UNIT-2

⇒ CHALLENGES IN FOG COMPUTING

1.) **Authentication & Trust Issues :-**

Authentication is one of the most Concerning Issues. Since most of Services are offered at large scale. Fog Service provider can be different parties like cloud Service providers, ISP & End users. This flexibility Complicates the whole Structure & Trust. A rouge fog Node is a fog device which pretends to be legal & coaxes end user to Connect to it. Once a user Connects to it, it can Manipulate Signals coming to & from user to cloud & easily launch attacks.

2.) **Privacy** –

It is Concerned when there are many N/w involved. Since fog Compuy is based on wireless technology, ~~a~~ large Concern regarding N/w ~~pol~~ privacy. More Sensitive Info is passes from End users to fog Nodes.

3) **Security** – It arises there are many devices Connected to fog Nodes & at different gateways. Each device has diffent IP adress & any hacker Can fake your IP address.

4.) **Fog Servers** –

The right placement of fog Servers Should be there So that it delievers its Max. Service. The Company Should analyse the demand & work done by fog Node.

(5) Energy Consumption

It is very high in fog computing as No of fog Nodes Present in fog Environment is high & require Energy to work

(6) Control & Management Issues

Nature of Nodes is Mobility, So changes are frequent which leads to change in Storage, Bandwidth.

(7) Task Scheduling

The Scheduling of task is Not Easy in fog. Bcoz task can move between various physical devices like fog Nodes.

⇒ PRIVACY & SECURITY ISSUE IN FOG COMPUTING

- Fog Computing Security Issues arises as there are many devices connected to fog Nodes & at different gateways.
- Authentication plays a major role in Establishing the Initial set of relation b/w IOT devices & fog Nodes in N/w but this is Not Sufficient as devices are always Malfunction to attacks.

Privacy preservation is more challenging since fog Nodes may Collect Sensitive data. As a result, Concerning the Identity of End users Compared to the remote cloud Servers that lies in Core N/w.

- Since fog Nodes are Scattered, Centralized Control is difficult

Network Security.

Due to the predominance of wireless in fog, wireless Security is big Concern. Ex:- attacks are Jamming attacks, Sniffer attacks. In N/w, we have to trust the Configurations Manually generated by the N/w administrator. Fog Nodes ~~attacks~~ deploy at Edge of Internet, which bring heavy burden on Net.

Secure data storage

User data is outsourced & user's Control over data is handed over to fog Node which Introduces Same Security threats. It is hard to Ensure data Integrity

Privacy

The leakage of private Info like data, location are gaining attentions when End users are using Servics like Cloud computing, IoT.

Fog Nodes are Vicinity of End users & Collect more Sensitive Info than remote Cloud

- Data privacy :- Fog Node at Edge Collects Sensitive Info generated by Senors & End devices.
- Usage privacy :- usage pattern with which a fog Client utilises the fog Services Ex: In Smart grid. the reading of Smart meter will ~~di~~ disclose lot of Info of household like at what time TV is on etc which absolutely breaches user privacy.

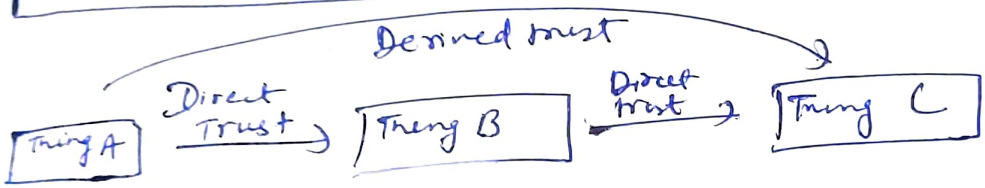
- Location privacy :- As fog clients offload its task to Nearest fog Node, the fog Node to whom task is given can infer that fog client is Nearby & farther from Nodes.

