

**DEPARTMENT OF COMPUTING TECHNOLOGIES**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2023 - 2024 (ODD)**

**Test: CLA - T1**

**Date: 11-08-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 50 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 25**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	3	3	-	-	-	-	-	-	-	-	-	-
2	CO2	3	-	-	-	-	-	-	-	-	-	-	-

**PART - A**

**(10 x 1 = 10 Marks)**

**Instructions: Answer all**

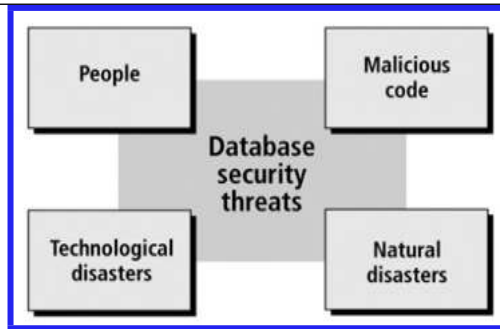
Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	_____ is a set of processes and procedure that transform data into information and knowledge.	1	L1	1	1	1.6.1
	A Knowledge system					
	<b>B Information system</b>					
	C Database system					
	D Computer system					
2.	A(n) _____ is a collection of programs that allows the user to operate the computer hardware.	1	L1	1	1	1.6.1
	A information system					
	B database					
	C DBA					
	<b>D operating system</b>					
3.	The main component of the operating system security environment is_____	1	L1	1	1	1.6.1
	<b>A services</b>					
	B file transfer					
	C memory					
	D file sharing					
4.	A _____ is a place where database security must be protected and applied.	1	L1	1	1	1.6.1
	A security gap					
	<b>B security access point</b>					
	C security threat					
	D security vulnerability					
5.	_____ is used for tactical management tasks and contains collection of business models	1	L1	1	1	1.6.1
	A Transaction Processing System (TPS)					
	<b>B Decision Support System (DSS)</b>					

	C	Expert System (ES)					
	D	Client / Server					
6.	764	File Permission means?	1	L1	1	1	1.6.1
	A	Everyone can read, write and execute.					
	B	Everyone can read, group can execute only and the owner can read and write.					
	C	Everyone can read, write and execute.					
	D	Everyone can read, group including owner can write, owner can execute.					
7.		_____ is used by network devices to provide a centralized authentication mechanism	1	L1	1	1	1.6.1
	A	SSL					
	B	RADIUS					
	C	SRP					
	D	PKI					
8.		_____ is a process that decides whether users are permitted to perform the functions they request.	1	L1	1	1	1.6.1
	A	Identification					
	B	Authentication					
	C	Authorization					
	D	Verification					
9.		_____ is a weakness that can be exploited by attackers.	1	L1	1	1	1.6.1
	A	System with Virus					
	B	System without firewall					
	C	System with vulnerabilities					
	D	System with strong password					
10.		_____ allows you to sign on once to a server (host machine) and then not have to sign on again if you go to another server where you have an account.	1	L1	1	1	1.6.1
	A	Password history					
	B	Password reuse					
	C	Logon retries					
	D	Single sign-on					

**PART – B**  
(3 x 5 = 15 Marks)

**Instructions: Answer any 3 Questions**

11.	<p>Sketch out the Information Security Architecture.</p> <pre> graph TD     subgraph Pillars         direction TB         C[Confidentiality • Privacy Laws • Confidential Classification • Policies and Procedures • Access Rights • Customer Concerns • Social and Cultural issues]         I[Integrity • Security Technology • Security Models • Cryptography Technology • DBMS Technology • Database and Data Design • Application Technology]         A[Availability • Threats and Attacks • System Vulnerabilities • Authorization methodology • Authentication Technology • Network Interface • Disaster and Recovery Strategy]     end     C --&gt; ISA[Information Security Architecture]     I --&gt; ISA     A --&gt; ISA     ISA &lt;--&gt; LPA[Logical and Physical Assets]         </pre>	5	L3	1	1	1.6.1
12.	<p>List the few DBMS functionalities and the major responsibilities of a database administrator.</p> <p><b>DBMS functionalities:</b></p> <ul style="list-style-type: none"> <li>✓ Allow developer and administrators to Organize data</li> <li>✓ Allow user to Store and retrieve data efficiently</li> <li>✓ Allow user to Manipulate data (update and delete)</li> <li>✓ Enforce referential integrity and consistency</li> <li>✓ Enforce and implement data security policies and procedures</li> <li>✓ Back up, recover, and restore data</li> </ul> <p><b>Major responsibilities of a database administrator.</b></p> <ul style="list-style-type: none"> <li>✓ Software Installation and Maintenance</li> <li>✓ Data Extraction, Transformation, and Loading</li> <li>✓ Specialised Data Handling</li> <li>✓ Database Backup and Recovery</li> <li>✓ Security</li> <li>✓ Authentication</li> <li>✓ Capacity Planning</li> <li>✓ Performance Monitoring</li> <li>✓ Database Tuning</li> <li>✓ 10. Troubleshooting</li> </ul>	5	L3	1	1	1.6.1
13.	<p>Describe the categories of database security threats.</p> <ul style="list-style-type: none"> <li>✓ Threat is defined as “ An indication of impending(i.e. will happen soon) danger or harm”</li> <li>✓ Vulnerabilities can escalate into threats</li> <li>✓ DBA , IS Administrator should aware of vulnerabilities and threats</li> <li>✓ Four types of threats contribute to security risks as shown in below figure</li> </ul>	5	L3	1	1	1.6.1



Threat type	Definition	Examples
People	People intentionally or unintentionally inflict damage, violation or destruction to all or any of the database components (People, Applications, Networks, OS, DBMS, Data files or data)	<ul style="list-style-type: none"> <li>✓ Employees</li> <li>✓ Govt. Authorities or Person who are in charge</li> <li>✓ Contractors</li> <li>✓ Consultants</li> <li>✓ Visitors</li> <li>✓ Hackers</li> <li>✓ Organised Criminals</li> <li>✓ Spies</li> <li>✓ Terrorists</li> <li>✓ Social Engineers</li> </ul>
Malicious Code	Software Code that in most cases is intentionally written to damage or violate one or more database environment components (People, Applications, Networks, OS, DBMS, Data files or data)	<ul style="list-style-type: none"> <li>✓ Viruses</li> <li>✓ Boot Sector Viruses</li> <li>✓ Worms</li> <li>✓ Trojan Horses</li> <li>✓ Spoofing Code</li> <li>✓ Denial-of-service flood</li> <li>✓ Rookits</li> <li>✓ Bots</li> <li>✓ Bugs</li> <li>✓ E-Mail Spamming</li> <li>✓ Back Door</li> </ul>

14.	<p>Discuss the any two digital authentication mechanisms used by operating systems.</p> <p><b>Digital Certificate</b></p> <ul style="list-style-type: none"> <li>✓ Widely used in e-commerce</li> <li>✓ Is a passport that identifies and verifies the holder of the certificate</li> <li>✓ Is an electronic file issued by a trusted party ( Known as certificate authority ) and cannot be forged or tampered with.</li> </ul> <p><b>Digital Token (Security Token)</b></p> <ul style="list-style-type: none"> <li>✓ Is a small electronic device that users keep with them to be used for authentication to a computer or network system.</li> <li>✓ This device displays a unique number to the token holder, which is used as a PIN ( Personal Identification Number) as the password</li> </ul> <p><b>Digital Card</b></p> <ul style="list-style-type: none"> <li>✓ Also known as security card or smart card</li> <li>✓ Similar to credit card in dimensions but instead of magnetic strip</li> <li>✓ It has an electronic circuit that stores the user identification information</li> </ul> <p><b>Kerberos</b></p> <ul style="list-style-type: none"> <li>✓ Developed by Massachusetts Institute of Technology (MIT) , USA</li> <li>✓ It is to enable two parties to exchange information over an open network by assigning a unique key. Called ticket , to each user.</li> <li>✓ The ticket is used to encrypt communicated messages</li> </ul>	5	L3	1	1	1.6.1
-----	--	---	----	---	---	-------

**DEPARTMENT OF COMPUTING TECHNOLOGIES**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2023 - 2024 (ODD)**

**Test: CLA - T1**

**Date: 11-08-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 50 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 25**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	3	3	-	-	-	-	-	-	-	-	-	-
2	CO2	3	-	-	-	-	-	-	-	-	-	-	-

**PART - A**  
**(10 x 1 = 10 Marks)**

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	Which of the following system supports non-structured problems and provide recommendations or answer to solve these problems?	1	L1	1	1	1.6.1
	A <b>Decision Support System</b>					
	B Transaction Processing System					
	C Expert System					
	D Database Management system					
2.	The concept behind a(n) _____ application is based on the business model of a customer ordering a service or product and the representative of a business granting that request.	1	L1	1	1	1.6.1
	A <b>information system</b>					
	B C.I.A. triangle					
	C DBMS					
	D client/server					
3.	In CIA triangle, A stands for _____	1	L1	1	1	1.6.1
	A Atomicity					
	B Accessibility					
	C Authority					
	D <b>Availability</b>					
4.	A _____ is a security violation or attack that can happen any time because of a security vulnerability.	1	L1	1	1	1.6.1
	A Security risk					
	B Security privilege					
	C Security policy					
	D <b>Security threat</b>					
5.	Business application, in house programs, purchased software, operating systems, databases are example of	1	L1	1	1	1.6.1

	A	Physical Asset					
	B	Logical Asset					
	C	Intangible Asset					
	D	Human Asset					
6.	_____code that compromises the integrity and state of the system		1	L1	1	1	1.6.1
	A	Worm					
	B	Spoofing Code					
	C	Virus					
	D	Trojan Horse					
7.	LDAP stands for _____.		1	L1	1	1	1.6.1
	A	Lightweight Direct Access Protocol					
	B	Lightweight Directory Access Protocol					
	C	Lightweight Directory Access Permission					
	D	Limited Directory Access Protocol					
8.	Authentication information is transmitted over the network in an encrypted form using_____.		1	L1	1	1	1.6.1
	A	SRP					
	B	RADIUS					
	C	SSL					
	D	PKI					
9.	How many types of permissions a file has in UNIX?		1	L1	1	1	1.6.1
	A	1					
	B	2					
	C	3					
	D	4					
10.	_____ tells the system how many days a password can be in effect before it must be changed		1	L1	1	1	1.6.1
	A	Password aging					
	B	Password Limit					
	C	Password Validity					
	D	Password reuse					

**PART – B**  
(3 x 5 = 15 Marks)

**Instructions: Answer any 3 Questions**

11.	<p>Enumerate the various components of Information systems.</p> <div data-bbox="277 757 986 1223" data-label="Diagram"> </div> <p><b>Data</b>– The information stored in the Database for future references or processing  <b>Procedures</b>– Manual , Guidelines, Business rules and Policies  <b>Hardware</b> – Computer System, Fax, Scanner, Printer, Disk  <b>Software</b> – DBMS, OS, Programming Languages, Other Utilities or Tools  <b>Network</b> –Communication Infrastructure  <b>People</b> – DBA, System Admin, Programmers, Users, Business Analyst, System Analyst</p>	5	L3	1	1	1.6.1
12.	<p>Elaborate the typical use of system applications at various management levels.</p> <ul style="list-style-type: none"> <li>✓ An information can be a back bone of the day-to-day operations of a company as well as the beacon of long-term strategies and vision.</li> <li>✓ Information systems are categorized based on usage.</li> <li>✓ The following figure shows the typical use of system applications at various management levels</li> </ul>	5	L3	1	1	1.6.1

	<div><div><div><div><div>Information</div><div>Long-term goals</div><div>Strategic</div></div><div><div>Expert systems (ESs)</div><div>Decision support systems (DSSs)</div><div>Transaction-processing systems (TPSs)</div></div><div><div>Upper-level management</div><div>Middle-level management</div><div>Lower-level management</div></div><div><div>Management information systems (MISs)</div><div>Short-term goals</div><div>Operational</div></div></div><div><div>↑</div><div>↓</div></div><div>Data</div></div><div>✓ Information System mainly classified into three categories</div><div><div>1) Transaction Processing System (TPS)</div><div>2) Decision Support System (DSS)</div><div>3) Expert System (ES)</div></div></div>																				
13.	<div>Describe the categories of database security risks.</div> <div><div>✓ Risks are simply the a part of doing business</div><div>✓ Managers at all the levels are constantly working to assess and mitigate risks to ensure the continuity of the department operations.</div><div>✓ Administrators should understand the weakness and threats related to the system</div><div>✓ Categories of database security risks are shown in the below figure</div></div> <div><div><div><div>People</div><div>Data</div><div>Hardware</div><div>Confidence</div></div><div>Database security risks</div></div></div> <div>Definitions and examples of Risk types</div> <table><tr><th>Risk Type</th><th>Definition</th><th>Examples</th></tr><tr><td>People</td><td>The loss of people who are vital components of the database environments and know critical information can create risks</td><td><div>✓ Loss of key persons ( Registration, Migration, Health problems)</div><div>✓ Key person downtime due to sickness personal or family problems, or burnout</div></td></tr><tr><td>Hardware</td><td>A risk that mainly results in hardware unavailability or interoperability</td><td><div>✓ Downtime due to hardware failure, mal functions, or inflicted damages</div><div>✓ Failure due to unreliable or poor quality equipment</div></td></tr><tr><td>Data</td><td>Data loss or data integrity is a major concern of the database administration and management</td><td><div>✓ Data loss</div><div>✓ Data corruption</div><div>✓ Data Privacy loss</div></td></tr><tr><td>Confidence</td><td>The loss of public confidence in the data produced by the company causes a loss of public confidence in the company itself ie. Customer satisfaction fails</td><td><div>✓ Loss of procedural and policy documentation</div><div>✓ DB performance degradation</div><div>✓ Fraud</div><div>✓ Confusion and uncertainty about database information</div></td></tr></table>	Risk Type	Definition	Examples	People	The loss of people who are vital components of the database environments and know critical information can create risks	<div>✓ Loss of key persons ( Registration, Migration, Health problems)</div> <div>✓ Key person downtime due to sickness personal or family problems, or burnout</div>	Hardware	A risk that mainly results in hardware unavailability or interoperability	<div>✓ Downtime due to hardware failure, mal functions, or inflicted damages</div> <div>✓ Failure due to unreliable or poor quality equipment</div>	Data	Data loss or data integrity is a major concern of the database administration and management	<div>✓ Data loss</div> <div>✓ Data corruption</div> <div>✓ Data Privacy loss</div>	Confidence	The loss of public confidence in the data produced by the company causes a loss of public confidence in the company itself ie. Customer satisfaction fails	<div>✓ Loss of procedural and policy documentation</div> <div>✓ DB performance degradation</div> <div>✓ Fraud</div> <div>✓ Confusion and uncertainty about database information</div>	5	L3	1	1	1.6.1
Risk Type	Definition	Examples																			
People	The loss of people who are vital components of the database environments and know critical information can create risks	<div>✓ Loss of key persons ( Registration, Migration, Health problems)</div> <div>✓ Key person downtime due to sickness personal or family problems, or burnout</div>																			
Hardware	A risk that mainly results in hardware unavailability or interoperability	<div>✓ Downtime due to hardware failure, mal functions, or inflicted damages</div> <div>✓ Failure due to unreliable or poor quality equipment</div>																			
Data	Data loss or data integrity is a major concern of the database administration and management	<div>✓ Data loss</div> <div>✓ Data corruption</div> <div>✓ Data Privacy loss</div>																			
Confidence	The loss of public confidence in the data produced by the company causes a loss of public confidence in the company itself ie. Customer satisfaction fails	<div>✓ Loss of procedural and policy documentation</div> <div>✓ DB performance degradation</div> <div>✓ Fraud</div> <div>✓ Confusion and uncertainty about database information</div>																			
14.	Discuss the different categories of information assets	5	L3	1	1	1.6.1															



	<p>and their values.</p> <ul style="list-style-type: none"> <li>✓ People always tend to protect assets regardless of what they are</li> <li>✓ Corporations treat their assets in the same way</li> <li>✓ Assets are the infrastructure of the company operation</li> </ul> <p><b>There are four main types of assets</b></p> <ul style="list-style-type: none"> <li>▪ <b>Physical assets</b> – Also known as tangible assets, these include buildings, cars, hardware and so on...</li> <li>▪ <b>Logical assets</b> – Logical aspects of an information system such as business applications, in-house programs, purchased software, OS, DBs, Data</li> <li>▪ <b>Intangible assets</b> – Business reputation, quality, and public confidence</li> <li>▪ <b>Human assets</b> – Human skills, knowledge and expertise</li> </ul>					
--	--	--	--	--	--	--

**DEPARTMENT OF COMPUTING TECHNOLOGIES**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2023 - 2024 (ODD)**

**Test: CLA - T1**

**Date: 11-08-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 50 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 25**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	3	3	-	-	-	-	-	-	-	-	-	-
2	CO2	3	-	-	-	-	-	-	-	-	-	-	-

**PART - A**  
**(10 x 1 = 10 Marks)**

**Instructions: Answer all**

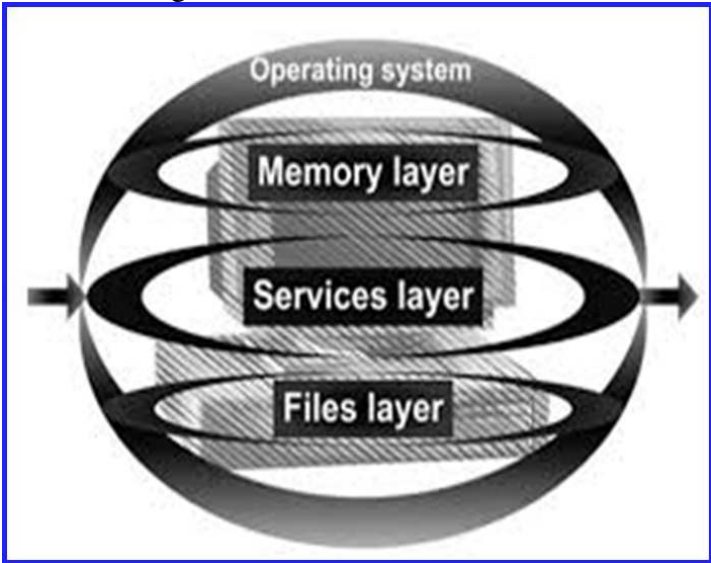
Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	Data is processed or transformed by a collection of components working together to produce and generate accurate information. These components are known as a(n)_____.	1	L1	1	1	1.6.1
	<b>A</b> information system					
	B database					
	C DBA					
	D operating system					
2.	NSTISSC stand for _____	1	L1	1	1	1.6.1
	A National Service Telecommunications & Information Systems Security Committee					
	<b>B</b> National Security Telecommunications & Information Systems Security Committee					
	C National Security Telecommunications & Information Systems Security Company					
	D National Security Telecommunications & Integration Systems Security Committee					
3.	_____ means the protection of data from modification by unknown users.	1	L1	1	1	1.6.1
	A Confidentiality					
	<b>B</b> Integrity					
	C Authentication					
	D Non-repudiation					
4.	The model designed for guiding the policies of Information security within a company, firm or organization is referred as _____.	1	L1	1	1	1.6.1
	A Confidentiality					
	B Non-repudiation					
	<b>C</b> CIA Triangle					

	D	Authenticity					
5.	From the following, which is not common file permission?		1	L1	1	1	1.6.1
	A	Write					
	B	Execute					
	C	Stop					
	D	Read					
6.	Software that defines a database, stores the data, supports a query language, produces reports and creates data entry screens is a _____		1	L1	1	1	1.6.1
	A	Data Dictionary					
	B	Database Management System					
	C	Decision Support System					
	D	Relational Database					
7.	_____ enforce and implement data security policies and procedures on data base levels.		1	L1	1	1	1.6.1
	A	Database designer					
	B	Database analyst					
	C	Database Administrator					
	D	Database manager					
8.	Which layer authenticates information that is transmitted over the network in an encrypted form?		1	L1	1	1	1.6.1
	A	Socket base layer					
	B	Secure socket layer					
	C	Security application layer					
	D	Security software					
9.	Which of the following method is efficient for reading but not suited for frequently changing information?		1	L1	1	1	1.6.1
	A	Public Key Infrastructures (PKI)					
	B	Secure Remote Password (SRP)					
	C	Lightweight Directory Access Protocol (LDAP)					
	D	NT LAN Manager (NTLM)					
10.	_____is a small electronic device that users keep with them to be used for authentication of a computer or network		1	L1	1	1	1.6.1
	A	Kerberos					
	B	Digital Card					
	C	Digital Token					
	D	Digital Certificate					

**PART – B**  
**(3 x 5 = 15 Marks)**

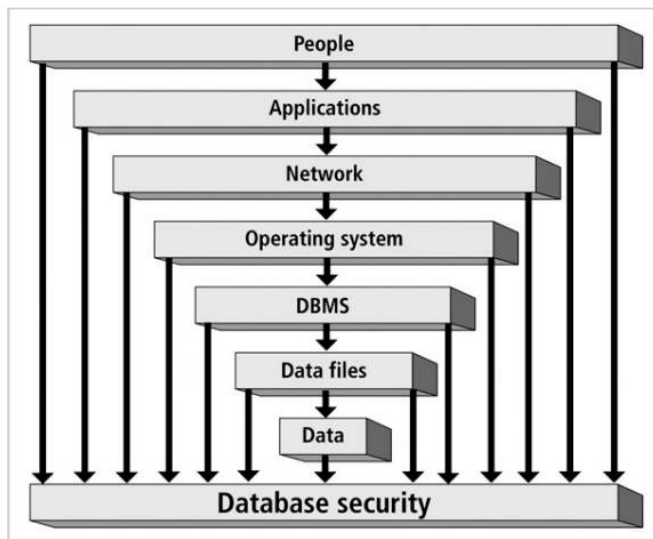
**Instructions: Answer any 3 Questions**

