CT3 Set D Answer key

Database Security And Privacy (SRM Institute of Science and Technology)

SRM Institute of Science and Technology

College of Engineering and Technology

School of Computing **SETD**

DEPARTMENT OF COMPUTING TECHNOLOGIES

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year: 2022 -2023 **(ODD)**

Test **: CLAT-3** **Date** **: 07/11/2022**

Course Code & Title **: 18CSE455T & DATABASE SECURITY AND PRIVACY**

Duration **:** 2 periods

Year & Sem **:** IV Year & VII Semester **Max. Marks** **:** 50 Marks

Course Articulation Matrix:

Course Outcome	PO1	PO2	PO3	PO4	PO5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	H														
CO2	H	H													
CO3	H														
CO4	H	H													
CO5	H			H											
CO6	H														

Part - A

(10*1 = 10 Marks)Answer all Questions.

Q. No	Question	Marks	BL	CO	PO	PI Code
1	------- Utility event in SQL Server events? A) BACKUP / RESTORE/ B) BULL INSERT / BCP (Bulk Copies) / C) DBCC (Database Consistency Checker) D) All the above	1	2	5	1	2.1.2

2	The Oracle _____ Log is another method of auditing database activities. A) ALERT B) REVOKE C) COMMIT D) CHECK	1	2	5	1	2.1.3
3	The audit final report should include, at a minimum, the following: (choose the one NOT required.) A) Type of audit conducted B) Characteristics of audit C) Identification of involved parties: auditor, auditee, and third party D) Audit team members	1	1	5	1	2.2.2
4	Point out the wrong statement. A) Users with the ALTER ROLE permission can create server audit specifications and bind them to any audit B) SQL Server audit uses Extended Events to help create an audit C) You can have multiple audits per SQL Server instance D) You can create one server audit specification per audit	1	1	5	4	2.2.3
5	An audit which is compulsory by the law is _____. A. Government Audit B. Internal Audit C. Cost Audit D. Statutory Audit	1	2	5	4	2.2.3
6	kind of partitioning is used for the data sets across multiple entities which same set of attributes? A) Key B) Horizontal C) Vertical	1	1	6	4	1.3.1

	D) Hash					
7	The _____ model was designed to handle some weaknesses in the k-anonymity model *A)* t-closeness *B)* l-diversity *C)* Incognito *D)* data swapping,	1	2	6	4	2.1.3
8	The Method for compromising the privacy of genomic data A) trail re-identification B) Prediction C) Masking D) Decoding	1	1	6	1	3.4.2
9	The values across different records are swapped in order to perform the privacy-preservation is _____ . A) Data Encryption B) Data Swapping C) Data Hiding D) Data masking	1	2	6	1	2.2.2
10	Methods are used prevent disclosure of sensitive information *A)* k-anonymity, *B)* l-diversity *C)* t-closeness *D)* all the above	1	1	6	4	2.2.3
Part B (4*5=20Marks) Answer all Questions						
11	Describe the activities of Oracle alert log and explain with example in detail. The alert log file (also referred to as the ALERT.LOG) is a chronological log of messages and errors written out by an Oracle Database. Typical messages found in this file is:	5	3	5	1	1.6.1

	database startup, shutdown, log switches, space errors, etc. This file should constantly be monitored to detect unexpected messages and corruptions. Location of the ALERT.LOG file Oracle will write the alert.log file to the directory as specified by the BACKGROUND_DUMP_DEST parameter. If this parameter is not set, the alert.log will be created in a directory below the value of the DIAGNOSTIC_DEST parameter: DIAGNOSTIC_DEST/diag/rdbms/DB_NAME/ORACLE_SID/trace. If this later parameter is not set, the alert.log file is created in the ORACLE_HOME/rdbms/trace directory. SQL> show parameter BACKGROUND_DUMP_DEST NAME TYPE VALUE ---------- ---------- ---------- background_dump_dest string /app/oracle/diag/rdbms/o11gr1/o11gr1/trace Writing to the ALERT.LOG file Users can write messages to the alert.log file. Example: -- Write message to alert.log exec dbms_system.ksdwrt(2, 'Look Ma, I can write to the alert.log file!'); PL/SQL procedure successfully completed. -- Flush the buffer exec dbms_system.ksdfls; PL/SQL procedure successfully completed.					
12	Describe about audit command syntax along with diagram. Audit command syntax **AUDIT** **{** **{ { statement_option | ALL }** **[,{statement_option | ALL }] ……** **|,{syetem_privilege | ALL PRIVILEGES }**	5	3	5	4	2.2.3

}

[BY { proxy [,proxy]…..

| user [,user]…..

