4 IoT Security and Challenges

Syllabus

IOT Security, Dangers, Assigning values to Information, Security Components, Key Management, Update Management, Challenges in IoT security.

Contents

4.1 IoT Security Issues and Need

- The Internet of Things (IoT) refers to a concept of connected objects and devices of all types over the Internet wired or wireless. The popularity of IoT or the Internet of Things has increased rapidly, as these technologies are used for various purposes, including communication, transportation, education, and business development.
- The unconscious use, not changing passwords and the lack of device updates have increased cybersecurity risks and access to malicious applications to the IoT systems sensitive data.
- Most of the security professionals consider IoT as the vulnerable point for cyber-attacks due to weak security protocols and policies. Even though several security mechanisms were developed to protect IoT devices from cyber-attacks, security guidelines are not appropriately documented.
- IoT enabled devices have been used in industrial applications and for multiple business purposes. The apps help these businesses to attain a competitive edge over their competitors.
- However, due to the excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services.
- IoT system functionalities :
  1. Security patch must be upload time to time in microprocessor firmware.
  2. Monitor the access and usage of public network.
  3. User authentication is necessary.
  4. Only after authentication can the controller direct commands for things control that are present in the system.
- The Internet of Things (IoT) has become a ubiquitous term to describe the tens of billions of devices that have sensing or actuation capabilities and are connected to each other via the Internet.

Risks :

- The IoT includes everything from wearable fitness bands and smart home appliances to factory control devices, medical devices and even automobiles. Security has not been a high priority for these devices until now.
- The security of the Internet of Things, the following principles can be established.
  a) **Identity :** Trust is always tied to an identity. Therefore every device needs a unique identity that can't be changed. The device must also be able to prove its identity at all times.

b) **Positive intention :** The device and linked service have positive intentions.

c) **Predictability and transparency :** The functional scope of the service provided by devices is known to its full extent. There are no undocumented (secret) functions. The behaviour of the system can be checked at any time by independent third parties.

d) **Reputation :** An increasing number of positive interactions between the things gradually form a reputation based intelligent network.

4.1.1 Security Architecture

- Fig. 4.1.1 shows IoT security architecture. (See Fig. 4.1.1 on next page.)
- IoT systems are often highly complex, requiring end-to-end security solutions that span cloud and connectivity layers, and support resource-constrained IoT devices that often aren't powerful enough to support traditional security solutions.
- Application layer support user services. This layer helps users access IoT through the interface using PC, mobile equipment etc. This layer also support secure communication protocol and authentication protocols.
- Network layer support wired and wireless communication protocol and technology. This layer is responsible for dependable broadcast of data and information from the below layer.
- Sensors are the monitors that pick up data and relay it for further analysis. Actuators are devices that act as robotic controls. Many IoT attacks have used actuators, such as printers, as launch points into a business's network.
- An IoT security architecture is a blueprint that illustrates all components of the IoT infrastructure for all IoT projects and details how to secure each component.
- In both cases, it is imperative to ensure device access is controlled via settable passwords, encrypt any data stored locally and monitor and contain any executable code run by the device.
- Physical layer gathers all types of information with the help of physical equipment. IoT devices face many threats, including malicious data that can be sent over authenticated connections, exploiting vulnerabilities and/or misconfigurations.
- Such attacks frequently exploit many weaknesses, including but not limited to
  a) Failure to use code signature verification and secure boot,
  b) Poorly implemented verification models which can be bypassed.