11.	<p>Annotate CIA triangle.</p> <p>CIA TRIANGLE</p> <div><div>Confidentiality Information is classified into different levels of confidentiality to ensure that only authorised users access the information</div><div>Integrity Information is accurate and protected from tampering by unauthorised persons Information is consistent and validated</div><div>Availability Information is available all the times only for authorised and authenticated persons System is protected from being shutdown due to external or internal threats or attacks</div><div>Information Security</div></div>	5	L2	1	1	1.6.1									
12.	<p>Describe the various characteristics of information system categories.</p> <table><tr><th>Category</th><th>Characteristics</th><th>Typical Application System</th></tr><tr><td>Transaction Processing System (TPS)</td><td><ul style="list-style-type: none"><li>✓ Also Known as ONLINE TRANSACTION PROCESSING (OLTP)</li><li>✓ Used for operational tasks</li><li>✓ Provides solutions for structured problems</li><li>✓ Includes business transactions</li><li>✓ Logical Components of TPS applications ( Derived from business procedures , business rules and policies)</li></ul></td><td><ul style="list-style-type: none"><li>▪ Order tracking</li><li>▪ Customer service</li><li>▪ Payroll</li><li>▪ Accounting</li><li>▪ Student Registration</li><li>▪ Car Sales</li></ul></td></tr><tr><td>Decision Support System (DSS)</td><td><ul style="list-style-type: none"><li>✓ Deals with nanostructured problems and provide recommendations or answer to solve these problems</li><li>✓ Is capable of "What-if?" analysis</li><li>✓ Contains collection of business models</li><li>✓ Is used for tactical management tasks</li></ul></td><td><ul style="list-style-type: none"><li>▪ Risk Management</li><li>▪ Fraud Detection</li><li>▪ Sales forecasting</li><li>▪ Case resolution</li></ul></td></tr></table>	Category	Characteristics	Typical Application System	Transaction Processing System (TPS)	<ul style="list-style-type: none"><li>✓ Also Known as ONLINE TRANSACTION PROCESSING (OLTP)</li><li>✓ Used for operational tasks</li><li>✓ Provides solutions for structured problems</li><li>✓ Includes business transactions</li><li>✓ Logical Components of TPS applications ( Derived from business procedures , business rules and policies)</li></ul>	<ul style="list-style-type: none"><li>▪ Order tracking</li><li>▪ Customer service</li><li>▪ Payroll</li><li>▪ Accounting</li><li>▪ Student Registration</li><li>▪ Car Sales</li></ul>	Decision Support System (DSS)	<ul style="list-style-type: none"><li>✓ Deals with nanostructured problems and provide recommendations or answer to solve these problems</li><li>✓ Is capable of "What-if?" analysis</li><li>✓ Contains collection of business models</li><li>✓ Is used for tactical management tasks</li></ul>	<ul style="list-style-type: none"><li>▪ Risk Management</li><li>▪ Fraud Detection</li><li>▪ Sales forecasting</li><li>▪ Case resolution</li></ul>	5	L3	1	1	1.6.1
Category	Characteristics	Typical Application System													
Transaction Processing System (TPS)	<ul style="list-style-type: none"><li>✓ Also Known as ONLINE TRANSACTION PROCESSING (OLTP)</li><li>✓ Used for operational tasks</li><li>✓ Provides solutions for structured problems</li><li>✓ Includes business transactions</li><li>✓ Logical Components of TPS applications ( Derived from business procedures , business rules and policies)</li></ul>	<ul style="list-style-type: none"><li>▪ Order tracking</li><li>▪ Customer service</li><li>▪ Payroll</li><li>▪ Accounting</li><li>▪ Student Registration</li><li>▪ Car Sales</li></ul>													
Decision Support System (DSS)	<ul style="list-style-type: none"><li>✓ Deals with nanostructured problems and provide recommendations or answer to solve these problems</li><li>✓ Is capable of "What-if?" analysis</li><li>✓ Contains collection of business models</li><li>✓ Is used for tactical management tasks</li></ul>	<ul style="list-style-type: none"><li>▪ Risk Management</li><li>▪ Fraud Detection</li><li>▪ Sales forecasting</li><li>▪ Case resolution</li></ul>													

	<div> <div>Expert System (ES)</div> <div> <ul style="list-style-type: none"> <li>✓ Captures reasoning of human experts</li> <li>✓ Executive Expert Systems(EESs) are a type of expert system used by top level management for strategic management goals</li> <li>✓ A branch of Artificial Intelligence within the field of computer science studies</li> <li>✓ Software consists of : Knowledge Base Inference Engine Rules</li> <li>✓ People Consists of : Domain Experts Knowledge Engineers Power Users</li> </ul> </div> <div> <ul style="list-style-type: none"> <li>✓ Virtual University Simulation</li> <li>✓ Financial Enterprise</li> <li>✓ Statistical Trading</li> <li>✓ Loan Expert</li> <li>✓ Market Analysis</li> </ul> </div> </div>					
13.	<p>Discuss the different components of an OS Security Environment.</p> <ul style="list-style-type: none"> <li>✓ The three components (layers) of the OS are represented in the figure</li> <li>✓ Memory component is the hardware memory available on the system</li> <li>✓ Files component consists of files stored on the disk</li> <li>✓ Service component compromise such OS features and functions as N/W services, File Management and Web services</li> </ul>  <p>The diagram illustrates the layers of an Operating System's security environment. It features a central stack of three rectangular blocks labeled 'Memory layer', 'Services layer', and 'Files layer' from top to bottom. These blocks are enclosed within a larger, rounded rectangular frame. Two thick, curved arrows, one on the left and one on the right, point horizontally across the middle of the stack, passing behind the central blocks. The entire diagram is set against a light gray background with a subtle grid pattern.</p>	5	L3	1	1	1.6.1
14.	<p>Define Database security and give various database security access points.</p> <p><b>Database security</b> is a collection of security polices and procedures, data constraints, security methods , security tools blended together to implement all necessary measures to secure the integrity, accessibility and confidentiality of every component of the database environment.</p> <ul style="list-style-type: none"> <li>• One of the functions of DBMS is to empower DBA to implement and enforce security at all</li> </ul>	5	L3	1	1	1.6.1

levels of security

- A security access point is a place where database security must be protected and applied
- The Major Security access points illustrated in the below figure



Database security access points

- ✓ People – Individuals who have been granted privileges and permissions to access networks, workstations, servers, databases, data files and data
- ✓ Applications – Application design and implementation which includes privileges and permissions granted to people
- ✓ Network – One of the most sensitive security access points. Protect the network and provide network access only to applications, operating systems and databases.
- ✓ Operating Systems – This access point is defined as authentication to the system, the gateway to the data
- ✓ DBMS – The logical structure of the database, which includes memory, executables and other binaries
- ✓ Data files – Another access point that influences database security enforcement is access to data files where data resides.
- ✓ Data – The data access point deals with data design needed to enforce data integrity

**DEPARTMENT OF COMPUTING TECHNOLOGIES**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2023 - 2024 (ODD)**

**Test: CLA - T1**

**Date: 11-08-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 50 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 25**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	3	3	-	-	-	-	-	-	-	-	-	-
2	CO2	3	-	-	-	-	-	-	-	-	-	-	-

**PART - A**  
**(10 x 1 = 10 Marks)**

**Instructions: Answer all**

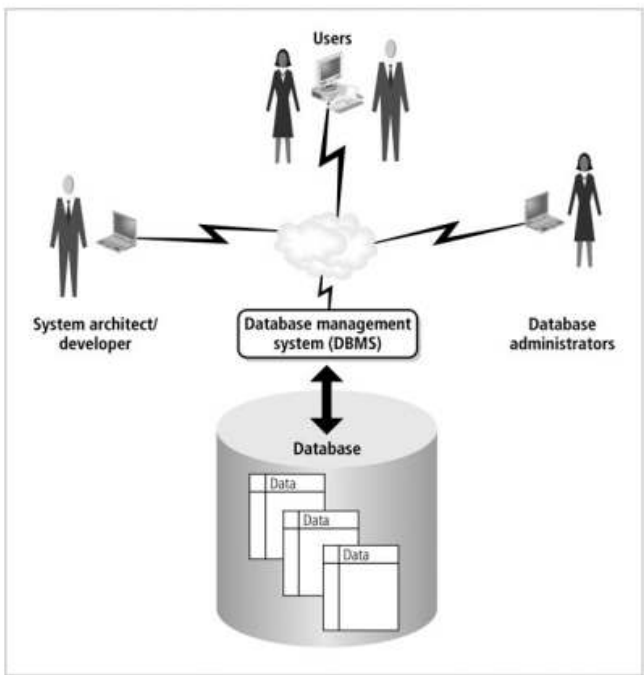
Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	_____ is a gateway of the database access.	1	L1	1	1	1.6.1
	A Server					
	<b>B Operating System</b>					
	C Network					
	D Internet					
2.	_____ is a collection of security policies and procedures, data constraints, security methods, security tools blended together to implement all necessary measures to secure the integrity, accessibility and confidentiality of every component of the database environment.	1	L1	1	1	1.6.1
	A Operating System					
	B Firewall					
	<b>C Database security</b>					
	D Gateway					
3.	In CIA triangle, I stands for _____	1	L1	1	1	1.6.1
	A Information					
	<b>B Integrity</b>					
	C Issues					
	D Identification					
4.	Operating system, database and data are the example of _____.	1	L1	1	1	1.6.1
	A Physical assets					
	<b>B Logical assets</b>					
	C Intangible assets					
	D Human assets					
5.	Database security is the _____ to which all the data is fully protected from tampering and unauthorized acts.	1	L1	1	1	1.6.1

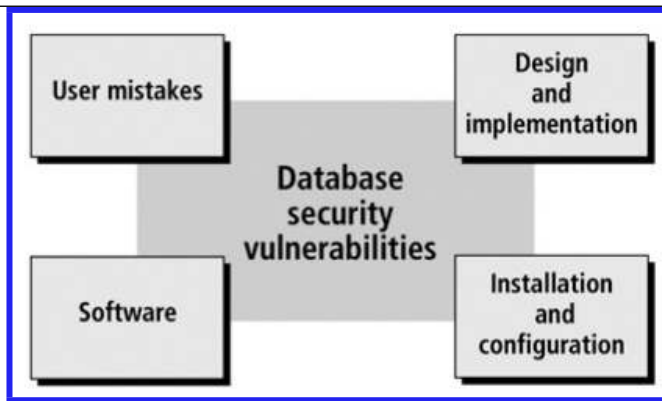
	<b>A</b>	<b>Degree</b>					
	<b>B</b>	Reliability					
	<b>C</b>	Durability					
	<b>D</b>	Percentile					
<b>6.</b>	_____device displays a unique number to the token holder, which is used as a PIN ( Personal Identification Number) as the password.		1	L1	1	1	1.6.1
	<b>A</b>	<b>Digital Token</b>					
	<b>B</b>	Digital Card					
	<b>C</b>	Digital Certificate					
	<b>D</b>	Kerberos					
<b>7.</b>	The _____method is the process of verifying the identity of the user by means of a digital mechanism or software.		1	L1	1	1	1.6.1
	<b>A</b>	Digital Certificate .					
	<b>B</b>	Digital Token					
	<b>C</b>	Digital Card					
	<b>D</b>	<b>Digital authentication</b>					
<b>8.</b>	In UNIX, a file can be recognized as an ordinary file or directory by ____ symbol.		1	L1	1	1	1.6.1
	<b>A</b>	#					
	<b>B</b>	\$					
	<b>C</b>	-					
	<b>D</b>	*					
<b>9.</b>	Two parties to exchange information over an open network by assigning a unique key is called_____.		1	L1	1	1	1.6.1
	<b>A</b>	Token					
	<b>B</b>	<b>Ticket</b>					
	<b>C</b>	Keys					
	<b>D</b>	Password					
<b>10.</b>	Malicious code that looks like a legitimate code is known as _____		1	L1	1	1	1.6.1
	<b>A</b>	Passcode					
	<b>B</b>	<b>Spoofing code</b>					
	<b>C</b>	Virus code					
	<b>D</b>	Trojan code					



**PART – B**  
(3 x 5 = 15 Marks)

**Instructions: Answer any 3 Questions**

11.	<p>Explain about database and database environment.</p> <ul style="list-style-type: none"> <li>✓ A collection of meaningful Integrated Information System</li> <li>✓ It is both Physical and Logical</li> <li>✓ Representing the logical information in a physical device</li> <li>✓ Mainly used for storing and retrieving the data for processing</li> <li>✓ Using CLIENT / SERVER Architecture</li> <li>✓ Request and Reply protocols are used to communicate client and server</li> </ul>	5	L3	1	1	1.6.1
	 <p>The diagram illustrates the database and DBMS environment. At the top, 'Users' are shown interacting with the system. Below them, 'System architect/developer' and 'Database administrators' are connected to the 'Database management system (DBMS)'. The DBMS is represented by a cloud-like shape. Below the DBMS is the 'Database', depicted as a cylinder containing 'Data' blocks. A double-headed arrow connects the DBMS and the Database, indicating bidirectional communication.</p> <p><b>FIGURE 1-4</b> Database and DBMS environment</p>					
12.	<p>Write short note on database security vulnerabilities.</p> <ul style="list-style-type: none"> <li>✓ Vulnerability means “Susceptible to Attacks” (Source :<a href="http://www.dictionary.com">www.dictionary.com</a>)</li> <li>✓ Intruders, Attackers and Assailers exploit vulnerabilities in Database environment to prepare and start their attacks.</li> <li>✓ Hackers usually explore the weak points of a system until they gain entry</li> <li>✓ Once the intrusion point is identified , Hackers unleash their array of attacks <ul style="list-style-type: none"> <li>▪ Virus</li> <li>▪ Malicious Code</li> <li>▪ Worms</li> <li>▪ Other Unlawful violations</li> </ul> </li> <li>✓ To protect the system the administrator should understand the types of vulnerabilities</li> <li>✓ The below figure shows the types of vulnerabilities</li> </ul>	5	L3	1	1	1.6.1



### Types of Vulnerabilities ...

Category	Description	Examples
Installation and Configuration	<ul style="list-style-type: none"> <li>✓ Results from default installation</li> <li>✓ Configuration that is known publicly</li> <li>✓ Does not enforce any security measures</li> <li>✓ Improper configuration or Installation may result in security risks</li> </ul>	<ul style="list-style-type: none"> <li>✓ Incorrect application configuration</li> <li>✓ Failure to change default passwords</li> <li>✓ Failure to change default privileges</li> <li>✓ Using default installation which does not enforce high security measures</li> </ul>
User Mistakes	<ul style="list-style-type: none"> <li>✓ Security vulnerabilities are tied to humans too</li> <li>✓ Carelessness in implementing procedures</li> <li>✓ Failure to follow through</li> <li>✓ Accidental errors</li> </ul>	<ul style="list-style-type: none"> <li>✓ Lack of Auditing controls</li> <li>✓ Untested recovery plan</li> <li>✓ Lack of activity monitoring</li> <li>✓ Lack of protection against malicious code</li> <li>✓ Lack of applying patches as they are released</li> <li>✓ Bad authentication or implementation</li> <li>✓ Social Engineering</li> <li>✓ Lack of technical information</li> <li>✓ Susceptibility to scam</li> </ul>

13. Describe the various security methods that are used to protect the different components of a database environment.

Security methods used to protect database environment components

Database Component Protected	Security Methods
People	<ul style="list-style-type: none"> <li>✓ Physical limits on access to hardware and documents</li> <li>✓ Through the process of identification and authentication make certain that the individual is who is claim s to be through the use of devices, such as ID cards, eye scans, and passwords</li> <li>✓ Training courses on the importance of security and how to guard assets</li> <li>✓ Establishment of security policies and procedures</li> </ul>

5

L3

1

1

1.6.1

	<table><tr><td>Applications</td><td><ul style="list-style-type: none"><li>✓ Authentication of users who access applications</li><li>✓ Business rules</li><li>✓ Single sign-on ( A method for signing on once for different applications and web sites)</li></ul></td></tr><tr><td>Network</td><td><ul style="list-style-type: none"><li>✓ Firewalls to block network intruders</li><li>✓ Virtual Private Network (VPN)</li><li>✓ Authentication</li></ul></td></tr></table>	Applications	<ul style="list-style-type: none"><li>✓ Authentication of users who access applications</li><li>✓ Business rules</li><li>✓ Single sign-on ( A method for signing on once for different applications and web sites)</li></ul>	Network	<ul style="list-style-type: none"><li>✓ Firewalls to block network intruders</li><li>✓ Virtual Private Network (VPN)</li><li>✓ Authentication</li></ul>					
Applications	<ul style="list-style-type: none"><li>✓ Authentication of users who access applications</li><li>✓ Business rules</li><li>✓ Single sign-on ( A method for signing on once for different applications and web sites)</li></ul>									
Network	<ul style="list-style-type: none"><li>✓ Firewalls to block network intruders</li><li>✓ Virtual Private Network (VPN)</li><li>✓ Authentication</li></ul>									
14.	<p>Write short note on E-Mail security.</p> <ul style="list-style-type: none"><li>✓ E-mail may be the tool most frequently used by hackers to exploit viruses, worms, and other computer system invaders.</li><li>✓ E-mail is widely used by public and private organizations as a means of communication</li><li>✓ E-mail was the medium used in many of the most famous worm and virus attacks</li><li>✓ For example :<ul style="list-style-type: none"><li>▪ Love Bug Worm</li><li>▪ Mydoom worm</li><li>▪ Melissa virus</li></ul></li><li>✓ E-mail is not only to used to send viruses and worms, nut to send spam e-mail, private and confidential data as well as offensive messages</li><li>✓ To prevent from these activities ,<ul style="list-style-type: none"><li>▪ Do not configure e-mail server on a machine in which the sensitive data resides</li><li>▪ Do not disclose the e-mail server technical details</li></ul></li></ul>	5	L3	1	1	1.6.1				

**Test: CLA2**
**Date: 10-10-2023**
**Course Code & Title: 18CSE455T -Database Security and Privacy**
**Duration: 1 Hour 40 Minutes**
**Year & Sem: IV / VII**
**Max. Marks: 50**
**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO3	1	-	1	2	2	1	-	-	-	-	-	-
2	CO4	1	-	3	1	1	1	-	-	-	-	-	-

**PART - A**  
(15 x 1 = 15 Marks)

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	When we update any tuple in the relation, which Authorization on a relation allows a user to?	1	1	3	4,5	1.3.1
	A Select authorization					
	B Update authorization					
	C Grant authorization					
	D Define authorization					
2.	Which statement is used to revoke an authorization,	1	1	3	4,5	1.3.1
	A Revoke					
	B Modify					
	C grant					
	D alter					
3.	Who are the oracle default users?	1	1	3	4,5	1.3.1
	A SYS and SYSTEM					
	B SYSTEM and SCOTT					
	C SYS, SYSTEM and SCOTT					
	D SYS and SCOTT					
4.	Identify the other two names used by ORACLE to refer VPD?	1	1	4	3	1.3.1
	A Column level security and Row level security					
	B Column level security and Fine grained access					
	C Row level security and Fine grained access					
	D Fine grained access and information security					
5.	_____algorithm uses same cryptographic keys for both encryption and decryption of cipher text	1	1	4	3	1.3.1
	A Asymmetric key encryption					
	B Private key encryption					
	C Public key encryption					
	D Symmetric key encryption					
6.	Oracle _____ views enable you to see everything created and stored in the database.	1	1	4	3	1.3.1
	A Storage					

	B	Data dictionary					
	C	Service					
	D	Users					
7.		_____ is the indication that a password has a limited time left before it expires.	1	1	3	4,5	1.3.1
	A	Password complexity					
	B	Password storage					
	C	Password usage					
	D	Password aging					
8.		Command that comes under DCL is/are -	1	1	3	4,5	1.3.1
	A	grant					
	B	revoke					
	C	Both A & B					
	D	None of the above					
9.		Which command can be used to obtain the table's records?	1	1	3	4,5	1.3.1
	A	retrieve					
	B	select					
	C	create					
	D	alter					
10.		Give the command to change the default password TIGER to LION for the user SCOTT	1	1	3	4,5	1.3.1
	A	alter user identified by lion;					
	B	alter user scott identified by lion;					
	C	alter user scott by lion;					
	D	alter user identified by lion;					
11		What does the following code snippet do? Delete from students where age=15; Rollback;	1	1	3	4,5	1.3.1
	A	Performs an undo operation on the delete operation					
	B	Delete the rows from the table where age=15					
	C	Deletes the entire table					
	D	None of the above					
12		Virtual private database is a function of	1	1	4	3	1.3.1
	A	Oracle					
	B	Java					
	C	SQL					
	D	DB2					
13		Virtual private database provides authorization at the level of	1	1	4	3	1.3.1
	A	Rows					
	B	Tuples					
	C	Relations					
	D	All of the above					
14		To add or remove server role membership use	1	1	3	4,5	1.3.1
	A	Alter role					
	B	Alter any login					
	C	Alter server role					
	D	None of the mentioned					
15		Farmer goes to ATM center to withdraw an amount of Rs.300/- . Which type of user farmer is?	1	1	4	3	1.3.1
	A	Application programmer					
	B	Unsophisticated User					
	C	Sophisticated User					
	D	Specialized User					

