IoT Security & Forensics

M.Sc. CyberSecurity

Submitted to :
Dr. Manu VT

Submitted by : Raj Shekhar
Roll no. : 24054500200 4
Session : 2024 - 2026
Semester : III rd

Date / /
Page No.
Shivalal

UNIT - 1 INTRODUCTION TO IoT
(Internet of Things)

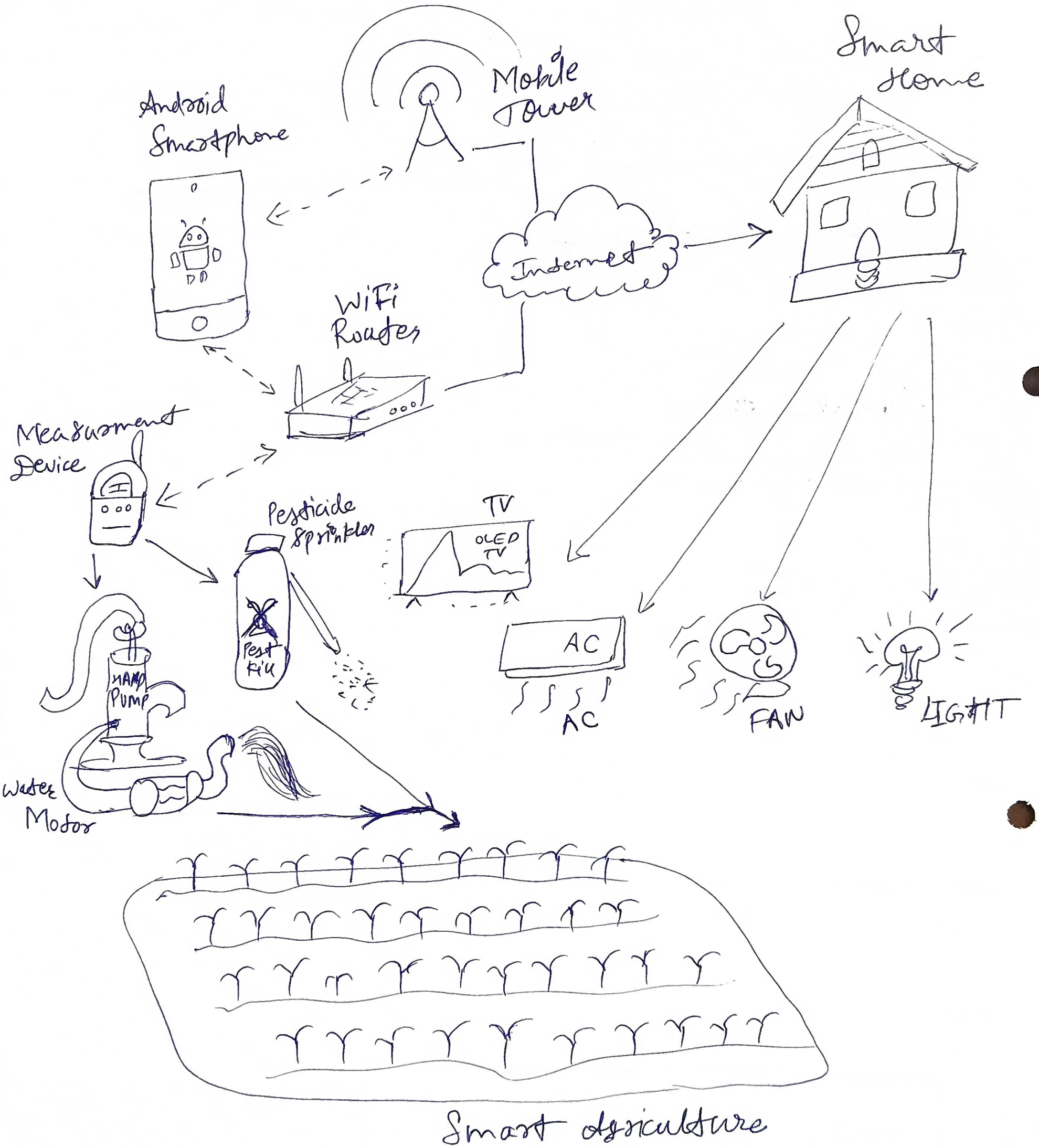
1. IoT Architecture

→ Physical Design : It consists of several interfaces Connectivity, Processor, Audio/Video interfaces, Memory Interfaces, Graphics, Storage, I/O, and for communication the system consist of Link layer, Network layer, Transport layer, Application layer.