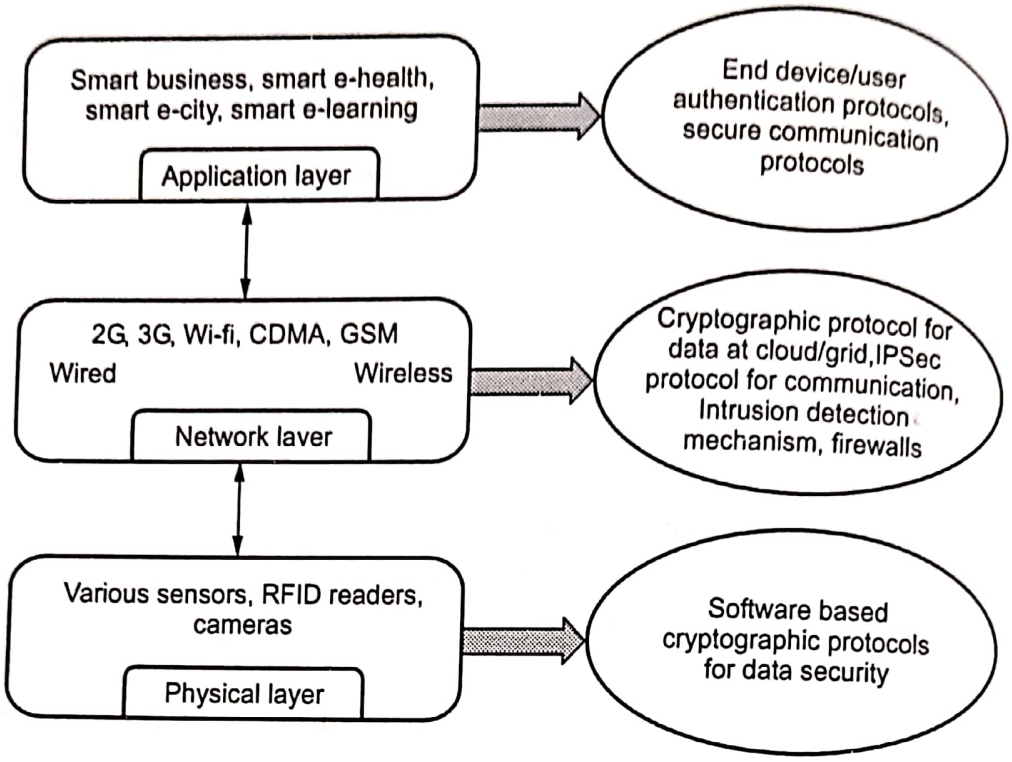

Fig. 4.1.1

- Attackers often use those weaknesses to install backdoors, sniffers, data collection software, file transfer capabilities to extract sensitive information from the system, and sometimes even Command & Control (C & C) infrastructure to manipulate system behaviour.

4.1.2 Security Requirement

- The key requirements for any IoT security solution are :
  1. Device and data security, including authentication of devices and confidentiality and integrity of data.
  2. Implementing and running security operations at IoT scale.
  3. Meeting compliance requirements and requests.
  4. Meeting performance requirements as per the use case.
- Application layer : Verification and user's confidentiality
- Support layer : Various encryption algorithms
- Network layer : Distributed denial of service attack
- Physical layer : Authentication.

4.2 Assigning Values to Information

- An information asset can be described as information or data that is of value to the organization, including such information as patient records, intellectual property, or customer information. These assets can exist in physical form (on paper) or electronically (stored on databases, in files, on PC).
- An information asset container is where information assets are stored, transported, or processed.
- Identification, valuation and categorization of information systems assets are critical tasks of the process to properly develop and deploy the required security control for the specified IT assets.
- Quantitative measurement of risk impact is implemented based on the following formula :

  Risk impact = Potential risk × Probability of occurrence
- Potential risk is a product of total asset value, severity of vulnerability and severity of threat :

  Potential risk = Total asset value × Severity of vulnerability × Severity of threat
- Asset valuation : This is a method of assessing the worth of the organization's information system assets based on its Confidentiality, Integrity and Availability (CIA) security.

  Total asset value = Asset value × Weight of asset
- Assumptions for asset valuation include :
  a) The value of an asset depends on the sensitivity of data inside the container and their potential impact on CIA.
  b) CIA of information will have a minimum value of 1 for each.
  c) The value of levels for CIA are as follows: A rating of 3 is high, 2 is medium and 1 is low.
  d) The value of the information asset is determined by the sum of the three (C + I + A) attributes.