**PART – B**  
(3 x 5 = 15 Marks)

**Instructions: Answer any 3 Questions**

16.	<p>Describe the various privileges available in the security data model.</p> <p>Privilege is a method to permit or deny access to data or to perform database Operations (Data Manipulation).</p> <ul style="list-style-type: none"> <li>➤ System Privileges – Privileges granted only by DBA or users who have been granted the administration option.</li> <li>➤ Object Privileges – Privileges granted to an ORACLE user by the scheme owner of a database object or a user who has been granted the GRANT option.</li> </ul> <p><b>System Privileges</b> ADMIN, ALTER ANY CACHE GROUP, ALTER ANY TABLE, CREATE ANY PROCEDURE, CREATE ANY TABLE</p> <p><b>Object privileges:</b> DELETE, EXECUTE, INSERT, SELECT, UPDATE</p> <p>Note: Write single line description about each privilege.</p>	5	2	3	4	1.6.1
17.	<p>Explain in detail data encryption.</p> <p>Data encryption is a method of protecting data by encoding it in such a way that it can only be decrypted or accessed by an individual who holds the correct encryption key. When a person or entity accesses encrypted data without permission, it appears scrambled or unreadable.</p> <p><b>How does data encryption work?</b></p> <p>The data that needs to be encrypted is termed plaintext or clear text. The plaintext needs to be passed via some encryption algorithms, which are mathematical calculations to be done on raw information. There are multiple encryption algorithms, each of which differs by application and security index.</p> <div style="text-align: center;"> <pre> graph LR     Sender[Sender] --&gt; Plaintext1[Plaintext]     Plaintext1 -- "Encryption Key" --&gt; Ciphertext[Ciphertext]     Ciphertext -- "Decryption Key" --&gt; Plaintext2[Plaintext]     Plaintext2 --&gt; Receiver[Receiver] </pre> </div> <p>Apart from the algorithms, one also needs an encryption key. Using said key and a suitable encryption algorithm, the plaintext is converted into the encrypted piece of data, also known as cipher text. Instead of sending the plaintext to the receiver, the cipher text is sent through insecure channels of</p>	5	1	4	3	1.6.1

	communication. Once the cipher text reaches the intended receiver, he/she can use a decryption key to convert the cipher text back to its original readable format i.e. plaintext. This decryption key must be kept secret at all times, and may or not be similar to the key used for encrypting the message.																																						
18.	<p>Compare the access modes model's static and dynamic modes.</p> <p>Static Modes</p> <table><thead><tr><th>Access Mode</th><th>Level</th><th>Description</th></tr></thead><tbody><tr><td>use</td><td>1</td><td>Allows the subject to use the object without modifying the object</td></tr><tr><td>read</td><td>2</td><td>Allows the subject to read the contents of the object</td></tr><tr><td>update</td><td>3</td><td>Allows the subject to modify the contents of the object</td></tr><tr><td>create</td><td>4</td><td>Allows the subject to add instances to the object</td></tr><tr><td>delete</td><td>4</td><td>Allows the subject to remove instances of the object</td></tr></tbody></table> <p>Dynamic Modes</p> <table><thead><tr><th>Access Mode</th><th>Level</th><th>Description</th></tr></thead><tbody><tr><td>grant</td><td>1</td><td>Allows the subject to grant any static access mode to any other subject</td></tr><tr><td>revoke</td><td>1</td><td>Allows the subject to revoke a granted static access mode from a subject</td></tr><tr><td>delegate</td><td>2</td><td>Allows the subject to grant the grant privilege to other subjects</td></tr><tr><td>abrogate</td><td>2</td><td>Allows the subject to grant the revoke privilege to other subjects</td></tr></tbody></table>	Access Mode	Level	Description	use	1	Allows the subject to use the object without modifying the object	read	2	Allows the subject to read the contents of the object	update	3	Allows the subject to modify the contents of the object	create	4	Allows the subject to add instances to the object	delete	4	Allows the subject to remove instances of the object	Access Mode	Level	Description	grant	1	Allows the subject to grant any static access mode to any other subject	revoke	1	Allows the subject to revoke a granted static access mode from a subject	delegate	2	Allows the subject to grant the grant privilege to other subjects	abrogate	2	Allows the subject to grant the revoke privilege to other subjects	5	1	4	3	1.6.1
Access Mode	Level	Description																																					
use	1	Allows the subject to use the object without modifying the object																																					
read	2	Allows the subject to read the contents of the object																																					
update	3	Allows the subject to modify the contents of the object																																					
create	4	Allows the subject to add instances to the object																																					
delete	4	Allows the subject to remove instances of the object																																					
Access Mode	Level	Description																																					
grant	1	Allows the subject to grant any static access mode to any other subject																																					
revoke	1	Allows the subject to revoke a granted static access mode from a subject																																					
delegate	2	Allows the subject to grant the grant privilege to other subjects																																					
abrogate	2	Allows the subject to grant the revoke privilege to other subjects																																					
19.	<p>Write about the following in SQL server</p> <p>I. Removing user</p> <p>II. Modifying user</p> <p>Removes a user from the current database.</p> <p>Syntax:</p> <p>DROP USER [ IF EXISTS ] user_name</p> <p>Example:</p> <p>DROP USER AbolrousHazem;</p> <p>GO</p> <p>To change the name of a user requires the ALTER ANY USER permission. To change the target login of a user requires the CONTROL permission on the database.</p> <p>Syntax:</p> <p><b>Rename user</b></p> <p>ALTER USER user_name</p> <p>WITH NAME new_name;</p> <p>Create login srm with password ='srm';</p> <p>Create user Robert for login srm;</p> <p>alter user srm with name=srmist;</p>	5	3	3	4	1.6.1																																	

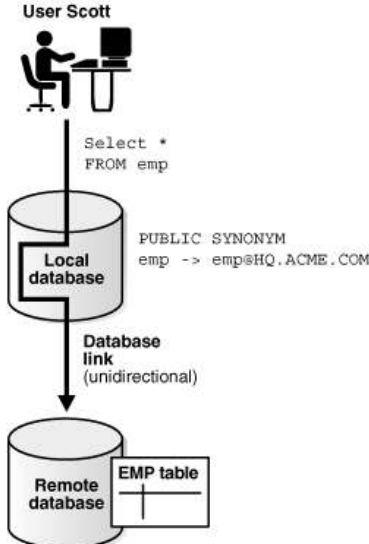
**PART – C**  
**(2 x 10 = 20 Marks)**

20.	<p>Describe the many kinds of authentication techniques used for database security.</p> <p><b>Common Authentication Techniques are</b>            Password-based Authentication            Multi-Factor Authentication            Certificate-based Authentication            Biometric Authentication            Token-based Authentication</p> <p><b>1. Password-based Authentication</b></p> <ul style="list-style-type: none"> <li>❖ Passwords are the <b>most common methods</b> of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to <b>create strong passwords</b> that include a combination of all possible options.</li> <li>❖ The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. <b>Most people use simple passwords instead of creating reliable passwords because they are easier to remember.</b></li> <li>❖ The bottom line is that <b>passwords have a lot of weaknesses and are not sufficient in protecting online information.</b> Hackers can easily guess user credentials by running through all possible combinations until they find a match.</li> </ul> <p><b>2. Multi-factor Authentication</b></p> <ul style="list-style-type: none"> <li>❖ Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include <i>codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.</i></li> <li>❖ MFA authentication methods and technologies <b>increase the confidence of users</b> by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code.</li> </ul> <p><b>3. Certificate-based Authentication</b></p> <ul style="list-style-type: none"> <li>❖ Certificate-based authentication technologies <b>identify users, machines or devices by using digital certificates.</b> A digital certificate is an electronic document based on the idea of a driver's license or a passport.</li> <li>❖ The certificate contains the digital identity of a user <b>including a public key, and the digital signature</b> of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.</li> </ul>	10	1	3	5	6.1.1
-----	---	----	---	---	---	-------



	<ul style="list-style-type: none"> <li>❖ Users provide their digital certificates when they sign in to a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.</li> </ul> <p><b>4. Biometric Authentication</b></p> <ul style="list-style-type: none"> <li>❖ Biometrics authentication is a security process that <b>relies on the unique biological characteristics of an individual</b>. Here are key advantages of using biometric authentication technologies:</li> <li>❖ Biological characteristics can be easily compared to authorized features saved in a database.</li> <li>❖ Biometric authentication can control physical access when installed on gates and doors.</li> <li>❖ You can <b>add biometrics into your multi-factor authentication process</b>.</li> </ul> <p><b>5. Token-based Authentication</b></p> <p>Token-based authentication technologies enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange. You can then use the token to access protected systems instead of entering your credentials all over again. The digital token proves that you already have access permission.</p>					
--	---	--	--	--	--	--

**OR**

21.	<p>Describe in detail the following.</p> <p>I. Database links</p> <p>A database link, is a mechanism in a database management system that <b>allows a user to access data from a remote database</b>. It creates a connection between two databases, allowing the user to query, insert, update, and delete data from the remote database as if it were a local database. This is useful when you need to access data from multiple databases, but you don't want to replicate the data in all of them.</p> 	10	1	3	4	2.2.4
-----	---	----	---	---	---	-------

To create a shared database link, use the keyword **SHARED** in the **CREATE DATABASE LINK** statement:

**Syntax:**

```
CREATE SHARED DATABASE LINK dblink_name
[CONNECT TO username IDENTIFIED BY
password][CONNECT TO CURRENT_USER]
AUTHENTICATED BY schema_name IDENTIFIED
BY password
[USING 'service_name'];
```

**Example:**

```
CREATE SHARED DATABASE LINK link2sales
CONNECT TO scott IDENTIFIED BY tiger
AUTHENTICATED BY linkuser IDENTIFIED BY
ostrich
USING 'sales';
```

**What is DB link good for?**

1. Sharing of data between two databases.
2. For import/export style purposes.
3. You can get direct access to the database of a different application.
4. For Security and Confidentiality.

**II. Linked Server**

The linked server is basically the way you defined a **'connection' between two servers**. i.e. Connecting a Database-A from Server 1 with Database-B from Server 2 and doing queries from both databases.



**Querying Data Over a SQL Server Linked Server**

To read data from a Linked Server any tables or views must be referenced using a 4-part identifier consisting of the **Linked Server name, database name, schema name, and object name** – in that order.

**For example:**

```
SELECT * FROM
[.\\SECURITY_TEST].master.sys.databases
SELECT * FROM
[.\\SECURITY_TEST].WideWorldImporters.Sales.
```

**Orders**

First the Linked Server name is provided which is [\\SECURITY\_TEST] for our example. In this example it must be bracketed due its format. Not all Linked Server names must be bracketed. Next is the database name, master and WideWorldImporters respectively. Third is the schema name, sys and Sales respectively. Lastly, the object name is listed. In these examples the objects are databases and Orders.

22.

Define the security model. Describe several database application security model types with a clear diagram.

- ❖ Security models are useful tools for evaluating and comparing security policies.
- ❖ Security models allow us **to test security policies for completeness and consistency**. They describe what mechanism are necessary to implement security policy.
- ❖ **To eliminate threats, it is necessary to define proper security policy**. Security policies are governing principles adopted by organizations.
- ❖ They capture the security requirements of an organization, specify what security properties the system must provide and describe steps an organization must take to achieve security.

**Security models are described in terms of the following elements:**

- ❖ **Subjects:** Entities that request access to objects.
- ❖ **Objects:** Entities for which access request is being made by subjects.
- ❖ **Access Modes:** Type of operation performed by subject on object (read, write, create etc.).
- ❖ **Policies:** Enterprise wide accepted security rules.
- ❖ **Authorizations:** Specification of access modes for each subject on each object.
- ❖ **Administrative Rights:** Who has rights in system administration and what responsibilities administrators have.
- ❖ **Axioms:** Basic working assumptions.

#### Access Matrix Model

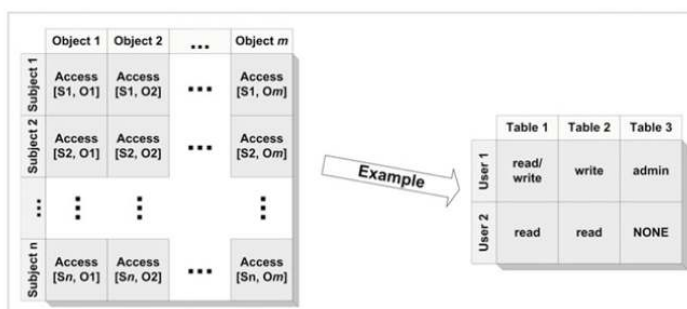
It represents two main entities

1. Objects
2. Subjects

Columns represent objects and rows represent subjects. Object can be a tables, views, procedures, database objects.

Subjects can be a users, roles, privileges, modules.

Authorization cells- Access details on the objects granted to the subject, access, operation, or commands



#### Access Modes Model

It uses objects and subjects

It specifies access modes: static and dynamic modes

10

1

4

4

6.1.1

	Access levels: A subject has access to objects at its level and all levels below it.					
<b>OR</b>						
23.	<p>Justify, how oracle helps in implementing VPD using views.</p> <p>Virtual Private Database(VPD) is the most popular secured database which was introduced by Oracle Database Enterprise. <b>It is used when the object privileges and database roles are inadequate to achieve security requirements.</b> The policies or protocols are directly proportional to security requirements.</p> <p>When a user directly or indirectly accesses a table, view, or synonym that is protected with an Oracle Virtual Private Database policy, Oracle Database dynamically modifies the SQL statement of the user. This modification creates a WHERE condition (called a predicate) returned by a function implementing the security policy. Oracle Database modifies the statement dynamically, transparently to the user, using any condition that can be expressed in or returned by a function. You can apply Oracle Virtual Private Database policies to SELECT, INSERT, UPDATE, INDEX, and DELETE statements.</p> <p>For example, suppose a user performs the following query:  SELECT * FROM OE.ORDERS;</p> <p>The Oracle Virtual Private Database policy dynamically appends the statement with a WHERE clause. For example:  SELECT * FROM OE.ORDERS WHERE SALES_REP_ID = 159;</p> <p>In this example, the user can only view orders by Sales Representative 159.</p> <p><b>Advantages of VPD</b></p> <ul style="list-style-type: none"> <li>✓ Higher Accessibility: Users can easily access the data from anywhere.</li> <li>✓ Flexibility: It can be easily modified without breaking the control flow.</li> <li>✓ Higher Recovery Rate: The data can be retrieved very easily.</li> <li>✓ Dynamically Secured: No need to maintain complex roles.</li> <li>✓ No back doors: The security policy is attached to the data so no by-passing is allowed.</li> </ul> <p><b>Dis-Advantages of VPD</b></p> <ul style="list-style-type: none"> <li>• Difficult column-level security.</li> <li>• Oracle account ID is required to use this service.</li> <li>• Hard to examine.</li> </ul> <p><b>1. First we will create the users needed for our environment</b></p> <p>a) <b>Owner of the schema</b> which will have the objects of tables</p>	10	3	4	5	1.7.1

	<p>b) <b>Security admin_user</b></p> <p>c) Non owner user or <b>user which will have limited access</b> as per data in the rows.</p> <p><u>a) <b>Owner of the schema</b> which will have the objects of tables</u></p> <p>SQL&gt; create user schemaowner identified by schemaowner</p> <p>default tablespace users temporary tablespace temp</p> <p>quota unlimited on users;</p> <p>The schema owner represents the Oracle user that owns all your database objects, while application users are Oracle users that need access to those schema objects.</p> <p><b>SQL&gt; grant connect, resource to schemaowner;</b></p> <p>grant succeeded.</p> <p>b) Create <b>Security admin_user</b></p> <p>SQL&gt; grant execute on <b>dbms_session</b> to sec_adm;</p> <p>grant succeeded.</p> <p>SQL&gt; grant execute on <b>dbms_rls</b> to sec_adm;</p> <p>grant succeeded.</p> <p>//RLS is for Row Level Security</p> <p><b>c) Create users with restricted access on table</b></p> <p>SQL&gt;create user user1 identified by <b>user1</b></p> <p>default tablespace users temporary tablespace temp;</p> <p>user created.</p> <p>SQL&gt; grant connect,resource to <b>user1;</b></p> <p>grant succeeded.</p> <p>SQL&gt; create user user2 identified by <b>user2</b></p> <p>default tablespace users temporary tablespace temp;</p> <p>user created.</p> <p>SQL&gt; grant connect,resource to <b>user2;</b></p> <p>grant succeeded</p> <p>create or replace function vpdf1(schema varchar2,object varchar2) return varchar2</p> <p>as begin</p> <p>return</p> <p>'sname=sys_context("userenv","session_user");</p> <p>end;</p> <p>/</p> <p>exec</p> <p>dbms_rls.add_policy('s_owner','emp','india','s_owner','vpdf');</p> <p>BEGIN</p> <p>dbms_rls.add_policy('s_owner','emp','india','s_owner','vpdf'); END;</p>					
--	--	--	--	--	--	--

**DEPARTMENT OF COMPUTING TECHNOLOGIES**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2023 - 2024 (ODD)**

**Test: CLA – T2**

**Date: 10-10-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 2 Hours**

**Year & Sem: IV / VII**

**Max. Marks: 50**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO3	3	-	-	-	-	-	-	-	-	-	-	-
2	CO4	3	3	-	-	-	-	-	-	-	-	-	-

**PART - A**  
**(15 x 1 = 15 Marks)**

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	Which of the following is not a privilege in SQL Server?	1	L1	3	1	1.6.1
	a) Diskadmin					
	b) Bulkadmin					
	c) Serveradmin					
	d) <b>Clientadmin</b>					
2.	This password parameter specifies the number of days before a user can reuse a password.	1	L1	3	1	1.6.1
	a) <b>PASSWORD_REUSE_TIME</b>					
	b) PASSWORD_REUSE_MAX					
	c) PASSWORD_REUSE_DAYS					
	d) PASSWORD_REUSE_MIN					
3.	When creating a DB link, which cannot be the authentication method?	1	L1	3	1	1.6.1
	a) CURRENT USER					
	b) FIXED USER					
	c) CONNECT USER					
	d) <b>DYNAMIC USER</b>					
4.	Which of the following is not an account status?	1	L1	3	1	1.6.1
	a) OPEN					
	b) <b>CLOSE</b>					
	c) EXPIRED					
	d) LOCKED					
5.	Which statement creates the same role as an external role?	1	L1	3	1	1.6.1
	a) CREATE ROLE dw_manager IDENTIFIED BY warehouse;					

	b)	CREATE ROLE warehouse_user IDENTIFIED GLOBALLY;					
	c)	<b>CREATE ROLE warehouse_user IDENTIFIED EXTERNALLY;</b>					
	d)	CREATE ROLE dw_manager IDENTIFIED LOCALLY;					
6.	When a user logs on to the DB through the machine where the DB is not located, called as _____		1	L1	3	1	1.6.1
	a)	Local user					
	b)	Internal user					
	c)	External user					
	d)	<b>Remote user</b>					
7.	Which database privilege explicitly denied SELECT and READTEXT statements?		1	L1	3	1	1.6.1
	a)	db_datareaderdenial					
	b)	db_denieddatareader					
	c)	db_denialdatareader					
	d)	<b>db_denydatareader</b>					
8.	An account that has access to the database through another database account; a virtual user is referred to in some cases as a _____		1	L1	1	1	1.6.1
	a)	Schema Owner					
	b)	Application User					
	c)	Database User					
	d)	<b>Proxy User</b>					
9.	A conceptual model that specifies the right that each subject possesses for each object is _____		1	L1	1	1	1.6.1
	a)	Static access mode					
	b)	Dynamic access mode					
	c)	<b>Access Matrix</b>					
	d)	Subject Object Matrix					
10.	The static access mode in the level 2 is _____		1	L1	1	1	1.6.1
	a)	Create					
	b)	Delete					
	c)	<b>Read</b>					
	d)	Use					
11.	The Dynamic access mode Revoke is at level _____		1	L1	1	1	1.6.1
	a)	1					
	b)	<b>2</b>					
	c)	3					
	d)	4					
12.	This component found in Client/Server architecture Contains all the codes related to data validations.		1	L1	1	1	1.6.1
	a)	User interface					
	b)	<b>Business Logic</b>					
	c)	Data Logic					
	d)	Data Access					
13.	Application server layer in the Web application architecture is found in _____						
	a)	Tier 1					

	b)	Tier 2					
	c)	<b>Tier 3</b>					
	d)	Tier 4					
14.	The _____ package is used to apply the security policy.						
	a)	<b>DBMS_RLS</b>					
	b)	RLS_DBMS					
	c)	PL/SQL					
	d)	Security_Package					
15.	This model is business-function specific						
	a)	Database Role based					
	b)	Application Role based					
	c)	<b>Application Function based</b>					
	d)	Application Table based					

<b>PART – B</b> <b>(3 x 5 = 15 Marks)</b> <b>Instructions: Answer any 3 Questions</b>						
16.	<p>Brief about the creation and dropping a role in ORACLE.</p> <ul style="list-style-type: none"> <li>The following statement creates the role dw_manager: <pre>CREATE ROLE dw_manager;</pre> <li>You can add a layer of security to roles by specifying a password, as in the following example: <pre>CREATE ROLE dw_manager IDENTIFIED BY warehouse;</pre> <li>The following statement creates global role warehouse_user: <pre>CREATE ROLE warehouse_user IDENTIFIED GLOBALLY;</pre> <li>The following statement creates the same role as an external role: <pre>CREATE ROLE warehouse_user IDENTIFIED EXTERNALLY;</pre> <p>To drop the role dw_manager, issue the following statement</p> <ul style="list-style-type: none"> <li>DROP ROLE dw_manager;</li> </ul> </li></li></li></li></ul>	5	L3	3	1	1.6.1
17.	<p>Brief about the creation of a SQL server User.</p> <ul style="list-style-type: none"> <li>To create a login id in SQL server can be member of SYSTEMADMIN OR SECURITYADMIN</li> </ul>	5	L3	3	1	1.6.1

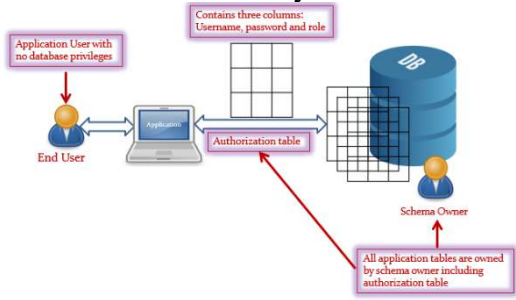
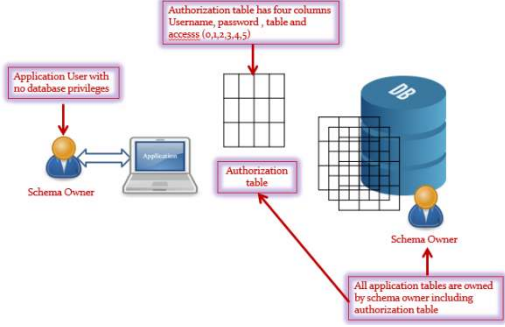


	<ul style="list-style-type: none"> <li>• There are two types of login IDs: <ul style="list-style-type: none"> <li>○ Windows Integrated (Trusted) Logins</li> <li>○ User can associate a Microsoft Windows account or group with either the server in which SQL Server is installed or the domain in which the server is a member</li> <li>○ SQL Server Login</li> </ul> </li> </ul>					
18.	<p>Briefly explain about the different Application Types.</p> <ul style="list-style-type: none"> <li>○ Mainframe applications</li> <li>○ Client / Server Applications</li> <li>○ Web Applications</li> <li>○ Data warehouse applications</li> </ul>	5	L3	4	1	1.6.1
19.	<p>Briefly about the Column level Security with SQL Server.</p> <p>Column level Security with SQL Server</p> <ul style="list-style-type: none"> <li>✓ Column level permissions provide a more granular level of security for data in your database. You do not need to execute a separate GRANT or DENY statements for each column; just name them all in a query:</li> </ul> <pre>GRANT SELECT ON data1.table (column1, column2) TO user1;  GO  DENY SELECT ON data1.table (column3) TO user1;  GO</pre> <ul style="list-style-type: none"> <li>✓ If you execute a DENY statement at table level to a column for a user, and after that you execute a GRANT statement on the same column, the DENY permission is removed and the user can have access to that column. Similarly, if you execute GRANT and then DENY, the DENY permission will be in force.</li> </ul>	5	L3	4	1	1.6.1

**PART – C**

**(2 x 10 = 20 Marks)**

**Instructions: Answer all the Questions**

20.	<p>a) Explain the architecture of security data model based on Application roles.</p> <ul style="list-style-type: none"> <li>Architecture of Security model</li> </ul>  <ul style="list-style-type: none"> <li>Characteristics</li> </ul> <p style="text-align: center;"><b>OR</b></p>	10	L3	3	1	1.6.1
21.	<p>b) Elaborate on the different Application Tables.</p> <ul style="list-style-type: none"> <li>Architecture of Security model</li> </ul>  <ul style="list-style-type: none"> <li>Characteristics</li> </ul>	10	L3	3	1	1.6.1
22.	<p>a) Elaborate on the creation of Profiles in ORACLE.</p> <ul style="list-style-type: none"> <li>✓ Define a Profile</li> <li>✓ Resource parameters</li> <li>✓ Password parameters</li> <li>✓ Setting Profile Resource Limits</li> <li>✓ Modify a limit for Profile</li> <li>✓ Assign a profile</li> </ul>	✓	L3	4	2	1.6.1
23.	<p style="text-align: center;"><b>OR</b></p> <p>b) Define a Database Link. Discuss the different ways of creating the Database Links. Explain the different methods of creating a Database Link.</p> <ul style="list-style-type: none"> <li>○ It is a connection from one DB to another DB</li> </ul> <p>The linked DBs can be like</p>					

