BoS Chairman

Dr. Ram Joshi
Dean of Academics

J.S.P.M.'s Rajarshi Shahu College of Engineering
Pune University
I.D. No.
PU/PN/Engg./173/(2001)
Tathawade, Pune-33.

Dr. Rakesh K. Jain
Director