National Institute of Technology Karnataka, Surathkal

Department of Computer Science and Engineering

# Course Plan

## (Part-A)

| | | |
|---|---|---|
| **Name of the course:** Database Security | **Course Code:** CS850 | **No. of Credits (L-T-P):** 4 (3-0-2) |
| **Year:** M-Tech I year (CSE-IS) **Semester:** II | **Course Type:** PC | **Academic Session:** Even 2025-2026 |

**A. Prerequisites (if any):** NIL

**B. Name and Contact Details of the Course Instructor**

**Prof. P. SANTHI THILAGAM**
**Room # 410,**
**Dept of Computer Science and Engineering, NITK-Surathkal.**
**Phone: 0824-2473404 (O),**
**Email : santhi@nitk.edu.in**

**C. Assessment Pattern (Use Bloom's taxonomy to design rubrics for evaluating students performance)**

| Level No. | Knowledge Level | Evaluation Component | | | | Assessment (%) |
|---|---|---|---|---|---|---|
| | | Mid-Sem (20%) | Tests / Quizzes (10%) | Project (30%) | End-Sem (40%) | |
| K1 | Remember | 20 | 30 | - | 20 | 15 |
| K2 | Understand | 20 | 20 | 10 | 25 | 19 |
| K3 | Apply | 30 | 30 | 30 | 25 | 28 |
| K4 | Analyse | 20 | 10 | 10 | 20 | 16 |
| K5 | Evaluate | 10 | 10 | 10 | 10 | 10 |
| K6 | Create | - | - | 40 | - | 12 |
| Total | | | | | | 100 |

**D. Assessment Process**

| Evaluation Components | Assessment Frequency | Assessed by | Reviewed by |
|---|---|---|---|
| Midsem Exam | Once (In the middle of the semester) | Course Instructor | DPGC |
| Quizzes | Once (Before the endsem exam) | Course Instructor and Teaching Assistants | DPGC |
| Project | Twice (Once before midsem exam and the other before the endsem exam) | Course Instructor and Teaching Assistants | DPGC |
| Endsem Exam | Once (At the end of semester) | Course Instructor | DPGC |

**E. Course Objectives**

| Sl.No. | Course Objectives |
|---|---|
| 1 | Acquire a deep understanding of security principles and apply them effectively. |
| 2 | Develop the skills to protect databases through robust security measures. |
| 3 | Learn strategies to prevent and detect attacks, as well as methods to minimize their impacts on databases. |
| 4 | Acquire a comprehensive understanding of database auditing principles and practices. |
| 5 | Acquire the skills to create secure and resilient database designs. |

**F. Course (Learning) Outcomes (COs)**

| COs | Course Outcomes |
|---|---|
| 1 | Develop the proficiency to safeguard data and databases against potential threats. |
| 2 | Acquire a comprehensive understanding of security principles and their practical application. |
| 3 | Learn techniques for preventing and detecting attacks, as well as mitigating their impacts on |

| | |
|---|---|
| | databases. |
| 4 | Gain insight into database auditing processes and principles |
| 5 | Develop the ability to formulate secure database designs for enhanced data protection. |

### G. Course Articulation Matrix

(**Note:** Enter correlation levels 1, 2, or 3 as defined below: 1 - Slight (Low), 2 - Moderate (Medium) 3 - Substantial (High), and If there is no correlation, put "-"_)

| COs | PO-1 | PO- 2 | PO- 3 | PO- 4 | PO- 5 | PO- 6 | PO- 7 | PO- 8 | PO- 9 | PO-10 | PO- 11 | PO- 12 | PSO-1 | PSO-2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 3 | 3 | 3 | 3 |
| 2 | 3 | 3 | 2 | 3 | 2 | - | - | 2 | - | 2 | 3 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | - | 3 | 2 | 3 | 3 | 3 | 3 |
| 4 | 3 | 3 | 3 | 2 | 2 | - | 2 | - | 3 | 2 | 3 | 3 | 3 | 3 |
| 5 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 |
| Avg. | 3 | 3 | 2.8 | 2.6 | 2.4 | 2 | 2 | 2.67 | 2.75 | 2 | 3 | 3 | 3 | 3 |