Weight of Asset

- The actual value of an asset is determined by the sensitivity value of data in the container. The reason is that all similar containers are not equally important to the organization, and the value of a container is determined by the data it holds, processes or transfers.
- For example, servers with equal capacity, technology and cost may have different weights due to the data they hold, process or transfer.

- A database containing employee information may have less value than one containing customer transactions. Equally, data on prominent customers may have more value than data on ordinary/walk-in customers, based on business/organizational objectives.

4.2.1 Risk Assessment

- Risk assessment basically involves the calculation of the magnitude of potential consequences (levels of impacts) and the likelihood (levels of probability) of these consequences to occur. Essentially, the higher the probability of a "worse" effect occurring, the greater the level of risk.

  Risk = Threats × Vulnerabilities

- This is a common formula that is used to determine the likelihood of risk. It's a good way to approach finding risk because it addresses the key factors in a cyber security threat.

  Risk = (Likelihood of occurrence of vulnerability) × (Value of the information asset) – (% of risk mitigated by current controls) + (Uncertainty of current knowledge of vulnerability).

- Fig. 4.2.1 shows risk assessment steps.

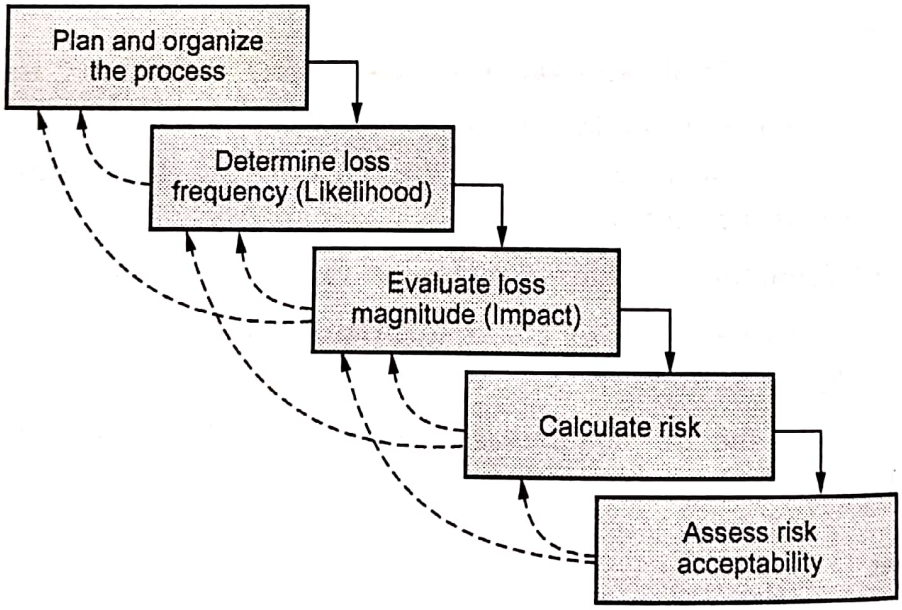

Fig. 4.2.1 Risk assessment steps

Step 1 : Identify the hazards

Step 2 : Decide who might be harmed and how

Step 3 : Evaluate the risks and decide on precautions

Step 4 : Record your findings and implement them

Step 5 : Review your assessment and update if necessary

- The objective of risk assessment is to determine the level of risk exposure on the information asset by analyzing the vulnerability factor (extent of impact), threat likelihood (likelihood of exploitation) and the risk occurrence rate. There are two sub-processes for conducting the risk assessment - Risk analysis and Risk evaluation.
- Risk analysis can be undertaken either qualitatively or quantitatively or semi-quantitatively. In this procedure, qualitative information security risk assessment method has been adopted.
- Risk evaluation : Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about future action
- Risk assessment is a term used to describe the overall process or method where you:
  1. Identify hazards and risk factors that have the potential to cause harm (hazard identification).
  2. Analyze and evaluate the risk associated with that hazard (risk analysis, and risk evaluation).
  3. Determine appropriate ways to eliminate the hazard, or control the risk when the hazard cannot be eliminated (risk control).
- A risk assessment is a thorough look at your workplace to identify those things, situations, processes, etc. that may cause harm, particularly to people. After identification is made, you analyze and evaluate how likely and severe the risk is. When this determination is made, you can next, decide what measures should be in place to effectively eliminate or control the harm from happening.