	<ul style="list-style-type: none"> <li>○ Both be ORACLE10g</li> <li>○ Both be SQL Server</li> <li>○ Mix of ORACLE10g and SQL Server</li> </ul> <p>A DB link enables a user to perform Data Manipulation Language (DML) or any other valid SQL statements on a DB.</p> <p>In Oracle 10g ,DB Links can be created in two ways as</p> <ul style="list-style-type: none"> <li>○ 1. Public – Which makes the database links accessible by every user in DB</li> <li>○ 2.Private – Which gives the ownership of the database to a user</li> <li>○ The DB is not accessible by any other user unless the user has been access by the owner</li> <li>○ Authentication Method 1: CURRENT USER <ul style="list-style-type: none"> <li>○ This authentication method orders ORACLE10g to use the current user credentials for authentication to the DB to which the user is trying to link.</li> </ul> </li> <li>○ Authentication Method 2: FIXED USER <ul style="list-style-type: none"> <li>○ This authentication method orders ORACLE10g to use the user password provided in this clause for authentication to the DB to which the user is trying to link.</li> </ul> </li> <li>○ Authentication Method 3: CONNECT USER <ul style="list-style-type: none"> <li>○ This authentication method orders ORACLE10g to use credentials of the connected user who has an existing account in the database to which the user is trying to link.</li> </ul> </li> </ul>		L3	4	2	1.6.1
--	---	--	----	---	---	-------

**Test: CLA 2**

**Date: 10-10-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 1 Hour 40 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 50**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO3	1	-	1	2	2	1	-	-	-	-	-	-
2	CO4	1	-	3	1	1	1	-	-	-	-	-	-

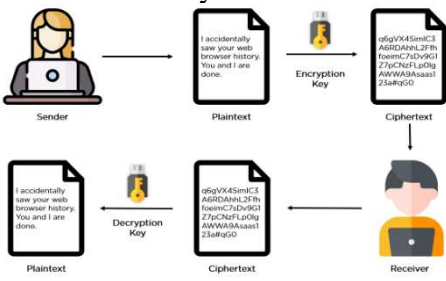
<div><div>PART - A</div><div>Instructions: Answer all (15 x 1 = 15 Marks)</div></div>							
Q. No	Questions		Marks	BL	CO	PO	PI Code
1.	External name for_____authenticated user.		1	1	3	4,5	1.3.1
	A	Global					
	B	Drop					
	C	Expire					
	D	Private					
2.	User which interact with the system using database query language is called as		1	1	4	3	1.3.1
	A	Application Programmer					
	B	Sophisticated User					
	C	Specialized User					
	D	Naive User					
3.	_____ is the indication of how long a password can be used before it expires.		1	1	3	4,5	1.3.1
	A	Password Complexity					
	B	Password storage					
	C	Password Usage					
	D	Password Aging					
4.	Command that comes under DCL is/are -		1	1	3	4,5	1.3.1
	A	grant					
	B	revoke					
	C	Both A & B					
	D	None of the above					
5.	..... is level 3 access mode in static mode?		1	1	4	3	1.3.1
	A	update					
	B	use					
	C	grant					
	D	delete					
6.	Which command used to give privileges to oracle user?		1	1	3	4,5	1.3.1
	A	grant					
	B	revoke					
	C	expire					

	D	identify					
7.		Virtual private database is a function of	1	1	4	3	1.3.1
	A	Java					
	B	Oracle					
	C	SQL					
	D	DB2					
8.		What is general syntax to create user in oracle?	1	1	3	4,5	1.3.1
	A	create user <username> identified by					
	B	create user <user> identified by <password>;					
	C	create user <username> identified by <password>;					
	D	create user <username> <password>;					
9.		Row and Column access can be implemented by using the database object.	1	1	4	3	1.3.1
	A	Edit					
	B	View					
	C	Delete					
	D	Drag					
10.		Which user plays a super role that allows assigned user to perform any task within SQL SERVER?	1	1	3	4,5	1.3.1
	A	SYSADMIN					
	B	ADMIN					
	C	SYSSERVER					
	D	SQLSERVER					
11		Which among the following is not included in virtual private database?	1	1	4	3	1.3.1
	A	Setup Test Environment					
	B	Create an Application Context					
	C	Create Security Policies					
	D	Documentation in administration					
12		.....command is used to drop a user who owns objects?	1	1	3	4,5	1.3.1
	A	CASCADE					
	B	DROP					
	C	GRANT					
	D	DELETE					
13		What does the following code snippet do? Delete from students where age=15; Rollback;	1	1	3	4,5	1.3.1
	A	Performs an undo operation on the delete operation					
	B	Delete the rows from the table where age=15					
	C	Deletes the entire table					
	D	None of the above					
14		Schema definition is written by	1	1	4	3	1.3.1
	A	Database administrator					
	B	Application programmer					
	C	Sophisticated user					
	D	Naïve user					
15		Business layer level ..... layer contains a program that implements business rules in web application architecture?	1	1	3	4,5	1.3.1
	A	Application layer					
	B	Web application					
	C	Business logic layer					
	D	Service oriented					

**PART – B**  
(3 x 5 = 15 Marks)

**Instructions: Answer any 3 Questions**

16.	<p>Explain the process of granting and revoking privileges in oracle/sql server.</p> <p>We can GRANT and REVOKE privileges <b>on various database objects (Table, View)</b> in SQL Server.</p> <p>Data Control Language is used to control privileges in Databases. In Data Control Language we have two commands.</p> <p><b>GRANT:-</b> GRANT command is used to provide access or privileges on the database.</p> <p><b>REVOKE:-</b> REVOKE command removes user access rights or privileges to the database objects.</p> <p>You can grant users various privileges to tables. These permissions can be any combination of SELECT, INSERT, UPDATE, DELETE, REFERENCES, ALTER, or ALL.</p> <p>Example: GRANT SELECT, INSERT, UPDATE, DELETE ON employees TO student; GRANT <b>ALL</b> ON employees TO student; REVOKE <b>DELETE</b> ON <b>employees</b> FROM <b>student</b>;</p>	5	3	3	4,5	1.6.1
17.	<p>Discuss the many components of the database security model.</p> <p><b>Security models are described in terms of the following elements:</b></p> <ul style="list-style-type: none"> <li>❖ <b>Subjects:</b> Entities that request access to objects.</li> <li>❖ <b>Objects:</b> Entities for which access request is being made by subjects.</li> <li>❖ <b>Access Modes:</b> Type of operation performed by subject on object (read, write, create etc.).</li> <li>❖ <b>Policies:</b> Enterprise wide accepted security rules.</li> <li>❖ <b>Authorizations:</b> Specification of access modes for each subject on each object.</li> <li>❖ <b>Administrative Rights:</b> Who has rights in system administration and what responsibilities administrators have.</li> <li>❖ <b>Axioms:</b> Basic working assumptions.</li> </ul>	5	1	4	3	1.6.1
18.	<p>Write notes on the creation, assignment, and withdrawal of user roles in oracle/sql server.</p> <p>Roles are a <b>collection of privileges or access rights</b>.</p> <p>When there are many users in a database it becomes difficult to grant or revoke privileges to users. Therefore, if you define roles, you can grant or revoke privileges to users, thereby automatically granting or revoking privileges. You can either create Roles or use the system roles pre-defined by oracle.</p> <p><b>Syntax:</b> CREATE ROLE role_name</p>	5	1	3	4,5	1.6.1

	<p>[IDENTIFIED BY password];</p> <p>CREATE ROLE testing</p> <p>Second, <b>grant a CREATE TABLE privilege to the ROLE testing.</b> You can add more privileges to the ROLE.</p> <p>GRANT CREATE TABLE TO testing;</p> <p><b>Third, grant the role to a user.</b></p> <p>GRANT testing TO user1;</p> <p><b>To revoke a CREATE TABLE privilege from testing ROLE, you can write:</b></p> <p><b>REVOKE CREATE TABLE FROM testing;</b></p> <p><b>The Syntax to drop a role from the database is as below:</b></p> <p>DROP ROLE role_name;</p> <p><b>For example: To drop a role</b> called developer, you can write:</p> <p>DROP ROLE testing;</p>					
19.	<p>Explain in detail data encryption.</p> <p>Data encryption is a method of protecting data by encoding it in such a way that it can only be decrypted or accessed by an individual who holds the correct encryption key. When a person or entity accesses encrypted data without permission, it appears scrambled or unreadable.</p> <p><b>How does data encryption work?</b></p> <p>The data that needs to be encrypted is termed plaintext or clear text. The plaintext needs to be passed via some encryption algorithms, which are mathematical calculations to be done on raw information. There are multiple encryption algorithms, each of which differs by application and security index.</p>  <p>Apart from the algorithms, one also needs an encryption key. Using said key and a suitable encryption algorithm, the plaintext is converted into the encrypted piece of data, also known as cipher text. Instead of sending the plaintext to the receiver, the cipher text is sent through insecure channels of communication.</p> <p>Once the cipher text reaches the intended receiver, he/she can use a decryption key to convert the cipher text back to its original readable format i.e. plaintext. This decryption key must be kept secret at all times, and may or not be similar to the key used for encrypting the message.</p>	5	1	4	3	1.6.1

**PART – C**  
**(2 x 10 = 20 Marks)**

20.	<p>Explain the following with an appropriate query</p> <ol style="list-style-type: none"> <li>1. Create a user (for example, HOD with administrative privileges).</li> <li>2. Create a user (for example, a student with limited privileges).</li> <li>3. Create a table with the following fields: Name, Rollno (primary key), Gender, Department, and Mobile Number (HOD login).</li> <li>4. Put in five records</li> <li>5. Delegate select, update privileges from the HOD to a Student.</li> <li>6. Revoke the student's privileges</li> </ol> <p><b>Answer:</b> <b>Create two users</b></p> <ol style="list-style-type: none"> <li>1. HOD</li> <li>2. Student</li> </ol> <p>Connect /as sysdba; Show user; <b><u>Create a user (for example, HOD with administrative privileges).</u></b> Create user HOD identified by HOD; Grant dba,resource to HOD; <b><u>Create a user (for example, a student with limited privileges).</u></b> Create user student identified by student; Grant create session to student; <b><u>Create a table with the following fields: Name, Rollno (primary key), Gender, Department, and Mobile Number (HOD login).</u></b> Connect HOD/HOD; Create table student(name varchar2(15), rollno number(4) primary key, gender varchar2(15), dept varchar2(15), mob_no number(10)); //Insert 5 records Insert into student values ( '&amp;name',&amp;rollno,'&amp;gender','&amp;dept',&amp;mob_no); Select * from student; //It will list all the records from the table. <b><u>Delegate select, update privileges from the HOD to a Student.</u></b> Grant select,update on student to student; <b><u>Revoke the student's privileges</u></b> Revoke select, update on student from student;</p>	10	3	3	4	1.7.1
<b>OR</b>						
21.	<p>What is virtual private database? How can it be implemented on oracle? What are the policies involved?</p> <p>Virtual Private Database(VPD) is the most popular secured database which was introduced by Oracle Database Enterprise. <b>It is used when the object privileges and database roles are inadequate to</b></p>	10	3	4	3	1.7.1



**achieve security requirements.** The policies or protocols are directly proportional to security requirements.

When a user directly or indirectly accesses a table, view, or synonym that is protected with an Oracle Virtual Private Database policy, Oracle Database dynamically modifies the SQL statement of the user. This modification creates a WHERE condition (called a predicate) returned by a function implementing the security policy. Oracle Database modifies the statement dynamically, transparently to the user, using any condition that can be expressed in or returned by a function. You can apply Oracle Virtual Private Database policies to SELECT, INSERT, UPDATE, INDEX, and DELETE statements.

For example, suppose a user performs the following query:

```
SELECT * FROM OE.ORDERS;
```

The Oracle Virtual Private Database policy dynamically appends the statement with a WHERE clause. For example:

```
SELECT * FROM OE.ORDERS WHERE  
SALES_REP_ID = 159;
```

In this example, the user can only view orders by Sales Representative 159.

#### **Advantages of VPD**

- ✓ Higher Accessibility: Users can easily access the data from anywhere.
- ✓ Flexibility: It can be easily modified without breaking the control flow.
- ✓ Higher Recovery Rate: The data can be retrieved very easily.
- ✓ Dynamically Secured: No need to maintain complex roles.
- ✓ No back doors: The security policy is attached to the data so no by-passing is allowed.

#### **Dis-Advantages of VPD**

- Difficult column-level security.
- Oracle account ID is required to use this service.
- Hard to examine.

#### **1. First we will create the users needed for our environment**

a) **Owner of the schema** which will have the objects of tables

b) **Security admin\_user**

c) Non owner user or **user which will have limited access** as per data in the rows.

a) **Owner of the schema** which will have the objects of tables

```
SQL> create user schemaowner identified by  
schemaowner
```

```
default tablespace users temporary tablespace temp  
quota unlimited on users;
```

	<p>The schema owner represents the Oracle user that owns all your database objects, while application users are Oracle users that need access to those schema objects.</p> <p><b>SQL&gt; grant connect, resource to schemaowner;</b> grant succeeded.</p> <p>b) Create <b>Security admin_user</b></p> <p>SQL&gt; grant execute on <b>dbms_session</b> to sec_adm; grant succeeded.</p> <p>SQL&gt; grant execute on <b>dbms_rls</b> to sec_adm; grant succeeded.</p> <p>//RLS is for Row Level Security</p> <p>c) <b>Create users with restricted access on table</b></p> <p>SQL&gt; create user user1 identified by <b>user1</b> default tablespace users temporary tablespace temp; user created.</p> <p>SQL&gt; grant connect,resource to <b>user1</b>; grant succeeded.</p> <p>SQL&gt; create user user2 identified by <b>user2</b> default tablespace users temporary tablespace temp; user created.</p> <p>SQL&gt; grant connect,resource to <b>user2</b>; grant succeeded</p> <p>create or replace function vpdf1(schema varchar2,object varchar2) return varchar2 as begin return 'sname=sys_context("userenv","session_user"); end; / exec dbms_rls.add_policy('s_owner','emp','india','s_owner','v pdf'); BEGIN dbms_rls.add_policy('s_owner','emp','india','s_owner','v pdf'); END;</p>					
22.	<p>Describe in detail the creation and application of password policies.</p> <p><b>Definition-Password Policies:</b> A password policy is a <b>set of rules</b> designed to enhance computer security by encouraging users to create and implement stronger passwords.</p> <p><b>Why is a password policy important?</b> There are significant benefits to having a well-designed password policy.</p> <ul style="list-style-type: none"> <li>✓ <b>Prevent Data Breaches</b> (Safeguarding your business' data and customer details is paramount.)</li> <li>✓ <b>Maintain Order</b> (A password policy is meant for everyone using your network, regardless of their status. )</li> <li>✓ <b>Build Trust</b></li> <li>✓ <b>Cultivate Cybersecurity Culture</b></li> </ul>	10	2,3	3	4	6.1.1

**What are the most crucial components of a Password policy?**

1. **Password Strength-** Password strength refers to the nature of your password. The more complex your password is, the stronger it is.
2. **Password Expiry-** Having an expiry date for passwords encourages users to change their passwords regularly.
3. **Password History-** Program your system to save previously used passwords in users' password history and restrict them from reusing those passwords.

**Password Change-** Users should have the freedom to change their passwords at any time

**Implementing a Password Policy**

**1. Identifying Settings Related to Password Policies**

There are, at the most basic level, five settings you can configure that relate to password characteristics: Enforce password history, Maximum password age, Minimum password age, Minimum password length, and Passwords must meet complexity requirements.

**Enforce password history** determines the number of unique new passwords a user must use before an old password can be reused. The value of this setting can be between 0 and 24; if this value is set to 0, enforce password history is disabled.

**Maximum password age** determines how many days a password can be used before the user is required to change it. The value of this is between 0 and 999; if it is set to 0, passwords never expire. Setting this value too low can cause frustration for your users; setting it too high or disabling it gives potential attackers more time to determine passwords.

**Minimum password age** determines how many days a user must keep new passwords before they can change them. This setting is designed to work with the Enforce password history setting so that users cannot quickly reset their passwords the required number of times and then change back to their old passwords. The value of this setting can be between 0 and 999; if it is set to 0, users can immediately change new passwords.

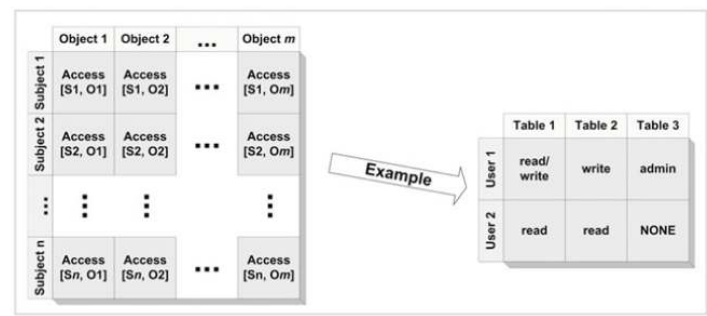
**Minimum password length** determines how short passwords can be.

Passwords must meet complexity requirements determines whether password complexity is enforced. If this setting is enabled, user passwords meet the following requirements:

1. The password is at least **six characters** long.
2. The password contains characters from at least three of the following four categories:
  - ❖ English uppercase characters (**A – Z**)
  - ❖ English lowercase characters (**a – z**)
  - ❖ Base 10 digits (**0 – 9**)

	<p>❖ Non-alphanumeric (For example: !, \$, #, or %)</p> <p><b>Some other important factors to create and implement password policy are</b></p> <ol style="list-style-type: none"> <li>Limit login time</li> <li>Send Email notification</li> <li>Be impersonal</li> <li><b>Avoid repetitive or sequential characters</b> like 111111 or abcd1234</li> <li>Implement multi-factor authentication</li> <li>Prohibit login sharing</li> <li>Use a password generator</li> <li>Use an encrypted database to manage passwords</li> <li>Reset administrators passwords periodically</li> <li>Use unique, randomly generated passwords</li> </ol>					
<b>OR</b>						
23.	<p>Define the security model. Describe several database application security model types with a clear diagram.</p> <ul style="list-style-type: none"> <li>❖ Security models are useful tools for evaluating and comparing security policies.</li> <li>❖ Security models allow us <b>to test security policies for completeness and consistency</b>. They describe what mechanism are necessary to implement security policy.</li> <li>❖ <b>To eliminate threats, it is necessary to define proper security policy</b>. Security policies are governing principles adopted by organizations.</li> <li>❖ They capture the security requirements of an organization, specify what security properties the system must provide and describe steps an organization must take to achieve security.</li> </ul> <p><b>Security models are described in terms of the following elements:</b></p> <ul style="list-style-type: none"> <li>❖ <b>Subjects:</b> Entities that request access to objects.</li> <li>❖ <b>Objects:</b> Entities for which access request is being made by subjects.</li> <li>❖ <b>Access Modes:</b> Type of operation performed by subject on object (read, write, create etc.).</li> <li>❖ <b>Policies:</b> Enterprise wide accepted security rules.</li> <li>❖ <b>Authorizations:</b> Specification of access modes for each subject on each object.</li> <li>❖ <b>Administrative Rights:</b> Who has rights in system administration and what responsibilities administrators have.</li> <li>❖ <b>Axioms:</b> Basic working assumptions.</li> </ul> <p><b>Access Matrix Model</b></p> <p>It represents two main entities</p> <ol style="list-style-type: none"> <li>Objects</li> <li>Subjects</li> </ol> <p>Columns represent objects and rows represent subjects. Object can be a tables, views, procedures, database</p>	10	1	4	4	6.1.1

objects.  
Subjects can be a users, roles, privileges, modules.  
Authorization cells- Access details on the objects  
granted to the subject, access, operation, or commands



**Access Modes Model**

It uses objects and subjects  
It specifies access modes: static and dynamic modes  
Access levels: A subject has access to objects at its  
level and all levels below it.

