CHAPTER-5 Security & Future of IoT Application

Q.1. Write short notes on the following:

a) Malware
b) Phishing
c) Active Attack
d) Vulnerability
e) Cryptography

प्रश्न 1. **निम्नलिखित पर संक्षिप्त टिप्पणी लिखिए :**

ए) मैलवेयर

बी) फ़िशिंग

ग) सक्रिय हमला

घ) सुभेद्यता

ई) क्रिप्टोग्राफी

a. Ans. Malware (malicious software) are the software programs designed to damage or do other unwanted actions on a computer system. Some examples of malware include viruses, worms, Trojan horses, and spyware.
Malware can cause havoc on the computer hard drive by deleting files or directory information.

b. Phishing is an attempt of acquiring sensitive information, such as usernames, passwords, and credit card details, by hacker in an electronic communication.

C. Modification of messages being transmitted, capturing authentication sequences and obtaining extra privileges, creation of false messages etc. are a few active attacks. Active attacks are difficult to prevent because they require protection of all communication facilities and paths at all times. But one can detect and recover from the disruptions caused by them.

d. Vulnerabilities are weaknesses in a system or its design that allow an in a system or its design that allow an intruder to execute commands, access unauthorized data, and? Or conduct denial-of-service attacks.

e. Cryptography is technique of securing information and communication through use of codes so that only that person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information.

ए. उत्तर। मैलवेयर (दुर्भावनापूर्ण सॉफ़्टवेयर) ऐसे सॉफ़्टवेयर प्रोग्राम हैं जिन्हें कंप्यूटर सिस्टम पर अन्य अवांछित क्रियाओं को नुकसान पहुंचाने या करने के लिए डिज़ाइन किया गया है। मैलवेयर के कुछ उदाहरणों में वायरस, वर्म्स, ट्रोजन हॉर्स और स्पाइवेयर शामिल हैं।

मैलवेयर फ़ाइलों या निर्देशिका जानकारी को हटाकर कंप्यूटर की हार्ड ड्राइव पर कहर ढा सकता है।

बी. फ़िशिंग एक इलेक्ट्रॉनिक संचार में हैकर द्वारा संवेदनशील जानकारी, जैसे उपयोगकर्ता नाम, पासवर्ड और क्रेडिट कार्ड विवरण प्राप्त करने का एक प्रयास है।

C. प्रेषित किए जा रहे संदेशों का संशोधन, प्रमाणीकरण अनुक्रमों को कैप्चर करना और अतिरिक्त विशेषाधिकार प्राप्त करना, झूठे संदेशों का निर्माण आदि कुछ सक्रिय हमले हैं। सक्रिय हमलों को रोकना मुश्किल है क्योंकि हर समय सभी संचार सुविधाओं और रास्तों की सुरक्षा की आवश्यकता होती है। लेकिन कोई भी उनसे होने वाले व्यवधानों का पता लगा सकता है और उनसे उबर सकता है।

डी. कमजोरियां एक सिस्टम या उसके डिजाइन में कमजोरियां हैं जो एक सिस्टम या उसके डिजाइन में एक घुसपैठिए को कमांड निष्पादित करने, अनधिकृत डेटा तक पहुंचने की अनुमति देती हैं, और? या सेवा से इनकार करने वाले हमलों का संचालन करते हैं।

Q.2. Define Encryption and why it is used?

प्रश्न 2. **एन्क्रिप्शन को परिभाषित करें और इसका उपयोग क्यों किया जाता है**?

Ans. It is a process of converting the data of file into an unreadable format to protect the data from attack. It is being widely used in an organization to secure their data.

Ans. **यह डेटा को हमले से बचाने के लिए फ़ाइल के डेटा को एक अपठनीय प्रारूप में परिवर्तित करने की प्रक्रिया है। किसी संगठन में अपने डेटा को सुरक्षित रखने के लिए इसका व्यापक रूप से उपयोग किया जा रहा है।**

Q.3. what are terms of security?

प्रश्न 3. **सुरक्षा की शर्तें क्या हैं**?