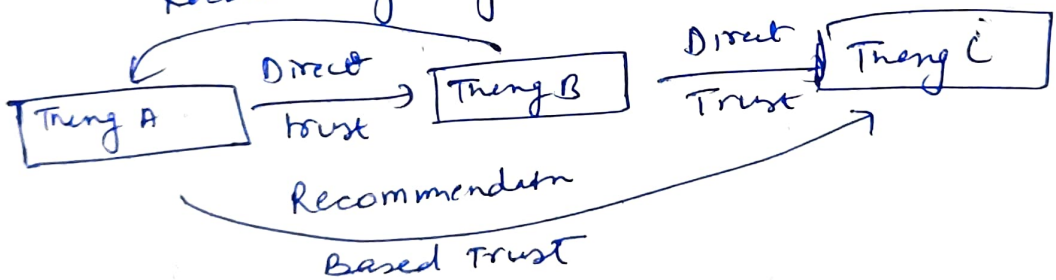
~~Access Control~~

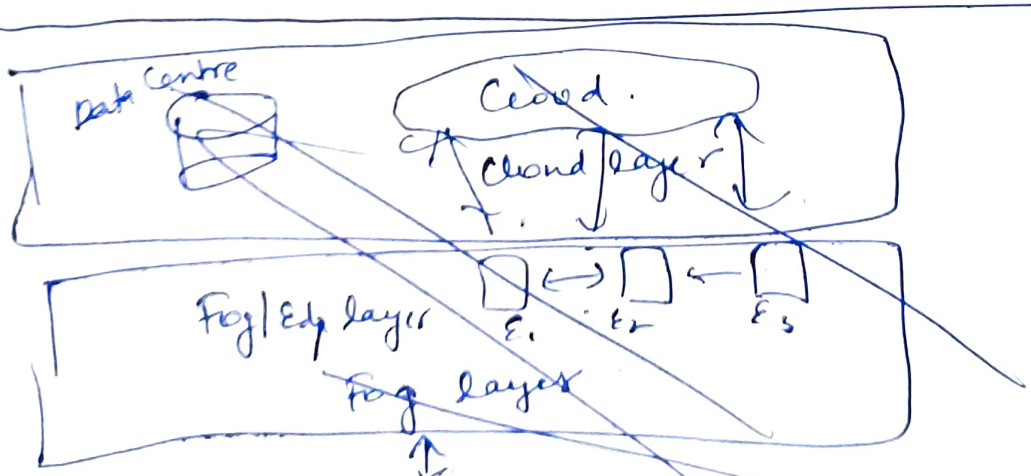
Intrusion detection

To Mitigate attacks like flooding, port, Scanning on VM or in Smart grid to Monitor power measurements & detect abnormal measurement that could have been Compromised by attackers.

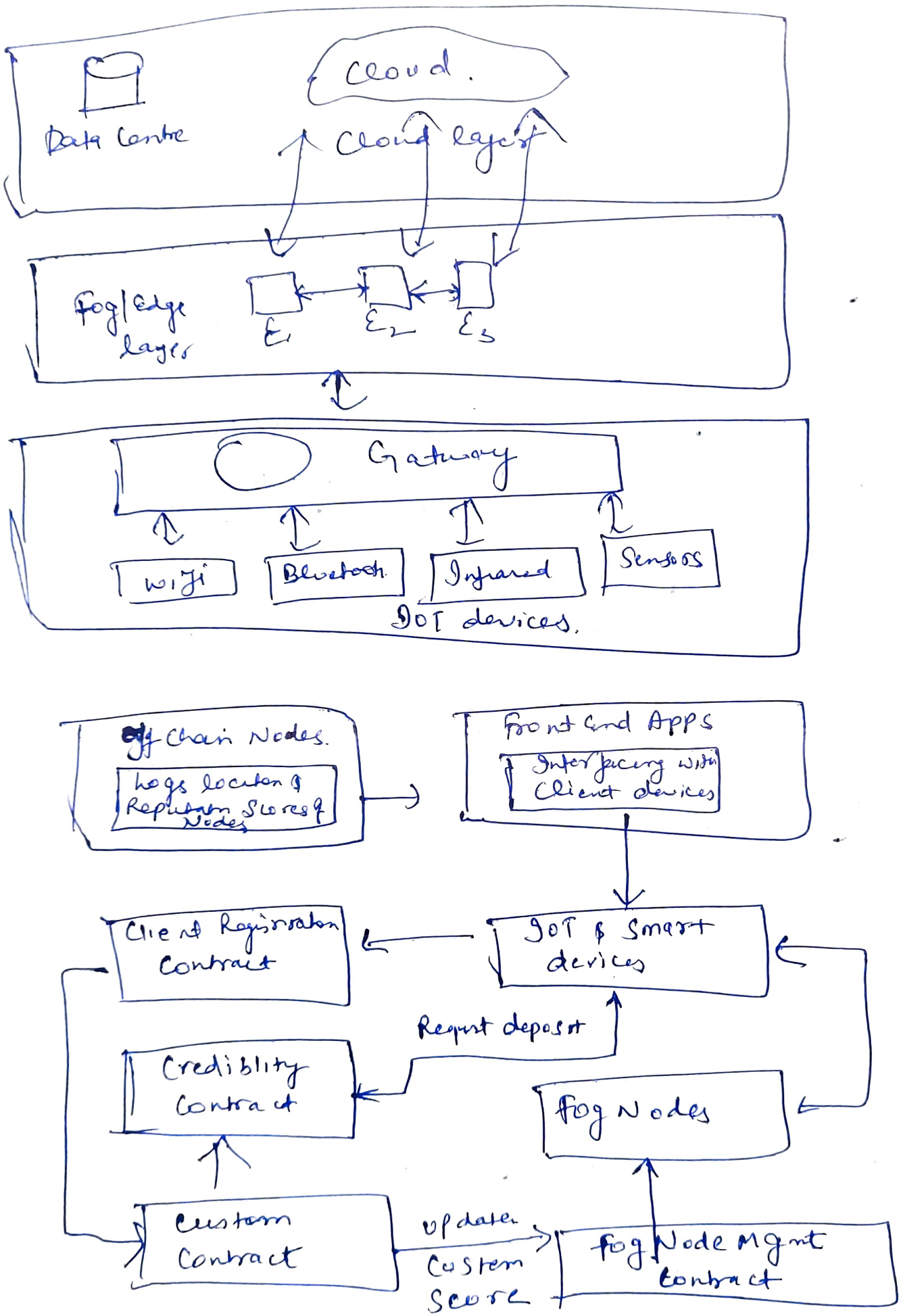
⇒ TRUST & REPUTATION MODEL of FOG COMPUTING