**DEPARTMENT OF COMPUTING TECHNOLOGIES**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2023 - 2024 (ODD)**

**Test: CLA - T1**

**Date: 06-10-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 2 Hours**

**Year & Sem: IV / VII**

**Max. Marks: 50**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO3	3	-	-	-	-	-	-	-	-	-	-	-
2	CO4	3	3	-	-	-	-	-	-	-	-	-	-

**PART - A**

**(15 x 1 = 15 Marks)**

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	----- software program residing on a computer that is used for data processing and for interfacing to the business logic and database server.	1	L1	3	1	1.6.1
	a) Database server layer					
	b) Business logic layer					
	c) Web browser layer					
	<b>d) Web server layer</b>					
2.	In these which one is used to enable the user to connect to the database	1	L1	3	1	1.6.1
	a) GRANT SESSION TO EXTERNAL_USER					
	b) GRANT SESSION IDENTIFIED BY EXTERNAL_USER					
	<b>c) GRANT CREATE SESSION TO EXTERNAL_USER</b>					
	d) GRANT CREATE USER TO EXTERNAL_SESSION					
3.	----- clause of CREATE USER statement specifies the storage of the user.	1	L1	3	1	1.6.1
	a) TEMPORARY TABLESPACE					
	<b>b) DEFAULT TABLESPACE</b>					
	c) QUOTA					
	d) PROFILE					
4.	----- clause of CREATE USER statement informs oracle of how much space a user is allowed for a specified tablespace.	1	L1	3	1	1.6.1
	a) TEMPORARY TABLESPACE					

	b)	DEFAULT TABLESPACE					
	c)	<b>QUOTA</b>					
	d)	PROFILE					
5.	Which of the following does not specify the authentication type?		1	L1	3	1	1.6.1
	a)	EXTERNAL - CREATE USER user1 IDENTIFIED EXTERNALLY;					
	b)	<b>INTERNAL - CREATE USER user1 IDENTIFIED INTERNALLY;</b>					
	c)	GLOBAL - CREATE USER user2 IDENTIFIED GLOBALLY;					
	d)	PASSWORD - CREATE USER user3 IDENTIFIED BY user3;					
6.	When a user logs on to the DB through the machine where the DB is located, called as _____		1	L1	3	1	1.6.1
	a)	<b>Local user</b>					
	b)	Internal user					
	c)	External user					
	d)	Remote user					
7.	Which of the following is not the level of permission in SQL server?		1	L1	3	1	1.6.1
	a)	System or Server level					
	b)	Database level					
	c)	Table (Object) level					
	d)	<b>Row level</b>					
8.	The access mode abrogate occupies the level		1	L1	1	1	1.6.1
	a)	1					
	b)	<b>2</b>					
	c)	3					
	d)	4					
9.	Which component is not found in Client/Server architecture?		1	L1	1	1	1.6.1
	a)	User interface					
	b)	Business Logic					
	c)	<b>Object Access</b>					
	d)	Data Access					
10.	Which of the software program residing on a computer that Is used for data processing?		1	L1	1	1	1.6.1
	a)	Web server layer					
	b)	Database server layer					
	c)	Business logic layer					
	d)	<b>Application server layer</b>					
11.	This model is flexible in implementing application security.		1	L1	1	1	1.6.1
	a)	Application Role based					
	b)	Application Function Based					
	c)	<b>Application Role and Function Based</b>					
	d)	Application Table Based					
12.	In this model Maintenance of application security does not require specific DB privileges		1	L1	1	1	1.6.1
	a)	Application Role based					
	b)	Application Function Based					

	c)	<b>Application Role and Function Based</b>					
	d)	Application Table Based					
<b>13.</b>	This model uses real database user to log on						
	a)	<b>Database Role based</b>					
	b)	Application Role based					
	c)	Application Function Based					
	d)	Application Role and Function Based					
<b>14.</b>	The static access mode Create is at Level _____						
	a)	1					
	b)	2					
	c)	3					
	d)	<b>4</b>					
<b>15.</b>	This control column Contains the username that created the record or last updated the record.						
	a)	CTL_INS_USERS					
	b)	CTL_INS_DTIM					
	c)	CTL_REC_USERS					
	d)	<b>CTL_UPD_USERS</b>					

<b>PART – B</b> <b>(3 x 5 = 15 Marks)</b>						
<b>Instructions: Answer any 3 Questions</b>						
16.	List out the best practices for Administrators and Managers. <ul style="list-style-type: none"> <li>Follow you company ‘s procedures and policies to create , remove or modify database users.</li> <li>Always change the default password and never write it, or save it in a file that neither encrypted nor safe.</li> <li>Never share the user accounts with anyone , especially DBA accounts.</li> <li>Always document and create logs for</li> </ul>	5	L3	3	1	1.6.1



	<p>changes to removals of database user accounts.</p> <ul style="list-style-type: none"> <li>▪ Never remove an account even if it is out dated, Instead <u>disable or revoke</u> connections privileges of the account.</li> <li>▪ Give <u>access permission</u> to users only as required and use different logins and passwords for different applications.</li> <li>▪ <u>Educate</u> users, developers and administrators on user administration best practices as well as the <u>company policies and procedures</u>.</li> <li>▪ Keep abreast (up-to date) of database and security technology. Should be <u>aware of all new vulnerabilities</u> that may increase database security risks.</li> <li>▪ <u>Constantly review and modify the procedures</u> as necessary to be in line up with the company's policies and procedures. Keep procedures up to date with the dynamic nature of database and security technology</li> </ul>					
17	<p>Brief about the creation of an Oracle user.</p> <ul style="list-style-type: none"> <li>• User</li> <li>• IDENTIFIED clause</li> <li>• BY Password</li> <li>• EXTERNALLY clause</li> <li>• AS '<i>certificate_DN</i>'</li> <li>• GLOBALLY Clause</li> <li>• DEFAULT TABLESPACE Clause</li> <li>• TEMPORARY TABLESPACE Clause</li> <li>• QUOTA Clause</li> <li>• PASSWORD EXPIRE Clause</li> <li>• ACCOUNT Clause</li> </ul>	5	L3	3	1	1.6.1
18.	<p>Briefly explain about the Access matrix model and Access Modes model.</p> <p style="text-align: center;">✓ Access Matrix Model</p> <ul style="list-style-type: none"> <li>▪ A conceptual model that specifies the right that each subject</li> </ul>	5	L3	4	1	1.6.1

	<ul style="list-style-type: none"> <li>▪ possesses for each object</li> <li>▪ Subjects in rows and objects in columns</li> </ul> <p>Access Modes Model</p> <ul style="list-style-type: none"> <li>✓ This model based on the Take-Grant models</li> <li>✓ It uses both subject and object</li> <li>✓ Object is the main security entity</li> <li>✓ Access mode indicates that the subject can perform any task or not</li> <li>✓ There are two modes <ul style="list-style-type: none"> <li>▪ Static Modes</li> <li>▪ Dynamic Modes</li> </ul> </li> </ul>					
19.	<p>Briefly explain the architecture of Virtual Private Databases.</p> <p>The diagram illustrates the VPD architecture. A user submits a query 'SELECT * FROM PRODUCTS'. The VPD policy automatically adds a WHERE clause predicate 'Deptid = 20'. The query is rewritten to 'SELECT * FROM PRODUCTS WHERE DEPTID = 20' and executed against the EMP Table. The diagram also shows the DBMS_RLS Package, a Schema Owner, and a Policy Function.</p>	5	L3	4	1	1.6.1

### **PART – C**

**(2 x 10 = 20 Marks)**

**Instructions: Answer all the Questions**

20.	<p>a) Explain the architecture of security data model based on database roles.</p> <ul style="list-style-type: none"> <li>• Control columns and description</li> <li>• Architecture of a security data model based on database roles</li> <li>• Implementation in ORACLE</li> <li>• Creating Application Owner</li> <li>• Creating Proxy User</li> <li>• Creating Application Tables</li> <li>• Creating Application roles</li> <li>• Assigning grants</li> <li>• Add rows to the table</li> <li>• Add a row for an application user</li> <li>• Activate the role</li> <li>• Implementation in SQL server</li> <li>• Creating Application Roles using the command line</li> <li>• Dropping Application Roles</li> </ul>	10	L3	3	1	1.6.1
	<b>OR</b>					
21	<p>b) Elaborate on the different Application types.</p> <ul style="list-style-type: none"> <li>• Mainframe applications</li> <li>• Client / Server Applications</li> <li>• Web Applications</li> <li>• Data warehouse applications</li> </ul>	10	L3	3	1	1.6.1
22	<p>a) Elaborate on the Granting and Revoking of User Privileges &amp; Roles.</p> <ul style="list-style-type: none"> <li>• System Privileges</li> <li>• Object privileges</li> <li>• SQL Grant</li> <li>• SQL revoke</li> <li>• Privileges in SQL Server</li> <li>• Server privileges</li> <li>• Database privileges</li> <li>• Creating role with ORACLE</li> <li>• Assigning role to user</li> </ul>	10	L3	4	2	1.6.1

23..	<ul style="list-style-type: none"> <li>• Create Roles</li> <li>• Dropping a role</li> </ul> <p style="text-align: center;"><b>OR</b></p> <p>b) Give the importance of password policies. Explain in detail about the design and implementation of password policies.</p> <ul style="list-style-type: none"> <li>• Importance of Password Policies <ul style="list-style-type: none"> <li>○ The frontline defence of your account is your password.</li> <li>○ If your password is weak, the hacker can break in, destroy your data, and violate your sense of security .</li> <li>○ For this specific reason, most of the companies invest considerable resources to strengthen authentication by adopting technological measures that protect their assets.</li> </ul> </li> <li>• Guidelines</li> <li>• Password policies in oracle</li> <li>• Password security parameters</li> <li>• NTLM</li> <li>• Kerberos</li> </ul>	10	L3	4	2	1.6.1
------	--	----	----	---	---	-------

**Test: CLA3**

**Date: 02-11-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 1 Hour 40 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 50**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO4	3	2	2	-	-	-	-	-	-	-	-	-
2	CO5	2	2	2	-	-	-	-	-	-	-	-	-

**PART - A**  
**(15 x 1 = 15 Marks)**

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	Auditing is the responsibility of -----	1	1	4	4,5	1.3.1
	a) Developers					
	b) DBA					
	c) Business Managers					
	d) All of the Above					
2.	A document that contains all activities that are being audited ordered in a chronological manner	1	1	4	4,5	1.3.1
	a) Auditing					
	b) Audit objectives					
	c) Audit log					
	d) None of the Above					
3.	A chronological record of database activities , such as shutdown, start-up, logons, and data structure changes of database objects	1	1	4	4,5	1.3.1
	a) Data audit					
	b) Database auditing					
	c) Audit report					
	d) Audit procedure					
4.	Identify the Components of Auditing Environment	1	1	4	3	1.3.1
	a) Objectives & Procedures					
	b) People & Audited Entries					
	c) None of the Above					
	d) All of the Above					
5.	The first auditing model is called -----because it is easy to understand and develop	1	1	4	3	1.3.1
	a) User Friendly					
	b) Simple					
	c) Flexibility					
	d) Effective					
6.	The National Security Administration has given a C2 security rating to	1	1	4	3	1.3.1
	a) Microsoft SQL Server 2000					
	b) MY SQL					
	c) ORACLE 10G					

	d)	MONGO DB					
7.	The _____ triggers will be fired before the INSERT, UPDATE, or DELETE operation		1	1	4	4,5	1.3.1
	a)	Delete					
	b)	Update					
	c)	Insert					
	d)	All of the Above					
8.	What is the syntax of DROP TRIGGER statement?		1	1	4	4,5	1.3.1
	a)	DELETE TRIGGER trigger_name;					
	b)	REMOVE TRIGGER trigger_name;					
	c)	DROP TRIGGER trigger_name;					
	d)	None of the Above					
9.	PPDM means		1	1	5	4,5	1.3.1
	a)	Privacy preserving data mining					
	b)	Privacy producing data mining					
	c)	Privacy preserving data modeling					
	d)	Privacy producing data modeling					
10.	In which method noise is added to data		1	1	5	4,5	1.3.1
	a)	The randomization method					
	b)	The k-anonymity model and l-diversity					
	c)	Distributed privacy preservation					
	d)	Downgrading Application Effectiveness					
11	The values across different records are swapped in order to perform the privacy-preservation in		1	1	5	4,5	1.3.1
	a)	Data mapping					
	b)	Data swapping					
	c)	Data swapping and mapping					
	d)	Data ordering					
12	K-anonymity techniques uses		1	1	5	3	1.3.1
	a)	Generalization					
	b)	Suppression					
	c)	Generalization and suppression					
	d)	Randomization					
13	The individual records are spread out across multiple entities, each of which have the same set of attributes are in		1	1	5	3	1.3.1
	a)	Vertically partitioned					
	b)	Horizontally partitioned					
	c)	Diagonally partitioned					
	d)	Randomly partitioned					
14	In association rule hiding if the entry for a given transaction is modified to a different value then it is called as		1	1	5	4,5	1.3.1
	a)	Blocking					
	b)	Aborting					
	c)	Distortion					
	d)	Hiding					
15	Which one is not suitable for k-anonymity techniques uses in		1	1	5	3	1.3.1
	a)	Generalization					
	b)	Suppression					
	c)	Generalization and suppression					
	d)	Randomization					

**PART – B**  
**(3 x 5 = 15 Marks)**

**Instructions: Answer any 3 Questions**

Q. No	Questions	Marks	BL	CO	PO	PI Code
16.	<p><b>Describe the need of auditing database? In what are the ways it can be audited?</b></p> <p>Auditing a database is a critical aspect of maintaining data security, integrity, and compliance. There are several reasons why auditing a database is necessary:</p> <ol style="list-style-type: none"><li>1.Data Security: Auditing helps in identifying unauthorized access to the database. It can track who accessed the data, what changes were made, and when those changes occurred. This is essential for detecting and preventing security breaches and data leaks.</li><li>2. Compliance: Many industries and organizations are subject to regulatory requirements, such as HIPAA in healthcare, GDPR in Europe, or SOX for publicly traded companies. Auditing databases is crucial to demonstrate compliance with these regulations by providing an audit trail of data access and changes.</li><li>3.Data Integrity: Auditing ensures the integrity of the data by monitoring changes and helping to prevent data corruption or fraudulent activities.</li><li>4. Troubleshooting and Debugging: Auditing can be helpful for diagnosing and resolving issues within the database. It allows administrators to trace problems, understand what went wrong, and identify the responsible parties.</li><li>5. Accountability: Database auditing promotes accountability among users and administrators. When individuals know that their actions are being monitored, they are more likely to follow best practices and adhere to security and data management policies.</li></ol> <p>There are several ways to audit a database, depending on the database management system (DBMS) in use and the specific needs of the organization. Here are</p>	5	2	4	2	1.6.1

	<p>common methods for auditing databases:</p> <ol style="list-style-type: none"> <li>1. Database Logs: Most DBMSs maintain logs that record activities, such as login attempts, SQL statements executed, and changes to data. These logs can be reviewed to track database access and modifications.</li> <li>2. Database Triggers: Triggers are database objects that can be set to automatically perform actions, like logging changes to a separate audit table, whenever specific events occur in the database.</li> <li>3. Database Audit Trails: Some DBMSs offer built-in auditing features that allow you to define and configure audit policies, specifying which actions to audit, and where to store the audit data.</li> <li>4. Third-Party Auditing Tools: There are specialized software tools and solutions designed for auditing databases. These tools often provide more advanced features and reporting capabilities.</li> <li>5. Manual Review: Database administrators and security personnel can manually review database logs and other records to identify unauthorized access and changes. However, this can be time-consuming and less efficient than automated methods.</li> <li>6. Intrusion Detection Systems (IDS): IDS can be employed to monitor database activity and trigger alerts when suspicious or unauthorized activities occur.</li> </ol> <p>It's important to note that the choice of auditing method and the extent of auditing implemented should be based on the specific security and compliance requirements of the organization. Regularly reviewing and analyzing the audit data is also crucial to detect and respond to security incidents and maintain the integrity of the database.</p>					
17.	<p><b>Explain triggers in oracle? How do you create a trigger using oracle?</b></p> <p>✓ Trigger is an event driven program Executed automatically based on event occurs</p>	5	2	4	3	1.6.1



	<ul style="list-style-type: none"> <li>✓ ORACLE has six DML events also known as trigger timings</li> <li>✓ Trigger mainly used for the following purposes</li> <li>✓ Performing audits (Primary use) and Preventing invalid data from being inserted into the tables</li> <li>✓ Implementing business rules (Not highly recommended if the business rule is complex)</li> </ul> <p>Generating values for columns</p> <p>Trigger Syntax</p> <pre> <b>CREATE [ OR REPLACE ] TRIGGER</b> &lt;trigger_name&gt; [BEFORE   AFTER   INSTEAD OF ] [INSERT   UPDATE   DELETE.....] ON&lt;name of underlying object&gt; [FOR EACH ROW] [WHEN&lt;condition for trigger to get execute&gt; ] <b>DECLARE</b> &lt;Declaration part&gt; <b>BEGIN</b> &lt;Execution part&gt; <b>EXCEPTION</b> &lt;Exception handling part&gt; <b>END;</b> </pre> <p>Example : Row level Trigger</p> <pre> CREATE OR REPLACE TRIGGER customers_update_credit_trg BEFORE UPDATE OF credit_limit ON customers FOR EACH ROW WHEN (NEW.credit_limit &gt; 0) BEGIN -- check the credit limit IF :NEW.credit_limit &gt;= 2 * :OLD.credit_limit THEN raise_application_error(-20101,'The new credit '    :NEW.credit_limit    ' cannot increase to more than double, the current credit '    :OLD.credit_limit); END IF; END; </pre>					
18.	<p><b>Explain the applications of privacy preserving data mining?</b></p> <p>Privacy-preserving data mining (PPDM) is a field of research and practice that focuses on mining useful patterns and insights from data while protecting the privacy of individuals or entities whose data is being analyzed. PPDM techniques are essential in scenarios where sensitive information needs to be kept confidential. Here are some key applications of privacy-preserving data mining:</p> <p>1.Healthcare:</p> <p>Medical Research: Researchers can analyze patient</p>	5	2	5	2	1.6.1

<p>records or genomic data while preserving patient privacy.</p> <p>Disease Surveillance: Public health agencies can monitor disease outbreaks without revealing individual patients' identities.</p> <p>Finance:</p> <p>2.Fraud Detection: Banks and financial institutions can detect fraudulent transactions while preserving customer privacy.</p> <p>Credit Scoring: Credit agencies can assess creditworthiness without exposing personal financial details.</p> <p>Market Research:</p> <p>3.Customer Segmentation: Companies can analyze customer behavior without disclosing individual identities.</p> <p>Targeted Advertising: Advertisers can target specific demographics without revealing personal data.</p> <p>Social Networks:</p> <p>4.Privacy-Preserving Analytics: Social media platforms can analyze user interactions and content preferences without exposing personal details.</p> <p>Anonymized User Studies: Researchers can conduct studies on user behavior while protecting user identities.</p> <p>Government and Law Enforcement:</p> <p>5.Crime Analysis: Law enforcement agencies can analyze crime data without revealing the identities of victims and witnesses.</p> <p>Census Data: Governments can release anonymized census data for research and policy planning.</p> <p>Machine Learning:</p> <p>6.Federated Learning: Organizations can collaborate on building machine learning models without sharing sensitive training data.</p> <p>Homomorphic Encryption: Machine learning models can be trained on encrypted data, preserving privacy during model development.</p> <p>IoT and Smart Devices:</p> <p>7.Smart Home Analytics: Companies can analyze smart home data without exposing personal activities or habits.</p> <p>Healthcare Monitoring: Remote patient monitoring can be conducted while preserving health data privacy.</p> <p>Data Sharing:</p> <p>8.Secure Data Sharing: Organizations can share data with partners or third parties while ensuring that</p>					
---	--	--	--	--	--

	<p>sensitive information remains protected.</p> <p><b>Data Aggregation:</b> Data from multiple sources can be combined without exposing individual source details.</p> <p><b>Collaborative Research:</b></p> <p>9. <b>Secure Multi-party Computation:</b> Researchers from different organizations can collaborate on data analysis projects while preserving data privacy.</p> <p><b>Confidential Data Exchange:</b> Institutions can share research data without exposing confidential information.</p> <p><b>Personalization:</b></p> <p>10. <b>Recommender Systems:</b> Online platforms can provide personalized recommendations without revealing individual preferences.</p> <p><b>Personalized Healthcare:</b> Healthcare providers can tailor treatment plans without exposing patient medical histories.</p> <p>Privacy-preserving data mining techniques include differential privacy, secure multiparty computation, homomorphic encryption, and data anonymization methods. These methods help strike a balance between the need to extract valuable insights from data and the imperative to protect individuals' privacy, particularly in the face of increasing data collection and analysis activities.</p>					
19.	<p><b>Apply the concepts of Horizontal Partitioning in data mining with Example?</b></p> <p>Horizontal partitioning in data mining involves dividing a large dataset into smaller, more manageable subsets based on certain criteria or attributes. This technique can be helpful for improving data analysis, reducing computational complexity, and managing data storage more efficiently. Here's an example to illustrate horizontal partitioning in data mining:</p> <p><b>Example:</b> Let's consider a large e-commerce database that contains information about millions of products, including their attributes like product ID, name, category, price, manufacturer, and customer reviews. This dataset is used for various data mining tasks such as market basket analysis, recommendation systems, and customer segmentation.</p> <p>Horizontal partitioning can be applied in the following way:</p> <p>1. <b>Data Partitioning Criteria:</b> We decide to horizontally partition the dataset based on</p>	5	3	5	4	1.7.1

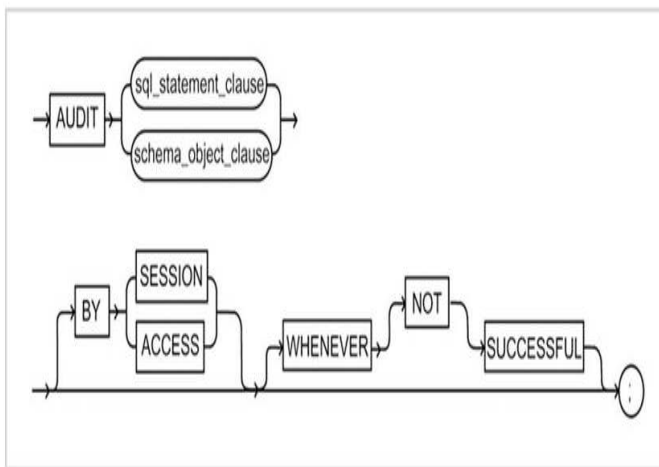
	<p>product categories. Each partition will contain products belonging to a specific category. For example, we might have partitions for "Electronics," "Clothing," "Home and Garden," "Toys," and so on.</p> <p>2. Partition Creation: Data mining experts create separate datasets or tables for each category. For instance:</p> <p><b>Electronics:</b> Product ID Name Category Price Manufacturer Customer Reviews Clothing:</p> <p><b>Product ID</b> Name Category Price Manufacturer Customer Reviews Home and Garden:</p> <p>Product ID Name Category Price Manufacturer Customer Reviews Toys:</p> <p>Product ID Name Category Price Manufacturer Customer Reviews</p> <p>3. Data Mining Analysis: With the dataset divided into partitions, data mining tasks can be performed more efficiently. For example, when running a recommendation system for electronics, the system only needs to access the "Electronics" partition, reducing the computational load and improving query performance. Similarly, marketing campaigns or customer segmentation can be applied to each partition independently.</p>					
--	--	--	--	--	--	--

<b>PART – C</b> <b>(2 x 10 = 20 Marks)</b>						
20.	<b>Explain in detail about how the database activities are audited using oracle?</b>	<b>10</b>	<b>2</b>	<b>4</b>	<b>2</b>	<b>6.2.1</b>

- ✓ 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 command syntax

##### AUDIT

```

{
{ { statement_option | ALL }
  [{statement_option | ALL}] .....
  [{system_privilege | ALL PRIVILEGES }
}
  [BY { proxy [,proxy].....
    | user [,user].....
  ]
|
{Object_option [, object_option ] ..... | ALL }
ON { [ schema. ] object
    |DIRECTORY directory_name
    |DEFAULT
  }
}
  [ BY {SESSION | ACCESS } }
  [WHENEVER [NOT] SUCCESSFUL ] ;
  
```

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

### **DDL activities Example**

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

```
SQL> CREATE TABLE CUSTOMER
```

```
2 (
3   ID    NUMBER ,
4   NAME   VARCHAR2 (20),
5   CR_LIMIT  NUMBER
6 );
```

Table created

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

```
SQL > INSERT INTO CUSTOMER VALUES (2,
'BMNANTHA', 200);
```

1 row created

```
SQL > INSERT INTO CUSTOMER VALUES (3,
'MURUGAN', 300);
```

1 row created

```
SQL > INSERT INTO CUSTOMER VALUES (1,
'GANESH', 100);
```

1 row created

```
SQL > COMMIT;
```

Commit complete

**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

```
SQL > CONNECT SYSTEM @ SEC
```

Enter password : \*\*\*\*\*

Connected.

```
SQL > AUDIT ALTER ON DBSEC.CUSTOMER BY
ACCESS WHENEVER
```

```
2 SUCCESSFUL;
```

Audit succeeded.

```
SQL > AUDIT DELETE ON DBSEC.CUSTOMER
BY ACCESS WHENEVER
```

```
2 SUCCESSFUL;
```

Audit succeeded.