### H. Program Articulation Matrix

**(Note:** Enter correlation levels 1, 2, or 3 as defined below: 1 - Slight (Low), 2 - Moderate (Medium) 3 - Substantial (High), and If there is no correlation, put "-")

| PO-1 | PO-2 | PO-3 | PO-4 | PO-5 | PO-6 | PO-7 | PO-8 | PO-9 | PO- 10 | PO- 11 | PO- 12 | PSO- 1 | PSO- 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 2 | 3 | 3 | 2 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 3 |

### I. Course Syllabus

| Module | Topic to be covered | No. of hrs. |
|---|---|---|
| 1 | Course Description and Introduction | 1 |
| 2 | Design Principles | 3 |
| 3 | Access Control Models: Discretionary Access Control | 2 |
| 4 | Access Control Models: Virtual Private Database | 2 |
| 5 | Access Control Models: Mandatory Access Control, Oracle Label Security | 2 |
| 6 | Access Control Models: Role-based Access Control | 2 |
| 7 | XML Access Control | 3 |

| | | |
|---|---|---|
| 8 | Database as a Service – Query authentication | 2 |
| 9 | SQL Injection, Insider Threats | 3 |
| 10 | Database as a Service – Encryption-based | 2 |
| 11 | Data Privacy, Privacy in Location Based Service | 2 |
| 12 | Steganographic File Systems | 1 |
| 13 | Database auditing models | 3 |
| 14 | Practices of database auditing | 2 |
| 15 | Selected advanced topics such as Trust Management. | 2 |

**J. Course Project Description**

| | |
|---|---|
| Objective | The course project is designed to offer you practical exposure to applying theoretical concepts related to database security. |
| Instructions | In this course, you will work in a team to implement the course project. Groups will consist of 2 members. It is expected that each group will begin their project when topics are approved, then present system components by the scheduled progress reporting dates. |
| Stages | **I. Develop a proposal for the project**: First, groups should submit for approval their project ideas. Informal discussions with the professor can help to refine the project and proposal. Groups should not continue working on the project unless it has been approved by the course instructor. This proposal should include:<br>1. A separate cover page indicating the title of your project, the full names of the group members (with e-mail), the course number and course section.<br>2. A narrative description of the project. This should also include a description of the problem being addressed.<br>3. Identification of the information needs - what information would help solve the problem.<br>4. Distribution of duties for the project. List the names of each group member and what their primary role will be.<br>**II. Project Implementation**: Groups should then implement the approved project. Groups will periodically submit status updates.<br>**III. Project Demonstration**: The final step is to prepare a formal demonstration and brief presentation. |