It helps in Evaluating trust worthiness of a user


Cloud.
Data Centre
Cloud layer
Fog/Edge layers
E_1
E_2
E_3
Gateway
WiFi
Bluetooth
Infrared
Sensors
IOT devices.
Chain Nodes.
Logs location & Reputation Scores of Nodes
Front end Apps
Interfacing with Client devices
Client Registration Contract
IOT & Smart devices
Request deposit
Credibility Contract
Fog Nodes
Custom Contract
update Custom Score
Fog Node Mgnt Contract

⇒ CURRENT RESEARCH IN FOG COMPUTING

(1) DITAS :- (Data Intensive applications Improvement by moving data & Computation in cloud Environment) is focussed on providing an abstraction layer for data storage by hiding complex architecture. It is composed of SDK & EE (Execution Environment)

(2) PROFESTO CLOUD - (Proactive cloud resources Management at Edge for Efficient real time Big data processing) Provides configurable fog computing architecture in order to support Big data streams at edge.

(3) mf2c :- It constitutes an open, Secure & decentralised Managment framework. It will try to set the bases of distributed System architecture. with privacy & Security

(4) RE DESIGN :- is a European project start in 2019 It aims to design distributed & Scalable wireless Fog N/W with ground & Mobile fog Nodes

(5) FOGHORN - It aims at developing the theoritical & algorithmic bases of fog aided wireless N/W.

(6) RECAP - Aims to develop the Next generation of fog Computing acc. to user Needs.

(7) ~~STORLET~~

(F) SOFIE - It is based on Existing open Standards like FIWARE, W3C

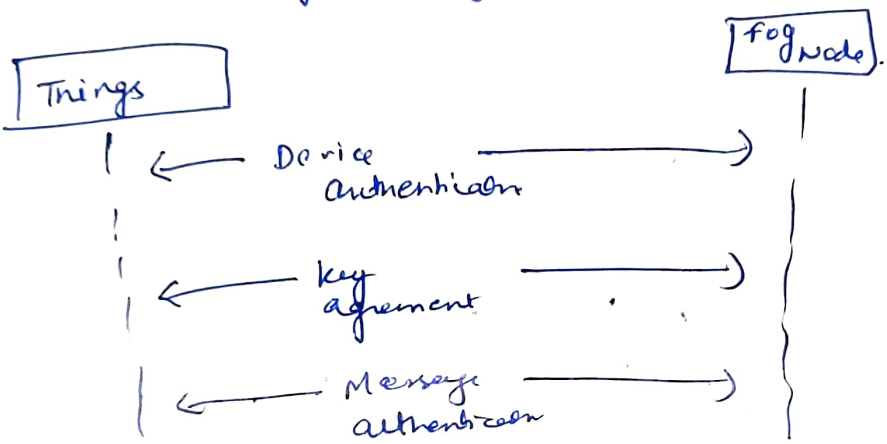
AUTHENTICATION IN FOG COMPUTING

The general authentication scheme is divided into 3 phases device authentication, Key agreement for Message authentication & Message authentication itself.

In first Phase both devices authenticate Each other.

Second phase is Exchange of keys for Message.

The result of key Exchange are then used in third phase of Message authentication



① Device Authentication phase.

Five alternative Sol. proposed for device authentication.

