CHAPTER 5

Security and Future of IoT Ecosystem
(IoT ईकोसिस्टम की सुरक्षा एवं भविष्य)

PART ONE (भाग–1)

(Objective Type Questions & Answers) (वस्तुनिष्ठ प्रश्न एवं उत्तर)

MULTIPLE CHOICE QUESTIONS (बहुविकल्पीय प्रश्न)

1.1. Process of identifying any individual

(a) Auditing (b) Authorisation

(c) Authentication (d) Accounting

किसी भी व्यक्ति को पहचानने की प्रक्रिया

(a) ऑडिटिंग (b) ऑथोराइजेशन

(c) ऑथेंटिकेशन (d) एकाउंटिंग

1.2. Process of keeping track of user's activity

(a) Authentication (b) Authoring

(c) Authorisation (d) Accounting

यूज़र की एक्टिविटी का लेखा-जोखा रखना

(a) ऑथेंटिकेशन (b) ऑथरिंग

(c) ऑथोराइजेशन (d) एकाउंटिंग

1.3. Secret words or numbers used for protection of devices is called

(a) Biometric Data (b) passwords

(c) Private data (d) backup

गुप्त शब्द या नंबर्स जो डिवाइसेस की सुरक्षा के लिए इस्तेमाल किये जाते हैं

(a) बायोमेट्रिक डेटा (b) पासवर्ड

(c) निजी डेटा (d) बैकअप

1.4. The process of converting data into a format that cannot be read by another user

(a) Encryption (b) Decryption

(c) Locking (d) Registering

डेटा को एक ऐसे फॉर्मेट में परिवर्तित करने की प्रक्रिया जिसे कोई भी दूसरा यूज़र पढ़ न सके

(a) एन्क्रिप्शन (b) डिक्रिप्शन

(c) लॉकिंग (d) रजिस्टरिंग

1.5. **Which concept determines what resources users can access after they log on?**
(a) Auditing (b) Actuation
(c) Authentication (d) Access Control

कौन-सी अवधारणा यह निर्धारित करती है कि यूज़र लॉग ऑन करने के बाद कौन-से रिसोर्सेज़ को एक्सेस कर सकता है?
(a) ऑडिटिंग (b) ऐक्चुएशन
(c) ऑथेंटिकेशन (d) एक्सेस कण्ट्रोल

1.6. **The _____ hack, is one of the most famous IoT security attack**
(a) Mirai botnet (b) cipher
(c) Stuxnet (d) none of the above

_____ हैक, एक सबसे मशहूर IoT सुरक्षा पर हमलों में से एक है
(a) Mirai बॉटनेट (b) सिफर
(c) स्टक्सनेट (d) उपरोक्त में से कोई नहीं

1.7. **What is the first line of defence when setting up a network?**
(a) configure authentication (b) physically secure a network
(c) configure ACL (d) configure encryption

नेटवर्क स्थापित करते समय रक्षा की पहली पंक्ति क्या है?
(a) कॉन्फिगर ऑथेंटिकेशन (b) फिजिकल रूप से एक नेटवर्क सुरक्षित करना
(c) कॉन्फिगर ACL (d) कॉन्फिगर एन्क्रिप्शन

1.8. **What kind of electronic document contains a public-key?**
(a) PIN (b) PAN
(c) Digital Certificates (d) Biometrics

किस तरह के इलेक्ट्रॉनिक डॉक्यूमेंट्स में पब्लिक-की होती है?
(a) पिन (b) पैन
(c) डिजिटल सर्टेफिकेट्स (d) बायोमेट्रिक्स

1.9. **What type of attack tries to guess password by trying common words?**
(a) brute force attack (b) man in the middle attack
(c) smurf attack (d) dictionary attack

किस प्रकार का हमला आम शब्दों की कोशिश कर पासवर्ड का अनुमान लगाने की कोशिश करता है?
(a) ब्रूट फोर्स अटैक (b) मैन इन द मिडल अटैक
(c) स्मर्फ अटैक (d) डिक्शनरी अटैक

1.10. **Which of the following is not a correct way to secure communication layer?**
(a) cloud initiated communication (b) TLS/SSL
(c) IPS (Intrusion Prevention System) (d) Firewall

निम्नलिखित में से कौन-सा कम्यूनिकेशन लेयर को सुरक्षित करने का सही तरीका नहीं है?
(a) क्लाउड इनिशिएटेड कम्यूनिकेशन (b) TLS/SSL
(c) IPS (इन्ट्रूशन प्रिवेंटेशन सिस्टम) (d) फायरवॉल

TRUE/FALSE (सत्य/असत्य)

2.1. It is vital to provide secure update mechanisms that don't allow for cyber criminals to misuse the update system to install malware and other harmful programs on users' IoT devices.