| | |
|---|---|
| Deadlines for different stages | 1. Team formation- 15th January 2026<br>2. Project proposal submission- 25th January 2026<br>3. Midsem evaluation- 10-14th March 2026<br>4. Continuous evaluation- 25th March 2026<br>5. Endsem evaluation- 10th April - 17th April 2026 |
| Sample Projects (For reference) | Your project can involve implementing something related to database security ideas. Here are a few suggestions – other topics can, of course, be suggested:<br><br>1. Context Aware RBAC Model for Wearable Devices.<br>2. Access Control: Delegation in access control, Access control for Workflow, attribute- based access control, access control/privacy for big data, XACML.<br>3. Role Engineering.<br>4. Access Control Systems for Medical Sensor Networks-Secure Aggregation Algorithms.<br>5. Service-Oriented Architecture Security - Software-level (single service) security, Business-level (service composition) security, Forensics over Web Services - Develop criteria to evaluate correctness of composite application execution, Increase reliability using redundant services, Offer security as service, Develop defense models using distributed and collaborative components (E.g., detect malicious behavior based on collaborative nodes, verify execution correctness by comparing outcome of different services, deploy intelligent software etc. )<br>6. Security Tool to Detect Vulnerabilities at Application Level (XSS and cross site forgery).<br>7. Cross-Site Scripting Attack Detection, Content Sniffing Attack Detection, Cross-Site Request Forgery Attack Detection, Phishing Attack Detection.<br>8. Security as a service for cloud applications, Identification of indicators for insider attacks in the cloud environment is an open area of research.<br>9. The differentiation between a normal and malicious user within the cloud<br>10. Security in digital payments.<br>11. IOT security.<br>12. SNA security: Protecting user data from the OSN, Mitigating attacks from large- scale crawlers, Mitigating Sybil attacks, Mitigating social spam, Mitigating Distributed Denial-of-service attacks (DDoS) attacks, Spam campaigns detection, understanding the privacy leakage and associated risks when OSNs work as a Web tracker.<br>13. Outsourcing of database storage and access control/privacy.<br>14. Privacy preserving data mining, k-anonymity (l-diversity).<br>15. Integrity enhancing models/provenance.<br>16. Intrusion detection for databases.<br>17. Models of security and privacy for graph databases.<br>18. Writing a tool which can query a MySQL database for a list of dates and times and exporting the resulting list to Google Calendar which will display them in the user's account.<br>19. Virtual Private Databases. |

**K. List of Textbooks & Reference books, Online Course Resources:**

| Items | Sl. No. | Title, Author, Publisher, etc. |
|---|---|---|
| Textbooks | 1 | Sam Afyouni, Database Security and Auditing: Protecting Data Integrity and Accessibility. Thomson. ISBN: 0-619-21559-3, 2005. |
| | 2 | Marshall D. Abrams, Sushil Jajodia, and Harold J. Podell, eds. Information Security: An Integrated Collection of Essays, IEEE Computer Society Press, 1995. Available on line at http://www.acsac.org/secshelf/book001/book001.html |
| | 3 | Hassan A. Afyouni, Database Security and Auditing: Protecting Data Integrity and Accessibility, Thomson Course Technology (c2006). |
| | 4 | Charles P. Pfleeger and Shari L. Pfleeger: Security in Computing, 4th Edition, Prentice Hall, 2006. |
| Reference books | 1 | Implementing Database Security and Auditing By Ron Ben-Natan. |
| | 2 | William Stallings: Cryptography and Network Security, 4th Edition, Prentice Hall, 2006. |
| | 3 | David C. Knox: Effective Oracle Database 10g Security by Design, McGraw-Hill, 2004. |
| | 4 | We will also draw material from the literature in the relevant journals and conferences (e.g., SIGMOD, VLDB, IEEE S&P, CCS). Students will read and present the selected papers and to complete a term project. Matt Bishop. Computer Security: Art and Science. Addison Wesley Professional, 2002, ISBN: 0201440997. |
| Online Resources | 1 | https://www.udemy.com/course/implementing-database-security-for-beginners/?utm_source=adwords&utm_medium=udemyads&utm_campaign=DSA_Catchall_la.EN_cc.INDIA&utm_content=deal4584&utm_term=_._ag_82569850245_._ad_533220805574_._kw__._de_c_._dm__._pl__._ti_dsa-554065857551_._li_9152740_._pd__._&matchtype=&gad_source=1&gclid=Cj0KCQiAtOmsBhCnARIsAGPa5yb666DCyjDaRJdtrHTrAMR7PZY4Jc5A3iBhUulvujJOs8SJJkfSFrIaAtpQEALw_wcB |
| | 2 | https://www.udemy.com/course/database-security-for-cyber-professionals/ |

| | | |
|---|---|---|
| | 3 | https://iisecurity.in/courses/database-security-course |

Name and signature of course instructor with date:

Name and signature of DUGC/DPGC Secretary with date:

Name and signature of DUGC/DPGC Chairman with date:

Name and signature of HOD with date:

****** END ******