Kurukshetra University, Kurukshetra

(Established by the State Legislature Act XII of 1956)

('A++' Grade, NAAC Accredited)

|| योगस्थ: कुरु कर्माणि ||

समबुद्धि व योग युक्त होकर कर्म करो

(Perform Actions while Stead fasting in the State of Yoga)

Modified Scheme of Examination (5th and 6th Semester) for Under-Graduate Programmes

Bachelor of Computer Applications (BCA) (CLOUD TECHNOLOGY & INFORMATION SECURITY): SCHEME D

according to

Curriculum Framework for Under-Graduate Programmes

As per NEP-2020 (Multiple Entry-Exit, Internships and Choice Based Credit System)

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS

(For the Batches Admitted From 2023-2024)

Kurukshetra University Kurukshetra
Modified Scheme of Examination (5th and 6th Semester) for Undergraduate programmes
Subject: BCA (Cloud Technology & Information Security)
According to
Curriculum Framework for Undergraduate Programmes
as per NEP 2020 (Multiple Entry-Exit, Internships, and Choice Based Credit System)

Sem	Course Type	Course Code	Nomenclature of paper	Credits	Contact hours	Internal marks	End term Marks	Total Marks	Duration of exam (Hrs) T + P
5	CC-A5	B23-CTS-501	Cloud Service Models	3	3	20	50	70	3
			Practical	1	2	10	20	30	3
	CC-B5	B23-CTS-502	Cloud Infrastructure and Virtulaization	3	3	20	50	70	3
			Practical	1	2	10	20	30	3
	CC-C5	B23-CTS-503	Network Security and Cryptography	3	3	20	50	70	3
			Practical	1	2	10	20	30	3
	CC-M5(V)	To be taken from VOC Pool							
	SEC-4	Internship @ 4 Credits							
6	CC-A6	B23-CTS-601	Ethical Hacking and Penetration Testing	3	3	20	50	70	3
			Practical	1	2	10	20	30	3
	CC-B6	B23-CTS-602	Cyber Forensics and Incident Response	3	3	20	50	70	3
			Practical	1	2	10	20	30	3
	CC-C6	B23-CTS-603	Cloud Deployment and Automation	3	3	20	50	70	3
			Practical	1	2	10	20	30	3
	CC-M6	B23-CTS-604	Basics of Blockchain	3	3	20	50	70	3

			Practical	1	2	10	20	30	3
	CC-M7(V)	To be taken from VOC Pool							

Kurukshetra University, Kurukshetra
(Established by the State Legislature Act XII of 1956)
('A++' Grade, NAAC Accredited)

|| योगस्थ: कुरु कर्माणि ||
समबुद्धि व योग युक्त होकर कर्म करो
(Perform Actions while Stead fasting in the State of Yoga)

Syllabus of Examination (5th & 6th Semester) for Under-Graduate Programmes
Bachelor of Computer Applications (BCA) (Cloud Technology and Information Security)
Scheme D
according to
Curriculum Framework for Under-Graduate Programmes
As per NEP-2020 (Multiple Entry-Exit, Internships and Choice Based Credit System)
DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
(For the Batches Admitted From 2023-2024)

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
KURUKSHETRA UNIVERSITY, KURUKSHETRA

<table>
<tr><th colspan="4">Scheme: 2023-24, Syllabus: 2025-26</th></tr>
<tr><th colspan="4">Part A - Introduction</th></tr>
<tr><td>Subject</td><td colspan="3">BCA(CTIS)</td></tr>
<tr><td>Semester</td><td colspan="3">V</td></tr>
<tr><td>Name of the Course</td><td colspan="3">Cloud Service Models</td></tr>
<tr><td>Course Code</td><td colspan="3">B23-CTS-501</td></tr>
<tr><td>Course Type: (CC/MCC/MDC/CC-M/DSEC/VOC/DSE/PC/AEC/ VAC)</td><td colspan="3">CC-A5</td></tr>
<tr><td>Level of the course (As per Annexure-I</td><td colspan="3">300-399</td></tr>
<tr><td>Pre-requisite for the course (if any)</td><td colspan="3">Knowledge of Basics of Cloud Computing</td></tr>
<tr><td>Course Learning Outcomes(CLO):</td><td colspan="3">After completing this course, the learner will be able to:
1. Understand and compare the key characteristics of IaaS, PaaS, and SaaS.
2. Apply cloud service models for development, deployment, and scaling of applications.
3. Demonstrate the use of cloud platforms for storage, compute, and software services.
4. Analyze pricing, security, and adoption factors for cloud-based solutions.
5*. Implement a basic project combining multiple service models.</td></tr>
<tr><td rowspan="2">Credits</td><td>Theory</td><td>Practical</td><td>Total</td></tr>
<tr><td>3</td><td>1</td><td>4</td></tr>
<tr><td>Contact Hours</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td colspan="2">Max. Marks:100(70(T)+30(P))
Internal Assessment Marks:30(20(T)+10(P))
End Term Exam Marks: 70(50(T)+20(P))</td><td colspan="2">Time: 3 Hrs.(T), 3Hrs.(P)</td></tr>
<tr><th colspan="4">Part B- Contents of the Course</th></tr>
<tr><td colspan="4"><u>Instructions for Paper-Setter</u>
The examiner will set a total of nine questions. Out of which first question will be compulsory. Remaining eight questions will be set from four unit selecting two questions from each unit. The examination will be of three-hour duration. All questions will carry equal marks. The first question will comprise short answer-type questions covering the entire syllabus.
Candidate will have to attempt five questions in all, selecting one question from each unit. First question will be compulsory.
The practicum will be evaluated by an external and an internal examiner. The examination will be of</td></tr>
</table>