	<p><b>DCL Activities Example:</b></p> <ul style="list-style-type: none"> <li>✓ You are auditing the GRANT privilege issued on a TEMP table owned by DBSEC.</li> <li>✓ The following steps shows how to audit the DCL statements audited.</li> <li>✓ The same steps to be followed for all DCL Commands.</li> </ul> <p><b>Step 1 : Log on as SYSTEM or SYS and issue an AUDIT statement as follows</b></p> <p>SQL&gt; CONN SYSTEM Enter password : ***** Connected SQL&gt; DELETE SYS.AUD\$; 1 row deleted. SQL&gt; COMMIT; Commit complete. SQL&gt; AUDIT GRANT ON DBSEC.TEMP; Audit succeeded</p> <p><b>Step 2: Log on as DBSEC and grant SELECT and UPDATE privileges to SYSTEM on TEMP table</b></p> <p>SQL&gt; CONN DBSEC Enter password : ***** Connected. SQL&gt; GRANT SELECT ON TEMP TO SYSTEM; Grant succeeded. SQL&gt; GRANT UPDATE ON TEMP TO SYSTEM Grant succeeded.</p>					
<b>OR</b>						
21.	<p><b>Compare and Contrast the difference between oracle server and SQL server 2000 in auditing database?</b></p> <p>Oracle Server and SQL Server 2000 are two popular relational database management systems (RDBMS), and both offer auditing capabilities to track and monitor database activities for security and compliance purposes. However, there are significant differences between the two in terms of how they handle database auditing.</p> <p><b>Auditing Model:</b></p> <p style="text-align: center;"><b>Oracle:</b></p> <p>Oracle Database offers a comprehensive auditing framework that allows fine-grained control over audit policies and events. You can audit various types of events, such as SELECT, INSERT, UPDATE, DELETE, and administrative actions like user logins. Auditing can be enabled at the database, schema, or</p>	10	2	4	2	2.2.4

object level, providing a high level of granularity.  
Oracle provides both standard database auditing and unified auditing, which consolidates audit data into a single location for easier management.

#### **SQL Server 2000:**

SQL Server 2000 provides a basic auditing mechanism called SQL Server Profiler, which is primarily used for performance monitoring and tracing rather than security auditing.

It lacks the fine-grained auditing capabilities of Oracle and doesn't offer built-in auditing for data manipulation actions like SELECT statements.

#### **Security Features:**

##### **Oracle:**

Oracle provides robust security features, including role-based access control, encryption, and advanced authentication mechanisms.

Auditing in Oracle is tightly integrated with these security features, allowing you to control who can enable and manage auditing policies.

#### **SQL Server 2000:**

SQL Server 2000 also offers security features like user roles and permissions, but it lacks some of the advanced security features found in later versions of SQL Server.

#### **Compliance and Reporting:**

##### **Oracle:**

Oracle Database provides tools like Oracle Audit Vault and Database Firewall for centralized audit data management and reporting.

These tools enable more comprehensive auditing for compliance with various regulations and standards.

#### **SQL Server 2000:**

SQL Server 2000 lacks centralized audit data management and reporting tools, making it less suitable for compliance requirements. You would need to develop custom solutions or rely on third-party tools for compliance reporting.

#### **Database Version:**

SQL Server 2000 is quite outdated, and it's essential to note that Microsoft has released several newer versions of SQL Server with improved auditing capabilities and enhanced security features. It is highly recommended to upgrade to a more recent version for better auditing and security.

#### **Performance Impact:**



	<p>The performance impact of auditing in both systems can vary based on the level of auditing and the database workload. Oracle's unified auditing is designed to have a lower performance overhead compared to traditional auditing methods.</p> <p>In summary, Oracle Database offers more robust and fine-grained auditing capabilities compared to SQL Server 2000, which has limited auditing features. If you're working with SQL Server, it is strongly recommended to consider upgrading to a more recent version of SQL Server for improved auditing and security features, as SQL Server 2000 is no longer supported and lacks many of the modern security features.</p>					
22.	<p><b>Illustrate the privacy preserving algorithms available in data mining? Explain anyone in detail?</b></p> <p>Privacy-preserving data mining refers to the practice of conducting data mining and analysis on sensitive or private data while ensuring the confidentiality and privacy of the data subjects or information contained within the dataset. It involves the development and implementation of techniques and methods to extract valuable insights, patterns, and knowledge from data, while minimizing the risk of disclosing sensitive information.</p> <ul style="list-style-type: none"> <li>✓ Statistical Methods for Disclosure Control</li> <li>✓ Measures of Anonymity</li> <li>✓ The <math>k</math>-anonymity Method</li> <li>✓ The Randomization Method</li> <li>✓ Quantification of Privacy</li> <li>✓ Utility Based Privacy-Preserving Data Mining</li> <li>✓ Mining Association Rules under Privacy Constraints</li> <li>✓ Cryptographic Methods for Information Sharing and Privacy</li> <li>✓ Privacy Attacks</li> <li>✓ Query Auditing and Inference Control</li> <li>✓ Privacy and the Dimensionality Curse</li> <li>✓ Personalized Privacy Preservation</li> </ul> <p>Privacy-Preservation of Data Streams</p>	10	2	5	5	6.1.1
<b>OR</b>						
23.	<p><b>Justify, Why the data mining techniques preferred for preserving privacy?</b></p> <p>Data mining techniques are often preferred for preserving privacy because they allow organizations to extract valuable insights and patterns from data while minimizing the risk of exposing sensitive or personally identifiable information (PII). Here are several reasons why data mining techniques are considered valuable for privacy preservation:</p>	10	3	5	2	1.7.1

	<ol style="list-style-type: none"> <li>1. <b>Anonymization and Data Masking:</b> Data mining methods can be used to anonymize or mask sensitive information. For example, by aggregating or generalizing data, it becomes much more challenging to identify individuals or reveal personal details. This allows organizations to use data for analysis without exposing private information.</li> <li>2. <b>Differential Privacy:</b> Differential privacy is a mathematical framework that can be integrated with data mining algorithms to ensure that the inclusion or exclusion of a specific data point does not significantly impact the results. This technique adds noise to the data to protect individual privacy while still providing accurate aggregate insights.</li> <li>3. <b>Secure Multiparty Computation (SMC):</b> SMC techniques enable multiple parties to jointly compute functions on their individual datasets without revealing the underlying data to each other. This approach allows organizations to collaborate and mine data while maintaining the privacy of their data sources.</li> <li>4. <b>Homomorphic Encryption:</b> Homomorphic encryption allows computations to be performed on encrypted data without decrypting it first. This enables data mining on encrypted data, reducing the risk of data exposure during the analysis.</li> <li>5. <b>Data Perturbation:</b> Data perturbation techniques introduce controlled noise or distortion to the data before analysis, making it challenging for adversaries to reverse engineer the original data or identify individuals. This protects privacy while still enabling meaningful analysis.</li> <li>6. <b>K-anonymity and L-diversity:</b> These are privacy-preserving techniques that ensure that individual records in a dataset cannot be easily distinguished from a group of at least k individuals. This helps protect privacy by making it more challenging to identify specific individuals within the data.</li> <li>7. <b>Limited Data Disclosure:</b> Data mining techniques can be employed to extract aggregated or summarized information from a dataset, rather than exposing raw or granular data. This reduces the risk of privacy breaches</li> </ol>					
--	--	--	--	--	--	--

	<p>by only revealing essential insights.</p> <p>8. Privacy-Preserving Machine Learning: Techniques like federated learning and secure multi-party computation enable machine learning models to be trained on distributed data sources without sharing the raw data. This protects the privacy of the data while still allowing model development.</p> <p>9. Data Minimization: Data mining encourages organizations to only collect and retain the data necessary for their specific analysis or business purposes. This reduces the volume of sensitive data that needs protection and limits the potential privacy risks.</p> <p>10. Regulatory Compliance: Many data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, require organizations to implement privacy-preserving measures. Using data mining techniques for privacy protection can help organizations comply with these regulations.</p> <p>In summary, data mining techniques provide a range of methods to balance the need for data analysis and insights with the imperative to protect individual privacy. By applying these techniques, organizations can derive valuable knowledge from data while minimizing the risk of exposing sensitive information, meeting legal requirements, and respecting individuals' privacy rights.</p>					
--	---	--	--	--	--	--

**Test: CLA – T3**

**Date: 02-11-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 1 Hour 40 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 50**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO3	1	-	1	2	2	1	-	-	-	-	-	-
2	CO4	1	-	3	1	1	1	-	-	-	-	-	-

**PART - A**  
**(15 x 1 = 15 Marks)**

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	----- tool is used for purpose of data auditing for SQL Server only?	1	1	3	4,5	1.3.1
	A Apex SQL					
	B SQL Ninja					
	C SQL Audit					
	D Idera					
2.	----- command used to turn off the audit?	1	1	3	4,5	1.3.1
	A REVOKE AUDIT					
	B NO AUDIT					
	C COMMIT Audit					
	D DBA_AUDIT_STATEMENT					
3.	----- catalog view is used for SQL Server Extended Events?	1	1	3	4,5	1.3.1
	A sys.server_sessions					
	B sys.server_event_sess					
	C sys.server_event_session_actions					
	D All of the mentioned					
4.	Auditing activities conducted by the staff members of the organization.	1	1	4	3	1.3.1
	A Internal Auditing					
	B External auditing					
	C Security audit					
	D Financial audit					
5.	----- tool provides the user interface for auditing events in SQLServer 2000?	1	1	4	3	1.3.1

	A	SQL profiler					
	B	SQL Ninja					
	C	SQL Audit					
	D	SQL Idera					
6.	_____, the attacker has a collection of independent data samples from the same distribution from which the original data was drawn		1	1	4	3	1.3.1
	A	Known Sample Attack					
	B	Packet sniffer					
	C	Distributed denial of service					
	D	Man in the middle Attack					
7.	_____ method has been proposed for computing a k-minimal generalization with the use of bottom-up aggregation along domain generalization hierarchies.		1	1	3	4,5	1.3.1
	A	Incognito					
	B	l-diversity					
	C	l-closeness					
	D	k-anonymity					
8.	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.		1	1	3	4,5	1.3.1
	A	Malicious					
	B	Semi-Honest Adversaries					
	C	Distributed denial of service					
	D	Man in the middle Attack					
9.	In _____ the entry is not modified but is left incomplete. Thus, unknown entry values are used to prevent discovery of association rules.		1	1	3	4,5	1.3.1
	A	Additive perturbation					
	B	Multiplicative perturbation					
	C	Blocking					
	D	Distortion					
10.	The _____ System was one of the earliest practical applications of privacy preserving transformations.		1	1	3	4,5	1.3.1
	A	Datafly					
	B	Homeland Security Applications					
	C	Video Surveillance					
	D	Watch list Problem					
11	What is the k-anonymity method?		1	1	3	4,5	1.3.1
	A	A method for privacy de-identification.					
	B	A method for measuring privacy.					
	C	A method for privacy preservation.					
	D	None of the above.					
12	SQL Profiler tool used.		1	1	4	3	1.3.1
	A	User interface for auditing					

	B	Modification of attributes					
	C	Change of table name					
	D	Deleting table					
13		Which one of the following team retested every database application function and try to find bugs?	1	1	4	3	1.3.1
	A	Quality assurance					
	B	Quality control					
	C	Quality testing					
	D	Quality manager					
14		An audit that is conducted by a staff member of the company being audited.	1	1	3	4,5	1.3.1
	A	External audit					
	B	Company audit					
	C	Internal audit					
	D	Policy audit					
15		In randomization technique, large volume of data analysis can be done using	1	2	4	3	1.3.1
	A	PCA technique					
	B	CPA technique					
	C	APP technique					
	D	DAA technique					

**PART – B**  
(3 x 5 = 15 Marks)

**Instructions: Answer any 3 Questions**

16.	Describe the purpose of the SQL Profiler Tools  SQL Profiler is used to:  <ul style="list-style-type: none"> <li>• analyze the application</li> <li>• Determine the optimality of requests sent to the server</li> <li>• Identify Transact-SQL commands that generate an error</li> <li>• Collect information about user activity over a long period of time</li> <li>• Monitor the server operation in real time</li> </ul>	5	2	3	4	1.6.1
17.	List the steps for determining the location of the audit trail records  1.Open the Audit Query widget.  2.To use an existing query, click the query selector and choose one from the drop down list.  3.To create a new query, click Add Query Parameter and select a column name from the drop down list. ...	5	1	4	3	1.6.1

	<p>4.Click Search at the bottom of the widget. ...</p> <p>5.Click Find to look for specific values or fields within the search results.</p>					
18.	<p>What are top ten database auditing objectives?</p> <ul style="list-style-type: none"> <li>▪ Data Integrity – Ensure that data is valid and in full referential integrity</li> <li>▪ Applications Users and roles – Ensures that users are assigned roles that correspond to their responsibilities and duties</li> <li>▪ Data Confidentiality – Identify who can read data and what data can be read</li> <li>▪ Access Control – Ensures that the application records times and duration when a user logs onto the database or application</li> <li>▪ Data changes – Create an audit trail of all data changes</li> <li>▪ Data Structure Changes – Ensures that the database logs all data structure changes</li> <li>▪ Database or application availability – Record the number of occurrences and duration of application or database shutdowns all the start-up times . Also, record all reason for any unavailability.</li> <li>▪ Change Control – Ensure that a change control mechanism is incorporated to track necessary and planned changes to the database or application.</li> <li>▪ Physical Access – Record the physical access to the application or the database where the software and hardware resides.</li> <li>▪ Auditing Reports – Ensure that reports are generated on demand or automatically , showing all auditable activities</li> </ul>	5	2	4	3	1.6.1
19.	<p>What are the two kinds of attacks are possible with some prior knowledge?</p> <p>✓ <b>Known Input-Output Attack:</b></p> <p>✓ In this case, the attacker knows some linearly independent collection of records, and their</p>	5	1	3	4	1.6.1

	<p>corresponding perturbed version. In such cases, linear algebra techniques can be used to reverse-engineer the nature of the privacy preserving transformation.</p> <p>✓ <b>Known Sample Attack:</b></p> <p>✓ In this case, the attacker has a collection of independent data samples from the same distribution from which the original data was drawn. In such cases, principal component analysis techniques can be used in order to reconstruct the behaviour of the original data.</p>					
--	---	--	--	--	--	--

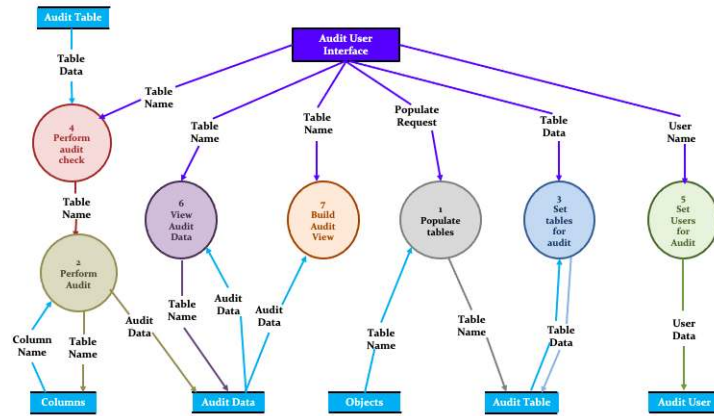
<p align="center"><b><u>PART – C</u></b> <b>(2 x 10 = 20 Marks)</b></p>						
20.	<p>Describe the distributed algorithm for k-anonymity?</p> <p>In many applications, the data records are made available by simply removing key identifiers such as the name and social-security numbers from personal records.</p> <p><input type="checkbox"/> other kinds of attributes (known as pseudo-identifiers) can be used in order to accurately identify the records.</p> <p><input type="checkbox"/> For example, attributes such as age, zip-code and gender are available in public records such as census rolls.</p> <p><input type="checkbox"/> When these attributes are also available in a given data set, they can be used to infer the identity of the corresponding individual.</p> <p>A combination of these attributes can be very</p>	10	1	3	5	6.1.1



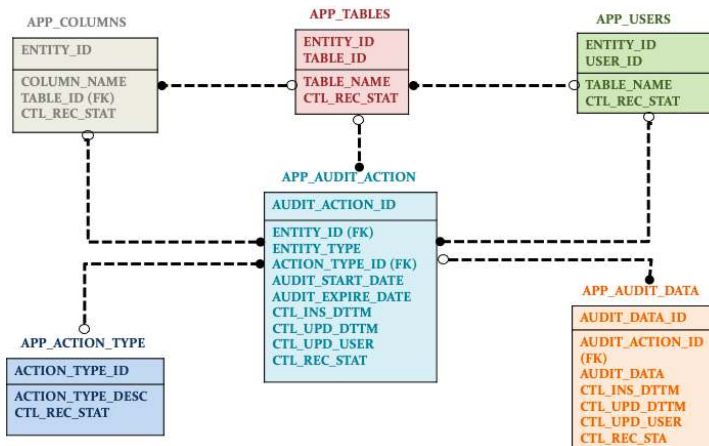
	<p>powerful, since they can be used to narrow down the possibilities to a small number of individuals</p> <p>□k-anonymity approach can be formalized as follows:</p> <p>□Each release of the data must be such that every combination of values of quasi-identifiers (are pieces of information that are not of themselves unique identifiers) can be indistinguishably matched to at least k respondents.</p> <p>□The first algorithm for k-anonymity approach uses domain generalization hierarchies of the quasi-identifiers in order to build k-anonymous tables.</p> <p>□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.</p>					
<b>OR</b>						
21.	<p>Explain in detail about advanced auditing model?</p> <p>Advanced Auditing Model</p> <ul style="list-style-type: none"> <li>✓ This Model is called “advanced” because of its flexibility</li> <li>✓ More flexible than simple models</li> <li>✓ Used as an auditing application with a user interface</li> <li>✓ Of course the repository for tis model is more complex than previous models</li> </ul>	10	1	3	4	2.2.4

- ✓ It contains data stores to register all entities that can be audited

The following figure presents the flow of the user interface



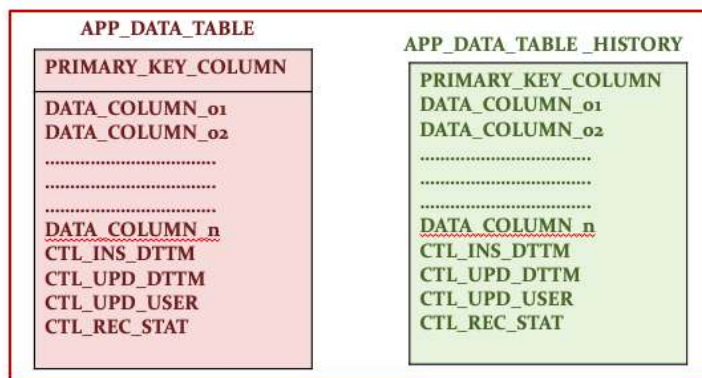
Data model of the repository for an Advanced Auditing Model



## Historical Data Model

- ✓ This model is used for applications that require a record of the whole row when a DML transaction is performed on the table
- ✓ Typically used in most financial applications
- ✓ With this model , the whole row is stored in the HISTORY table, before it is changed or deleted

The following figures illustrates this model



### Auditing Application Actions Model

- ✓ There may be a requirement for an application to audit specific operations or actions
- ✓ The following figure represents a Data Model of a repository for auditing application actions



22. Explain *l*-diversity method and *t*-closeness model in detail?

*l*-diversity method:

- ✓ The *k*-anonymity is an attractive technique because of the simplicity of the definition and the numerous algorithms available to perform the anonymization.
- ✓ The *k*-anonymity is an attractive technique because of the simplicity of the definition and the numerous algorithms available to perform the anonymization.
- ✓ Nevertheless the technique is susceptible to many kinds of attacks especially when background knowledge is available to the attacker
- ✓ Some kinds of such attacks are as follows:
  - **Homogeneity Attack:**
    - ✓ In this attack, all the values for a sensitive attribute within a group of *k* records are the same. Therefore, even though the data is *k*-anonymized, the value of the sensitive attribute for that group of *k* records can be predicted exactly.
  - **Background Knowledge Attack:**

10

3

4

4

6.1.1

	<ul style="list-style-type: none"> <li>✓ In this attack, the adversary can use an association between one or more quasi-identifier attributes with the sensitive attribute in order to narrow down possible values of the sensitive field further</li> <li>✓ While <math>k</math>-anonymity is effective in preventing <i>identification</i> of a record, it may not always be effective in preventing inference of the sensitive values of the attributes of that record.</li> <li>✓ Therefore, the technique of <math>l</math>-diversity was proposed which not only maintains the minimum group size of <math>k</math>, but also focuses on maintaining the diversity of the sensitive attributes.</li> <li>✓ Therefore, the <math>l</math>-diversity model for privacy is defined as follows: <ul style="list-style-type: none"> <li>▪ Let a <math>q^*</math>-block be a set of tuples such that its non-sensitive values generalize to <math>q^*</math>.</li> <li>▪ A <math>q^*</math>-block is <math>l</math>-diverse <ul style="list-style-type: none"> <li>✓ if it contains <math>l</math> “well represented” values for the sensitive attribute <math>S</math>.</li> <li>✓ A table is <math>l</math>-diverse, if every <math>q^*</math>-block in it is <math>l</math>-diverse.</li> <li>✓ when there are multiple sensitive attributes, then the <math>l</math>-diversity problem becomes especially challenging because of the curse of dimensionality.</li> </ul> </li> </ul> </li> </ul> <p><math>t</math>-closeness model:</p> <ul style="list-style-type: none"> <li>• The <math>t</math>-closeness model is a further enhancement on the concept of <math>l</math>-diversity.</li> <li>• One characteristic of the <math>l</math>-diversity model is that it treats all values of a given attribute in a similar way irrespective of its distribution in the data.</li> <li>• A <math>t</math>-closeness model was proposed which uses the property that the distance between the distribution of the sensitive attribute within an anonymized group should not be different from the global distribution by more than a threshold <math>t</math>.</li> </ul>					
<b>OR</b>						
23.	<p>Explain different applications of privacy-preserving data mining methods?</p> <ul style="list-style-type: none"> <li>✓ Medical Databases: The Scrub and Datafly Systems</li> </ul>	10	3	4	5	1.7.1

- ✓ Bioterrorism Applications
- ✓ Homeland Security Applications
- ✓ Genomic Privacy

#### Medical Databases: The Scrub and Datafly Systems

##### Scrub :

- ✓ The scrub system was designed for de-identification of clinical notes and letters which typically occurs in the form of textual data.
- ✓ Clinical notes and letters are typically in the form of text which contain references to patients, family members, addresses, phone numbers or providers.
- ✓ Traditional techniques simply use a global search and replace procedure in order to provide privacy.
- ✓ However clinical notes often contain cryptic references in the form of abbreviations which may only be understood either by other providers or members of the same institution.
- ✓ Therefore traditional methods can identify no more than 30-60% of the identifying information in the data
- ✓ The Scrub System uses local knowledge sources which compete with one another based on the certainty of their findings.
- ✓ Such a system is able to remove more than 99% of the identifying information from the data.

