

UNIVERSITY OF DELTA, AGBOR, NIGERIA
COMPUTING
INFORMATION AND COMMUNICATION TECHNOLOGY
B.Sc. Information and Communication Technology

UNIDEL-ICT 403: Database Security (2 Units; **Compulsory**; LH=15; PH=45)

Senate-approved Relevance

The training of high-skilled graduates who are knowledgeable in the design and use of tools, processes, and methodologies which establish security of database systems in modern businesses and industries in Nigeria is in tandem with the vision and mission of University of Delta, Agbor, of producing well motivated, skilfull graduates that are capable of exhibiting expertise in proffering solutions for the workplace of tomorrow. This entails producing computing graduates with demonstrable potentials and skills to answer pressing modern security issues database administrators from businesses and industries in Delta State, Nigeria, and the world at large. The relevance of this is seeing in computing graduates of the University of Delta, Agbor being able to develop different defensive methods, techniques & solutions to mitigate cybercrime occasioned by both human and machine activities trying to have illegal access to databases which can have disastrous consequences for critical organization, state, regional, national and world data assets.

Overview

Databases are a core part of every organization and are used to store large quantities of highly sensitive and personal information. Every organization must ensure there are sufficient technical controls in place to safeguard these databases and prevent their contents getting accessed by unauthorized personnel. Database security refers to the collection of procedures, policies and tools that are used to protect a database or a database management software from malicious threat actors. The focus is not just about protecting the data stored within the database, but also about securing the physical or virtual database servers and third-party applications that can access it. A compromised database can result in data breaches or other information security incidents which can have disastrous consequences for organization. Data breaches have the ability to close organizations down, so it is imperative that controls be put in place to help mitigate the likelihood of one happening. Similarly, insider threats are a common root cause of database security breaches. Database security programs are designed to protect not only the data within the database, but also the data management system itself, and every application that accesses it, from misuse, damage, and intrusion. Database security encompasses tools, processes, and methodologies which establish security inside a database environment.

Therefore, the course introduces the principles & practices of implementing database security and the security challenges & threats in database systems in modern businesses and industries in megacities in Delta state and provides an understanding of the state-of-the art security technologies to address the current databases security issues in modern organizations and industries in Delta State and Nigeria at large. The course will educate students on how to safeguard database containing data, database management systems, physical database servers or the database server virtual, and the hardware that runs it, and the infrastructure for computing or network that is used to connect to the database. The course will also serve as benchmark for the database administrators for overhauling the database configurations to withstand against threat waves in the Delta State

and Nigeria at large. Students will also learn a variety of measures used to secure open source and commercial database platforms in both private and private organizations from modern malicious cyber-attacks vectors and illegitimate use. The course is executed through a combination of lectures, assignments, labs, and a term project. The objectives of the course, learning outcomes, and course synopsis are provided to address this need.

Objectives

The objectives of this course are to: (i) introduce the database security issues; (ii) describe the security features in databases; (iii) describe security architecture; (iv) describe the various state-of-art database security methods and techniques; (v) describe and implement multilevel secure relational model; (vi) implement auditing in relational databases; and (vii) describe XML access control and enforcement.

Learning outcomes

Upon completion of this course, students should be able to: (i) describe security architecture; (ii) describe two databases security models; (iii) describe and implement multilevel secure relational model; (iv) implement auditing in relational databases; and (v) describe XML access control and enforcement.

Course Contents

Database basics and SQL. The role of databases in information systems. Introduction to database security and auditing. Security architecture fundamentals. Operating systems security fundamentals. Administration of users' profiles. Password policies, privileges, and roles. Database application security models. Multilevel secure relational model. poly instantiation. Access control models: MAC, DAC, RBAC. Stored procedures and functions: PL/SQL I. PL/SQL II. Virtual private databases. SQL Injection. Database vault. Auditing database activities. XML Access Control. Watermarking in relational database. Regulations. compliance and privacy protection. Database as a service: challenges in outsourced database, Merkle hash tree, data confidentiality: relational encryption. NoSQL.

Lab Work: Database installation and basics, implementation of discretionary access control, implementation of mandatory access control using Oracle label security, implementation of virtual private databases and SQL Injection

Minimum Academic Standards

Computing laboratory with both adequate software tools and hardware devices
Open source databases, Oracle database
NUC minimum academic standards' requirement facilities