three-hour duration.		
Unit	**Topics**	**Contact Hours**
I	**Introduction to Cloud Service Models**: Cloud computing service models – overview and need, Characteristics of IaaS, PaaS, and SaaS, Comparison among service models, Service model architecture and abstraction layers, Deployment responsibilities of cloud providers and consumers, Service model selection criteria based on business needs.	11
II	**Infrastructure as a Service (IaaS)**: Definition and scope of IaaS, Virtual machines: creation, management, and provisioning, Storage services and networking in IaaS, IaaS providers: AWS EC2, Azure VMs, Google Compute Engine, Elasticity and scaling, Security measures and shared responsibility model.	11
III	**Platform as a Service (PaaS)**: Concept and components of PaaS, Application development and runtime environments, Deployment pipelines and DevOps in PaaS, PaaS providers: AWS Elastic Beanstalk, Google App Engine, Azure App Services, Auto-scaling, performance, and integration features, Security challenges and PaaS limitations.	11
IV	**Software as a Service (SaaS) and Case Studies**: SaaS model overview and architecture, Benefits and limitations of SaaS, SaaS product lifecycle, SaaS providers: Microsoft 365, Salesforce, Google Workspace, Pricing models: subscription-based, usage-based, Multitenancy and customization, Case studies on model adoption in business and public sectors, Cloud vendor lock-in and interoperability.	11
V*	Practicum: Students are advised to do laboratory/practical practice not limited to but including the following types of problems: • Create and manage a virtual machine instance on AWS EC2 • Deploy a static/dynamic website using Google App Engine • Use Azure App Services to build and deploy a sample web app • Upload and access files using cloud object storage (e.g., S3) • Build a mini SaaS application using Firebase or Heroku • Monitor cloud resources using dashboards and metrics tools • Estimate pricing for IaaS and PaaS using cloud provider calculators • Integrate cloud database services like RDS or Firestore • Set up and test auto-scaling in AWS or Azure • Mini project involving a combination of IaaS + PaaS + SaaS components	30
Suggested Evaluation Methods		

Internal Assessment: ➢ **Theory** • Class Participation: 5 • Seminar/presentation/assignment/quiz/class test etc.: 5 • Mid-Term Exam: 10 ➢ **Practicum** • Class Participation: NA • Seminar/Demonstration/Viva-voce/Lab records etc.: 10 • Mid-Term Exam: NA	**End-Term Examination:** A three-hour exam for both theory and practicum. **End Term Exam Marks: 70(50(T)+20(P))**

Part C-Learning Resources

Recommended Books/e-resources/LMS:

- Rajkumar Buyya, Christian Vecchiola, and Thamarai Selvi – *Mastering Cloud Computing*, McGraw-Hill
- Gautam Shroff – *Enterprise Cloud Computing*, Cambridge University Press
- Michael J. Kavis – *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*, Wiley
- Anthony T. Velte, Toby J. Velte, and Robert Elsenpeter – *Cloud Computing: A Practical Approach*, McGraw-Hill
- Thomas Erl, Zaigham Mahmood, and Ricardo Puttini – *Cloud Computing: Concepts, Technology & Architecture*, Prentice Hall.

*Applicable for courses having practical components.

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
KURUKSHETRA UNIVERSITY, KURUKSHETRA

<table>
<tr><th colspan="4">Scheme: 2023-24, Syllabus: 2025-26</th></tr>
<tr><th colspan="4">Part A - Introduction</th></tr>
<tr><td>Subject</td><td colspan="3">BCA (CTIS)</td></tr>
<tr><td>Semester</td><td colspan="3">V</td></tr>
<tr><td>Name of the Course</td><td colspan="3">Cloud Infrastructure and Virtualization</td></tr>
<tr><td>Course Code</td><td colspan="3">B23-CTS-502</td></tr>
<tr><td>Course Type: (CC/MCC/MDC/CC-M/DSEC/VOC/DSE/PC/AEC/ VAC)</td><td colspan="3">CC-B5</td></tr>
<tr><td>Level of the course (As per Annexure-I</td><td colspan="3">300-399</td></tr>
<tr><td>Pre-requisite for the course (if any)</td><td colspan="3">None</td></tr>
<tr><td>Course Learning Outcomes(CLO):</td><td colspan="3">After completing this course, the learner will be able to:
1. Understand the architecture and components of cloud infrastructure.
2. Explain different types of virtualization and hypervisors.
3. Configure and manage virtual machines, virtual storage, and virtual networks.
4. Use infrastructure management tools to monitor and optimize virtual resources.
5. *Apply cloud infrastructure concepts in real-world use cases and labs.</td></tr>
<tr><td rowspan="2">Credits</td><td>Theory</td><td>Practical</td><td>Total</td></tr>
<tr><td>3</td><td>1</td><td>4</td></tr>
<tr><td>Contact Hours</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td colspan="2">Max. Marks:75(50(T)+25(P))
Internal Assessment Marks:20(15(T)+5(P))
End Term Exam Marks: 55(35(T)+20(P))</td><td colspan="2">Time: 3 Hrs.(T), 3Hrs.(P)</td></tr>
<tr><th colspan="4">Part B- Contents of the Course</th></tr>
<tr><td colspan="4"><u>Instructions for Paper-Setter</u>
The examiner will set a total of nine questions. Out of which first question will be compulsory. The remaining eight questions will be set from four units selecting two questions from each unit. The examination will be of three-hour duration. All questions will carry equal marks. The first question will comprise short answer-type questions covering the entire syllabus.
The candidate must attempt five questions, selecting one from each unit. The first question will be compulsory.</td></tr>
</table>