]

|

{Object_option [, object_option] …… | ALL }

ON { [schema.] object

|DIRECTORY directory_name

|DEFAULT

}

}

[BY {SESSION | ACCESS } }

[WHENEVER [NOT] SUCESSFUL] ;

Where :

Statement option – Tells ORACLE to audit the specified DDL or DCL statement

DDL – CREATE, ALTER, DROP and TRUNCATE

DCL – GRANT , REVOKE

System privilege – Tell ORACLE to audit the specified privilege such as SELECT, CREATE ANY, or ALTER ANY

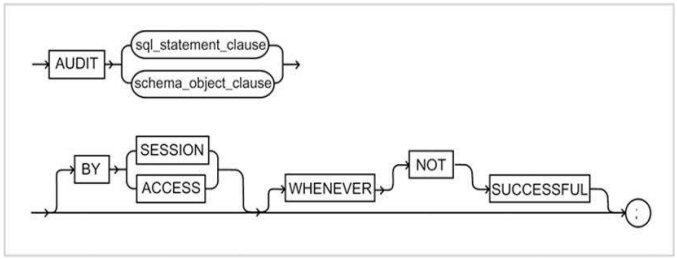
Object option – Specifies the type of privileges for the specified object to be audited

BY SESSION – Tells ORACLE to record audit data once per session even if the audited statement issued multiple times in session

BY ACCESS - Tells ORACLE to record audit data every time audited statement is issued.

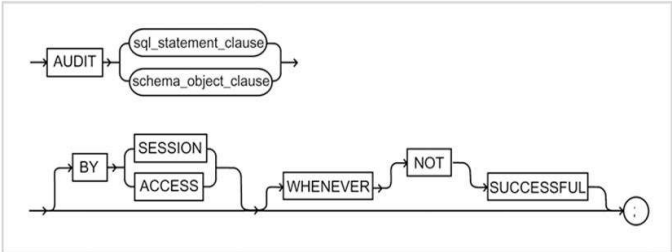
WHENEVER SUCCESSFUL – Tells ORACLE to capture audit data only when the audited command is successful

WHENEVER NOT SUCCESSFUL- Tells ORACLE to capture audit data only when the audited command fails

						
13	List out the mining Association rules under privacy constraints. ✓ association rule mining is one of the important problems in data mining ✓ There are two aspects to the privacy preserving association rule mining problem 1. When the input to the data is perturbed, it is a challenging problem to accurately determine the association rules on the perturbed data. 2. A different issue is that of output association rule privacy. o In this case, to ensure that none of the association rules in the o output result in leakage of sensitive data. o This problem is referred to as *association rule hiding* by the o database community, and that of *contingency table privacy-* o *preservation* by the statistical community.	5	2	6	4	2.2.3
14	• Elaborate Rule hiding? • Association rule hiding refers to the process of modifying the original database in such a way that certain sensitive association rules disappear without seriously affecting the data and the non-sensitive rules. • The association rule hiding technique is to remove the sensitive rules from the transactional database during association rule mining. • ARH technique protects sensitive data items by concealing the sensitive rules from miners and	5	3	6	1	2.2.2

	discloses all the non-sensitive rules to the miners. • Data perturbation is used by Privacy Preserving Data Mining (PPDM) approach takes single-level trust on data miners. • The technique establishes the ambiguity regarding individual values than the data released to the third parties for data mining purposes. In single trust level assumption, a data owner creates disturbed copy of its data with an amount of uncertainty. • This assumption is restricted in many functions where a data owner trusts the data miners at various level					
Part C (2*10=20 Marks) (Answer any two)						
15	Explain curse dimensionality. What are the ways by which the curse is cured? Especially in distributed environment ✓ Many privacy-preserving data-mining methods are inherently limited by the curse of dimensionality in the presence of public information. ✓ For example, the technique in analyzes the *k*-anonymity method in the presence of increasing dimensionality. ✓ The curse of dimensionality becomes especially important when adversaries may have considerable background information, as a result of which the boundary between pseudo-identifiers and sensitive attributes may become blurred. ✓ This is generally true, since adversaries may be familiar with the subject of interest and may have greater information about them than what is publicly available. ✓ This is also the motivation for techniques such as *l*-diversity in which background knowledge can be used to make further privacy attacks.	10	2	6	1	1.6.1
16	Describe the distributed algorithm for k-anonymity. ✓ In many applications, the data records are made available by simply removing key	10	3	6	1	1.7.1