Identify Possible Controls

- **Residual risk** is the risk to the information asset that remains even after the application of controls. Either there are no control measures that could prevent it, or they would be disproportionate to the level or risk presented.
- General categories of controls are policies, programs, and technologies.
- Policies are documents that specify an organization's approach to security. Various types of security policies are general security, program security, issue-specific and systems-specific policies.
  1. General security policy : These policies are an executive-level document that outlines the organization's approach and attitude toward information security and relates the strategic value of information security within the organization.
  2. Program security policy : This policy contains planning documents. It is an outline the process of implementing security in the organization. This policy act as a blueprint for the analysis, design, and implementation of security.

3. Issue-specific policies : This policy gives idea about specific implementations of policy. These policies are typically developed to provide detailed instructions and restrictions associated with security issues. Examples include policies for Internet use, e-mail, and access to the building.
4. Systems-specific policies address the particular use of certain systems

4.3 Security Components

- How to protect the valuable assets ? It is necessary to keep in safe place like a bank to protect the valuable assets. But bank is not a safe place now a day. There are so many examples where bank robbery in our country.
- Bank robbery is the crime of stealing from a bank during opening hours. Protecting assets was difficult and not always effective.
- Now a day, protection is easier because many factors working against the potential criminal. Very sophisticated alarm and camera systems silently protect secure places like banks.
- Traditionally information security provided by physical i.e. rugged filing cabinets with locks and administrative mechanisms i.e. personnel screening procedures during hiring process.
- Asset protection systems are designed to recover stolen cash and high value assets, apprehend criminals and deter crime. The system has the capacity to track, protect and manage critical assets in real-time.
- The techniques of criminal investigation have become so effective that a person can be identified by genetic material, voice, retinal pattern, fingerprints etc.
- Use of networks and communications links requires measures to protect data during transmission.
- Data security is the science and study of methods of protecting data from unauthorized disclosure and modification.
- Data and information security is about enabling collaboration while managing risk with an approach that balances availability versus the confidentiality of data.
- Computer security : Generic name for the collection of tools designed to protect data and to hackers.
- Network security : Measures to protect data during their transmission.
- Internet security : Measures to protect data during their transmission over a collection of interconnected networks.
- Physical security : To protect physical items, objects, or areas from unauthorized access and misuse

- Personnel security : To protect the individual or group of individuals who are authorized to access the organization and its operations
- Operations security : To protect the details of a particular operation or series of activities
- The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.
- Fig. 4.3.1 shows components of information security.