The practicum will be evaluated by an external and an internal examiner. The examination will be of three-hour duration.		
Unit	**Topics**	**Contact Hours**
I	**Introduction to Cloud Infrastructure**: Overview of cloud infrastructure components: compute, storage, networking, Principles of scalable and distributed computing, Data centers: architecture, power, cooling, and racks, Resource pooling and abstraction, Multi-tenancy and elasticity, Introduction to Infrastructure as a Service (IaaS), Cloud delivery and deployment models.	11
II	**Virtualization Concepts**: Definition and need for virtualization, Types of virtualization: hardware, OS, storage, network, Hypervisors: Type 1 (bare-metal) and Type 2 (hosted), Comparison of leading hypervisors: VMware ESXi, Microsoft Hyper-V, KVM, VirtualBox, VM lifecycle management, Benefits and limitations of virtualization in cloud environments.	11
III	**Virtual Machines, Storage, and Networking**: Creating and managing virtual machines (VMs), VM snapshots, cloning, and templates, Virtual storage types – block, object, and file storage, Storage virtualization, Virtual network components: virtual switches, routers, firewalls, VLANs, SDN (Software Defined Networking) basics, Network Function Virtualization (NFV) overview.	12
IV	**Infrastructure Management and Automation**: Infrastructure monitoring tools (e.g., Nagios, Zabbix), Resource allocation and optimization, High availability and failover strategies, Backup and disaster recovery in virtualized environments, Containerization vs. virtualization (Docker vs. VMs), Infrastructure provisioning tools – Vagrant, Terraform (intro), Cloud-native infrastructure – introduction to Kubernetes.	11
V*	The following activities be carried out/ discussed in the lab during the initial period of the semester. Programming Lab: • Installing and configuring VirtualBox or VMware Workstation • Creating and managing virtual machines (Linux and Windows) • Setting up virtual networks and shared folders between VMs • Creating VM snapshots and performing rollbacks • Installing and configuring KVM on a Linux system • Simulating SDN using Mininet or Open vSwitch • Managing cloud resources using AWS Free Tier (EC2, EBS, VPC) • Using basic Docker commands to create and run containers	30

	• Using monitoring tools (Nagios/Zabbix) to track VM health • Mini project: Design a virtual cloud lab with compute, storage, and network	
Suggested Evaluation Methods		
Internal Assessment: ➢ **Theory** • Class Participation: 5 • Seminar/presentation/assignment/quiz/class test etc.:5 • Mid-Term Exam: 10 ➢ **Practicum** • Class Participation: NA • Seminar/Demonstration/Viva-voce/Lab records etc.:10 • Mid-Term Exam: NA		**End Term Examination:** **A three-hour exam for both theory and practicum.**
Part C-Learning Resources		
Recommended Books/e-resources/LMS: • Barrie Sosinsky – *Cloud Computing Bible*, Wiley • Danielle Ruest and Nelson Ruest – *Virtualization: A Beginner's Guide*, McGraw-Hill • Thomas Erl, Ricardo Puttini, and Zaigham Mahmood – *Cloud Computing: Concepts, Technology & Architecture*, Prentice Hall • David Marshall, Wade A. Reynolds, and Dave McCrory – *Advanced Server Virtualization*, Auerbach Publications • James E. Smith and Ravi Nair – *Virtual Machines: Versatile Platforms for Systems and Processes*, Elsevier.		

*Applicable for courses having practical component.

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
KURUKSHETRA UNIVERSITY, KURUKSHETRA

Scheme: 2023-24, Syllabus: 2025-26			
Part A - Introduction			
Subject	BCA (CTIS)		
Semester	V		
Name of the Course	Network Security & Cryptography		
Course Code	B23-CTS-503		
Course Type: (CC/MCC/MDC/CC-M/DSEC/VOC/DSE/PC/AEC/ VAC)	CC-C5		
Level of the course (As per Annexure-I	300-399		
Pre-requisite for the course (if any)	Basic of Computer Networks		
Course Learning Outcomes(CLO):	After completing this course, the learner will be able to: 1. Explain the concepts of network security, threats, and attack surfaces. 2. Understand and apply various cryptographic techniques for secure communication. 3. Evaluate and configure secure network protocols and services. 4. Analyze security solutions such as firewalls, VPNs, and IDS/IPS. 5. *Demonstrate use of encryption, hashing, and security tools in practical settings.		
Credits	Theory	Practical	Total
	3	1	4
Contact Hours	3	2	5
Max. Marks:100(70(T)+30(P)) **Internal Assessment Marks:30(20(T)+10(P))** **End Term Exam Marks: 70(50(T)+20(P))**		**Time: 3 Hrs.(T), 3Hrs.(P)**	

Part B- Contents of the Course

Instructions for Paper- Setter

The examiner will set a total of nine questions. Out of which first question will be compulsory. Remaining eight questions will be set from four unit selecting two questions from each unit. Examination will be of three-hour duration. All questions will carry equal marks. First question will comprise of short answer type questions covering entire syllabus.

