b.	Privacy impact assessment and safety impact assessment segregates IoT security from traditional IT security. Justify.	10	2	3	3
29. a.	Design a high-level M2M architecture. Describe the functional and topological entities of architecture.	10	2	4	3
	(OR)				
b.	Identity the data agnostic protocol which runs on top of TCP/IP in IoT. Explain its operation.	10	2	4	3
30. a.	Describe proof of stake, proof of work and smart contracts.	10	2	5	4
	(OR)				
b.	Write about block chains and describe the essential entities transaction examples.	10	1	5	4

* * * * *

Reg. No.															

B.Tech. DEGREE EXAMINATION, NOVEMBER 2022
Sixth/ Seventh Semester

18CSE445T – INTERNET OF THINGS SECURITY
(For the candidates admitted from the academic year 2018-2019 to 2019-2020)

Note:
(i) **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.
(ii) **Part - B** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

		Marks	BL	CO	PO
	PART – A (25 × 1 = 25 Marks) Answer **ALL** Questions				
1.	The scenario where an employee registers his/her biometric attendance and checks it through a web app refers (A) Point to point web app (B) IoT (C) Cyber physical systems (D) Intrusion detection system	1	1	1	1
2.	Gateway are optional in (A) IoT (B) Intrusion detection system (C) Cyber physical system (D) IEEE 802.11 a/b/g/n	1	1	1	1
3.	Message queuing telemetry transport protocol is (A) A connection oriented protocol (B) A connection-less protocol (C) Is used in VOIP (D) Is similar to IPX	1	1	1	1
4.	Constrained application protocol is (A) A connection oriented protocol (B) A connectionless protocol (C) Is used for end-end process connection (D) Is similar to file transfer protocol	1	1	1	1
5.	Alice sends a message M to BOB at time t_1 and receives an ack. At time (t_1 + a), when BOB denied of receiving M, Alice proved the transaction. This scene refers to (A) Non repudiation (B) Trust value (C) Confidentiality (D) Integrity	1	1	1	1
6.	Port 23 is open in server and the username and password are admin/admin. When attacker Brute forces the commonly used username and password, it refers to (A) Denial of service attack (B) 0 day vulnerability (C) Code-breaking (D) Hacking	1	1	2	2
7.	When a new device is connected with IoT infrastructure, which one of the following should be given priority? (A) Secure bootstrapping (B) Check credential for authentication (C) Verify vulnerability index (D) Assign a static IP	1	1	2	2

8. Reversible, irreversible respectively are 1 1 2 2
(A) Confidentiality algorithm, integrity algorithm
(B) Integrity algorithm, confidentiality algorithm
(C) Integrity algorithm, authenticity algorithm
(D) Authenticity algorithm, confidentiality algorithm

9. Which one of the following IoT devices are strictly limited to resources 1 1 2 2
(A) Sensors (B) Access points
(C) Routers (D) Laptops

10. IoT infrastructure is an enabler for 1 1 2 2
(A) Robotics (B) Web 3.0
(C) Unmanned air crafts (D) 5G communication

11. The technology which supports resources constrained devices of IoT 1 1 3 2
(A) Wi-Fi (B) GSM
(C) Zigbee (D) SDN

12. The final phase of designing security model by security architects are 1 1 3 2
(A) Rating of attacks (B) Rating of threats
(C) Rating of damages (D) Rating of vulnerabilities

13. COAP is a _____ and _____ protocol. 1 1 3 2
(A) Connection oriented and reliable (B) Connectionless and reliable
(C) Network and reliable (D) Transport and reliable

14. COAP is a _____ protocol. 1 1 3 2
(A) Simple, small code print (B) Multicast, simple
(C) Many to one, multicast, simple, less over head (D) One-to-one, multicast, simple, less overhead

15. When multiple parties complete for limited shared resource, which of the following is used for decision making? 1 1 3 2
(A) Numerical methods (B) Fuzzy theory
(C) Game theory (D) Control theory

16. Assurance for preventing unauthorized disclosure of message is 1 1 4 3
(A) Confidentiality (B) Authenticity
(C) Integrity (D) Non-repudiation

17. Assurance for preventing unauthorized alteration of message is 1 1 4 3
(A) Confidentiality (B) Integrity
(C) Authenticity (D) Non-repudiation

18. Assurance for preventing unauthorized access of message is 1 1 4 2
(A) Confidentiality (B) Integrity
(C) Authenticity (D) Non-repudiation

19. Assurance for preventing denial of sender and recipient post legitimate transaction is 1 1 4 3
(A) Confidentiality (B) Integrity
(C) Authenticity (D) Non-repudiation

20. Block chain is 1 1 3 3
(A) A combination of centralized ledgers (B) A type of crypto-currency
(C) Exchange of distributed information (D) Distributed ledger in a peer-to-peer network

21. Block chain split is referred as 1 1 3 3
(A) Bit coin (B) Script
(C) Fork (D) Crypto-split

22. An algorithm that takes input of any length and gives a fixed size digest is 1 1 3 3
(A) Encryption algorithm (B) Hash algorithm
(C) Merkle-tree algorithm (D) MAC algorithm

23. Keyed hash is called 1 1 5 3
(A) Block chain (B) Message authentication code
(C) Medium access control (D) Encryption

24. A minor alteration in plaintext resulting in drastic effect in cipher text is called 1 1 5 3
(A) Avalanche effect (B) Complex effect
(C) Feistal effect (D) Shannon effect

25. Dissipating statistical structure of plaintext over cipher text is 1 1 5 3
(A) Merkle-Root (B) Complexity
(C) Diffusion (D) Confusion

PART – B (5 × 10 = 50 Marks) Marks BL CO PO
Answer **ALL** Questions

26. a. Justify the importance of security training for security engineers. 10 1 1 1

(OR)

b. Justify the importance of IoT security life cycle with a neat sketch. 10 2 1 1

27. a. Construct and demonstrate a smart parking threat matrix and analysis. 10 2 2 2

(OR)

b. List and describe any 4 assets that an attacker would be interested in attacking a bio metrics system. 10 1 3 3

28. a. Depict the public key crypto-system with a neat sketch. 10 1 3 4

(OR)