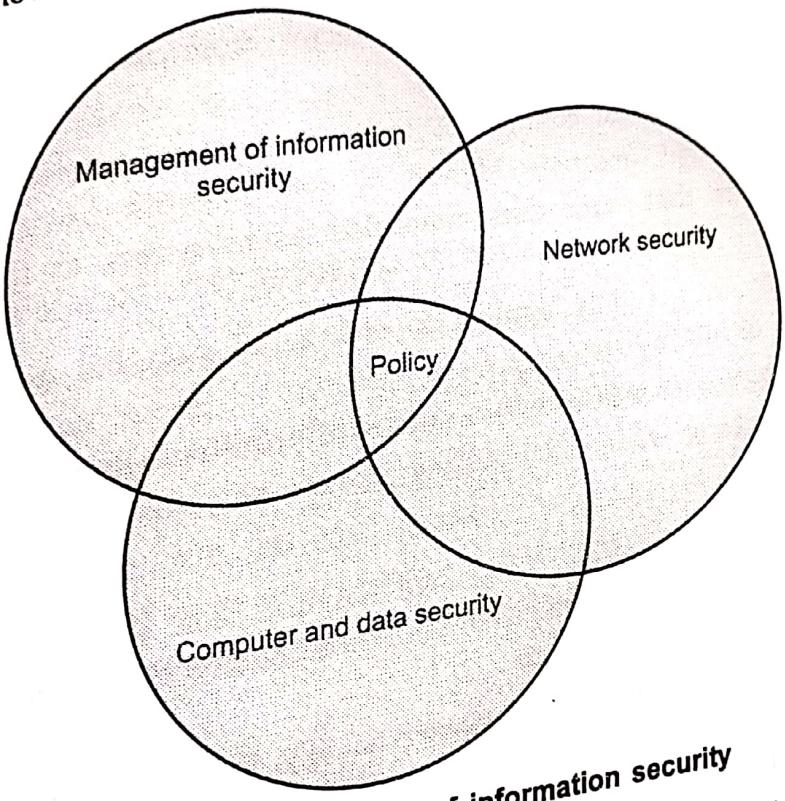

Fig. 4.3.1 Components of information security

- The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A triangle.
- The CIA triad is a widely used information security model that can guide an organization's efforts and policies aimed at keeping its data secure. The model has nothing to do with the U.S. Central Intelligence Agency; rather, the initials stand for the three principles on which infosec rests :
- Confidentiality : Only authorized users and processes should be able to access or modify data
- Integrity : Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously

- Availability : Authorized users should be able to access data whenever they need to do so.

Security Goals :

- **Security goals are as follows :** 1. Confidentially 2. Integrity 3. Availability

1. Confidentiality

- Confidentiality ensures that no one can read the message except intended receiver.
- Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones.
- Sensitive information should be kept secret from individuals who are not authorized to see the information.
- Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords that uniquely identify a data system's users, and supporting control methods that limit each identified user's access to the data system's resources.
- Confidentiality is not only applied to storage of data but also applies to the transmission of information.
- Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.

2. Integrity

- Integrity ensures that received message has not been altered in any way from origin. It refers to the trustworthiness of information resources. Integrity should not be altered without detection.
- It includes the concept of "data integrity" namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity.
- It also includes "origin" or "source integrity" that is, that the data actually came from the person or entity you think it did, rather than an imposter.
- Integrity ensures that information is not changed or altered in transit. Under certain attack models, an adversary may not have to power to impersonate an authenticated party or understand a confidential communication, but may have the ability to change the information being transmitted.
- On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

3. Availability

- Availability refers, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all.
- Availability means that people who are authorized to use information are not prevented from doing so. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.
- Almost all modern organizations are highly dependent on functioning information systems. Many literally could not operate without them.
- Availability, like other aspects of security, may be affected by purely technical issues (e.g. a malfunctioning part of a computer or communications device), natural phenomena (e.g. wind or water), or human causes (accidental or deliberate).

4.3.1 Components of an Information System

- An Information System can be defined technically as a set of interrelated components that collect (or retrieve), process, store and distribute information to support decision making and control in an organization
- An information system is essentially made up of five components hardware, software, database, network and people. These five components integrate to perform input, process, output, feedback and control.
- Fig. 4.3.2 shows components of information system.