Candidate will have to attempt five questions in all, selecting one question from each unit. First question will be compulsory.

Practicum will be evaluated by an external and an internal examiner. Examination will be of three-hour duration.

Unit	**Topics**	**Contact Hours**
I	**Introduction to Network Security**: Overview of network security, Security services – confidentiality, integrity, authentication, availability, Security attacks – active vs. passive, spoofing, sniffing, replay, DoS, Network security model and	11

	architecture, Security goals and principles, Introduction to threat modeling, OSI and TCP/IP security issues.	
II	**Cryptography Fundamentals**: Concepts of cryptography – plaintext, ciphertext, keys, Encryption techniques – symmetric and asymmetric, Classical ciphers – Caesar, Vigenère, transposition, Modern symmetric encryption – DES, AES, Block and stream ciphers, Asymmetric cryptography – RSA algorithm, Key exchange protocols – Diffie-Hellman, Applications of cryptography in networks.	12
III	**Network Security Protocols and Applications**: Authentication protocols – Kerberos, PAP, CHAP, Digital signatures and certificates, Public Key Infrastructure (PKI), IP Security (IPSec) – architecture, modes, and AH/ESP, Transport Layer Security – SSL/TLS, Secure Email – PGP and S/MIME, Virtual Private Networks (VPN), Network authentication using certificates.	11
IV	**Network Security Technologies and Tools**: Firewalls – types, architecture, packet filtering, proxy firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), Honeypots and network traps, Web security – HTTPS, secure cookies, browser-based attacks and protection, Wireless security – WEP, WPA, WPA2, Incident response and digital forensics basics.	11
V*	**Practicum**: Students are advised to do laboratory/practical practice not limited to but including the following types of problems: • Simulating sniffing attacks using Wireshark and detecting patterns • Implementing Caesar cipher, transposition cipher, and RSA in Python • Generating digital signatures and verifying certificates using OpenSSL • Setting up and analyzing VPN communication using OpenVPN • Configuring and testing iptables firewall rules in Linux • Setting up a basic IDS (e.g., Snort) and monitoring traffic • Capturing and analyzing SSL/TLS handshake using Wireshark • Encrypting and decrypting files using symmetric key tools • Secure email demonstration using PGP/GPG • Mini project: Simulate a secure communication system using cryptographic primitives	30

Suggested Evaluation Methods

Internal Assessment: ➢ **Theory** • Class Participation: 5 • Seminar/presentation/assignment/quiz/class test etc.: 5 • Mid-Term Exam: 10 ➢ **Practicum** • Class Participation: NA • Seminar/Demonstration/Viva-voce/Lab records etc.: 10 • Mid-Term Exam: NA	**End-Term Examination:** A three-hour exam for both theory and practicum. **End Term Exam Marks: 70(50(T)+20(P))**

Part C-Learning Resources

Recommended Books/e-resources/LMS:

- William Stallings – *Cryptography and Network Security: Principles and Practice*, Pearson
- Behrouz A. Forouzan and Debdeep Mukhopadhyay – *Cryptography and Network Security*, McGraw-Hill
- Charlie Kaufman, Radia Perlman, and Mike Speciner – *Network Security: Private Communication in a Public World*, Pearson
- Atul Kahate – *Cryptography and Network Security*, McGraw-Hill
- Mark Ciampa – *Security+ Guide to Network Security Fundamentals*, Cengage Learning.

* Applicable for courses having practical components.

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
KURUKSHETRA UNIVERSITY, KURUKSHETRA

<table>
<tr><th colspan="4">Scheme: 2023-24, Syllabus: 2025-26</th></tr>
<tr><th colspan="4">Part A - Introduction</th></tr>
<tr><td>Subject</td><td colspan="3">BCA (CTIS)</td></tr>
<tr><td>Semester</td><td colspan="3">VI</td></tr>
<tr><td>Name of the Course</td><td colspan="3">Ethical Hacking and Penetration Testing</td></tr>
<tr><td>Course Code</td><td colspan="3">B23-CTS-601</td></tr>
<tr><td>Course Type: (CC/MCC/MDC/CC-M/DSEC/VOC/DSE/PC/AEC/ VAC)</td><td colspan="3">CC-A6</td></tr>
<tr><td>Level of the course (As per Annexure-I</td><td colspan="3">300-399</td></tr>
<tr><td>Pre-requisite for the course (if any)</td><td colspan="3">None</td></tr>
<tr><td>Course Learning Outcomes(CLO):</td><td colspan="3">After completing this course, the learner will be able to:
1. Understand ethical hacking practices, methodologies, and professional ethics.
2. Identify vulnerabilities in systems, applications, and networks.
3. Perform footprinting, scanning, and enumeration of systems.
4. Use penetration testing tools and techniques to assess system security.
5. *Recommend practical solutions and generate professional vulnerability assessment reports.</td></tr>
<tr><td rowspan="2">Credits</td><td>Theory</td><td>Practical</td><td>Total</td></tr>
<tr><td>3</td><td>1</td><td>4</td></tr>
<tr><td>Contact Hours</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td colspan="2">Max. Marks:100(70(T)+30(P))
Internal Assessment Marks:30(20(T)+10(P))
End Term Exam Marks: 70(50(T)+20(P))</td><td colspan="2">Time: 3 Hrs.(T), 3Hrs.(P)</td></tr>
<tr><td colspan="4"><u>Instructions for Paper-Setter</u>
The examiner will set a total of nine questions. Out of which first question will be compulsory. Remaining eight questions will be set from four unit selecting two questions from each unit. The examination will be of three-hour duration. All questions will carry equal marks. The first question will comprise short answer-type questions covering the entire syllabus.
The candidate must attempt five questions in all, selecting one question from each unit. The first question will be compulsory.
The practicum will be evaluated by an external and an internal examiner. The examination will be of three-hour duration.</td></tr>
</table>