A.3.The key terms for security are Confidentiality, Integrity and Availability.

It is also known as CIA. These three things are considered to be the most important components of the security. Confidentiality means protecting the information and the information remain between the client and organization, and not sharing the information with other people.

Integrity means the reliability and trusted data, which refers to real and accurate data.

Availability refers to access information from the specified location.

A.3.**सुरक्षा के लिए प्रमुख शर्तें गोपनीयता, सत्यनिष्ठा और उपलब्धता हैं।**

इसे सीआईए के नाम से भी जाना जाता है। इन तीन चीजों को सुरक्षा का सबसे महत्वपूर्ण घटक माना जाता है। गोपनीयता का अर्थ है ग्राहक और संगठन के बीच जानकारी और जानकारी की रक्षा करना, और अन्य लोगों के साथ जानकारी साझा नहीं करना।

वफ़ादारी का अर्थ है विश्वसनीयता और विश्वसनीय डेटा, जो वास्तविक और सटीक डेटा को संदर्भित करता है।

उपलब्धता का तात्पर्य निर्दिष्ट स्थान से जानकारी तक पहुँचने से है।

Q.4. What is Block chain ?

Q.4.**ब्लॉकचैन क्या है**?

A.4 It is an incorruptible digital ledger of economic transactions that can be programmed to record not only financial transactions but virtually everything of value. In simple terms, it is a decentralized distributed database of immutable records that are managed by a group of computer but not owned by any single entity. It is stored as a database or a flat-file.

A.4 **यह आर्थिक लेन-देन का एक अविनाशी डिजिटल बहीखाता है जिसे न केवल वित्तीय लेनदेन बल्कि लगभग सभी मूल्य के रिकॉर्ड को रिकॉर्ड करने के लिए प्रोग्राम किया जा सकता है। सरल शब्दों में, यह अपरिवर्तनीय अभिलेखों का एक विकेन्द्रीकृत वितरित डेटाबेस है जो कंप्यूटर के**

एक समूह द्वारा प्रबंधित किया जाता है लेकिन किसी एक इकाई के स्वामित्व में नहीं होता है। इसे डेटाबेस या फ्लैट-फाइल के रूप में संग्रहीत किया जाता है।

Q.5. How does block chain works?

प्रश्न 5. **ब्लॉकचेन कैसे काम करता है**?

A.5. is consists of immutable records of data called blocks with are linked using cryptography. It is nothing but a process to encrypt and secure data communication from third parties in reading private messages. Once the data has been recorded, it will not be changed. It works like a digital notary with timestamps to avoid Tampering of information.

ए.5.में डेटा के अपरिवर्तनीय रिकॉर्ड होते हैं जिन्हें ब्लॉक कहा जाता है जो क्रिप्टोग्राफी का उपयोग करके जुड़े होते हैं। यह निजी संदेशों को पढ़ने में तीसरे पक्ष से डेटा संचार को एन्क्रिप्ट और सुरक्षित करने की प्रक्रिया के अलावा और कुछ नहीं है। एक बार डेटा रिकॉर्ड हो जाने के बाद, इसे बदला नहीं जाएगा। यह बचने के लिए टाइमस्टैम्प के साथ एक डिजिटल नोटरी की तरह काम करता है

सूचना के साथ छेड़छाड़।

Q.6. What do you mean by Encryption?

प्रश्न 6. **एन्क्रिप्शन से आप क्या समझते हैं**?

A.6. It is a process of converting the data of file into an unreadable format to protect the data from attack. It is being widely used in an organization to secure their data.

ए.6. यह डेटा को हमले से बचाने के लिए फ़ाइल के डेटा को एक अपठनीय प्रारूप में परिवर्तित करने की प्रक्रिया है। किसी संगठन में अपने डेटा को सुरक्षित रखने के लिए इसका व्यापक रूप से उपयोग किया जा रहा है।

Q.7. How will you make your smart home more secure ?

