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

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

Faculty of Engineering

End Sem (Even) Examination May-2022

CS5EL12 Cloud Security

Programme: M. Tech. Branch/Specialisation: CS

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

Note: All questions are compulsory. Internal choices, if any, are indicated.

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 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

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. What is the best reason to implement security policy? **1**

(a) It makes security harder to enforce

(b) It removes the employee's responsibility to make judgments

(c) It increases security

(d) It decreases security

x. What are the two basic types of attacks? **1**

(a) Active and passive (b) DOS and DDOS

(c) Virus and worm (d) None of these

Q.2 Attempt any two:

i. Compare the symmetric and asymmetric key cryptography. **5**

ii. Specify the four categories of security threats in brief. **5**

iii. Distinguish between direct and arbitrated digital signature. **5**

Q.3 i. Briefly explain about cloud Security services. **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 Cloud Service Provider in IAM Practice. **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" Describe it. **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**

******

Total No. of Questions: 6 *Total No. of Printed Pages:2*

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

Faculty of Engineering

End Sem (Even) Examination May-2020

Scheme of Marking

CS5EL12 Cloud Security

Programme: M.Tech. Branch/Specialisation: CS/Cloud Computing

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

Note: All questions are compulsory. Internal choices, if any, are indicated.

Q.1	i.	C	1
	ii.	D	1
	iii.	A	1
	iv.	D	1
	v.	C	1
	vi.	C	1
	vii.	B	1
	viii.	C	1
	ix.	C	1
	x.	D	1
Q.2	i.	2.5+2.5	5
	ii.	5	5
OR	iii.	2.5+2.5	5
Q.3	i.	Explanation required in 1 page	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.	Precise explain required in cloud service provider in IAM Practice	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.** 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	5

<table>
<tr>
<td>OR</td>
<td>i.</td>
<td>
<table>
<tr><th>Sr.No</th><th>Service Sector</th><th>Regulations</th></tr>
<tr><td>1.</td><td>Healthcare</td><td>HIPPA,PCI</td></tr>
<tr><td>2.</td><td>Retail</td><td>PCI,SOX</td></tr>
<tr><td>3.</td><td>Financial</td><td>PCI, SOX, and GLBA</td></tr>
<tr><td>4.</td><td>Government agencies</td><td>FISMA.</td></tr>
</table>
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.
</td>
<td>5</td>
</tr>
</table>

******