Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No......................................

Faculty of Engineering / Science

End Sem Examination May-2024

CA5EL13 Cloud Security

Programme: MCA / BCA-MCA (Integrated) Branch/Specialisation: Computer Application

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. Which of the following service provider provides the least amount of built in security? **1**

(a) SaaS (b) PaaS (c) IaaS (d) All of these

ii. Which of the following area of cloud computing is uniquely troublesome? **1**

(a) Auditing

(b) Data integrity

(c) e-Discovery for legal compliance

(d) All of these

iii. Which of the following was one of the weaker aspects of early cloud computing service offerings? **1**

(a) Logging (b) Integrity checking

(c) Consistency checking (d) None of these

iv. Which of the following is a compliance standard? **1**

(a) PCI-DSS (b) HIPPA

(c) GLBA (d) All of these

v. Which of the following is required by cloud computing? **1**

(a) That you establish an identity

(b) That the identity be authenticated

(c) That the authentication be portable

(d) All of these

vi. The four steps of role management (in the proper order) are: **1**

(a) Audit, research, plan and deploy

(b) Research, plan, deploy and integrate

(c) Research, plan, deploy and audit

(d) Research, audit, plan and deploy

vii. Patches must be deployed in a manner that guarantees. **1**

(a) Consistency (b) Status tracking

(c) Error logging (d) All of these

viii. What is the best approach for choosing a vulnerability assessment tool for your environment? **1**

(a) A statistical analysis of your environment's software and network traffic should be mapped to the functionality of the different products.

(b) Research third-party test results.

(c) Your current business drivers should be understood, and they will dictate the type of assessment tool you need

(d) An assessment of your physical security, personnel security or company's culture will dictate the type of assessment tool you need.

ix. Which of the following is one of the most actively developing and important areas of cloud computing technology? **1**

(a) Logging (b) Auditing

(c) Regulatory compliance (d) None of these

x. Which of the following is a common means for losing encrypted data? **1**

(a) Lose the keys (b) Lose the encryption standard

(c) Lose the account (d) None of these

Q.2 i. What do you mean by the term availability and integrity in the context of cloud security? **4**

ii. Describe different security considerations needed for IaaS and SaaS. **6**

OR iii. Write the user authentication mechanism in the cloud. **6**

Q.3 i. Briefly explain about CIA traid. **4**

ii. Write cloud information security objective according to the U.S department of defence for data and analysis centre for software. **6**

OR iii. Explain cloud security design principles in detail. **6**

Q.4 i. Explain trust boundaries in cloud. **4**

ii. Describe IAM architecture in detail. **6**

OR iii. Explain identity access management life cycle in details. **6**

Q.5 i. Explain the objective behind security vulnerability management in the cloud. **4**

ii. Write the objective behind access control in the cloud. **6**

OR iii. “You can have security and not have privacy. but you cannot have privacy without security” Justify your answer. **6**

Q.6 Attempt any two:

i. Explain five major rules for health insurance portability and accountability act (HIPPA). **5**

ii. Explain payment card industry data security standards (PCIDSS) for credit card industry. **5**

iii. Write the summary of service sectors with their corresponding regulations. **5**

******

Scheme of Marking

Cloud Security (T) - CA5EL13 (T)

Q.1	i)	C	**1**
	ii)	D	**1**
	iii)	A	**1**
	iv)	D	**1**
	v)	D	**1**
	vi)	C	**1**
	vii)	B	**1**
	viii)	C	**1**
	ix)	C	**1**
	x)	A	**1**
Q.2	i.	2+2	**4**
	ii.	3+3	**6**
OR	iii.	6 points must require for six marks	**6**
	iv.		
Q.3	i.	Explanation required in 1 page with diagram	**4**
	ii.	Following point must be covered.1)Dependability 2) Trustworthiness 3) Survivability (Resilience).and Many sub point also be Considered a)Confidentiality b) Integrity c) Availability d) .	**6**
OR	iii.	Point to be covered. 1) Least privilege 2) Separation of Duties 3)Defence in depth 4)Fail safe 5) Economy of mechanism 6) Complete mediation 7) open design 8) Least common mechanism 9) Psychological acceptability 10) Weakest Link 11)Leveraging existing components	**6**
Q.4	i.	Explain in trust boundaries	**4**
	ii.	IAM architecture -3 Marks Explanation-3Marks	**6**
OR	iii.	2 Marks Diagram+4 Marks explanation	**6**
Q.5	i.	**Explanation required. ½ page** To reduce risks resulting from exploitation of published technical vulnerabilities. Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. these considerations should include operating systems, and any other applications in use.	**4**
	ii.	**Objective: Point wise Explanation required(1 Page)** To ensure authorized user access and to prevent unauthorized access to information systems. Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls	**6**
OR	iii.	**Explanation required(1 Page)** Proverb given by “TIM MATHER” .Explanation expected according to the point .	**6**
Q.6			

i. HIPAA Rule: 1) Privacy rule 2) Security rule 3) Transaction and code set rule 4) Enforcement rule 5) Unique identifier rule **5**

ii. **Explanation of PCIDSS**. **5**

a) Install and maintain a firewall configuration to protect cardholder data

b) Do not use default passwords or security parameters .

c) Protect Stored cardholder data

d) Encrypt transmission of sensitive information across public network

e) Use and regularly update anti-virus and malware protection.

f) Develop and maintain secure systems and application

g)restrict access to data by using a need –to-know policy

And many more points

iii. **5**

Sr.No	Service Sector	Regulations
1.	Healthcare	HIPPA,PCI
2.	Retail	PCI,SOX
3.	Financial	PCI, SOX, and GLBA
4.	Government agencies	FISMA.

HIPPA: Health Insurance portability and Accountability act.

SOX- Sarbanes –Oxley Act

GLBA: - Gramm –Leach Bliley act (Federal regulation).

FISMA:- Federal information security and management act.

******