##### Datafly Systems:

- ✓ The Datafly System was one of the earliest practical applications of privacy-preserving transformations.
- ✓ This system was designed to prevent identification of the subjects of medical records which may be stored in multidimensional format.
- ✓ The multi-dimensional information may include directly identifying information such as the social security number, or indirectly identifying information such as age, sex or zip-code.
- ✓ The system was designed in response to the concern that the process of removing only directly identifying attributes such as social security numbers was not sufficient to guarantee privacy.

##### Bioterrorism Applications

- ✓ Often a biological agent such as anthrax produces symptoms which are similar to other common respiratory diseases such as the cough, cold and the flu.
- ✓ In the absence of prior knowledge of such an attack, health care providers may diagnose a patient affected by an anthrax attack of have symptoms from one of the more common respiratory diseases.

- ✓ In order to identify such attacks it is necessary to track incidences of these common diseases as well.
- ✓ Therefore, the corresponding data would need to be reported to public health agencies. However, the common respiratory diseases are not reportable diseases by law.

#### **Homeland Security Applications**

- ✓ A number of applications for homeland security are inherently intrusive because of the very nature of surveillance.
- ✓ Some examples of such applications are as follows:

##### - ✓ **Credential Validation Problem:**

- ✓ Trying to match the subject of the credential to the person presenting the credential.
  - ✓ For example, the theft of social security numbers presents a serious threat to homeland security.

##### - ✓ **Identity Theft:**

- ✓ A related technology is to use a more *active* approach to avoid identity theft.
  - ✓ The *identity angel* system, crawls through cyberspace, and determines people who are at risk from identity theft.
  - ✓ This information can be used to notify appropriate parties.

#### **Genomic Privacy**

- Recent years have seen tremendous advances in the science of DNA sequencing and forensic analysis with the use of DNA.
- As result, the databases of collected DNA are growing very fast in the both the medical and law enforcement communities.
- DNA data is considered extremely sensitive, since it contains almost uniquely identifying information about an individual.
- As in the case of multi-dimensional data, simple removal of directly identifying data such as social security number is not sufficient to prevent re-identification.
- It has been shown that a software called *CleanGene* can determine the identifiability of DNA entries independent of any other

	<p>demographic or other identifiable information.</p> <ul style="list-style-type: none"><li>• The software relies on publicly available medical data and knowledge of particular diseases in order to assign identifications to DNA entries.</li><li>• Another method for compromising the privacy of genomic data is that of <i>trail re-identification</i>, in which the uniqueness of patient visit patterns is exploited in order to make identifications.</li></ul>					
--	--	--	--	--	--	--

**Test: CLA3**
**Date: 02-11-2023**
**Course Code & Title: 18CSE455T -Database Security and Privacy**
**Duration: 1 Hour 40 Minutes**
**Year & Sem: IV / VII**
**Max. Marks: 50**
**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO4	3	2	2	-	-	-	-	-	-	-	-	-
2	CO5	2	2	2	-	-	-	-	-	-	-	-	-

**PART - A**  
(15 x 1 = 15 Marks)

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	Administration activities encompasses of	1	1	4	4,5	1.3.1
	a) SQL statements issued against application tables.					
	b) <b>Commands issued by the database administrators</b>					
	c) Commands issued by the operators for maintenance					
	d) None of the Above					
2.	AFTER LOGON and BEFORE LOGON commands included in	1	1	4	4,5	1.3.1
	a) DDL statements					
	b) DCL statements					
	c) <b>Database events</b>					
	d) SQL statements audit trail					
3.	Which one of the following tells Oracle to record audit data every time the audited statement is issued	1	1	4	4,5	1.3.1
	a) By Session					
	b) <b>By Access</b>					
	c) Whenever Successful					
	d) Whenever Not Successful					
4.	Selecting the _____ option can allow unaudited activity which could violate your security policies	1	1	4	3	1.3.1
	a) Fail					
	b) Shut down					
	c) <b>Continue</b>					
	d) Break					
5.	Grant _____ permission on the stored procedures to database roles for implementing call level security	1	1	4	3	1.3.1
	a) <b>Execute</b>					
	b) Exec					
	c) Read					
	d) Write					
6.	Trigger is special type of _____ procedure	1	1	4	3	1.3.1
	a) <b>Stored</b>					
	b) Function					



	c)	View					
	d)	Table					
7.	Selecting the _____ option can allow unaudited activity which could violate your security policies		1	1	4	4,5	1.3.1
	a)	Fail					
	b)	Shut down					
	c)	Continue					
	d)	Break					
8.	Triggers can be enabled or disabled with the _____ statement		1	1	4	4,5	1.3.1
	a)	Alter Table Statement					
	b)	Drop Table Statement					
	c)	Delete Table Statement					
	d)	Create Table Statement					
9.	In which of the Privacy preserving data mining method noise is added to data		1	1	5	4,5	1.3.1
	a)	The randomization method					
	b)	The k-anonymity model and l-diversity					
	c)	Distributed privacy preservation					
	d)	Downgrading Application Effectiveness					
10.	In which method noise is added to data		1	1	5	4,5	1.3.1
	a)	The randomization method					
	b)	The k-anonymity model and l-diversity					
	c)	Distributed privacy preservation					
	d)	Downgrading Application Effectiveness					
11	In which model we reduce the granularity of data representation with the use of techniques such as generalization and suppression		1	1	5	4,5	1.3.1
	a)	The randomization method					
	b)	The k-anonymity model and l-diversity					
	c)	Distributed privacy preservation					
	d)	Downgrading Application Effectiveness					
12	The values across different records are swapped in order to perform the privacy-preservation in		1	1	5	3	1.3.1
	a)	Data mapping					
	b)	Data swapping					
	c)	Data swapping and mapping					
	d)	Data ordering					
13	The t-closeness Model is the enhancement of		1	1	5	3	1.3.1
	a)	l-diversity model					
	b)	k-anonymity					
	c)	All of the Above					
	d)	None of the Above					
14	Which one is not suitable for k-anonymity techniques uses in		1	1	5	4,5	1.3.1
	a)	Generalization					
	b)	Suppression					
	c)	Generalization And Suppression					
	d)	Randomization					
15	Which one is not suitable for k-anonymity techniques uses in		1	1	5	3	1.3.1
	a)	Generalization					
	b)	Suppression					
	c)	Generalization and suppression					
	d)	Randomization					

**PART – B**  
(3 x 5 = 15 Marks)

**Instructions: Answer any 3 Questions**

Q. No	Questions	Marks	BL	CO	PO	PI Code
16.	<p><b>Summarize the advantages and Disadvantages of Auditing?</b></p> <p><b>Advantages of Auditing</b></p> <ul style="list-style-type: none"> <li>☞ Enforces company policies, government regulations and laws</li> <li>☞ Lowers the incidence of security violations</li> <li>☞ Identifies the security gaps and vulnerabilities</li> <li>☞ Provides an audit trail of activities</li> <li>☞ Provides another means to observe and evaluate operations of the audited entity</li> <li>☞ Provides the sense or state of security and confidence in the audited entity</li> <li>☞ Identifies or removes doubts</li> <li>☞ Makes the organisation being audited more accountable</li> <li>☞ Develops controls that can be used for purposes other than auditing</li> </ul> <p><b>Disadvantages of Auditing</b></p> <ul style="list-style-type: none"> <li>☞ Performance problems due to preoccupation with the audit instead of the normal work activities</li> <li>☞ Generation of many reports and documents that may not be easily or quickly disseminated</li> <li>☞ Disruption to the operations of the audited entity</li> <li>☞ Consumption of resources, and added costs from downtime</li> <li>☞ Friction between operators and auditor</li> <li>☞ From a DB perspective <ul style="list-style-type: none"> <li>• Could degrade the performance of the system</li> <li>• Also generate a massive number of logs, reports, and that require a system purge</li> </ul> </li> </ul>	5	2	4	2	1.6.1
17.	<p><b>Explain triggers in SQL? How do you create a trigger using SQL?</b></p> <p>In SQL, a trigger is a database object that defines a set</p>	5	2	4	2	1.6.1

of actions to be performed automatically in response to specific events or changes in the database. Triggers are typically used to enforce data integrity, implement business rules, or automate certain tasks, such as logging changes or generating audit records. They can be set to execute either before or after a specific event, like an INSERT, UPDATE, DELETE, or other data manipulation operations.

There are two main types of triggers in SQL:

**Before Triggers (BEFORE INSERT/UPDATE/DELETE):** These triggers execute before the specified data manipulation operation (e.g., INSERT, UPDATE, DELETE) takes place. They are commonly used to validate data or modify values before the change is applied to the database.

**After Triggers (AFTER INSERT/UPDATE/DELETE):** These triggers execute after the specified data manipulation operation has taken place. They are often used to perform actions such as logging changes, sending notifications, or maintaining audit trails.

Here's the basic syntax for creating a trigger in SQL:

```
CREATE [OR REPLACE] TRIGGER trigger_name
[BEFORE | AFTER] [INSERT | UPDATE | DELETE]
ON table_name
FOR EACH ROW
[WHEN (condition)]
BEGIN
    -- Trigger code or actions go here
END;
```

Let's break down the components of this syntax:

**trigger\_name:** This is a user-defined name for the trigger.

**BEFORE or AFTER:** Specifies whether the trigger should execute before or after the specified data manipulation operation.

**INSERT, UPDATE, or DELETE:** Indicates the event that triggers the execution of the trigger.

**table\_name:** The name of the table on which the trigger is defined.

**FOR EACH ROW:** This clause indicates that the trigger will fire once for each row affected by the triggering event.

**WHEN (condition):** An optional condition that, if specified, restricts the trigger's execution based on a specified condition.

**BEGIN...END:** The block of SQL statements or actions that the trigger should perform when it's executed.

	<p>Here's an example of creating a simple trigger that logs changes to a "employees" table after an update:</p> <pre>CREATE OR REPLACE TRIGGER log_employee_changes AFTER UPDATE ON employees FOR EACH ROW BEGIN     INSERT INTO employee_audit (employee_id, change_date, changed_data) VALUES (:OLD.employee_id, SYSDATE, 'Updated employee data'); END;</pre> <p>In this example, the trigger "log_employee_changes" is set to execute after an update on the "employees" table. It logs the changes by inserting a record into an "employee_audit" table with information about the employee and the modification timestamp.</p> <p>Triggers can be powerful tools, but they should be used with caution, as they can impact database performance and maintainability. It's important to ensure that triggers are well-designed, and their logic is thoroughly tested to avoid unintended side effects.</p>					
18.	<p><b>Illustrate the distributed privacy preserving data Mining?</b></p> <p>Distributed Privacy-Preserving Data Mining (DPDM) is a field of research and a set of techniques that aim to perform data mining on distributed datasets while preserving the privacy of the individuals or entities whose data is being analyzed. It addresses the challenge of extracting useful insights and patterns from data without compromising the sensitive information contained in that data.</p> <p>Here are some key aspects and techniques associated with Distributed Privacy-Preserving Data Mining:</p> <p>Privacy Concerns: The primary motivation for DPDM is to address privacy concerns. When data is distributed across different parties or organizations, there may be legal, ethical, or contractual obligations to protect the privacy of the data. DPDM ensures that data mining operations do not reveal sensitive information about individuals in the dataset.</p> <p>Cryptographic Techniques: One of the fundamental approaches to DPDM is the use of cryptographic techniques, such as secure multiparty computation and homomorphic encryption. These techniques allow</p>	5	2	5	2	1.6.1

<p>computations to be performed on encrypted data without revealing the data in its raw form.</p> <p>Differential Privacy: Differential privacy is a key concept in DPDM. It involves adding noise to the data or query responses in a way that makes it difficult to distinguish the contribution of any individual data point. This ensures that the privacy of individuals is preserved while still enabling useful aggregate analysis.</p> <p>Federated Learning: Federated learning is a technique that allows machine learning models to be trained on distributed datasets without sharing raw data. Instead, model updates are exchanged between the parties, and the model is trained collaboratively.</p> <p>Secure Aggregation: Secure aggregation techniques enable parties to compute aggregate statistics from their data without revealing the individual data points. This can be achieved through secure multi-party computation.</p> <p>Data Perturbation: Data perturbation involves adding random noise to the data before analysis. This makes it more challenging for an adversary to learn sensitive information from the data mining results.</p> <p>Trusted Third Parties: In some DPDM scenarios, a trusted third party may be involved to coordinate the data mining process without having access to the raw data. This third party ensures privacy and fairness in the data mining process.</p> <p>Privacy-Preserving Data Mining Algorithms: Researchers have developed data mining algorithms that are designed to operate on privacy-preserving data. These algorithms take into account the privacy constraints and utilize techniques such as differential privacy.</p> <p>Use Cases: DPDM has applications in various domains, including healthcare, finance, and social sciences. For example, medical researchers can perform distributed analysis of patient data across multiple hospitals without exposing individual patient records.</p> <p>Legal and Ethical Considerations: DPDM often intersects with legal and ethical considerations, such as data protection regulations (e.g., GDPR), data ownership, and consent. Compliance with these regulations is a critical aspect of DPDM.</p> <p>DPDM is a challenging and evolving field that requires a deep understanding of both data mining and privacy-</p>					
---	--	--	--	--	--

	preserving techniques. It enables organizations and researchers to glean insights from distributed datasets while respecting individuals' privacy rights.					
19.	<p><b>Illustrate the Utility Based Privacy-Preserving Data Mining</b></p> <p>Utility-Based Privacy-Preserving Data Mining (UBPPDM) is an approach that aims to strike a balance between preserving the privacy of individuals' sensitive data and extracting useful information for data analysis or mining purposes. It addresses the challenge of sharing data while protecting the privacy of individuals' information. Here's an illustration of UBPPDM:</p> <p><b>Data Collection:</b> Consider a healthcare organization collecting medical records from patients. These records may include sensitive information such as diagnoses, treatments, and personal identifiers. The organization wants to share this data with researchers or other parties for medical research without disclosing individual patients' identities or specific medical details.</p> <p><b>Privacy Concerns:</b> Patients' privacy is a top priority. Sharing the raw medical records as they are would breach their privacy, violating regulations like HIPAA in the United States. Anonymizing data by removing identifiers is not enough because it's still possible to re-identify individuals through auxiliary information or by linking it with other datasets.</p> <p><b>Data Transformation:</b> In UBPPDM, data transformation techniques are applied to the original data to protect privacy. For example, differential privacy mechanisms might be used to add random noise to the data, making it more challenging to identify specific individuals.</p> <p><b>Privacy Parameters:</b> To control the level of privacy preservation and utility, parameters are set. These parameters determine how much noise or distortion is added to the data. A balance must be struck to ensure that privacy is protected while still retaining useful patterns and insights in the data.</p> <p><b>Data Mining Process:</b> Data mining or analysis is performed on the transformed data. Researchers can extract valuable information, discover trends, and make important insights into the medical data without violating individual privacy. This may include identifying disease trends, treatment effectiveness, or risk factors.</p> <p><b>Privacy Guarantees:</b> UBPPDM provides privacy guarantees based on the chosen privacy mechanisms</p>	5	2	5	4	1.6.1

	<p>and parameters. Researchers and data analysts can work with the assurance that they are not exposing sensitive information about individuals in the dataset.</p> <p><b>Reporting and Visualization:</b> The results of the data analysis can be reported or visualized in a way that maintains privacy. For example, aggregated statistics or general trends can be presented instead of individual-level details.</p> <p><b>Iterative Process:</b> UBPPDM can be an iterative process. Researchers might need to fine-tune the privacy parameters or apply more advanced privacy-preserving techniques if the initial results are not satisfactory.</p> <p><b>Data Sharing:</b> The privacy-preserving data can be safely shared with other organizations, researchers, or the public for various purposes, such as academic research, policy making, or public health awareness.</p> <p><b>Continuous Improvement:</b> UBPPDM is an evolving field. Researchers and practitioners continually develop new techniques and algorithms to improve the balance between privacy and utility.</p> <p>In summary, Utility-Based Privacy-Preserving Data Mining is a crucial framework that allows organizations to share sensitive data for analysis while protecting individual privacy. It involves a careful balance between adding noise to protect privacy and maintaining the usefulness of the data for meaningful insights and discoveries.</p>					
--	---	--	--	--	--	--

<p align="center"><b><u>PART – C</u></b> <b>(2 x 10 = 20 Marks)</b></p>						
20.	<p><b>Explain the Auditing objectives and Classification in detail?</b></p> <ul style="list-style-type: none"> <li>🌐 Auditing objectives are established as a part of the development process of the entity to be audited</li> <li>🌐 For example , when a software application is being coded, the developers include in their software development design objectives the capability to audit the application</li> <li>🌐 Auditing objectives are established and documented for the following reasons: <ul style="list-style-type: none"> <li>📖 Complying – Identify all company policies , government regulations, laws and the industry standards with which your company comply.</li> <li>📖 Informing – All policies, regulations, laws and standards must be published</li> </ul> </li> </ul>	10	2	4	2	6.1.1

and communicated to all parties involved in the development and operation of the audited entity.

- 📖 Planning – Knowing all the objectives enables the author to plan and document procedures to assess the audited entity.
- 📖 Executing – Without auditing objectives, the person conducting the audit cannot evaluate, verify, or review the audited entity and cannot determine if the auditing objectives have been met

#### **The top ten database auditing objectives**

- 📖 Data Integrity – Ensure that data is valid and in full referential integrity
- 📖 Applications Users and roles – Ensures that users are assigned roles that correspond to their responsibilities and duties
- 📖 Data Confidentiality – Identify who can read data and what data can be read
- 📖 Access Control – Ensures that the application records times and duration when a user logs onto the database or application
- 📖 Data changes – Create an audit trail of all data changes
- 📖 Data Structure Changes – Ensures that the database logs all data structure changes
- 📖 Database or application availability – Record the number of occurrences and duration of application or database shutdowns all the startup times . Also, record all reason for any unavailability.
- 📖 Change Control – Ensure that a change control mechanism is incorporated to track necessary and planned changes to the database or application.
- 📖 Physical Access – Record the physical access to the application or the database where the software and hardware resides.
- 📖 Auditing Reports – Ensure that reports are generated on demand or automatically , showing all auditable activities

#### **Audit Classifications**

- 🌐 Every industry and business sector uses different classifications of audits.
- 🌐 Definition of each classification can differ from



	<p>business to business.</p> <ul style="list-style-type: none"> <li>Will discuss most generic definition of audit classifications.</li> </ul> <p><b>Internal Audit</b></p> <ul style="list-style-type: none"> <li>An internal audit is an audit that is conducted by a staff member of the company being audited</li> <li>The purpose and intention of an internal audit is to : <ul style="list-style-type: none"> <li>Verify that all auditing objectives are met by conducting a well-planned and scheduled audit</li> <li>Investigate a situation that was promoted by an internal event or incident. This audit is random , not planned or scheduled.</li> </ul> </li> </ul> <p><b>External Audit</b></p> <ul style="list-style-type: none"> <li>An external audit is conducted by a party outside the company that is being audited.</li> <li>The purpose and intention of an External audit is to : <ul style="list-style-type: none"> <li>Investigate the financial or operational state of the company . This audit is initiated at will by the government or promoted by suspicious activities or accusations.</li> <li>The person conducting this audit is usually employed and appointed by the government.</li> <li>Verify that all objectives are met. This audit is typically planned and scheduled.</li> <li>Ensure objectivity and accuracy.</li> </ul> </li> </ul> <p>This audit is typically performed to certify that the company is complying with standards and regulations</p> <p><b>Automatic Audit</b></p> <ul style="list-style-type: none"> <li>An automatic audit is promoted and performed automatically.</li> <li>Automatic audits are mainly for systems and DB systems.</li> <li>Some systems that employ this type of audit to generate reports and logs.</li> </ul> <p><b>Manual Audit</b></p> <ul style="list-style-type: none"> <li>Completely performed by humans</li> <li>The team uses various methods to collect audit data, including interviews, document reviews and observation.</li> <li>The auditors may even perform the operational task of the audited entity.</li> </ul> <p><b>Hybrid Audit</b> Combination of Automatic and Manual Audits</p>					
<b>OR</b>						
21.	<b>Explain in detail about how the database activities are audited using SQL Server 2000?</b>	10	2	4	2	6.1.1

SQL Server 2000 is an older version of Microsoft's relational database management system. While it's no longer officially supported, understanding how database activities can be audited in this version can provide some historical context for auditing in more recent SQL Server versions.

Auditing in SQL Server 2000 typically involves tracking and recording various database activities to ensure data integrity, security, and compliance. To achieve this, you can use several methods and features within SQL Server 2000:

#### **SQL Profiler:**

SQL Server 2000 includes SQL Profiler, a tool that allows you to capture and analyze SQL Server events, including SQL statements executed, login attempts, errors, and more. To set up auditing using SQL Profiler, follow these steps:

#### **Launch SQL Profiler.**

Create a new trace or open an existing one.

Define the events you want to capture (e.g., "T-SQL" for SQL statements).

Specify filters to focus on specific databases, users, or applications.

#### **Start the trace to begin auditing.**

SQL Profiler allows you to capture detailed information about database activities and provides valuable insights into what's happening in the system. However, it's not the most efficient method for long-term or continuous auditing.

#### **Triggers:**

SQL Server 2000 supports database triggers, which are programmable actions that automatically execute when specific events occur in the database. You can use triggers to audit changes to data or specific actions performed on database objects. Common triggers include:

**DML Triggers:** These triggers fire in response to Data Modification Language (DML) statements like INSERT, UPDATE, and DELETE, allowing you to log changes to data.

**DDL Triggers:** These triggers respond to Data Definition Language (DDL) statements like CREATE, ALTER, and DROP, enabling you to track changes to database schema.

To implement triggers, you would write T-SQL code that defines the trigger's behavior and attach it to a table or the database itself. When the specified event occurs, the trigger executes, allowing you to log relevant information to an audit table or take other actions.

