CT3 Set A Answer key

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

SRM Institute of Science and Technology

College of Engineering and Technology **SETA**

School of Computing

DEPARTMENT OF COMPUTING TECHNOLOGIES

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year: 2022 (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

Answer Key

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.

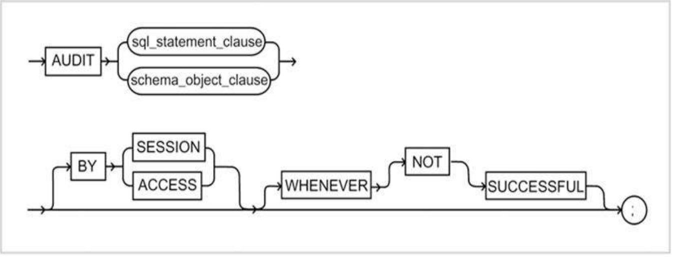
Q. No	Question	Marks	BL	CO	PO	PI Code
1	Expected to provide the resources needed and select staff members to accompany the auditors. A) auditor B) client C)Internal auditor D). auditee	1	2	5	1	2.1.2
2	The document that contains all activities that are being audited ------- ordered in a chronological manner. A) Audit log B) Audit Profile C) Audit File D)Audit Document	1	2	5	1	2.1.3
3	Selecting the __________ option can allow unaudited activity which could violate your security policies.	1	1	5	1	2.2.2

	A) Fail B) Shut Down C)Continue D) Break					
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	------------ statement is used to enable auditing from SQL Server? A) auditpol /set /subcategory:" application generated" /success: enable/failure: enable B) polaudit /set /subcategory:"application generated" /success:enable /failure:enable C) auditpolenable /set /subcategory:"application generated" /success:enable /failure:enable D) auditenable /set /subcategory:"application generated" /success:enable /failure:enable	1	2	5	4	2.2.3
6	Bioterrorism-application, the data analyzed for privacy-preserving data mining purposes is A) medical data B) Statistical data C)Spatio temporal data D) Timestamped data	1	1	6	4	1.3.1
7	The attacker knows some linear independent collection of records. A) Known Input-Output Attack B) Packet sniffer C) Distributed denial of service D) Man in the middle Attack	1	2	6	4	2.1.3
8	Kind of partitioning is used for the data sets across multiple	1	1	6	1	3.4.2

	entities which same set of attributes? A) Horizontal B) Vertical C) Hash D) Key					
9	A method based on chance alone by which study participants are assigned to a treatment group is _________________ . A) k-anonymity B) l-diversity C) t-closeness D) Randomization	1	2	6	1	2.2.2
10	The _________ model was designed to handle some weaknesses in the k-anonymity model A) k-anonymity B) l-diversity C) incognito D) Data Swapping	1	1	6	4	2.2.3
Part B (4*5=20Marks) Answer all Questions						
11	Enumerate three different types of operations involved with the database Auditing activities. QA- During development - before the product commissioned into production -Test the product to make sure it is not working properly and is not defective Auditing- After the product commissioned into production - Verify that the product or system is working and complies with the policies, standards, regulations or laws Performance Monitoring- After the product commissioned into production- Monitor Performance in terms of Response time	5	1	2	1	1.6.1
12	Elaborate SQL server event descriptions. ✓ SQL Server provides a trigger mechanism that fires automatically when a DML statement occurs ✓ The CREATE TRIGGER statement allows you to create a new trigger that is fired automatically whenever an event such as INSERT, DELETE,	5	1	2	4	2.2.3

	or UPDATE occurs against a table. CREATE TRIGGER trigger_name ON table_name AFTER {[INSERT],[UPDATE],[DELETE]} [NOT FOR REPLICATION] AS {sql_statements} ✓ The schema_name is the name of the schema to which the new trigger belongs. The schema name is optional. ✓ The trigger_name is the user-defined name for the new trigger. ✓ The table_name is the table to which the trigger applies. ✓ The event is listed in the AFTER clause. The event could be INSERT, UPDATE, or DELETE. A single trigger can fire in response to one or more actions against the table. ✓ The NOT FOR REPLICATION option instructs SQL Server not to fire the trigger when data modification is made as part of a replication process. ✓ The sql_statements is one or more Transact-SQL used to carry out actions once an event occurs.					
13	List out the algorithm used in the privacy preserving data mining and explain any two algorithms in detail ✓ Statistical Methods for Disclosure Control ✓ Measures of Anonymity ✓ The *k*-anonymity Method ✓ The Randomization Method ✓ Quantification of Privacy ✓ Utility Based Privacy-Preserving Data Mining ✓ Mining Association Rules under Privacy Constraints ✓ Cryptographic Methods for Information Sharing and Privacy **Measures of Anonymity** ✓ There are a very large number of definitions of anonymity in the privacy-preserving data mining field. ✓ This is partially because of the varying goals of different privacy-preserving data mining algorithms. ✓ For example, methods such as *k*-anonymity, *l*-diversity and *t*-closeness are all designed to prevent identification, though the final goal is to preserve the underlying sensitive information. ✓ Each of these methods is designed to prevent	5	2	3	4	2.2.3