प्रश्न 7. **आप अपने स्मार्ट होम को और अधिक सुरक्षित कैसे बनाएंगे**?

A.7. To make your smart home secure, do the following:

- Give your router a name: Don't stick with the name the manufacturer gave it – it might identify the make or model. Give it an unusual name.
- Change default usernames and password:

- Cybercriminals probably already know the default passwords that come with many iot products. That makes it easy for them to products. That makes it easy for them to access your IoT devices and, potentially , the information on Them, so, change default usernames, and passwords. Use unique, complex passwords made up of letters, numbers, and symbols.
- Keep your software up-to-date: Mobile security is important, since you may connect to your smart home through mobile devices. Updates – or you might have to visit their websites to check for them. Be sure to download update and apply them to your device to help stay safe.

- **ए.7. अपने स्मार्ट होम को सुरक्षित बनाने के लिए, निम्न कार्य करें:**
- **अपने राउटर को एक नाम दें: निर्माता द्वारा दिए गए नाम से चिपके न रहें यह मेक या मॉडल की पहचान कर सकता है। इसे एक असामान्य नाम दें।**
- **डिफ़ॉल्ट उपयोगकर्ता नाम और पासवर्ड बदलें:**
- **साइबर अपराधी शायद पहले से ही डिफ़ॉल्ट पासवर्ड जानते हैं जो कई आईओटी उत्पादों के साथ आते हैं। इससे उनके लिए उत्पादों के लिए आसान हो जाता है। इससे उनके लिए आपके IoT उपकरणों तक पहुंचना आसान हो जाता है और संभावित रूप से की जानकारी तक पहुंचना आसान हो जाता है**
- **उन्हें, इसलिए, डिफ़ॉल्ट उपयोगकर्ता नाम और पासवर्ड बदलें। अक्षरों, संख्याओं और प्रतीकों से बने अद्वितीय, जटिल पासवर्ड का प्रयोग करें।**
- **अपने सॉफ़्टवेयर को अप-टू-डेट रखें: मोबाइल सुरक्षा महत्वपूर्ण है, क्योंकि आप मोबाइल उपकरणों के माध्यम से अपने स्मार्ट होम से जुड़ सकते हैं। अपडेट - या आपको उनकी वेबसाइटों पर जाकर उनकी जांच करनी पड़ सकती है। सुरक्षित रहने में सहायता के लिए अपडेट डाउनलोड करना और उन्हें अपने डिवाइस पर लागू करना सुनिश्चित करें।**

Q.8. How will you make a password strong?

प्रश्न 8. **आप पासवर्ड को कैसे मजबूत बनाएंगे**?

A.8. A strong password must:

- Be eight characters long (character which include uppercase A-Z, lower case a-z; numbers 0-9; symbols found on the keyboard and spaces which include' ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " '< > , . ? /)
- Not contain user, real or company name.
- Not contain a complete word and be different from previous passwords.

ए.8. **एक मजबूत पासवर्ड होना चाहिए:**

- **आठ वर्ण लंबे हों (अक्षर जिसमें अपरकेस** AZ, **लोअर केस** az; **संख्या** 0-9; **कीबोर्ड और रिक्त स्थान पर पाए जाने वाले प्रतीक शामिल हों** ~ ! @ # $ % ^ **और** * **(** **)** _ - + = { } [ ] \ | : ; " '< > , . ? /)
- **उपयोगकर्ता, वास्तविक या कंपनी का नाम शामिल नहीं है।**
- **पूरा शब्द न हो और पिछले पासवर्ड से अलग हो।**

Q.9. What is different between Trojan horse and worm?

प्रश्न 9. **ट्रोजन हॉर्स और वर्म में क्या अंतर है**?

A.9. A Trojan horse is a term used to describe malware that appears, to the user, to perform a desirable function but, facilitates unauthorized access to the user's computer system.

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes and it may do so without any user intervention.

