Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Faculty of Computer Applications

Programme	B.Sc. IT Honours (Cyber Security)	**Branch**	Computer Applications
Semester	V	**Version**	1.0.0.0
Effective from Academic Year	2026-27	**Effective for the batch Admitted in**	June 2024
Subject code	U65B4SAE	**Subject Name**	SECURITY ARCHITECTURE & ENGINEERING

Teaching scheme						**Examination scheme (Marks)**			
(Per week)	**Lecture (DT)**		**Practical (Lab.)**		**Total**		**CCE**	**SEE**	**Total**
	L	TU	P	TW					
Credit	4	-	-	-	4	Theory	50	50	100
Hours	4	-	-	-	4				

Objective:

To equip students with a comprehensive understanding of the principles, frameworks, and practical approaches used in designing and implementing secure architectures across systems, networks, applications, and emerging platforms, while aligning with industry best practices and compliance standards.

Pre-requisites:

Basic knowledge of computer networks, operating systems, cryptography, and cybersecurity fundamentals. Familiarity with software development lifecycle and programming concepts is recommended.

Learning Outcome:

Name of CO	Description
CO1	Explain the foundational concepts of security architecture, security models, and secure design principles.
CO2	Analyze and apply enterprise security architecture frameworks and perform threat modeling to identify and classify security controls.
CO3	Design secure communication systems using cryptographic techniques and Public Key Infrastructure (PKI).
CO4	Evaluate and implement security architectures for operating systems, networks, virtualization, and cloud environments.
CO5	Architect secure applications, apply secure coding practices, and assess emerging trends such as Zero Trust, SASE, and AI/ML in cybersecurity.

Mapping of CO and PO:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	2	1	0	1	3	2	0	1	1	0	0
CO2	3	3	3	2	2	2	1	0	1	1	0	1
CO3	2	2	3	1	3	3	1	0	1	1	0	0
CO4	2	3	3	2	3	3	2	1	2	2	1	1
CO5	2	3	3	1	3	3	3	3	3	2	3	3

Content:

Unit	Content	Hrs.
1	**Fundamentals of Security Architecture** Introduction to Security Architecture, Confidentiality, Integrity, and Availability (CIA Triad). Principles of Secure Design, Classical Security Models, Introduction to Risk Management: threats, vulnerabilities, and risk assessment. Security Governance – Security Policies, Standards and Procedures. Overview of industry frameworks	12
2	**Architecture Frameworks and Secure Design** Introduction to enterprise architecture frameworks, Overview of security architecture frameworks, Integration of security SDLC, Threat modeling fundamentals, Classification of security controls – administrative, technical, physical. Overview of CIS Controls, Security requirements traceability and risk treatment planning.	12

3	**Cryptographic Architecture and PKI** Introduction to cryptographic architecture, Symmetric and asymmetric encryption algorithms, Cryptographic hash functions, Digital signatures, Public Key Infrastructure (PKI) – components: CAs, RAs, CRLs, OCSP, X.509 certificate structure and lifecycle management. Secure communication protocols, Certificate pinning and best practices in secure communication.	12
4	**System, Network, and Virtualization Security Architecture** Operating system security, Access control models, Hardware-based security, Virtualization and cloud security, Cloud service models – PaaS, SaaS. Secure network design – segmentation, firewalls. Identity and Access Management, Security monitoring, High availability – clustering, failover, backup and recovery.	12
5	**Application Security Architecture and Emerging Trends** Secure application architecture, layers of web applications and threat vectors, Secure coding practices and code review. Static and dynamic application security testing. Container-native and serverless application security. Cloud-native security principles and patterns. Emerging trends, AI/ML for security analytics, Security-as-Code and Infrastructure-as-Code.	12

Practical Content:

Reference Books:

1	Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross Anderson, Wiley, 3rd Edition
2	Enterprise Security Architecture: A Business-Driven Approach" by John Sherwood et al., CRC Press
3	Computer Security: Art and Science" by Matt Bishop, Addison-Wesley
4	Principles of Information Security" by Michael E. Whitman and Herbert J. Mattord, Cengage Learning
5	NIST Special Publications: SP 800-53 and SP 800-160

Web Reference:

1	https://www.threatintelligence.com/blog/security-architecture
2	https://www.entrust.com/resources/learn/what-is-pki
3	https://www.simplilearn.com/top-cybersecurity-trends-article
4	https://www.zscaler.com/resources/security-terms-glossary/what-is-infrastructure-as-code-security

MOOC/Certificate Course:

1	https://www.coursera.org/learn/packt-security-architecture-and-engineering-f4vdz
2	https://www.coursera.org/learn/cybersecurity-architecture

Question Paper Scheme:

End Semester Examination Duration: (2 Hours Theory Examination)

Note for Examiner: -

Q-1 Any Five out of Seven (25 Marks)
Q-2 Any Two out of Three (06 Marks)
Q-3 Mandatory question (05 Marks)
Q-4 Any Two out of Three (08 Marks)
Q-5 Any Two out of Three(06 Marks)

*The question paper must comprehensively address all Course Outcomes (COs), align with Bloom's Taxonomy levels, and ensure complete syllabus coverage.