	<p><b>Extended Stored Procedures:</b> SQL Server 2000 allows you to create custom extended stored procedures using programming languages like C/C++. These procedures can be used for various purposes, including auditing. You can develop custom stored procedures to capture and record specific database activities in a custom audit table.</p> <p><b>System Log (Event Logs):</b> SQL Server 2000 also logs certain events in the Windows event logs. You can configure SQL Server to log security-related events, errors, and other important information. These logs can provide insights into login attempts, failed authentication, and other security-related activities.</p> <p>It's essential to secure and protect the audit data by ensuring that only authorized personnel have access to the audit logs. You may also want to consider periodically archiving and managing audit data to prevent it from growing excessively.</p> <p>Keep in mind that SQL Server 2000 is an outdated and unsupported version, and it's recommended to migrate to a more recent and supported version of SQL Server for enhanced security and auditing capabilities. SQL Server 2000 lacks many of the advanced auditing features available in modern versions, like SQL Server Audit, which provides more robust auditing and security capabilities.</p>					
22.	<p><b>Explain in detail for the following.</b> <b>A. t-closeness model</b></p> <p>T-closeness is a privacy model used in data anonymization and protection, particularly in the context of publishing sensitive information while preserving individual privacy.</p> <p>T-closeness extends the ideas of k-anonymity and l-diversity, which are also privacy models used in data anonymization. The primary goal of t-closeness is to ensure that the distribution of sensitive attributes in the anonymized dataset is not too different from the distribution of those attributes in the original dataset. In other words, it aims to provide a more refined privacy guarantee compared to k-anonymity and l-diversity.</p> <p><b>Here's a brief overview of the key components of t-closeness:</b></p> <p><b>Sensitive Attribute:</b> The t-closeness model is primarily concerned with preserving the privacy of a sensitive attribute. This attribute contains information that should be protected, such as medical conditions, income, or any other personal information.</p>	10	2	5	1	6.1.1

**Closeness Measure:** T-closeness introduces a closeness measure, often denoted as "t," which quantifies the similarity between the distribution of the sensitive attribute in the original dataset and the anonymized dataset. The value of "t" determines the level of privacy protection.

**Anonymization:** To achieve t-closeness, the dataset is anonymized in a way that the distribution of the sensitive attribute within each group (anonymized record) is not significantly different from its distribution in the original dataset. This prevents an attacker from inferring sensitive information easily.

**Grouping:** Records are grouped together based on quasi-identifiers, which are attributes that can be used to re-identify individuals. The goal is to create groups where the distribution of the sensitive attribute within each group is close to the overall distribution in the original dataset.

**Global t-Closeness:** This approach ensures that the entire dataset satisfies the t-closeness property.

**Local t-Closeness:** This approach ensures that each group (anonymized record) within the dataset satisfies the t-closeness property. Local t-closeness is often preferred when the data is highly skewed.

## B. *l*-diversity model

L-diversity is a privacy concept and model designed to protect sensitive information in data, particularly in the context of data anonymization and disclosure control. The primary goal of l-diversity is to prevent attribute disclosure by ensuring that each group of records with the same quasi-identifiers (attributes that can potentially be used to re-identify individuals) contains at least "l" distinct values for a sensitive attribute.

**Here's a more detailed explanation of the l-diversity model:**

**Quasi-identifiers:** These are attributes in a dataset that can be used in combination to potentially re-identify individuals. For example, a combination of attributes like ZIP code, age, and gender might make someone unique in a dataset.

**Sensitive attribute:** This is the attribute that you want to protect, such as medical information, income, or any other personal and sensitive data.

	<p><b>L-diversity:</b> The number "l" in l-diversity represents the minimum number of distinct values that must be present for the sensitive attribute within any group of records that share the same quasi-identifiers. In other words, for each unique combination of quasi-identifiers, there should be at least "l" different values for the sensitive attribute to make it more challenging to re-identify individuals.</p> <p>The main idea behind l-diversity is to add a level of diversity to the sensitive attribute values within each group, making it harder for an adversary to pinpoint an individual's sensitive information based on their quasi-identifiers. This helps protect privacy while still allowing useful information to be shared in a dataset.</p> <p>There are various techniques to achieve l-diversity, such as generalization and suppression of data values, and these methods aim to balance the trade-off between data utility and privacy. The choice of "l" value depends on the specific privacy requirements of the dataset and the desired level of protection.</p> <p>L-diversity is just one of the many techniques used in the field of privacy-preserving data publishing and anonymization. It addresses the limitations of traditional data anonymization methods, like k-anonymity, which do not consider diversity in the sensitive attribute values and can lead to attribute disclosure risks.</p>					
<b>OR</b>						
23.	<p><b>Justify, Why the data mining techniques preferred for preserving privacy?</b></p> <p>Data mining techniques are often preferred for preserving privacy because they allow organizations to extract valuable insights and patterns from data while minimizing the risk of exposing sensitive or personally identifiable information (PII). Here are several reasons why data mining techniques are considered valuable for privacy preservation:</p> <ol style="list-style-type: none"> <li>1. <b>Anonymization and Data Masking:</b> Data mining methods can be used to anonymize or mask sensitive information. For example, by aggregating or generalizing data, it becomes much more challenging to identify individuals or reveal personal details. This allows organizations to use data for analysis without exposing private information.</li> <li>2. <b>Differential Privacy:</b> Differential privacy is a mathematical framework that can be integrated</li> </ol>	10	3	5	4	1.7.1

	<p>with data mining algorithms to ensure that the inclusion or exclusion of a specific data point does not significantly impact the results. This technique adds noise to the data to protect individual privacy while still providing accurate aggregate insights.</p> <p>3. Secure Multiparty Computation (SMC): SMC techniques enable multiple parties to jointly compute functions on their individual datasets without revealing the underlying data to each other. This approach allows organizations to collaborate and mine data while maintaining the privacy of their data sources.</p> <p>4. Homomorphic Encryption: Homomorphic encryption allows computations to be performed on encrypted data without decrypting it first. This enables data mining on encrypted data, reducing the risk of data exposure during the analysis.</p> <p>5. Data Perturbation: Data perturbation techniques introduce controlled noise or distortion to the data before analysis, making it challenging for adversaries to reverse engineer the original data or identify individuals. This protects privacy while still enabling meaningful analysis.</p> <p>6. K-anonymity and L-diversity: These are privacy-preserving techniques that ensure that individual records in a dataset cannot be easily distinguished from a group of at least k individuals. This helps protect privacy by making it more challenging to identify specific individuals within the data.</p> <p>7. Limited Data Disclosure: Data mining techniques can be employed to extract aggregated or summarized information from a dataset, rather than exposing raw or granular data. This reduces the risk of privacy breaches by only revealing essential insights.</p> <p>8. Privacy-Preserving Machine Learning: Techniques like federated learning and secure multi-party computation enable machine learning models to be trained on distributed data sources without sharing the raw data. This protects the privacy of the data while still allowing model development.</p> <p>9. Data Minimization: Data mining encourages organizations to only collect and retain the data</p>					
--	---	--	--	--	--	--

	<p>necessary for their specific analysis or business purposes. This reduces the volume of sensitive data that needs protection and limits the potential privacy risks.</p> <p>10. Regulatory Compliance: Many data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, require organizations to implement privacy-preserving measures. Using data mining techniques for privacy protection can help organizations comply with these regulations.</p> <p>In summary, data mining techniques provide a range of methods to balance the need for data analysis and insights with the imperative to protect individual privacy. By applying these techniques, organizations can derive valuable knowledge from data while minimizing the risk of exposing sensitive information, meeting legal requirements, and respecting individuals' privacy rights.</p>					
--	---	--	--	--	--	--

**Test: CLA – T3**

**Date: 02-11-2023**

**Course Code & Title: 18CSE455T -Database Security and Privacy**

**Duration: 1 Hour 40 Minutes**

**Year & Sem: IV / VII**

**Max. Marks: 50**

**Course Articulation Matrix: (to be placed)**

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO3	1	-	1	2	2	1	-	-	-	-	-	-
2	CO4	1	-	3	1	1	1	-	-	-	-	-	-

**PART - A**  
**(15 x 1 = 15 Marks)**

**Instructions: Answer all**

Q. No	Questions	Marks	BL	CO	PO	PI Code
1.	Expected to provide the resources needed and select staff members to accompany the auditors	1	1	3	4,5	1.3.1
	A auditor					
	B client					
	C Internal auditor					
	D <b>auditee</b>					
2.	The values across different records are swapped in order to perform the privacy-preservation is _____.	1	1	3	4,5	1.3.1
	A Data Encryption					
	B <b>Data Swapping</b>					
	C Data Hiding					
	D Data masking					
3.	The document that contains all activities that are being audited ----- ordered in a chronological manner.	1	1	3	4,5	1.3.1
	A <b>Audit log</b>					
	B Audit Profile					
	C Audit File					
	D Audit Document					
4.	Selecting the _____ option can allow unaudited activity which could violate your security policies.	1	1	4	3	1.3.1
	A Fail					
	B Shut Down					
	C <b>Continue</b>					
	D Break					
5.	An audit which is compulsory by the law is _____.	1	1	4	3	1.3.1
	A Government Audit					
	B Internal Audit					
	C Cost Audit					
	D <b>Statutory Audit</b>					
6.	_____, the attacker has a collection of independent data samples from the same distribution from which the	1	1	4	3	1.3.1



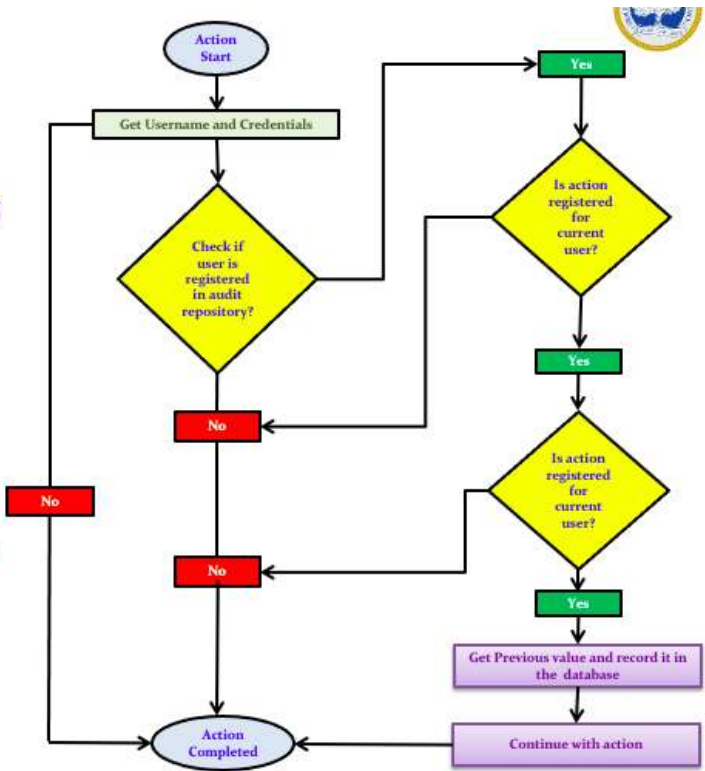
	original data was drawn					
	A Known Sample Attack					
	B Packet sniffer					
	C Distributed denial of service					
	D Man in the middle Attack					
7.	Kind of partitioning is used for the data sets across multiple entities which same set of attributes?	1	1	3	4,5	1.3.1
	A Horizontal					
	B Vertical					
	C Hash					
	D Key					
8.	A method based on chance alone by which study participants are assigned to a treatment group is _____.	1	1	3	4,5	1.3.1
	A k-anonymity					
	B l-diversity					
	C t-closeness					
	D Randomization					
9.	The _____ model was designed to handle some weaknesses in the k-anonymity model	1	1	3	4,5	1.3.1
	A k-anonymity					
	B l-diversity					
	C incognito					
	D Data Swapping					
10.	The Oracle _____ Log is another method of auditing database activities.	1	1	3	4,5	1.3.1
	A ALERT					
	B REVOKE					
	C COMMIT					
	D CHECK					
11	Bioterrorism-application, the data analyzed for privacy-preserving data mining purposes is	1	1	3	4,5	1.3.1
	A medical data					
	B Statistical data					
	C Spatio temporal data					
	D Timestamped data					
12	The Method for compromising the privacy of genomic data	1	1	4	3	1.3.1
	A trail re-identification					
	B Prediction					
	C Masking					
	D Decoding					
13	Which one of the following team retested every database application function and try to find bugs?	1	1	4	3	1.3.1
	A Quality assurance					
	B Quality control					
	C Quality testing					
	D Quality manager					
14	In _____ the entry is not modified, but is left incomplete. Thus, unknown entry values are used to prevent discovery of association rules.	1	1	3	4,5	1.3.1
	A Additive perturbation					
	B Multiplicative perturbation					

	C	Blocking					
	D	Distortion					
15		----- function returns Boolean value in PKG_APP_AUDIT?	1	2	4	3	1.3.1
	A	AUDIT_CHECK					
	B	AUDIT_REVOKE					
	C	AUDIT_COMMIT					
	D	AUDIT_ALERT					

**PART – B**  
**(3 x 5 = 15 Marks)**

**Instructions: Answer any 3 Questions**

	Describe the following terms in few lines					
	<p>Auditing</p> <p>Audit log</p> <p>Audit objectives</p> <p>Audit trail</p> <p>External auditing</p>					
16.	<p>📖 Auditing - The process of examining and validating documents, data, processes, systems, or other activities to ensure that the audited entity complies with its objective</p> <p>📖 Audit log – A document that contains all activities that are being audited ordered in a chronological manner.</p> <p>📖 Audit objectives – A set of business rules, system controls, government regulations or security policies against which the audited entity is measured to determine compliance</p> <p>📖 Audit trail – A chronological record of document changes, data changes, system activities, or operational events</p> <p>📖 External auditing - Auditing activities conducted by the staff members outside of the organization.</p>	5	2	3	4	1.6.1

17.	<p>Explain any one of the auditing model with neat diagram.</p> <ul style="list-style-type: none"> <li>Before auditing models, it is more important that , understand how audit is processed for data and DB activities</li> <li>The flowchart presents data auditing</li> <li>The flowchart shows what happens when a user perform an action to a DB object</li> <li>Specific checks occur to verify if the action , the user or the object are registered in auditing repository</li> <li>If they are registered the followings are recorded <ul style="list-style-type: none"> <li>State the object before the action was taken along with the time of action</li> <li>Description of the action that was performed</li> <li>Name of the user or userid who performed the action</li> </ul> </li> </ul>  <pre> graph TD     Start([Action Start]) --&gt; GetCreds[Get Username and Credentials]     GetCreds --&gt; CheckUser{Check if user is registered in audit repository?}     CheckUser -- No --&gt; ActionComp([Action Completed])     CheckUser -- Yes --&gt; CheckAction1{Is action registered for current user?}     CheckAction1 -- No --&gt; ActionComp     CheckAction1 -- Yes --&gt; CheckAction2{Is action registered for current user?}     CheckAction2 -- No --&gt; ActionComp     CheckAction2 -- Yes --&gt; GetPrev[Get Previous value and record it in the database]     GetPrev --&gt; Continue[Continue with action]     Continue --&gt; ActionComp </pre>	5	1	4	3	1.6.1
18.	<p>Explain Data Swapping?</p> <ul style="list-style-type: none"> <li>Noise addition or multiplication is not the only</li> </ul>	5	2	4	3	1.6.1

	<p>technique which can be used to perturb the data.</p> <ul style="list-style-type: none"> <li>🌐 A related method is that of data swapping, in which the values across different records are swapped in order to perform the privacy-preservation</li> <li>🌐 One advantage of this technique is that the lower order marginal totals of the data are completely preserved and are not perturbed at all. <ul style="list-style-type: none"> <li>📖 Therefore certain kinds of aggregate computations can be exactly performed without violating the privacy of the data.</li> <li>📖 This technique does not follow the general principle in randomization which allows the value of a record to be perturbed independently of the other records.</li> <li>📖 Therefore, this technique can be used in combination with other frameworks such as <i>k</i>-anonymity, as long as the swapping process is designed to preserve the definitions of privacy for that model.</li> </ul> </li> </ul>					
19.	<p>Write about mining association rules under privacy constraints.</p> <p><b>Mining Association Rules under Privacy Constraints</b></p> <ul style="list-style-type: none"> <li>🌐 Since association rule mining is one of the important problems in data mining</li> <li>🌐 There are two aspects to the privacy preserving association rule mining problem <ol style="list-style-type: none"> <li>1. When the input to the data is perturbed, it is a challenging problem to accurately determine the association rules on the perturbed data.</li> <li>2. A different issue is that of output association rule privacy.</li> </ol> <p>In this case, to ensure that none of the association rules in the output result in leakage of</p> </li> </ul>	5	1	3	4	1.6.1

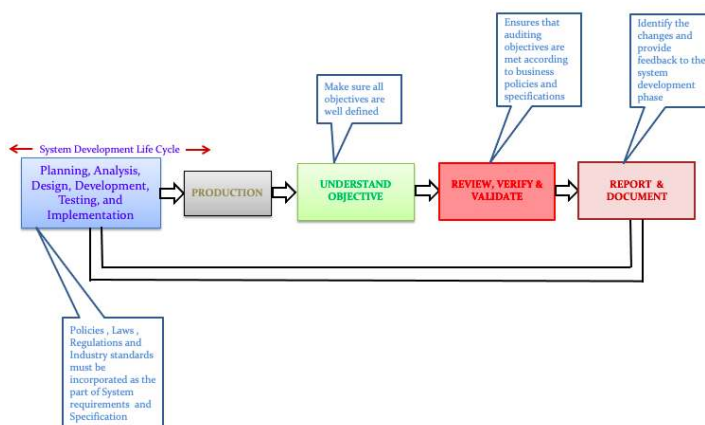
	<p>sensitive data.</p> <p>This problem is referred to as <i>association rule hiding</i> by the</p> <p>database community, and that of <i>contingency table privacy</i>-</p> <p><i>preservation</i> by the statistical community.</p>					
--	--	--	--	--	--	--

**PART – C**  
**(2 x 10 = 20 Marks)**

20.	<p>Explain auditing project case study for payroll.</p> <p><b>Case : Taking Care of Payroll</b></p> <ul style="list-style-type: none"> <li>🌐 Acme Payroll Systems is a small payroll services company that has been in business for two years and has had only one major customer</li> <li>🌐 Suddenly, it lands a contract with another large corporation</li> <li>🌐 If the company hired you as Database consultant to design and implement a virtual private database for the existing payroll application.</li> <li>🌐 The main objective of the virtual private database feature is allow each client to administer his own payroll data without violating the privacy of other clients.</li> </ul> <p>The given figure represents the payroll application model for case</p>	10	1	3	5	6.1.1
<b>OR</b>						
21.	<p>Explain auditing process? Differences in QA , Auditing and Performance Monitoring processes? Illustrates the auditing process flow with the neat diagram?</p> <p>🌐 Database applications widely used by major corporate companies, mostly large financial and online trading companies.</p>	10	1	3	4	2.2.4

- 🌐 The Quality Assurance (QA) team retested every database application function and try to find bugs.
- 🌐 This type of auditing resembles QA or even performance monitoring
- 🌐 The purpose of QA process in software engineering to make sure that the system is bug free and that the system is functioning according to its specification.
- 🌐 The auditing process ensures that the system is working and complies with the policies, standards, regulations or laws set forth by organization, industry or government.
- 🌐 Another way to distinguish between QA and Auditing Process is by examining the timing of each
- 🌐 QA – during development phase, before the implementation of the system.
- 🌐 Auditing Process – After the system is implemented and in production.
- 🌐 Auditing is also not the same as performance monitoring
- 🌐 Auditing objectives are totally different
- 🌐 Performance Monitoring is to observe the degradation in performance
- 🌐 Auditing validates compliance to policy not performance

PROCESS	ACTIVE TIMING	OBJECTIVES
QA	During development and 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,



22.

Elaborate privacy preserving data mining in detail.

10

3

4

4

6.1.1

	<ul style="list-style-type: none"> <li>🌐 Statistical Methods for Disclosure Control</li> <li>🌐 Measures of Anonymity</li> <li>🌐 The <math>k</math>-anonymity Method</li> <li>🌐 The Randomization Method</li> <li>🌐 Quantification of Privacy</li> <li>🌐 Utility Based Privacy-Preserving Data Mining</li> <li>🌐 Mining Association Rules under Privacy Constraints</li> <li>🌐 Cryptographic Methods for Information Sharing and Privacy</li> <li>🌐 Privacy Attacks</li> <li>🌐 Query Auditing and Inference Control</li> <li>🌐 Privacy and the Dimensionality Curse</li> <li>🌐 Personalized Privacy Preservation</li> <li>🌐 Privacy-Preservation of Data Streams</li> </ul> <p>Note: Explain all the above headings in detail.</p>					
<b>OR</b>						
23.	<p>Explain Randomization method in detail?</p> <ul style="list-style-type: none"> <li>🌐 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.</li> <li>🌐 The noise added is sufficiently large so that individual record values cannot be recovered.</li> <li>🌐 Therefore, techniques are designed to derive aggregate distributions from the perturbed records.</li> <li>🌐 Subsequently, data mining techniques can be developed in order to work with these aggregate distributions.</li> </ul> <p>The method of randomization can be described as follows.</p> <ul style="list-style-type: none"> <li>🌐 Consider a set of data records denoted by <math>X = \{x_1 \dots x_N\}</math></li> <li>🌐 For record <math>x_i \in X</math></li> <li>🌐 we add a noise component which is drawn from the probability distribution <math>f_Y(y)</math>.</li> <li>🌐 These noise components are drawn independently, and are denoted <math>y_1 \dots y_N</math>.</li> <li>🌐 Thus, the new set of distorted records are denoted by  <math display="block">x_1 + y_1 \dots x_N + y_N.</math> </li> <li>🌐 We denote this new set of records by  <math display="block">z_1 \dots z_N.</math> </li> <li>🌐 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 data.</li> <li>🌐 Thus, the original records cannot be recovered, but the distribution of the original records can be recovered.</li> </ul>	10	3	4	5	1.7.1

	<ul style="list-style-type: none"><li>Thus, if <math>X</math> be the random variable denoting the data distribution for the original record</li><li><math>Y</math> be the random variable describing the noise distribution</li><li><math>Z</math> be the random variable denoting the final record</li></ul> <p>We have:</p> $Z = X + Y$ $X = Z - Y$ <ul style="list-style-type: none"><li>Now, we note that <math>N</math> instantiations of the probability distribution <math>Z</math> are known, whereas the distribution <math>Y</math> is known publicly.</li><li>For a large enough number of values of <math>N</math>, the distribution <math>Z</math> can be approximated closely by using a variety of methods such as kernel density estimation.</li><li>By subtracting <math>Y</math> from the approximated distribution of <math>Z</math>, it is possible to approximate the original probability distribution <math>X</math></li><li>One key advantage of the randomization method is that it is relatively simple, and does not require knowledge of the distribution of other records in the data.</li><li>This is not true of other methods such as <math>k</math>-anonymity which require the knowledge of other records in the data.</li><li>Therefore, the randomization method can be implemented at <i>data collection time</i>, and does not require the use of a trusted server containing all the original records in order to perform the anonymization process.</li><li>While this is a strength of the randomization method, it also leads to some weaknesses, since it treats all records equally irrespective of their local density.</li></ul>					
--	--	--	--	--	--	--