ए.9. **ट्रोजन हॉर्स एक ऐसा शब्द है जिसका उपयोग मैलवेयर का वर्णन करने के लिए किया जाता है, जो उपयोगकर्ता को वांछनीय कार्य करने के लिए प्रकट होता है, लेकिन उपयोगकर्ता के कंप्यूटर सिस्टम तक अधिकृत पहुंच की सुविधा प्रदान करता है।**

एक कंप्यूटर वर्म एक स्व-प्रतिकृति कंप्यूटर प्रोग्राम है। यह अन्य नोड्स को स्वयं की प्रतियां भेजने के लिए एक नेटवर्क का उपयोग करता है और यह बिना किसी उपयोगकर्ता हस्तक्षेप के ऐसा कर सकता है।

Q.10. What is DNS spoofing?

प्र.10. डीएनएस स्पूफिंग क्या है?

A.10. Domain Name Server (DNS) poisoning or spoofing is a type (DNS) poisoning or spoofing is a type of cyber-attack that exploits system vulnerabilities in the domain name server to divert traffic away from legitimate servers and directs it towards fake ones.

ए.10. डोमेन नेम सर्वर (DNS) पॉइज़निंग या स्पूफ़िंग एक प्रकार (DNS) पॉइज़निंग या स्पूफ़िंग एक प्रकार का साइबर-हमला है जो ट्रैफ़िक को वैध सर्वर से दूर करने के लिए डोमेन नाम सर्वर में सिस्टम कमजोरियों का फायदा उठाता है और इसे नकली सर्वर की ओर निर्देशित करता है।

Q11. What is Brute Force Attack ?

प्रश्न11. ब्रूट फोर्स अटैक क्या है?

A11. A Brute Force Attack is the simplest method to gain access to a site or server (or anything that is password protected). It tries various combinations of usernames and passwords again and again until it gets in. the longer the password, the more combinations that will need to be tested. However, if the password is weak it could merely take seconds with hardly any effort.

ए11. किसी साइट या सर्वर (या कुछ भी जो पासवर्ड से सुरक्षित है) तक पहुंच प्राप्त करने के लिए ब्रूट फोर्स अटैक सबसे सरल तरीका है। यह उपयोगकर्ता नाम और पासवर्ड के विभिन्न संयोजनों को बार-बार तब तक आज़माता है जब तक कि यह अंदर न आ जाए। पासवर्ड जितना लंबा होगा, उतने ही अधिक संयोजनों का परीक्षण करने की आवश्यकता होगी। हालाँकि, यदि पासवर्ड कमजोर है, तो इसमें केवल कुछ सेकंड लग सकते हैं, बिना किसी प्रयास के।

Q.12. What is Ransomware?

प्रश्न 12. रैंसमवेयर क्या है?

A.12. Ransomware is a form of malware that encrypts a victim's files. The victim to restore access to the data upon payment.

ए.12. रैंसमवेयर मैलवेयर का एक रूप है जो पीड़ित की फाइलों को एन्क्रिप्ट करता है। भुगतान पर डेटा तक पहुंच बहाल करने के लिए पीड़ित।

Q.13. What is Botnet?

A.13 Botnets consist of many bots working together, may be used to gain unauthorized access to computer system and infect computers . For example, The

attack used the Mirai IoT Botnet, taking control of over 600,000 Iot devices to flood Dyn with traffic in a massive DDoS attack. The devices seemed to be mostly routers and IP cameras.

IP cameras are frequently targeted IoT devices.

A.13 **बॉटनेट में एक साथ काम करने वाले कई बॉट होते हैं, जिनका उपयोग कंप्यूटर सिस्टम तक अनधिकृत पहुंच प्राप्त करने और कंप्यूटरों को संक्रमित करने के लिए किया जा सकता है। उदाहरण के लिए, हमले ने मिराई आईओटी बॉटनेट का इस्तेमाल किया, जिसमें** 600,000 **से अधिक आईओटी उपकरणों का नियंत्रण ले लिया गया ताकि बड़े पैमाने पर डीडीओएस हमले में यातायात के साथ डायन को बाढ़ कर दिया जा सके। डिवाइस ज्यादातर राउटर और आईपी कैमरे लग रहे थे।**

आईपी कैमरे अक्सर IoT **उपकरणों को लक्षित करते हैं।**

Q.14. List few tips to identify phishing.

