SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

Course Name – Internet of Things & AI

III Year / V Semester

## Unit 3- INTERNET OF THINGS CHALLENGES

Trust for IoT

Trust IoT **enables chip-to-server secure data transmission and object secure authentication**. Trust IoT securely connects the IoT devices to server or cloud services. Integrate Trust IoT chip to your connected devices to get in a single command : secure authentication, data encryption and transaction uniqueness.

- AUTHENTICATE CONNECTED OBJECT
- OPTIONNAL RF-INTERFACE
- ENROL DEVICE SECURELY
- TRUST COLLECTED DATA
- EASY-TO-INTEGRATE
- ALL-IN-1-COMMAND
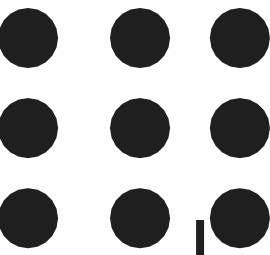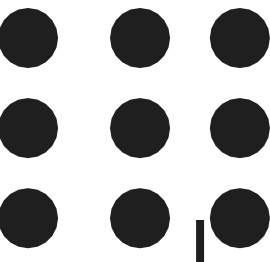
- **OBJECT AUTHENTICATION**

Trust IoT authenticates MCU and generates **encrypted, unique** and **unreplicable** CRYPTO-ID

Secure connection with proof of origin is made between authenticated device and clouds/servers

- **FIELD DATA PROTECTION**

Trust IoT permits to transmit up to **128 bytes of collected data** (protected by MAC or MAC + encryption)

Data from MCU can be transmitted to secure element in a secure session

- **OPTIONAL RF INTERFACE**

Trust IoT comply with **ISO/IEC 14443-A** standard

Data can consequently be collected directly on the field with an authorized NFC-device (External authenticate or CHV)

- Trust is developed when there are security and privacy in the object or entity.
- Trust is a very multifaceted concept that is influenced by many measurable and non-measurable belongings or parameters.
- It is associated to security and user safety in different facets of the entity, trust covers a big area as compare to security and privacy thus it is not as much as easy to build and accomplished the trust factor

MAIN ADVANTAGES

- Identify connected objects on the field and trust collected Data
- Secure authentication & Data encryption in one command
- Easy to integrate with internet-of-things devices
- End-to-End Security, from chip to server
- Direct interaction with RF-interface

The Top 10 IoT Use Cases

N= 1,640 IoT Projects

	Use Case	Type	Global Adoption[1]	Trend[2]
1	Remote asset monitoring (read-only)	Smart Operations	34%	
2	IoT-based process automation	Smart Operations	33%	
3	Remote asset monitoring and control (read/write)	Smart Operations	32%	
4	Vehicle fleet management	Smart Supply Chain	31%	
5	Location tracking	Connected Products	31%	
6	IoT for asset/plant performance optimization	Smart Operations	31%	
7	IoT-based quality control & management	Smart Operations	30%	
8	IoT-based goods condition monitoring in transit	Smart Supply Chain	29%	
9	Predictive maintenance	Smart Operations	29%	
10	On-site track & trace	Smart Supply Chain	29%	

of 48 use cases analyzed in total

Some Misuse cases in IoT

- Eavesdropping
- Fake server
- Fake device platform
- Flooding of TCP/SYN
- Unauthorised access to a data store
- Audit and accountability: Need each transaction to be securely stored to later on auditing and fixing accountabilities.