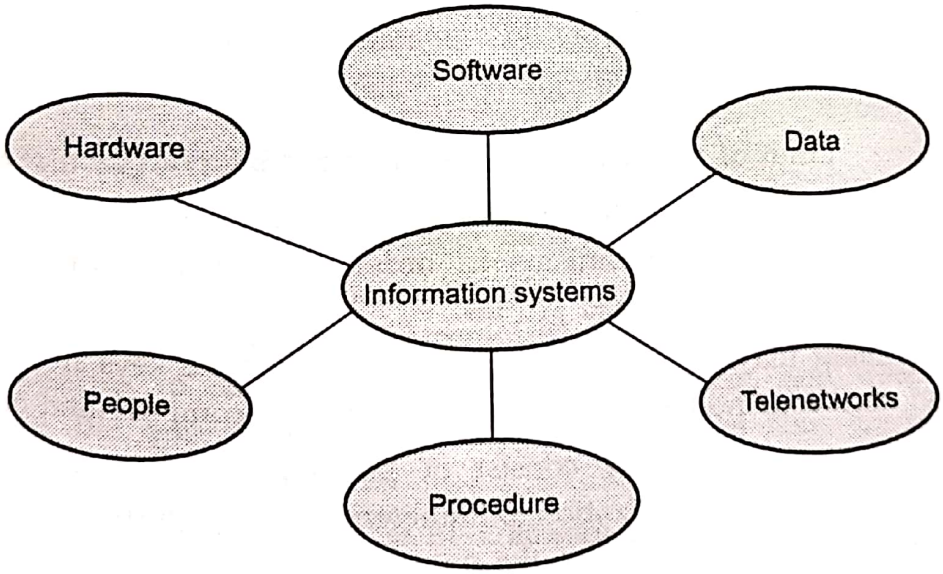

Fig. 4.3.2 Components of information system

- Information systems activities are Input, Processing and Output. 'Input' consists of acquisition of the 'raw data', which is transformed into more meaningful packets of 'Information' by means of 'Processing'.

- The processed information now flows to the users or activities also called as 'Output'. The shortcomings are analyzed and the information is sent back to the appropriate members of the organization to help them evaluate and refine the input. This is termed as 'feedback'.
- Hardware consists of input/output device, processor, operating system and media devices. Software consists of various programs and procedures.
- Database consists of data organized in the required structure. Network consists of hubs, communication media and network devices. People consist of device operators, network administrators and system specialist.
- Information processing consists of input; data process, data storage, output and control. During input stage data instructions are fed to the systems which during process stage are worked upon by software programs and other queries. During output stage, data is presented in structured format and reports.

4.4 Key Management

- Management and handling of the pieces of secret information is generally referred to as **key management.**
- Activities of key management includes selection, exchange, storage, certification, revocation, changing, expiration and transmission of the key.
- Key management is the set of processes and mechanisms which support key establishment and maintenance of ongoing keying relationship between parties, including replacing older key with new keys.
- Two major issues in key management are :
  1. Key life time
  2. Key exposure
- Key life time - Limit of use which can be measured as a duration of time.
- Key management is a set of techniques to initialize, register, update, and recover keys for cryptographic mechanisms in order to ensure privacy, integrity, and authentication among authorized parties.
- Key management may also be called a process to revoke keys from compromised or detected malicious nodes and update keys for non-compromised ones.
- The contents of the key may consist of public/private key pairs, secret keys, non-secret parameters, initialization parameters, and supporting key management in various instances, depending on the nature of the scheme being used.
- Symmetric key cryptography also known as shared key ciphers. It is type of cryptography in which the same key is used by both the sender and receiver for the encryption and decryption of plaintext and ciphertext, respectively.

- Asymmetric key cryptography uses two types in a pair called as public key and private key in a pair. It is also called as public key cryptography. The private key is used to decrypt the cipher text and generate the digital signature, whereas the public key is used to encrypt plaintext and to verify the digital signature.
- Trusted third party is certification authority that grants a digital certificate. The certificate is usually the public key of that organization to whom this certificate is issued. A third trust party acceptable by both sender and receiver is performing the task of guarantor.
- Dynamic Key Management Schemes (DKM) : In dynamic key management schemes, different keys are assigned for different sessions. Once the communication session terminated or finished between the sender and receiver, the keys for the next session will be dynamically assigned to nodes without any revocation or updating command.
- Contributory / Distributed key management schemes : Contributory/Distributive schemes are symmetric cryptographic based solutions characterized by the lack of a trusted third party which is normally responsible for the generation and distribution of the cryptographic keys.
- Centralized key management schemes : These schemes require centralized Trusted Authority (TA) which is designated to generate and distribute a unique session key for all concerned group members in the Internet of Things. The key in Internet of Things update is difficult to manage because of its dynamic topology and its connection is varied with multiarchitecture clients/nodes.
- In static key management schemes, the key is created for the overall lifetime of nodes by either mutual agreement, symmetric cryptography, or centralized certification authority, in asymmetric cryptography.

4.5 Update Management

- Update management represents another term for patch management.
- Patch management is the process that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones. Managing patches thus becomes easy and simple.
- Patch Management is mostly done by software companies as part of their internal efforts to fix problems with the different versions of software programs and also to help analyze existing software programs and detect any potential lack of security features or other upgrades.