प्रश्न 14. **फ़िशिंग की पहचान करने के लिए कुछ युक्तियों की सूची बनाएं।**

A.14. Few tips to identify the phishing are as follows:

- Do not trust the display name.
- Look at the content of the email, but do not click it.
- Do not give away any personal information.

ए.14. **फ़िशिंग की पहचान करने के लिए कुछ सुझाव इस प्रकार हैं:**

- **प्रदर्शन नाम पर भरोसा न करें।**
- **ईमेल की सामग्री को देखें, लेकिन उस पर क्लिक न करें।**
- **कोई भी व्यक्तिगत जानकारी न दें।**

Q.15. Discuss goal of Brute Force Attack.

प्रश्न 15. **ब्रूट फोर्स अटैक के लक्ष्य की चर्चा करें।**

A.15. Goal of Brute Force Attack are as follows:

- Theft of personal information such as passwords, passphrases and other information used to access online accounts and network resources.
- Collect credentials to sell to third parties.
- Defacement of websites and other information in the public domain that could damage the reputation of the organization.

- Redirecting domains to sites holding malicious content.

ए.15. ब्रूट फोर्स अटैक के लक्ष्य इस प्रकार हैं:

- **व्यक्तिगत जानकारी जैसे पासवर्ड, पासफ़्रेज़ और ऑनलाइन खातों और नेटवर्क संसाधनों तक पहुँचने के लिए उपयोग की जाने वाली अन्य जानकारी की चोरी।**
- **तृतीय पक्षों को बेचने के लिए क्रेडेंशियल एकत्र करें।**
- **सार्वजनिक डोमेन में वेबसाइटों और अन्य सूचनाओं का विरूपण जो संगठन की प्रतिष्ठा को नुकसान पहुंचा सकता है।**
- **दुर्भावनापूर्ण सामग्री रखने वाली साइटों पर डोमेन पुनर्निर्देशित करना।**

Q.16. How IoT and AI are used to track Endangered Species?

प्रश्न 16. **लुप्तप्राय प्रजातियों को ट्रैक करने के लिए** IoT **और** AI **का उपयोग कैसे किया जाता है**?

A.16. There are many animals that are endangered or going extinct in various countries So Wild Track's footprint identification technique (FIT) uses IoT and AI algorithms to identify the species, individual, age and gender of an animal from its unique footprint.

ए.16. ऐसे कई जानवर हैं जो विभिन्न देशों में लुप्तप्राय या विलुप्त हो रहे हैं, इसलिए वाइल्डट्रैक की पदचिह्न पहचान तकनीक (एफआईटी) आईओटी और एआई एल्गोरिदम का उपयोग किसी जानवर की प्रजातियों, व्यक्ति, उम्र और लिंग को उसके अद्वितीय पदचिह्न से पहचानने के लिए करती है।

Q.17. What is the difference between strong and weak artificial intelligence?

प्रश्न 17. **मजबूत और कमजोर कृत्रिम बुद्धिमत्ता में क्या अंतर है**?

A.17. The difference between strong and weak artificial Intelligence are listed below:

ए.17. मजबूत और कमजोर आर्टिफिशियल इंटेलिजेंस के बीच अंतर नीचे सूचीबद्ध हैं:

Weak AI	Strong AI
Narrow application, with very limited scope **बहुत सीमित दायरे के साथ संकीर्ण अनुप्रयोग**	Widely applied, with vast scope **व्यापक रूप से लागू, विशाल दायरे के साथ**
Good at specific tasks	Incredible human level intelligence

विशिष्ट कार्यों में अच्छा	**अतुल्य मानवीय स्तर की बुद्धिमत्ता**
Uses supervised and unsupervised learning to process data **डेटा को संसाधित करने के लिए पर्यवेक्षित और अनुपयोगी शिक्षण का उपयोग करता है**	Uses clustering and association to process data **डेटा को संसाधित करने के लिए क्लस्टरिंग और एसोसिएशन का उपयोग करता है**
For example Siri, Alexa, etc. **उदाहरण के लिए सिरी, एलेक्सा, आदि।**	For example advanced Robotics **उदाहरण के लिए उन्नत रोबोटिक्स**

Q.18. What is the difference between IoT and AI?