→ Logical Design : It consists of Application, Services, Communication, Management, Security, Device that enables capabilities for identification, sensing, actuation, communication & management.

There are 6 kinds of communication model:
1. Request - Response communication model
2. Publish - Subscribe communication model
3. Push - Pull communication model
4. Exclusive Pair communication model
5. REST based communication model
6. Websocket-based communication model

→ IoT Levels : There are 5 levels to deploy IoT as follows:
1. Level 1 : Data stored locally & analysed locally
2. Level 2 : Data stored in cloud & analysed locally
3. Level 3 : Data stored and analysed on cloud.
4. Level 4 : Data sensed from multiple sources else like Level 3.
5. Level 5 : A coordinator node to categorise data before anything else same as Level 4.

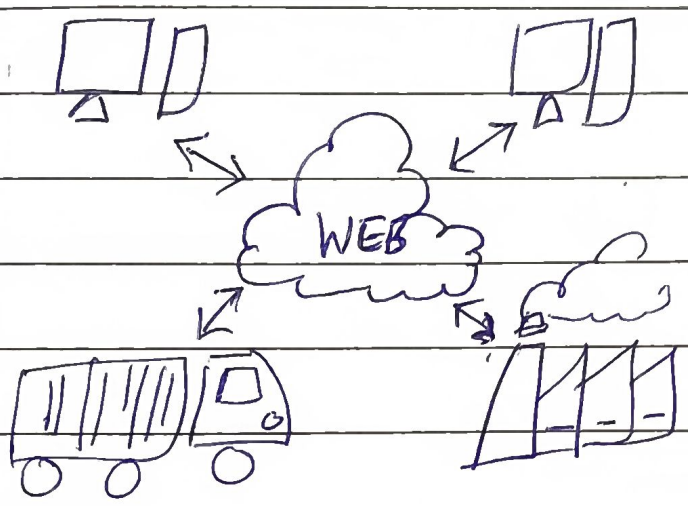
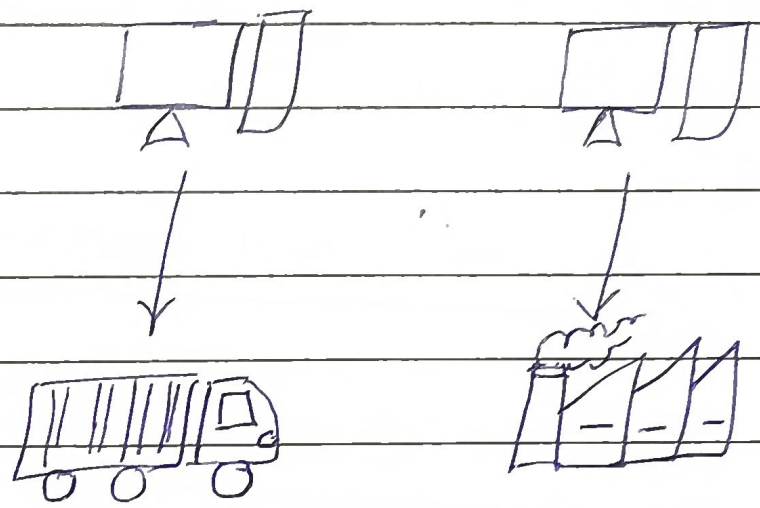

Android Smartphone
Mobile Tower
Smart Home
Internet
WiFi Router
Measurment Device
Pesticide Sprinkler
TV
OLED TV
Pest Rid
HAND PUMP
Water Motor
AC
AC
FAN
LIGHT
Smart agriculture

