राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUTE OF TECHNOLOGY PATNA
(शिक्षा मंत्रालय, भारत सरकार के अधीन एक राष्ट्रीय महत्व का संस्थान / An Institute of National Importance under Ministry of Education, Gov. of India)
संगणक विज्ञान एवं अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना - ८००००५, बिहार / Ashok Rajpath, Patna- 800005, Bihar
Tel. No. – 0612-2372715, 2370419 (Ext-200) email- cseoffice@nitp.ac.in

***CSXX02*69: Security Analytics**
L-T-P-Cr: 3-0-0-3

Prerequisite: Data structures and algorithms, probability and statistics, and introductory AI/ML concepts, cyber security

Learning Objectives:

1. Understand and explain the fundamental concepts of information and network security.
2. Apply data analytics and AI/ML techniques to detect and respond to security threats using real-world security datasets
3. Analyze and interpret security incidents using modern security tools, methodologies, and case studies
4. Evaluate privacy, adversarial machine learning, and ethical issues in security analytics, and propose appropriate solutions
5. Demonstrate the ability to design and implement security analytics workflows and solutions for contemporary cybersecurity challenges

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

Sl. No.	Outcome	Mapping to Pos
CO1	Understand fundamental concepts of information and network security.	PO1, PO2
CO2	Apply data analytics and AI/ML techniques to security data for threat detection and response.	PO1 – PO5
CO3	Analyze security incidents using modern tools and methodologies.	PO1 – PO5
CO4	Explore privacy, adversarial ML, and ethical issues in security analytics.	PO6-PO8, PO12

Syllabus:

Unit	Details	Lecture
I	**Introduction to Security Analytics** **Overview of Information and Network Security:** Key principles: Confidentiality, Integrity, Availability, Security threats, vulnerabilities, and risk management, Types of attacks: Malware, Phishing, Denial of Service, Insider threats **Security Analytics Fundamentals:** Definition, scope, and	**6 Hrs**

	applications, Role of analytics in modern security operations, Security data lifecycle and the importance of data-driven security	
II	**Data Collection and Pre-processing for Security** **Security Data Sources:** System logs, network traffic, endpoint data, application logs **Data Pre-processing:** Data cleaning, normalization, feature extraction , Handling missing and imbalanced data, Anonymization and privacy-preserving pre-processing **Security Data Challenges:** Volume, velocity, variety, and veracity in security datasets	**6 Hrs**
III	**Machine Learning for Security Analytics** **ML Basics for Security:** Supervised vs. unsupervised learning in security, Feature engineering for security data Threat Detection Techniques: Anomaly detection, clustering, classification Use cases: Intrusion detection, malware classification, phishing detection **Model Evaluation:** Metrics for security analytics (precision, recall, F1-score, ROC curves), Applying ML algorithms to security datasets (e.g., KDD Cup, UNSW-NB15)	**10 Hrs**
IV	**Network and Web Security Analytics** **Network Security Analytics:** Network intrusion detection: Signature-based and anomaly-based methods, Deep packet inspection, flow analysis, Alert aggregation and correlation **Web Security Analytics:** Web log analysis, detection of web-based attacks (SQL injection, XSS), Case studies: Detecting botnets, DDoS, and web fraud **Visualization:** Security event visualization and dashboards	**8 Hrs**
V	**Advanced Topics in Security Analytics** **Insider Threat and Masquerader Detection:** Behavioral analytics, user profiling **Adversarial Machine Learning:** Attacks on ML models, model robustness **Privacy and Ethics:** Privacy-preserving analytics, data protection laws (GDPR, etc.), Ethical hacking, responsible disclosure, bias and fairness in security analytics	**8 Hrs**
VI	**Tools, Frameworks, and Case Studies** **Security Analytics Platforms:** SIEM tools (e.g., Splunk, ELK Stack), open-source IDS (e.g., Snort) **Practical Case Studies:** Real-world attack scenario analysis, Fraud detection, incident response workflows	**7 Hrs**

Textbooks:

1. Nina Godbole, "Information Systems Security: Security Management, Metrics, Frameworks and Best Practices," Wiley (Unit : 1,2,6)

2. William Stallings, "Network Security Essentials: Applications and Standards" (Unit : 1,4)
3. Data Analytics for Cybersecurity, Cambridge University Press (Unit : 1,2,3,5,6)
4. Clarence Chio & David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms (Unit : 3)
5. Data Analysis for Network Cyber-Security, World Scientific Publishing (Unit : 4)
6. Mark Stamp, Information Security: Principles and Practice (Unit : 5)

REFERENCE BOOKS:

1. Rakesh M. Verma & David J. Marchette, Cybersecurity Analytics
2. Daniel Barbara & Sushil Jajodia, Applications of Data Mining in Computer Security
3. Adversarial Machine Learning in the Context of Network Security (Journal Article)