→ PKI - RSA :- a certificate is used for authentication

→ PKI-ECC - an Elliptic Curve Signature algo is used to create certificates.

→ Identity Based Encryption.

→ Authentication with Encryption. - Password.

② Key agreement phase

It is used to generate Symmetric key for Message authentication.

③ Message Authentication phase

It is Implement to avoid Reply attack.

⇒ DATA PREPROCESSING AND ANALYTICS

Fog Computing is highly Virtualized platform that Provides Compute Storage & Networking Services b/w End devices Google uses cloud Computing to Categorises photos.

Fog Analytics –

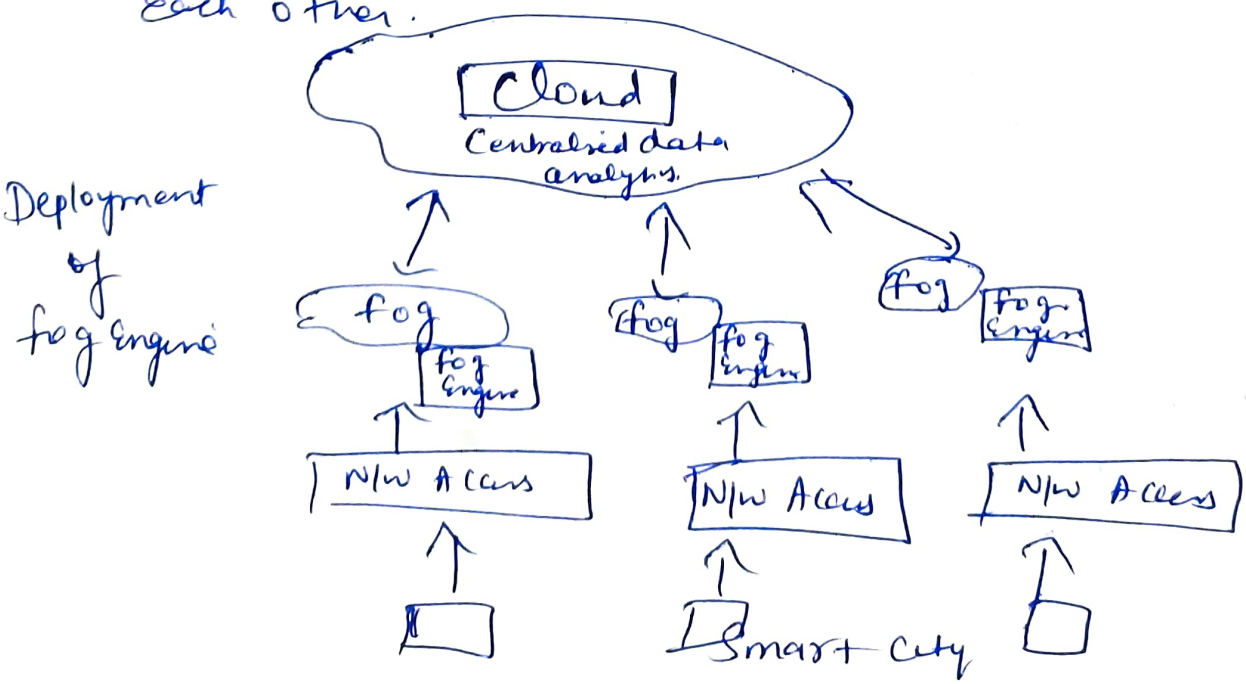
Collecting & transferring all data generated from IoT devices & Sensors into cloud for further processing Poses Serious Challenges on Internet.

Moving data to cloud for analytics work well for large volumes of historical data requiring low Bandwidth. Analytics give better approach.

Fog analytics require Standardization of device & data Interfaces, Integration with cloud to handle Incoming data.

Fog Engines –

End to End Solution called fog Engine that Provides data analytics as well as Capabilities for IoT devices to Communicate with Each other.



Data Analytics using fog Engine

Data Analytics performed near the data source using fog Engine before data volume grows significantly.

