Section - II

* IOT Security - technology segment focused on safeguarding connected devices & networks in IOT

def. OT :- Stands for Operational technology which is understood to comprise both h/w & s/w that control and monitor physical devices.

(design to meet unique security needs of operational technology environment)

OT used not only in production plants, but also in many other sectors such as energy & water providers & in medical technology.

IOT - Internet of things (Things that are embeded with sensor, s/w, & other tech for the purpose of connecting & exchanging data with other systems.

IIOT - Industrial internet of things (IIOT) refers to the extension & use of IOT in industrial sectors & appln.

ICS - Industrial Control Systems

While rise of smart devices & IOT is transforming industrial control system (ICS) networks, increasing usability, efficiency and productivity in ICS environments, they also have a significant impact on ICS security.

Intro to most widely used protocols in IOT

* **MQTT** :— Message queuing telemetry transport protocol is comm^n based protocol that is used for IOT devices. —

This protocol is based on publish-subscribe methodology in which clients receive the information through a broker only to subscribed topic

* **COAP** - Constrained Appl^n Protocol

- It is a client server based protocol.
- With this protocol COAP packet can be shared bet^n different client nodes which are commanded by the COAP server.
- Server is responsible to share the info depending on its logic but has not acknowledged it
- used with appl^n which support the state transfer model

* Block Chain :—

- It is a distributed database of records of all transactions or digital event that have been executed & shared among participating parties.
- each transaction verified by majority of participants of the system.
- Contains every single record of each transaction.
- Bitcoin is the most popular cryptocurrency an example of blockchain.

* Decentralised System :—

In blockchain, decentralization refers to transfer control & decision making from centralized entity (individual, organization or group thereof) to distributed network

* Distributed ledger tech :—

- It is a digital system for recording transaction of assets in which the transaction and their details are recorded in multiple places at the same time.

→

* Block chain computing power

* HASH - It is a fun^ that meets the encrypted demands needed to solve for a block chain computations.

* Merkle tree - Hash tree is also known as Merkle tree.
- It is a tree in which leaf node is labeled with hash value of data block & each non leaf node is labeled with hash value & its child nodes labels.

* Multiple Use-Cases of Blockchain

1. Money transfer
2. Smart contract
3. IOT
4. Logistics
5. education
6. medical field
7. cross border transactions

* Different types of block chain

1. Public Blockchain
2. Private Blockchain

M T W T F S S
Page No.
Date
YOUVA

* Public Blockchain :—

It is permissionless distributed ledger on which anybody can join & conduct transactions.

Can be used in voting to ensuring openness & trust.

* Private Blockchain :—

A blockchain network operates in private context, such as restricted network, or is controlled by single identity.

- Can be used in Company's supply chain

* Consensus —

- algorithm that makes the decentralized record keeping more similar to centralized database.
- Automated process to ensure that there exists only one single valid copy of record shared by all nodes.

Types :— ① Proof of Work
② Practical Byzantine fault tolerance
③ Proof of Stake
④ Proof of Burn
⑤ proof of Capacity
⑥ Proof of Elapsed time

* Need of Smart Contract :—

* Smart Contract :—

- Smart contract are Completer program that stored on etherium's blockchain.

- Contract can be used to build currencies and ~~stored~~

* Smart contract language is—

Solidity
jupiter
Vyper.

Solidity is high level object oriented prog. language used for creating Smart contract

* EVM in relation with Smart contracts

Etherium virtual machine is runtime environment for smart Contract in etherium.

Developer can create appl^n that run on evm using Solidity

* Ether :-

- ether is primary digital assets or cryptocurrency of ethereum platform.
- It is transactional token that facilates operation on ethereum.
- All Gas prices are paid ethers.

* Smart Contract in Ethereum Blockchain

It is simply a program that runs on ethereum block chain.

* Cryptoeconomics

It is use of incentives & encryption to create systems, appl^ & networks.

- Cryptocurrency

It is a digital currency, which an alternative form of payment created using encryption algo.

- currency that exists digitally or virtually

* Types of Cryptocurrency & Cryptography —

Types of Cryptocurrency — ① payment Cryptocurrency
② Utility tokens
③ Stablecoins
④ Central Bank Digital currencies

Types of Cryptography :—

Secret key cryptography
public key cryptography
Hash fun^{n}

* Valid And invalid Transactions :—

* Permissioned Blockchain :-

decentralized computation & info sharing platform that enables multiple authoritative domains which do not trust each other to co-operate, co-ordinate & collaborate in rational decision making process under closed environment with enablement of security such as authentication & authorization

* Permissioned Blockchain - RAFT Consensus

Idea behind Raft consensus algo is that nodes collectively select leader & remaining nodes become the followers.

* Byzatine Generals Problem

It is an impossibility result which means that soln to the problem has not been found yet as well as helps us to understand the importance of blockchain.