	disclosure of sensitive information in a different way. **The *k*-anonymity Method** ✓ *k*-anonymity technique is that many attributes in the data can often be considered pseudo-identifiers which can be used in conjunction with public records in order to uniquely identify the records. ✓ For example, if the identifications from the records are removed, attributes such as the birth date and zip-code an be used in order to uniquely identify the identities of the underlying records. ✓ For example, if the identifications from the records are removed, attributes such as the birth date and zip-code an be used in order to uniquely identify the identities of the underlying records.					
14	Explain in detail about randomization method? ✓ The randomization method is a technique for privacy-preserving data mining in which noise is added to the data in order to mask the attribute values of records. ✓ The noise added is sufficiently large so that individual record values cannot be recovered. ✓ Therefore, techniques are designed to derive aggregate distributions from the perturbed records. ✓ Subsequently, data mining techniques can be developed in order to work with these aggregate distributions. The method of randomization can be described as follows. ✓ Consider a set of data records denoted by $X = \{x1 \ldots xN\}$ ✓ For record $xi \in X$ ✓ we add a noise component which is drawn from the probability distribution $fY(y)$. ✓ These noise components are drawn independently, and are denoted $y1 \ldots yN$. ✓ Thus, the new set of distorted records are denoted by $x1 + y1 \ldots xN + yN$. ✓ We denote this new set of records by $z1 \ldots zN$. ✓ In general, it is assumed that the variance of the added noise is large enough, so that the original record values cannot be easily guessed from the distorted	5	1	3	1	2.2.2

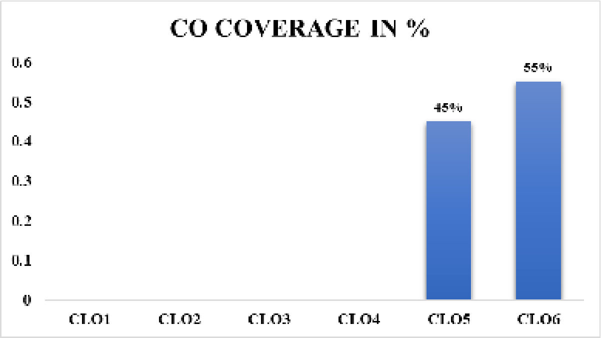
	data. ✓ Thus, the original records cannot be recovered, but the distribution of the original records can be recovered.					
	Part C (2*10= 20 Marks) Answer any two Questions					
15	Explain how oracle database auditing activities are performed using DDL triggers. ✓ ORACLE provides the mechanism for auditing 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  AUDIT sql_statement_clause schema_object_clause BY SESSION ACCESS WHENEVER NOT SUCCESSFUL ; 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	10	1	2	1	1.6.1
16	Discuss briefly about auditing database activities with oracle.	10	3	3	1	1.7.1

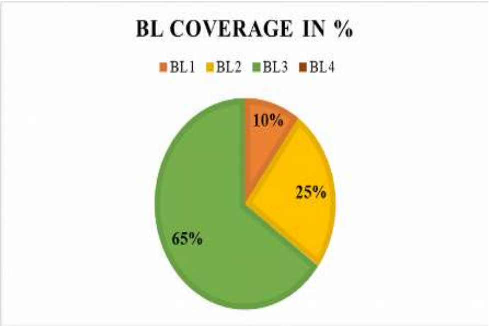
	✓ ORACLE provides the mechanism for auditing everything: ▪ From tracking who is creating and modifying the structure ▪ Who is granting privileges to whom ✓ The activities are divided into two types based on the type of SQL command statement used : ▪ Activities defined by DDL (Data Definition Language) Activities defined by DCL (Data Control Language DCL Activities Example: ✓ You are auditing the GRANT privilege issued on a TEMP table owned by DBSEC. ✓ The following steps shows how to audit the DCL statements audited. ✓ The same steps to be followed for all DCL Commands. Step 1 : Log on as SYSTEM or SYS and issue an AUDIT statement as follows Step 2: Log on as DBSEC and grant SELECT and UPDATE privileges to SYSTEM on TEMP table Step 3: Log on as SYSTEM and display the contents of DBA_AUDIT_TRAIL.					
17	Discuss in detail about distributed privacy preserving data mining. ✓ The key goal in most distributed methods for privacy-preserving data mining is to allow computation of useful aggregate statistics over the entire data set without compromising the privacy of the individual data sets within the different participant. ✓ Thus, the participants may wish to collaborate in obtaining aggregate results, but may not fully trust each other in terms of the distribution of their own data sets. ✓ For this purpose, the data sets may either be *horizontally partitioned* or be *vertically partitioned*. ✓ In horizontally partitioned data sets, the individual records are spread out across multiple entities, each of which have the same set of attributes. ✓ In vertical partitioning, the individual entities may have different attributes (or views) of the same set of records. ✓ Both kinds of partitioning pose different challenges to the problem of distributed privacy preserving data mining. ✓ The problem of distributed privacy-preserving data mining overlaps closely with a field in cryptography	10	4	3	4	1.7.1

for determining secure multi-party computations.

- The broad approach to cryptographic methods tends to compute functions over inputs provided by multiple recipients without actually sharing the inputs with one another.
- For example, in a 2-party setting, Alice and Bob may have two inputs *x* and *y* respectively, and may wish to both compute the function *f*(*x, y*) without revealing *x* or *y* to each other.
- This problem can also be generalized across *k* parties by designing the *k* argument function *h*(*x*1 . . . *xk*). Many data mining algorithms may be viewed in the context of repetitive computations of many such primitive functions such as the scalar dot product, secure sum etc.
- In order to compute the function *f*(*x, y*) or *h*(*x*1 . . . , *xk*), a *protocol* will have to designed for exchanging information in such a way that the function is computed without compromising privacy.
- That the robustness of the protocol depends upon the level of trust one is willing to place on the two participants Alice and Bob.
- This is because the protocol may be subjected to various kinds of adversarial behavior:
    - **Semi-honest Adversaries:**
        - In this case, the participants Alice and Bob are curious and attempt to learn from the information received by them during the protocol, but do not deviate from the protocol themselves. In many situations, this may be considered a realistic model of adversarial behavior.
    - **Malicious Adversaries:**
        - In this case, Alice and Bob may vary from the protocol, and may send sophisticated inputs to one another to learn from the information received from each other.

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





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