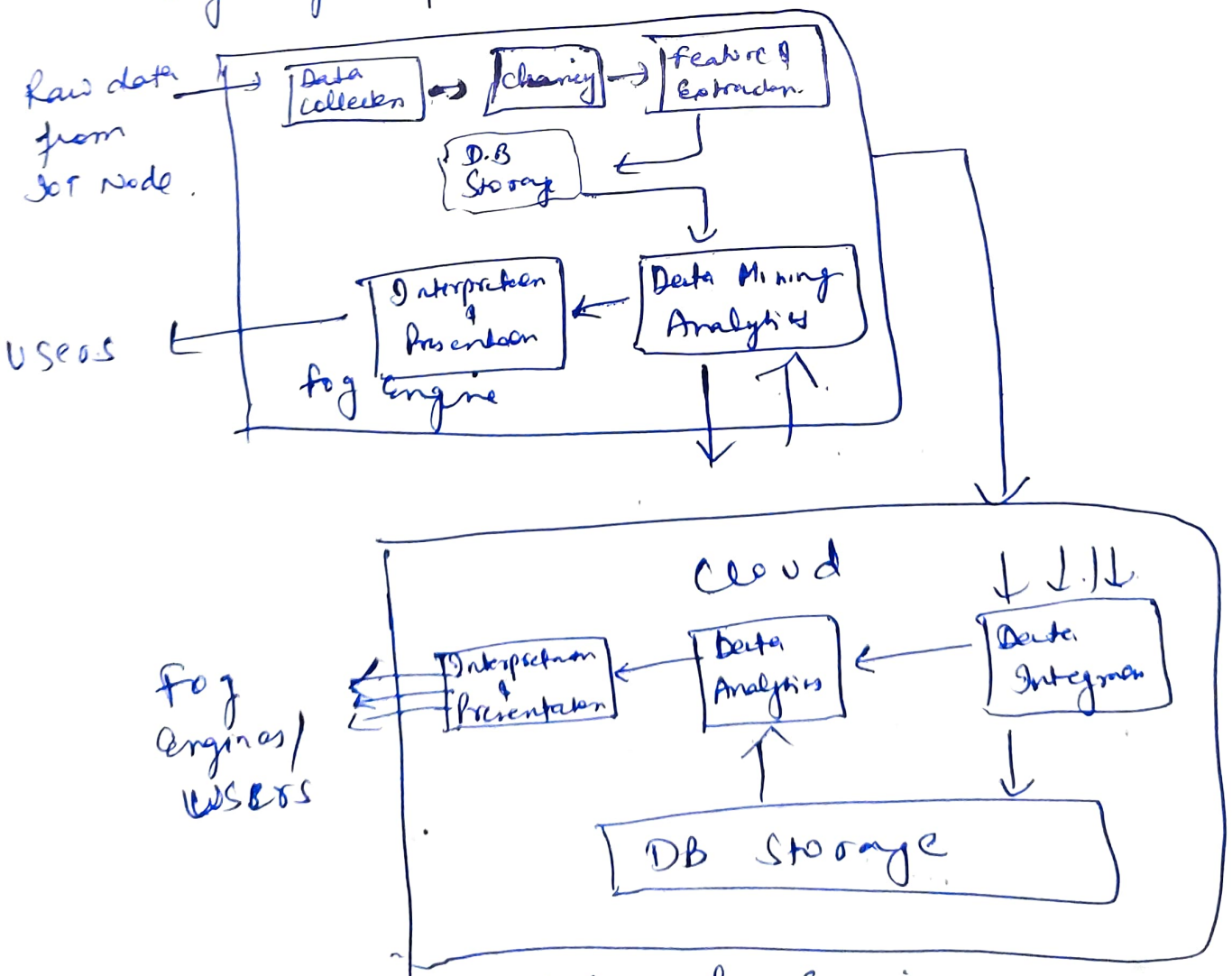
In stream data is analysed locally in fog Engines while data of fog Engines is collected & Transmitted to cloud.

The analytics Model Employed in fog Engine are updated based on polices

As data are processed, filtred & cleaned in the fog Engine prior to offloading to cloud the amount of transmitted data is lower

Analytics is real time.

Fog Engine provids limited Computy power



Data Analytic using fog Engine

⇒ DATA STORAGE & PLACEMENT

Data is stored locally on each end user device or devices b/w them.
To evaluate the performance behaviour of different data placement strategies, ~~this~~ 3 algo are used:-

① Edge-ward Algo -

It is FCFS ~~str~~ strategy, result in placing data as close as possible to edge of N/W. on fog Nodes.
If a specific Node cannot serve the requirements of application, Edge ward selects additional fog devices. The algo creates tuples of device representing path via application Modules.
Appl^n request are answered based on the order in which they arrive until are available computing resources at each level.
→ It presents better performance.

② Cloud only algo -

It is based on traditional Implementation executed in Cloud & uses a delay priority strategy. It assumes all appl^n Modules run in data centres. If sensors capture data, such data is processed on cloud, cloud send Info to actuators if needed.

③. Mapping algo -

It ~~rather~~ relies on Concurrent Strategy
Appl^n request are mapped preferably to fog devices. If CPU capacity of selected fog device does not fulfil to serve an appl^n, then mapping forms ~~on~~ a Processing Queue on fog Node