Part B- Contents of the Course		
Unit	**Topics**	**Contact Hours**
I	**Introduction to Ethical Hacking and Cyber Laws**: Introduction to ethical hacking – roles and responsibilities, Types of hackers – white hat, black hat, gray hat, Hacking phases – reconnaissance, scanning, gaining access, maintaining access, clearing tracks, Overview of penetration testing, Legal aspects – IT Act 2000, GDPR, cybercrime and digital forensics overview, Code of ethics and professional responsibilities.	11
II	**Footprinting, Scanning, and Enumeration**: Footprinting techniques – WHOIS, DNS interrogation, Google hacking, Network scanning – TCP/UDP scanning, ping sweep, port scanning, Enumeration techniques – SNMP, NetBIOS, LDAP enumeration, Banner grabbing, OS fingerprinting, Vulnerability scanning using tools like Nmap, Nessus.	11
III	**System Hacking and Exploitation Techniques**: Password cracking techniques – dictionary, brute force, rainbow tables, Privilege escalation methods, Keyloggers, spyware, Trojans, and rootkits, Malware types and behaviors, Exploiting common vulnerabilities – buffer overflow, SQL injection, Cross-site scripting (XSS), Cross-site request forgery (CSRF), Post-exploitation techniques and covering tracks.	12
IV	**Web, Wireless, and Network Penetration Testing**: Web application security testing – OWASP Top 10, Wireless hacking – WEP/WPA attacks, rogue access points, ARP poisoning, Man-in-the-Middle (MITM) attacks, Social engineering techniques – phishing, baiting, physical attacks, Penetration testing phases – planning, discovery, attack, reporting, Writing professional security assessment reports and recommendations.	11
V*	The following activities be carried out/ discussed in the lab during the semester. • Performing footprinting using tools like WHOIS, Nslookup, and Maltego • Network scanning using Nmap and identifying open ports and services • Vulnerability scanning using Nessus or OpenVAS • Performing enumeration using NetBIOS and SNMP tools • Password cracking using John the Ripper, Hydra, or Hashcat • Creating and analyzing malware (in a controlled environment) • Exploiting web application vulnerabilities using DVWA • Simulating Wi-Fi attacks using Aircrack-ng and Wireshark • Conducting phishing simulations using SET or Gophish • Mini project: Conduct and document a penetration test on a virtual lab	30
Suggested Evaluation Methods		
Internal Assessment: ➢ **Theory** • Class Participation: 5 • Seminar/presentation/assignment/quiz/class test etc.: 5 • Mid-Term Exam: 10		**End Term Examination: A three-hour exam for both**

➢ **Practicum** • Class Participation: NA • Seminar/Demonstration/Viva-voce/Lab records etc.: 10 • Mid-Term Exam: NA	**theory and practicum. End Term Exam Marks: 70(50(T)+20(P))**

Part C-Learning Resources

Recommended Books/e-resources/LMS:

- Patrick Engebretson – *The Basics of Hacking and Penetration Testing*, Syngress
- Georgia Weidman – *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press
- William Stallings – *Network Security Essentials: Applications and Standards*, Pearson
- Michael T. Simpson, Kent Backman, and James Corley – *Hands-On Ethical Hacking and Network Defense*, Cengage
- EC-Council – *Ethical Hacking and Countermeasures: Attack Phases*, Cengage Learning.

*Applicable for courses having practical components.

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
KURUKSHETRA UNIVERSITY, KURUKSHETRA

<table>
<tr><th colspan="4">Scheme: 2023-24, Syllabus: 2025-26</th></tr>
<tr><th colspan="4">Part A - Introduction</th></tr>
<tr><td>Subject</td><td colspan="3">BCA (CTIS)</td></tr>
<tr><td>Semester</td><td colspan="3">VI</td></tr>
<tr><td>Name of the Course</td><td colspan="3">Cyber Forensics and Incident Response</td></tr>
<tr><td>Course Code</td><td colspan="3">B23-CTS-602</td></tr>
<tr><td>Course Type: (CC/MCC/MDC/CC-M/DSEC/VOC/DSE/PC/AEC/ VAC)</td><td colspan="3">CC-B6</td></tr>
<tr><td>Level of the course (As per Annexure-I</td><td colspan="3">300-399</td></tr>
<tr><td>Pre-requisite for the course (if any)</td><td colspan="3">None</td></tr>
<tr><td>Course Learning Outcomes(CLO):</td><td colspan="3">After completing this course, the learner will be able to:
1. Understand digital forensics concepts and apply forensic investigation techniques.
2. Perform data acquisition, preservation, and analysis while maintaining integrity.
3. Handle and respond to various types of cybersecurity incidents.
4. Use forensic tools to examine files, systems, and networks for evidence.
5. *Prepare legally acceptable practical based forensic reports and maintain chain of custody.</td></tr>
<tr><td rowspan="2">Credits</td><td>Theory</td><td>Practical</td><td>Total</td></tr>
<tr><td>3</td><td>1</td><td>4</td></tr>
<tr><td>Contact Hours</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td colspan="2">Max. Marks:100(70(T)+30(P))
Internal Assessment Marks:30(20(T)+10(P))
End Term Exam Marks: 70(50(T)+20(P))</td><td colspan="2">Time: 3 Hrs.(T), 3Hrs.(P)</td></tr>
<tr><th colspan="4">Part B- Contents of the Course</th></tr>
<tr><td colspan="4"><u>Instructions for Paper- Setter</u>
Examiner will set a total of nine questions. Out of which first question will be compulsory. Remaining eight questions will be set from four unit selecting two questions from each unit. Examination will be of three-hour duration. All questions will carry equal marks. First question will comprise of short answer type questions covering entire syllabus.</td></tr>
</table>