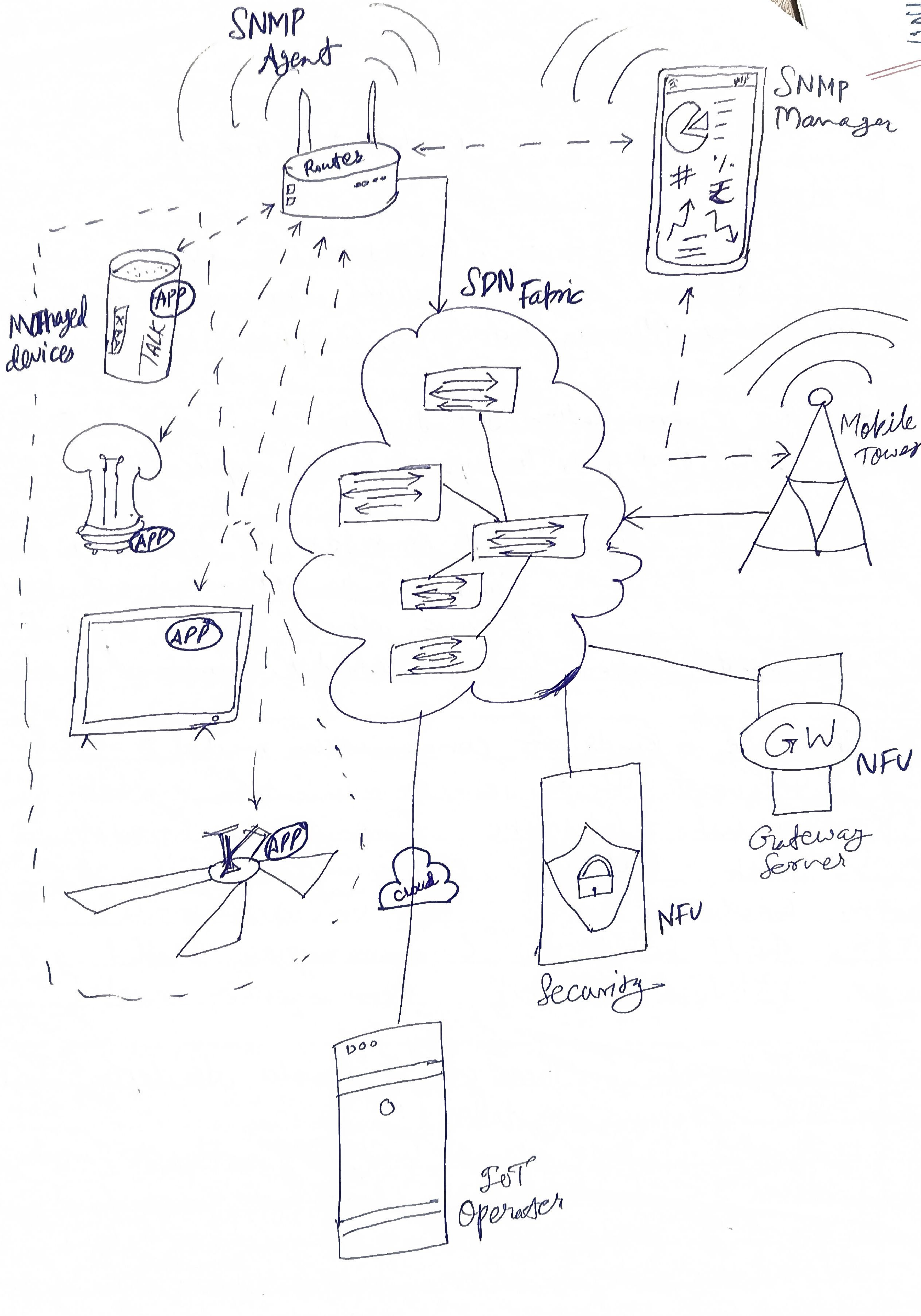
UNIT - II M2M & System Management

(Machine to Machine)

