ASSIGNMENT-1

NAME-KHUSHBOO CHAUDHARY

ROLL-NO.-U24CS038

AIM:

To analyze different information systems with respect to **Confidentiality, Integrity, and Availability (CIA)**, identify security concerns, and suggest suitable security practices.

1. Online Student Academic Portal

(1) System & Purpose

An online portal used by students to:

- Log in
- View attendance and marks
- Register for courses
- Download study materials

(2) Type of Information Handled

- Personal details (name, roll number, email)
- Academic records (marks, attendance)
- Login credentials
- Course registration data
- Learning resources

(3) Security Concerns (CIA)

Confidentiality:

- Unauthorized access to marks, attendance, or personal data
- Data leakage of login credentials

Integrity:

- Tampering with marks or attendance
- Unauthorized modification of course registrations

Availability:

- Portal downtime during exams/registration
- Server crashes or denial-of-service attacks

(4) Suggested Security Practices

For Confidentiality:

- Strong authentication (password + OTP / 2FA)
- HTTPS encryption
- Role-based access (student, faculty, admin)

For Integrity:

- Audit logs for changes
- Database access control
- Input validation
- Regular backups

For Availability:

- Server redundancy
- Cloud hosting & load balancing
- DDoS protection
- Scheduled maintenance

2. Digital Payment Application

(1) System & Purpose

A mobile app for:

- Money transfer
- Bill payments
- Online shopping

(2) Type of Information Handled

- Bank details
- Card information
- Transaction history
- User identity data

- Login credentials

(3) Security Concerns (CIA)

Confidentiality:

- Theft of financial and personal data
- Man-in-the-middle attacks

Integrity:

- Alteration of transaction amounts
- Fake or duplicate transactions

Availability:

- App/service downtime
- Transaction failure
- Network attacks

(4) Suggested Security Practices

For Confidentiality:

- End-to-end encryption
- Tokenization of card data
- Secure storage (no plain-text passwords)

For Integrity:

- Digital signatures
- Transaction verification
- Real-time fraud detection
- Hashing transaction records

For Availability:

- High-availability servers
- Disaster recovery systems
- Load balancing
- Offline transaction handling

3. Email Communication System

(1) System & Purpose

Used by faculty and students to exchange:

- Notes
- Assignments
- Notices
- Academic documents

(2) Type of Information Handled

- Personal communication
- Attachments (PDFs, docs)
- Academic records
- Login credentials

(3) Security Concerns (CIA)

Confidentiality:

- Email interception
- Unauthorized mailbox access

Integrity:

- Modification of message content
- Virus-infected attachments

Availability:

- Email server downtime
- Account lockouts
- Spam flooding

(4) Suggested Security Practices

For Confidentiality:

- TLS email encryption
- Secure passwords & 2FA
- End-to-end encryption (PGP, S/MIME)

For Integrity:

- Digital signatures
- Anti-virus and malware scanning
- Message authentication

For Availability:

- Reliable mail servers
- Spam filters
- Backup mail servers

4. Biometric Attendance System

(1) System & Purpose

Used to:

- Capture fingerprints/face scans
- Record attendance
- Store data on a central server

(2) Type of Information Handled

- Biometric data
- Student identity data
- Attendance logs
- Time and device records

(3) Security Concerns (CIA)

Confidentiality:

- Theft of biometric data
- Privacy violations

Integrity:

- Fake attendance entries
- Manipulation of attendance logs

Availability:

- Device failure
- Server crash

- Network issues

(4) Suggested Security Practices

For Confidentiality:

- Encrypt biometric templates
- Secure storage
- Restricted system access

For Integrity:

- Tamper-proof logs
- Device authentication
- Secure data transmission

For Availability:

- Regular device maintenance
- Backup servers
- Offline mode support
- Redundant systems