यह बहुत जरूरी है कि सुरक्षित अपडेट सिस्टम प्रदान किया जाये जो साइबर क्रिमिनल्स को अपडेट सिस्टम का अनुचित उपयोग करने की अनुमति न दे ताकि वे मैलवेयर और अन्य हानिकारक प्रोग्राम यूज़र की IoT डिवाइसेस पर इन्स्टॉल न कर सकें।

2.2. The software on IoT devices does not need to be verified with secure boot mechanisms like a hardware root of trust.

IoT डिवाइसेस पर जो सॉफ्टवेयर होता है उसे सुरक्षित बूट मेकेनिज़्म से वेरिफाई कराये जाने की आवश्यकता नहीं होती जैसे कि हार्डवेयर रूट ऑफ ट्रस्ट।

2.3. All IoT device passwords need to be same.

सभी IoT डिवाइसेस का पासवर्ड एक ही होना चाहिए।

2.4. Besides unique passwords, credentials and other sensitive data should be securely stored on IoT devices and services.

यूनीक पासवर्ड के अलावा क्रेडेंशियल और अन्य सेंसेटिव डेटा को IoT डिवाइसेस पर सुरक्षित रूप से स्टोर किया जाना चाहिए।

2.5. The input data need not be validated, as cyber criminals often try to exploit the systems through validated data.

क्योंकि साइबर क्रिमिनल्स अक्सर वेलिडेटिड डेटा के माध्यम से ही सिस्टम को एक्सप्लॉइट करने की कोशिश करते हैं, इसलिए इनपुट डाटा को वेलिडेट नहीं करना चाहिए।

2.6. All unnecessary interfaces on an IoT device need to be closed, and all approved ways of minimizing possible attack surfaces need to be implemented.

IoT डिवाइसेस के सभी ग़ैर जरूरी इंटरफेसेस को बंद कर देना चाहिए और सभी स्वीकृत तरीके जिनसे संभव हमले कम किये जा सकें उन्हें लागू किया जाना चाहिए।

2.7. For communication to be protected in the IoT ecosystem, the best practices of cryptography need to be used.

IoT ईकोसिस्टम में कम्यूनिकेशन को सुरक्षित करने के लिए क्रिप्टोग्राफी की सर्वोत्तम प्रथाओं को इस्तेमाल करना चाहिए।

2.8. Always give your router a usual name associated with you or your street address or personal belongings.

अपने राउटर को हमेशा अपने पते या अपने व्यक्तिगत सामान से जुड़ा एक सामान्य नाम दें।

2.9. Always use a strong encryption method, like WPA2, when you set up Wi-Fi network access.

वाई-फाई नेटवर्क एक्सेस को सेट करते समय हमेशा WPA2 जैसी एक मजबूत एन्क्रिप्शन विधि का उपयोग करें।

2.10. Avoid common words or passwords that are easy to guess, such as "password" or "123456."

सामान्य शब्दों और पासवर्ड जिनका आसानी से अनुमान लगाया जा सके जैसे "password" या "123456" को पासवर्ड रखने से बचना चाहिए।

MATCHING THE COLUMNS (स्तम्भों का मिलान)

	X		Y
3.1.	Strong Passwords/ शक्तिशाली पासवर्ड	A	process that converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext प्रक्रिया जो इन्फॉर्मेशन की ऑरिजिनल रिप्रेजेंटेशन को, जिसे प्लेन टेक्स्ट कहते हैं, एक अन्य रूप में परिवर्तित करती है जिसे सिफर टेक्स्ट कहते हैं
3.2.	Encryption/ एन्क्रिप्शन	B	Public Wi-Fi hotspots/ सार्वजनिक Wi-Fi हॉटस्पॉट
3.3.	When you provide your user id and password for logging in, an OTP is sent to your registered mobile number जब आप लॉगिंग इन करने के लिए अपना यूज़र id और पासवर्ड डालते हैं तो एक OTP आपके रजिस्टर्ड मोबाइल नंबर पर आता है	C	ciphertext/ सिफरटेक्स्ट
3.4.	Insecure network/ असुरक्षित नेटवर्क	D	Vulnerability Assessment वल्नेरेबिलिटी असेसमेंट
3.5.	The process of finding flaws on the target टारगेट में त्रुटियां खोजने की प्रक्रिया	E	Two-factor authentication टू-फैक्टर-ऑथेंटिकेशन
3.6.	The process of finding vulnerabilities on the target टारगेट में कमजोरियों को खोजने की प्रक्रिया	F	Combination of upper/lower case letters, numbers and special characters अपर/लोअर केस लेटर्स, नम्बर्स एवं विशेष करेक्टर्स का संयोजन
3.7.	a method used in a TCP/IP network to create a connection between a host and a client. होस्ट और क्लाइंट के बीच कनेक्शन बनाने के लिए TCP/IP में इस्तेमाल किया जाने वाला एक मेथड	G	Penetration Testing/ पेनिट्रेशन टेस्टिंग
3.8.	a tool that shows the path of a packet एक टूल जो पैकेट का पाथ दिखाता है	H	three-way handshake तीन तरफा हैंडशेक