Date / /
Page No.
Shivalal

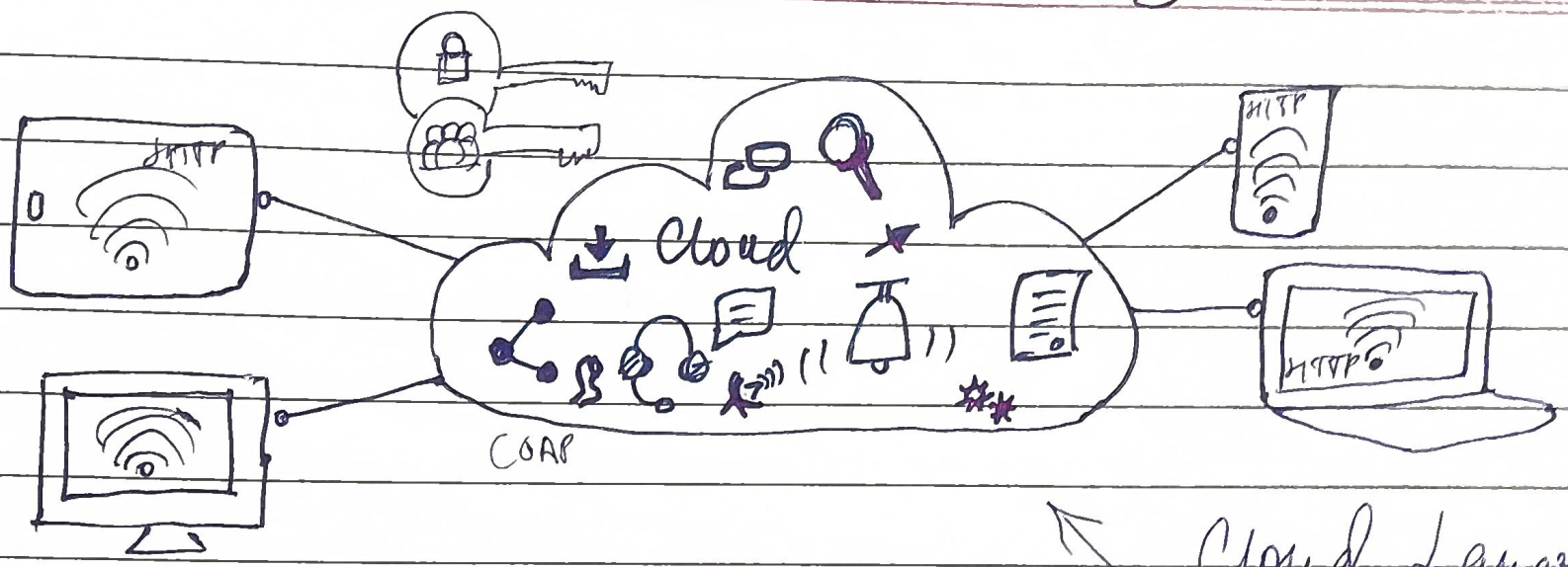
Architecture

IoT	M2M
	
(i) Decision making is involved	(i) Degree of intelligence is observed
(ii) HTTP, FTP, Telnet	(ii) Traditional Protocol
(iii) Data is shared to improve the end user experience between other applications	(iii) Data shared with only the communicating parties.
(iv) Internet connection required	(iv) Devices are not dependent on the internet
(v) Targets B2B & B2C	(v) Targets B2B only
Example: Cloud, BigData, etc	Example: Sensors, Data & Information, etc

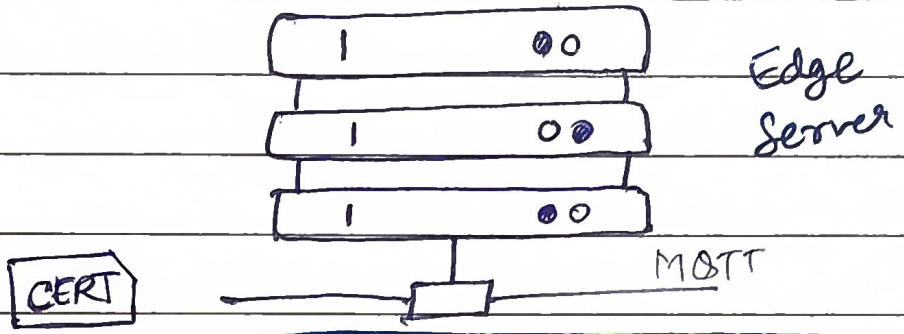

SNMP Agent
Router
SNMP Manager
Managed devices
APP
TALK
APP
APP
APP
SDN Fabric
Mobile Tower
GW
NFV
Gateway Server
Cloud
NFV
Security
IoT Operator