- Patching is a process to repair a vulnerability or a flaw that is identified after the release of an application or a software. Newly released patches can fix a bug or a security flaw, can help to enhance applications with new features, fix security vulnerability.
- Unpatched software can make the device a vulnerable target of exploits. Patching a software as and when the patch is released is critical to deny malware access.
- Software vendors release patches to fix vulnerabilities identified after the release of a software or application. Patch Management enables patch testing and deployment which is a critical aspect of cyber security. Quick and instant responses to patch updates would mitigate the chances of data breaches that can cause due to unpatched software.

4.6 Challenges in IoT Security

- The security challenges are as follows :
  a. **Devices are not reachable :** Most of the time a device is not connected.
  b. **Devices can be lost and stolen :** Makes security difficult when the device is not connected.
  c. **Devices are not crypto-engines :** Strong security difficult without processing power.
  d. **Devices have finite life :** Credentials need to be tied to lifetime.
  e. **Devices are transportable :** Will cross borders.
- IoT system has a cloud database that is connected to all your devices. These devices are connected to the internet and it could be accessed by the cybercriminals and hackers. As the number of connected devices increases, chances for hackers to breach the security system gets increased.

4.7 Fill in the Blanks

Q.1 _____ is the process of encoding a plain text message into non-readable form.

Q.2 _____ is a process of transferring an encrypted message back into its normal form.

Q.3 Update management represents another term for _____ management

Q.4 Symmetric key cryptography also known as _____ key ciphers

Q.5 In _____ key management schemes, the key is created for the overall lifetime of nodes by either mutual agreement, symmetric cryptography, in asymmetric cryptography

Q.6 _____ key cryptography uses two types in a pair called as public key and private key in a pair

Q.7 Confidentiality ensures that no one can _____ the message except intended receiver.

4.8 Multiple Choice Questions

Q.1 List the components of information security.

a Network security
b Computer and data security
c Management of information security
d All of these

Q.2 The _____ model of information security evolved from a concept developed by the computer security industry called the C.I.A triangle.

a NSS
b CNSS
c McCumber
d None of these

Q.3 _____ refers to the security flaws in a system that allows an attack to be successful.

a Vulnerability
b Availability
c Integrity
d Confidential

Q.4 When an entire message is encrypted for _____, using either symmetric or asymmetric encryption, the security of the scheme generally depends on the bit length of the key.

a integrity
b non-repudiation
c availability
d confidentiality

Q.5 Components of information system are _____

a software
b network
c database
d all of these

Q.6 The original message is called as _____.

a ciphertext
b plaintext
c cryptography
d encryption

Q.7 The process of converting plaintext to ciphertext is called as _____.

a encryption
b decryption
c substitution
d transposition

Q.8 Information has _____ when it is protected from disclosure or exposure to unauthorized individuals or systems.

a integrity
b confidentiality
c availability
d authentication

Q.9 Secret key cryptography is also known as _____.

a symmetric key cryptography
b asymmetric key cryptography
c private key cryptography
d quantum cryptography

Q.10 The _____ is a widely used information security model that can guide an organization's efforts and policies aimed at keeping its data secure.

a CIA triad
b ARPANET
c NIST
d None

Q.11 A loss of _____ is the unauthorized disclosure of information.

a integrity
b availability
c authentication
d confidentiality

Q.12 Which of the following are the security requirements triad ?

a Confidentiality
b Integrity
c Availability
d All of these

Q.13 _____ prevents either sender or receiver from denying a transmitted message.

a Nonrepudiation
b Replay
c Fabrication
d Masquerade

Answer Keys for Fill in the Blanks

Q.1	Encryption	Q.2	Decryption	Q.3	patch
Q.4	shared	Q.5	static	Q.6	Asymmetric
Q.7	read				

Answer Keys for Multiple Choice Questions

Q.1	d	Q.2	b	Q.3	a	Q.4	d
Q.5	d	Q.6	b	Q.7	a	Q.8	b
Q.9	a	Q.10	a	Q.11	d	Q.12	d
Q.13	a						