Candidate will have to attempt five questions in all, selecting one question from each unit. First question will be compulsory.

Practicum will be evaluated by an external and an internal examiner. The examination will be of three-hour duration.

Unit	Topics	Contact Hours
I	**Introduction to Cyber Forensics**: Definition, objectives and scope of cyber/digital forensics, Types of cybercrimes and attack vectors, Forensic process and principles: identification, preservation, analysis, documentation and presentation, Legal issues and cyber laws (IT Act 2000), Rules of evidence and admissibility in court, Chain of custody and documentation, Role of forensics in incident response.	11
II	**Data Acquisition and Analysis**: Types of data: volatile vs. non-volatile, live vs. static acquisition, Disk imaging and cloning techniques, Hashing and verification of data integrity, File systems: FAT, NTFS, Ext3/4 – forensic perspectives, Recovery of deleted files and partitions, Analyzing system logs and user activity, Keyword searching and pattern matching.	11
III	**Network and Email Forensics**: Basics of network forensics – sniffing, packet capturing, and session reconstruction, Tools: Wireshark, TCPDump, Log analysis and firewall audit trails, Intrusion detection and correlation of events, Email forensics: header analysis, attachments, spoofing detection, Identifying phishing and scam mails, Cloud forensics – issues in data ownership and jurisdiction.	12
IV	**Incident Response and Reporting**: Incident response lifecycle: preparation, detection, analysis, containment, eradication, recovery, and post-incident activities, Building an incident response team and policies, Threat intelligence and its role in IR, Forensic investigation using open-source tools (Autopsy, FTK Imager), Writing forensic reports and presentation of evidence, Case studies and scenarios.	11
V*	Practicum: Students are advised to do laboratory/practical practice not limited to but including the following types of problems: • Creating forensic disk images using FTK Imager or Guymager • Performing hash verification using MD5/SHA256 tools • Recovering deleted files and folders using forensic tools • Analyzing system event logs and user activity • Capturing and examining network packets using Wireshark • Tracing email origins and identifying spoofed headers • Simulating an incident and writing an incident report • Using Autopsy for file system analysis and keyword search • Performing browser history and registry analysis • Mini project: Perform an end-to-end investigation of a simulated	30

	cyberattack	
Suggested Evaluation Methods		
Internal Assessment: ➢ **Theory** • Class Participation: 5 • Seminar/presentation/assignment/quiz/class test etc.: 5 • Mid-Term Exam: 10 ➢ **Practicum** • Class Participation: NA • Seminar/Demonstration/Viva-voce/Lab records etc.: 10 • Mid-Term Exam: NA		**End Term Examination:** A three-hour exam for both theory and practicum.
Part C-Learning Resources		
Recommended Books/e-resources/LMS: • Nelson, Phillips, and Steuart – *Guide to Computer Forensics and Investigations*, Cengage • Marjie T. Britz – *Computer Forensics and Cyber Crime: An Introduction*, Pearson • Bill Nelson, Amelia Phillips, and Christopher Steuart – *Digital Forensics: Computer Crime Scene Investigation*, Cengage • Eoghan Casey – *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press • NIST – *Computer Security Incident Handling Guide (SP 800-61)*.		

*Applicable for courses having practical components.

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
KURUKSHETRA UNIVERSITY, KURUKSHETRA