प्रश्न 18. IoT **और** AI **में क्या अंतर है**?

A.18. The difference between IoT and AI are listed below:

IoT	AI
IoT is a concept based on the very idea of everyday physical objects with the ability to communicate directly over the Internet. IoT is a vast network of interrelated computing devices connected to the internet. These devices can sense, accumulate and transfer data over a network without any human interaction. IoT **इंटरनेट पर सीधे संवाद करने की क्षमता** **के साथ रोजमर्रा की भौतिक वस्तुओं के विचार पर आधारित एक अवधारणा है।** IoT **इंटरनेट से जुड़े परस्पर संबंधित कंप्यूटिंग उपकरणों का एक विशाल नेटवर्क है।** **ये डिवाइस बिना किसी मानवीय संपर्क के नेटवर्क पर डेटा को समझ सकते हैं, जमा कर सकते हैं और स्थानांतरित कर सकते हैं।**	Artificial Intelligence (AI), on the other hand, is an area of computer science to create machines to do intelligent things the way humans do, or possibly even better. AI, on the other hand, is all about creating smart, intelligent machines that can behave and react like humans, providing them with the actuation, data strong and processing. **दूसरी ओर, आर्टिफिशियल इंटेलिजेंस (एआई), कंप्यूटर विज्ञान का एक क्षेत्र है जो बुद्धिमान** **चीजों को करने के लिए मशीनों का निर्माण करता है जिस तरह से मनुष्य करते हैं, या संभवतः इससे भी बेहतर।** **दूसरी ओर, एआई स्मार्ट, बुद्धिमान मशीनें बनाने के बारे में है जो मनुष्यों की तरह व्यवहार और प्रतिक्रिया कर सकती हैं, उन्हें एक्चुएशन, डेटा मजबूत और प्रसंस्करण प्रदान कर सकती हैं।**

IoT is about connecting machines and making use of the data generated from those machines. IoT **मशीनों को जोड़ने और उन मशीनों से उत्पन्न डेटा का उपयोग करने के बारे में है।**	AI is about simulating intelligent behavior in machines of all kinds. **एआई सभी प्रकार की मशीनों में बुद्धिमान व्यवहार का अनुकरण करने के बारे में है।**
IoT will not work without AI. **बिना** AI **के** IoT **काम नहीं करेगा।**	AI is not dependable on IoT. AI IoT **पर निर्भर नहीं है।**
Applications include fitness trackers, health monitoring devices, smart wearable's, smart parking etc. **अनुप्रयोगों में फिटनेस ट्रैकर, स्वास्थ्य निगरानी उपकरण, स्मार्ट वियरेबल्स, स्मार्ट पार्किंग आदि शामिल हैं।**	Application of AI include machine learning, natural language processing, robotics, speech recognition etc. **एआई के अनुप्रयोग में मशीन लर्निंग, प्राकृतिक भाषा प्रसंस्करण, रोबोटिक्स, वाक् पहचान आदि शामिल हैं।**

Q.23. List some application of AI.

प्रश्न 23. **एआई के कुछ अनुप्रयोगों की सूची बनाएं।**

A.23. Some applications of AI are:

- Natural language processing
- Chatbots
- Sales prediction
- Self-driving card Facial expression recognition Image tagging

ए.23. **एआई के कुछ अनुप्रयोग हैं:**

- **प्राकृतिक भाषा प्रसंस्कर**
- **चैटबॉट**
- **बिक्री की भविष्यवाणी**
- **सेल्फ़-ड्राइविंग कार्ड चेहरे की अभिव्यक्ति पहचान छवि टैगिंग**