3.9.	industry-standard security technology creating encrypted connections between Web Server and a Browser वेब सर्वर और ब्राउजर के बीच एन्क्रिप्टेड कनेक्शन बनाने वाली इंडस्ट्री-स्टैण्डर्ड सिक्योरिटी टेक्नोलॉजी	I	Hacking/ हैकिंग
3.10.	an intentional or unintentional transmission of data from within the organization to an external unauthorized destination जानबूझकर या अनजाने में आर्गेनाइजेशन के अन्दर से बाह्य गैर कानूनी डेस्टिनेशन को डेटा का ट्रांसमिशन	J	SSL(Secure Sockets Layer) SSL (सिक्योर सॉकेट्स लेयर)
		K	Data Leakage/ डेटा का लीकेज
		L	Firewall/ फायरवॉल
		M	Traceroute / ट्रेसरूट

FILL IN THE BLANKS (रिक्त स्थान भरना)

A	Depth-First Search डेप्थ फर्स्ट सर्च	B	Spyware/ स्पाईवेयर	C	It discovers causal relationships यह कार्यकारण सम्बन्धों का प लगाता है
D	Network Security Wall नेटवर्क सिक्योरिटी वॉल	E	Spam/ स्पैम	F	Hacking/ हैकिंग
G	Perl/ पर्ल	H	Ignorance/ इग्नोरेंस	I	Cracking/ क्रैकिंग
J	The Turing Test द ट्यूरिंग टेस्ट	K	continuous-path control कन्टीन्यूअस पाथ कन्ट्रोल	L	White Hat/ व्हाइट हैट
M	Stalking/ स्टॉकिंग				

4.1. ..... monitors user activity on internet and transmits that information in the background to someone else.

_____ इन्टरनेट पर यूज़र की एक्टिविटी को मॉनिटर करता है और बैकग्राउंड में उसकी इन्फॉर्मेशन किसी और को ट्रांसमिट करता है।

4.2. Firewall is a type of ..... .

फायरवॉल एक प्रकार का _____ है।

4.3. Unsolicited commercial email is known as ..... .

अनचाहे कमर्शियल ई-मेल को _____ कहा जाता है।

4.4. ..... is not an external threat to a computer or a computer network.

_____ कंप्यूटर या कंप्यूटर नेटवर्क के लिए बाहरी खतरा नहीं है।

4.5. When a person is harassed repeatedly by being followed, called or be written to, he / she is a target of ..... .

जब किसी व्यक्ति को बार-बार पीछा कर, विभिन्न नामों से पुकारकर या लिखकर प्रताड़ित किया जाता है तो वह व्यक्ति _____ का शिकार होता है।

4.6. ..... is not the commonly used programming language for Artificial Intelligence.

आर्टिफिशियल इंटेलिजेंस के लिए _____ आमतौर पर इस्तेमाल होने वाली प्रोग्रामिंग लेंग्वेज नहीं है।

4.7. ..... search method takes less memory.

_____ सर्च मेथड कम मेमोरी लेता है।

4.8. ..... was originally called the imitation game by its creator.

_____ को मूलत: इसके सृजनकर्ता द्वारा इमीटेशन गेम के नाम से बुलाया गया।

4.9. Programming a robot by physically moving it through the trajectory you want it to follow is called ..... .

रोबोट को प्रोग्राम करने को जिससे वह एक ट्रेजेटरी को फॉलो करता हुआ मूव करे, इसे _____ कहते हैं।

4.10. ..... is FALSE regarding regression.

रिग्रेशन के सम्बन्ध में _____ गलत है।