<table>
<tr><th colspan="4">Scheme: 2023-24, Syllabus: 2025-26</th></tr>
<tr><th colspan="4">Part A - Introduction</th></tr>
<tr><td>Subject</td><td colspan="3">BCA (CTIS)</td></tr>
<tr><td>Semester</td><td colspan="3">VI</td></tr>
<tr><td>Name of the Course</td><td colspan="3">Cloud Deployment and Automation</td></tr>
<tr><td>Course Code</td><td colspan="3">B23-CTS-603</td></tr>
<tr><td>Course Type: (CC/MCC/MDC/CC-M/DSEC/VOC/DSE/PC/AEC/ VAC)</td><td colspan="3">CC-C5</td></tr>
<tr><td>Level of the course (As per Annexure-I</td><td colspan="3">300-399</td></tr>
<tr><td>Pre-requisite for the course (if any)</td><td colspan="3">Knowledge of basics of cloud computing.</td></tr>
<tr><td>Course Learning Outcomes(CLO):</td><td colspan="3">After completing this course, the learner will be able to:
1. Deploy and manage infrastructure and applications on AWS and Azure platforms.
2. Use cloud-native services for compute, storage, and networking.
3. Automate infrastructure provisioning using templates and scripting tools.
4. Design and implement basic CI/CD pipelines for cloud deployments.
5. * Practically Monitor, scale, and secure deployed cloud resources.</td></tr>
<tr><td rowspan="2">Credits</td><td>Theory</td><td>Practical</td><td>Total</td></tr>
<tr><td>3</td><td>1</td><td>4</td></tr>
<tr><td>Contact Hours</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td colspan="2">Max. Marks:100(70(T)+30(P))
Internal Assessment Marks:30(20(T)+10(P))
End Term Exam Marks: 70(50(T)+20(P))</td><td colspan="2">Time: 3 Hrs.(T), 3Hrs.(P)</td></tr>
<tr><th colspan="4">Part B- Contents of the Course</th></tr>
<tr><td colspan="4"><u>Instructions for Paper-Setter</u>
The examiner will set a total of nine questions. Out of which first question will be compulsory. Remaining eight questions will be set from four unit selecting two questions from each unit. The examination will be of three-hour duration. All questions will carry equal marks. The first question will comprise short answer-type questions covering the entire syllabus.
Candidate will have to attempt five questions in all, selecting one question from each unit. First question will be compulsory.
The practicum will be evaluated by an external and an internal examiner. The examination will be of</td></tr>
</table>

three-hour duration.		
Unit	**Topics**	**Contact Hours**
I	**Cloud Deployment Models and Infrastructure Services**: Overview of cloud deployment models – public, private, hybrid, and multi-cloud, AWS and Azure overview – services comparison, Regions, availability zones, and resource groups, Launching and managing virtual machines (EC2 in AWS, Azure VMs), Storage options – S3, Azure Blob, file and block storage, Networking services – VPC, subnets, NSG, Load Balancers.	11
II	**Deployment Tools and Automation Concepts**: Introduction to Infrastructure as Code (IaC), Scripting vs. declarative provisioning, AWS CloudFormation – stacks, templates, parameters, Azure Resource Manager (ARM) templates – structure, deployment methods, Introduction to AWS CLI and Azure CLI, Common automation use cases in cloud deployments.	11
III	**Configuration Management and DevOps Integration**: Configuration management tools – overview of Ansible, Chef, and Puppet, Automating with AWS Systems Manager and Azure Automation, Using AWS Lambda and Azure Functions for serverless automation, Introduction to CI/CD concepts, Setting up CI/CD pipelines using AWS CodePipeline, CodeBuild, Azure DevOps Services, Deployment strategies – rolling, blue-green, canary.	12
IV	**Monitoring, Scaling, and Security Automation**: Cloud monitoring tools – AWS CloudWatch, Azure Monitor, Auto-scaling configurations for VMs and containers, Security best practices in automation, IAM roles, policies and RBAC in AWS/Azure, Audit logs and alerts, Backup automation, Disaster recovery planning and testing, Case studies of deployment automation in enterprises.	11
V*	Practicum: Students are advised to do laboratory/practical practice not limited to but including the following types of problems: • Launching and configuring EC2 instances and Azure VMs • Creating and managing S3 buckets and Azure Blob containers • Deploying cloud infrastructure using AWS CloudFormation templates • Creating Azure resources using ARM templates • Automating infrastructure deployment using AWS CLI / Azure CLI • Writing simple Lambda and Azure Functions to automate tasks • Setting up a basic CI/CD pipeline in AWS CodePipeline / Azure DevOps • Configuring auto-scaling groups and load balancers in AWS • Monitoring VM performance using AWS CloudWatch and Azure Monitor • Mini project: Fully automated deployment of a web app with monitoring and scaling	30
Suggested Evaluation Methods		
Internal Assessment:		**End-Term**

➢ **Theory** • Class Participation: 5 • Seminar/presentation/assignment/quiz/class test etc.: 5 • Mid-Term Exam: 10 ➢ **Practicum** • Class Participation: NA • Seminar/Demonstration/Viva-voce/Lab records etc.: 10 • Mid-Term Exam: NA	**Examination:** A three-hour exam for both theory and practicum. **End Term Exam Marks: 70(50(T)+20(P))**

Part C-Learning Resources

Recommended Books/e-resources/LMS:

- Mark Wilkins – *Learning AWS: Design, Build, and Deploy Responsive Applications using AWS Cloud Components*, O'Reilly
- Yohan Wadia – *AWS Certified DevOps Engineer - Professional Certification and Beyond*, Packt
- Steve Smith and Mike Pfeiffer – *Azure for Architects*, Packt
- Scott Duffy – *Microsoft Azure Administrator Exam Ref AZ-104*, Microsoft Press
- Jeffrey Barr and Jeff Barr – *Host Your Web Site in the Cloud: Amazon Web Services Made Easy*, SitePoint.

*Applicable for courses having practical components.

DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS
KURUKSHETRA UNIVERSITY, KURUKSHETRA

<table>
<tr><th colspan="4">Scheme: 2024-25, Syllabus: 2025-26</th></tr>
<tr><th colspan="4">Part A - Introduction</th></tr>
<tr><td>Subject</td><td colspan="3">BCA (CTIS)</td></tr>
<tr><td>Semester</td><td colspan="3">VI</td></tr>
<tr><td>Name of the Course</td><td colspan="3">Basics of Blockchain</td></tr>
<tr><td>Course Code</td><td colspan="3">B23-CTS-604</td></tr>
<tr><td>Course Type: (CC/MCC/MDC/CC-M/DSEC/VOC/DSE/PC/AEC/ VAC)</td><td colspan="3">CC-M6</td></tr>
<tr><td>Level of the course (As per Annexure-I</td><td colspan="3">300-399</td></tr>
<tr><td>Pre-requisite for the course (if any)</td><td colspan="3">Must have basic knowledge of security</td></tr>
<tr><td>Course Learning Outcomes(CLO):</td><td colspan="3">After completing this course, the learner will be able to:
1. Explain the fundamental principles of blockchain and its architecture.
2. Understand and apply basic cryptographic principles in the context of blockchain.
3. Analyze various consensus mechanisms and their use in decentralized networks.
4. Describe the workings of Bitcoin, Ethereum, and smart contracts.
5. Develop and deploy basic smart contracts practically using blockchain platforms.</td></tr>
<tr><td rowspan="2">Credits</td><td>Theory</td><td>Practical</td><td>Total</td></tr>
<tr><td>3</td><td>1</td><td>4</td></tr>
<tr><td>Contact Hours</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td colspan="2">Max. Marks:100(70(T)+30(P))
Internal Assessment Marks:30(20(T)+10(P))
End Term Exam Marks: 70(50(T)+20(P))</td><td colspan="2">Time: 3 Hrs.(T), 3Hrs.(P)</td></tr>
<tr><th colspan="4">Part B- Contents of the Course</th></tr>
<tr><td colspan="4"><u>Instructions for Paper- Setter</u>
Examiner will set a total of nine questions. Out of which first question will be compulsory. Remaining eight questions will be set from four unit selecting two questions from each unit. The examination will be of three-hour duration. All questions will carry equal marks. The first question will comprise short answer-type questions covering the entire syllabus.</td></tr>
</table>

The candidate will have to attempt five questions in all, selecting one question from each unit. The first question will be compulsory.

The practicum will be evaluated by an external and an internal examiner. The examination will be of three-hour duration.

Unit	Topics	Contact Hours
I	**Introduction to Blockchain Technology**: Overview of blockchain – definition, features, and benefits, History and evolution of blockchain, Distributed ledger technology, Centralized vs. decentralized systems, Blockchain components: block, hash, timestamp, nonce, public and private keys, Types of blockchains – public, private, consortium, Applications of blockchain in finance, healthcare, supply chain.	11
II	**Cryptography and Consensus Mechanisms**: Cryptography basics: hash functions (SHA-256), digital signatures, Merkle trees, Blockchain identity – public/private keys, wallets, Transactions and blocks – structure and validation, Consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Mining and incentives, Blockchain security threats.	11
III	**Blockchain Platforms and Architecture**: Bitcoin overview – transactions, scripting, and UTXO model, Ethereum overview – Ether, Gas, Ethereum Virtual Machine (EVM), Accounts – EOA vs. contract account, Smart contracts – definition, use cases, creation, Blockchain layers – network, data, consensus, application, Introduction to Hyperledger Fabric and private blockchains.	12
IV	**Smart Contracts and Blockchain Use Cases**: Smart contract development using Solidity (basics), Writing and deploying smart contracts in Remix IDE, Decentralized applications (DApps) introduction, Blockchain in cloud security, identity management, healthcare, education, and logistics, Blockchain limitations and future trends – scalability, interoperability, energy consumption, Case studies of successful blockchain deployments.	11
V*	Practicum: Students are advised to do laboratory/practical practice not limited to but including the following types of problems: • Setting up MetaMask wallet and connecting to test networks • Exploring blockchain transactions on Bitcoin/Ethereum explorers • Generating hash values using SHA-256 algorithm • Creating and simulating blockchain using basic Python scripts • Writing and deploying a simple smart contract using Solidity • Interacting with smart contracts using Remix IDE • Creating and verifying Merkle trees • Sending and verifying transactions on a testnet	30

	(Ropsten/Goerli) • Simulating PoW with nonce and hash calculation • Mini project: Design and demo of a basic decentralized voting or record system using smart contracts	

Suggested Evaluation Methods

Internal Assessment: ➢ **Theory** • Class Participation: 5 • Seminar/presentation/assignment/quiz/class test etc.: 5 • Mid-Term Exam: 10 ➢ **Practicum** • Class Participation: NA • Seminar/Demonstration/Viva-voce/Lab records etc.: 10 • Mid-Term Exam: NA	**End Term Examination:** A three hour exam for both theory and practicum.

Part C-Learning Resources

Recommended Books/e-resources/LMS:

- Narayanan et al. – *Bitcoin and Cryptocurrency Technologies*, Princeton University Press
- Andreas M. Antonopoulos – *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media
- Imran Bashir – *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*, Packt
- Melanie Swan – *Blockchain: Blueprint for a New Economy*, O'Reilly Media
- Arvind Narayanan, Joseph Bonneau, Edward Felten – *Bitcoin and Cryptocurrency Technologies*, Princeton
- Roger Wattenhofer – *The Science of the Blockchain*, Createspace.

*Applicable for courses having practical component.