CT3 Set C Answer key

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

SRM Institute of Science and Technology

College of Engineering and Technology **SETC**

School of Computing

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	---------- tool provides the user interface for auditing events in SQLServer 2000? A)SQL profiler B) SQL Ninja C) SQL Audit D) SQL Idera	1	2	5	1	2.1.2
2	---------- security event in SQL Server events? A) GRANT REVOKE	1	2	5	1	2.1.3

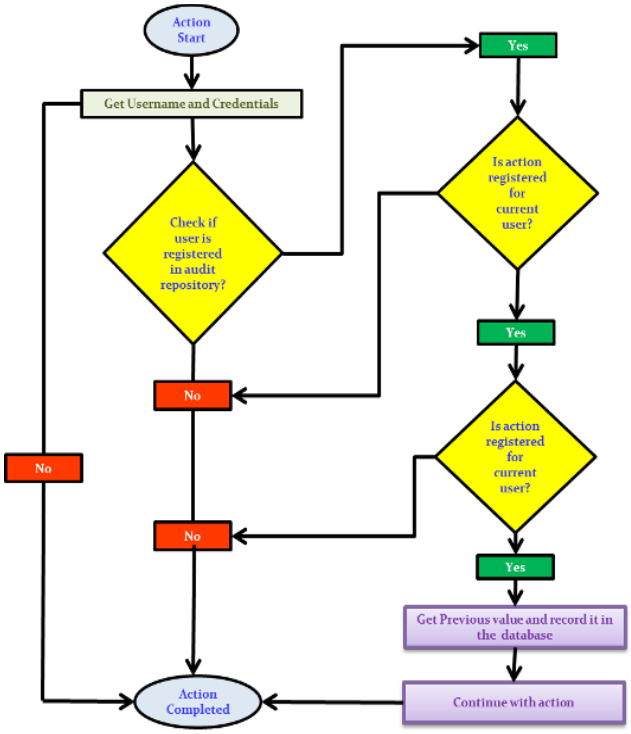
	B) DENY USER / LOGIN USER C) ROLE ADD / REMOVE / CONFIGURE D) All the above					
3	---------- function returns Boolean value in PKG_APP_AUDIT? A) AUDIT_CHECK B) AUDIT_REVOKE C) AUDIT_COMMIT D) AUDIT_ALERT	1	1	5	1	2.2.2
4	Perform an audit to identify problems before they occur is A) Preventive Audit B) Operational audit ... C) Compliance audit D) Payroll audit	1	1	5	4	2.2.3
5	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	2	5	4	2.2.3

6	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. A) Malicious B) Semi-Honest Adversaries C) Distributed denial of service D) Man in the middle Attack	1	1	6	4	1.3.1
7	The _____ System was one of the earliest practical applications of privacy preserving transformations. A) Datafly B) Homeland Security Applications C) Video Surveillance D) Watch list Problem	1	2	6	4	2.1.3
8	The scrub system was designed for _____ of clinical notes and letters which typically occurs in the form of textual data.	1	1	6	1	3.4.2

	A) Prediction B) de-identification C) Masking D) Decoding					
9	Query Output Perturbation for privacy preserving A) Add noise to the output query B) Add noise to the input C) Add noise to the predicted output D) Add noise to the expected output	1	2	6	1	2.2.2
10	Examples of utility measures A) Generalization height and Privacy information loss ratio B) Aggregation C) Masking D) Prediction	1	1	6	4	2.2.3
Part B (4*5=20Marks) Answer all Questions						
11	Summarize SQL statement audit trail? ✓ SQL statement audit trail, on the Events tab of your trace, you select **Object:Created** and **Object:Deleted** under the **objects** Category ✓ These two events audit all CREATE and DROP statements. ✓ To audit operations to the database files, select events under the Database category ✓ To audit errors that occur within the database, select the events under the Errors and Warnings category on the Events tab of your trace	5	2	5	1	1.6.1
12	List out necessary steps to track all database server errors On the general tab, you provide: ▪ A name for the trace ▪ The server you want to audit ▪ The base template to start with ▪ Where to save the audit data, either to a file or to a DB ▪ A stop time, if you don't want the trace to run indefinitely ▪ On the events tab, you specify events to be	5	1	5	4	2.2.3

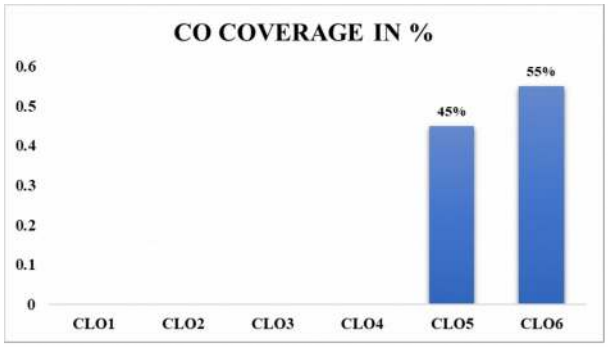
	audited and in which category they belong					
13	Describe the distributed algorithm for k-anonymity. ✓ In many applications, the data records are made available by simply removing key identifiers such as the name and social-security numbers from personal records. ✓ other kinds of attributes (known as 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.	5	3	6	4	2.2.3
14	Elaborate additive perturbation? Data Perturbation „ Hiding private data while mining patterns † Secure Multi-Party Computation „ Building a model over multi-party distributed databases without knowing others' inputs † Knowledge Hiding „ Hiding sensitive rules/patterns † Privacy-aware Knowledge Sharing	5	2	6	1	2.2.2

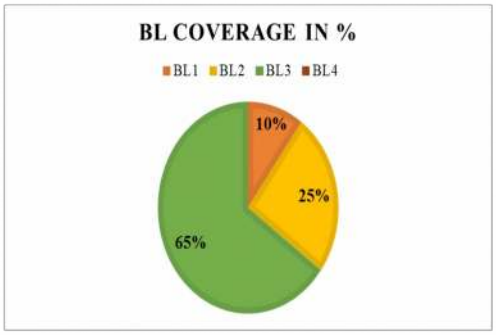
	„ Do the data mining results themselves violate privay					
Part C (2*10= 20 Marks) Answer any two Questions						
15	Describe the activities of Oracle alert log and explain with example in detail. The alert log file (also referred to as the ALERT.LOG) is a chronological log of messages and errors written out by an Oracle Database. Typical messages found in this file is: 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.	10	2	5	1	1.6.1

16	Determine the process of auditing with the help of case study examples.  	10	3	5	1	1.7.1
17	Elaborate data preserving methods employed in group-based anonymization ✓ In many applications, the data records are made available by simply removing key identifiers such as the name and social- security numbers from personal records. ✓ However, 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	10	2	6	4	1.7.1

	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. ▪ Subsequently, the topic of *k*-anonymity has been widely researched.					

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





Question Paper Setter Approved by the Audit Professor/Course Coordinator