	identifiers such as the name and social-security numbers from personal records. ✓ other kinds of attributes (known as pseudo-identifiers) can be used in order to accurately identify the records. ▪ For example, attributes such as age, zip-code and sex are available in public records such as census rolls. ▪ When these attributes are also available in a given data set, they can be used to infer the identity of the corresponding individual. A combination of these attributes can be very powerful, since they can be used to narrow down the possibilities to a small number of individuals ✓ *k*-anonymity approach can be formalized as follows: ▪ *Each release of the data must be such that every combination of values of quasi-identifiers (*are pieces of information that are not of themselves unique identifiers) *can be indistinguishably matched to at least k respondents.* ▪ The first algorithm for *k*-anonymity approach uses *domain generalization hierarchies* of the quasi-identifiers in order to build *k*-anonymous tables. The concept of *k*-minimal generalization has been proposed in order to limit the level of generalization for maintaining as much data precision as possible for a given level of anonymity.					
17	Explain how oracle database auditing activities are performed using DDL triggers. ✓ ORACLE provides the mechanism for auditing everything: ▪ From tracking who is creating and modifying the structure ▪ Who is granting privileges to whom ✓ The activities are divided into two types based on the type of SQL command statement used : ▪ Activities defined by DDL (Data Definition Language) Activities defined by DCL (Data Control Language Auditing DDL Activities ✓ ORACLE uses a SQL-based audit command The following figure presents the audit syntax diagram (ORACLE 10g	10	4	5	4	1.7.1



DDL activities Example :

- ✓ Suppose you want to audit a table named CUSTOMER every time it is altered or every time a record from a table deleted.
- ✓ The following steps show you how to do this.
- ✓ Before perform , drop are disable all triggers associated with CUSTOMER table.

Step 1 : Use any user other than SYS or SYSTEM to create the CUSTOMER

Step 2 : Add three rows into the CUSTOMER table and commit changes

Step 3 : Log on as SYS or SYSTEM to enable auditing , as specified in this example

the first statement for ALTER and the next is for DELETE

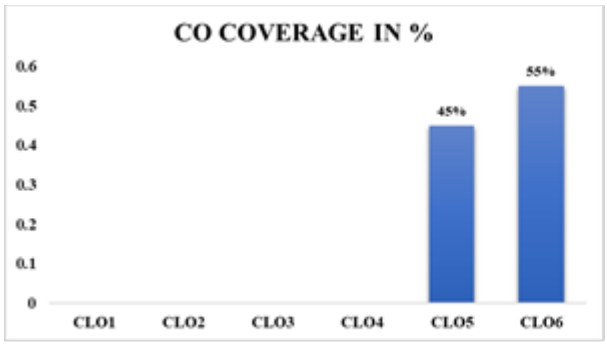
Step 4 : Login as the owner of CUSTOMER table, DBSEC delete a row and modify

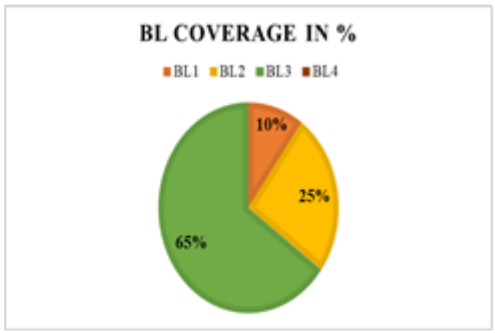
the structure of the table, as specified in the following code

In this step you will see the audit records stored in the auditing tables caused by the DELETE and ALTER statements issued in step 4.

Step 5 : Login in as SYSTEM and view the DBA_AUDIT_TRAIL

Course Outcome (CO) and Bloom's level (BL) Coverage in Questions





Question Paper Setter **Approved by the Audit Professor/Course Coordinator**