Date / /
Page No.
Shivalal

UNIT - III IoT Communication and Messaging Protocols



Cloud Layer



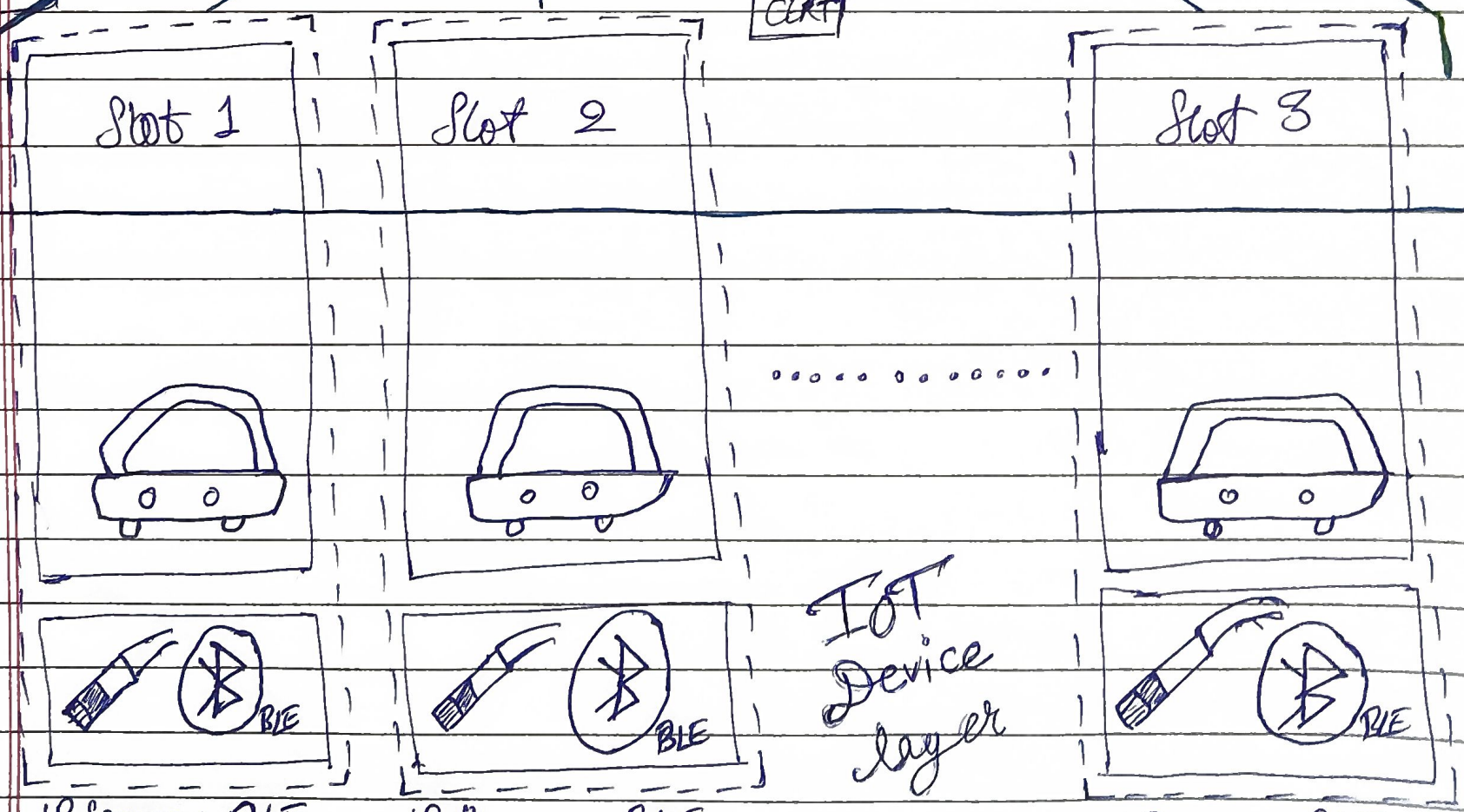
Edge Server

CERT

- Issued to device-gate
- Issued by Google Trust
- Validity 16 Oct
- Public Key

Edge Layer

CERT

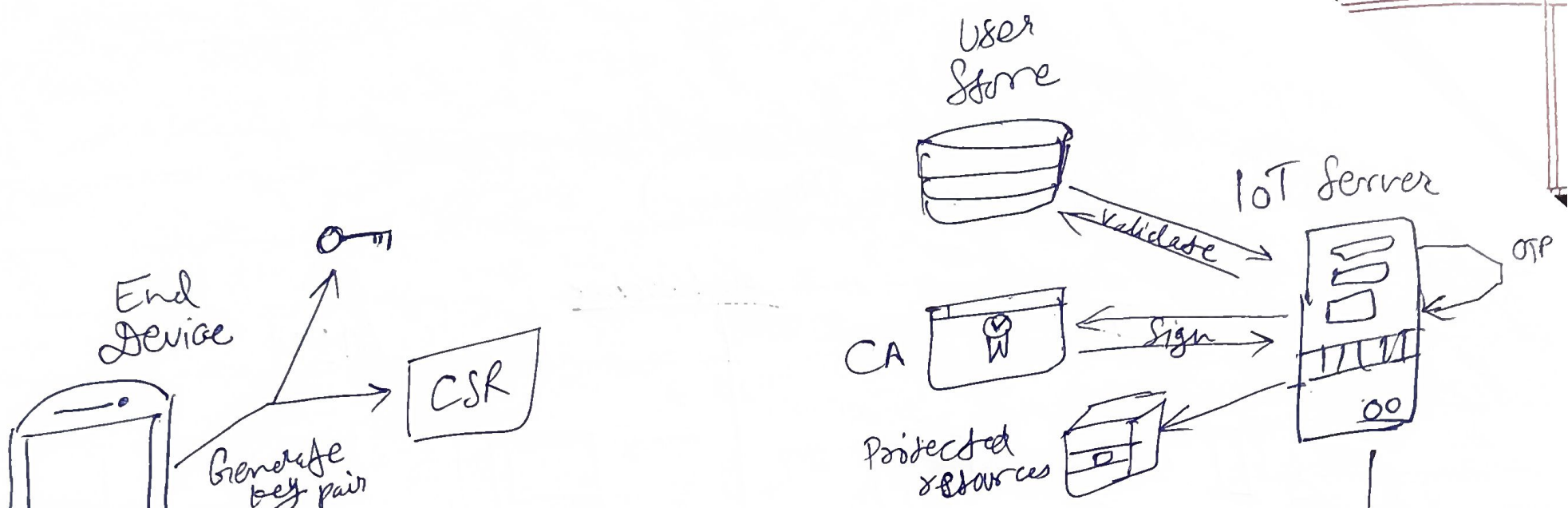


IR Sensor + BLE

IR Sensor + BLE

IoT Device layer

IR Sensor + BLE



1 Request & Download CA Certificate

2 Username , Password

3 One time Pad / Token

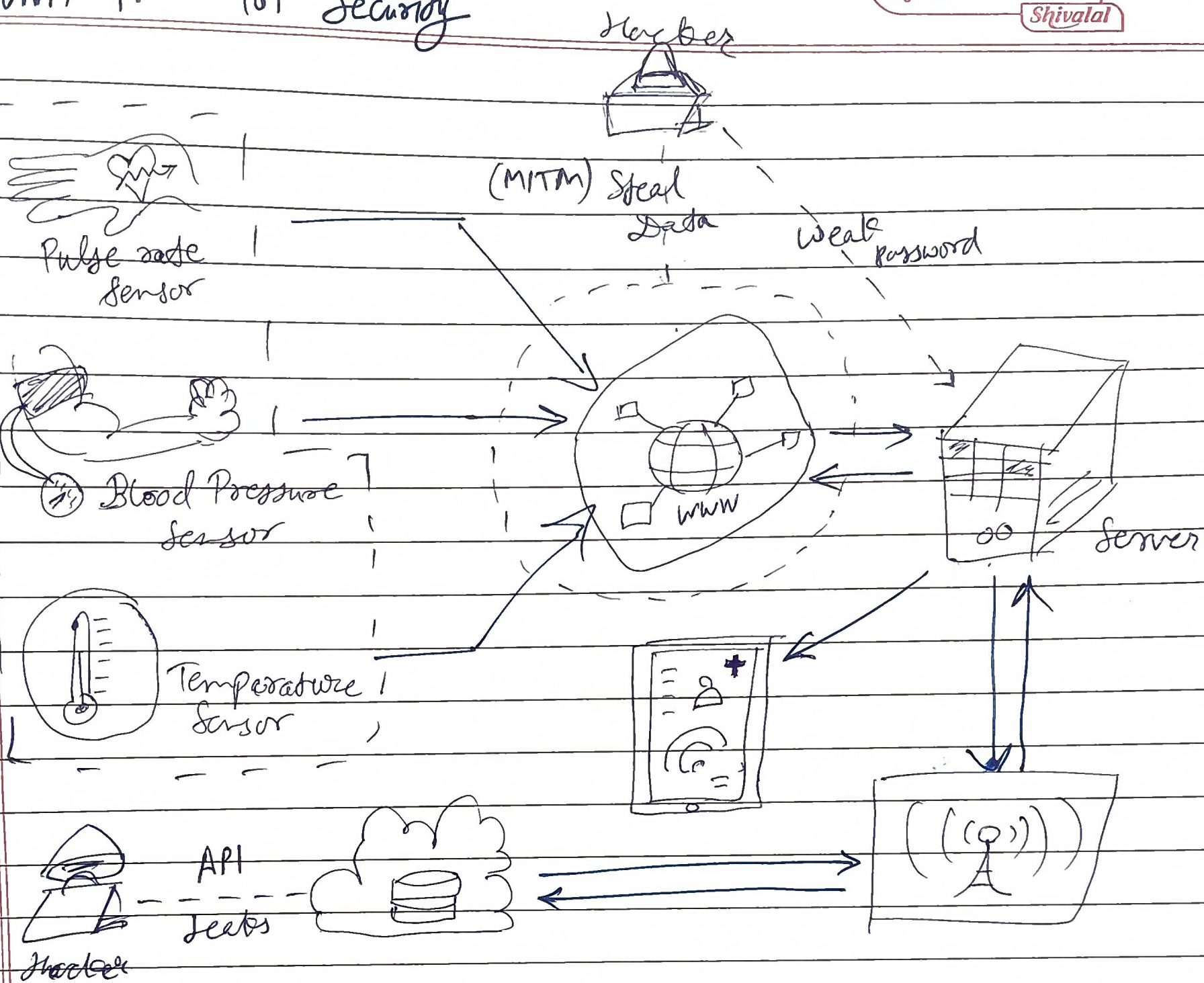
4 CSR, one time

5 Device Identity certificate

6 Device verification header

7 access to resource

UNIT IV IoT Security



Attack Surface : Device level vulnerabilities, Network Communication, Cloud Credentials leak, Third party integration.

Mapping threats : Weak Passwords, Insecure networks, Lack of Security updates, Insecure default configuration, No physical Hardening

Proposed : Strong Authedication, Encryption, Segmentation, Firewall rules, Access control, MFA, Data Anonymization, Automatic Updates, Vuln. Scanning, etc.

UNIT-V IoT Forensics, Standards & Guidelines

Date / /
Page No.
Shivalal

(i) Asses the incident's nature - what it involves like unauthorised access or physical tampering with the smart locks.
Then, document it including any alerts or user reports.

(ii) Sources like smart lock's log, for locks/unlocks and any failed attempts. Further delving into authentication data such as PIN, biometric.

(iii) Preserving the scene to prevent unauthorised access or overwriting of data. Disconnect it from the network to avoid backdoor entries.
A forensic image using write blockers to maintain integrity and data hashes to verify data later.

(iv) Analysis and Reporting of the timeline of incident by correlating logs. The summarised findings outlining incidents, key evidence gathered and any conclusions for legal consideration. To comply under DPDA, CCPA, GDPR, etc.

(v) NIST Cyber Security framework & NIST SP 800-53 ensures that the investigation adheres to best practices in IoT security. Additionally ISO/IEC 27037:2012 provides specific guidance and preservation of digital evidences.