Certificate Course

On

Internet of Things

Faculty Coordinators: Sri K. Pavan Kumar

Sri. N. Radha Krishna

Duration: 17/**05/2021 to 30/05/2021**

K.S.R.M. COLLEGE OF ENGINEERING

(UGC - AUTONOMOUS)
Kadapa, Andhra Pradesh, India - 516003

Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu.

An ISO 14001:2004 & 9001: 2015 Certified Institution

Lr./KSRMCE/ (Department of ECE)/2020-21

Date: 10/05/2021

To
The Principal
KSRM College of Engineering
Kadapa, AP.

Sub: KSRMCE - (Department of ECE) – Permission to conduct certification course on Internet of Things– Request – reg.

---***---

Respected Sir,

With reference to the cited, the Department of ECE is planning to conduct a certification course on Internet of Things for B.Tech VI sem ECE students from 17.05.2021 to 30.05.2021 in online mode. In this regard we kindly request you to grant permission to conduct certificate course. This is submitted for your kind perusal.

Thanking you sir,

forwarded to the principal sir
G. H

K. Pavan
Yours Faithfully,

Coordinators

Sri K. Pavan Kumar

Sri N. Radha Krishna

Permitted
U. S. S. Murthy
PRINCIPAL
K.S.R.M. COLLEGE OF ENGINEERING
KADAPA - 516 003. (A.P.)

Cc:
To The Director for Information

To All Deans/HODs

Dated: 10/05/2021

Circular

All the B.Tech VI sem ECE students are hereby informed that department of ECE is going to conduct 30 hours certification course on Internet of Things from 17/05/2021 to 30/05/2021. Interested students may register their names with following link on or before15/05/2021.

Registration Link: https://forms.gle/C954qihfoJCVTgiZ7

For any queries contact,

Coordinators

Sri K. Pavan Kumar, Asst. Prof, ECE Dept.

Sri N. Radha Krishna, Asst. Prof, ECE .Dept.

V. S. S. Murty

Principal

PRINCIPAL
K.S.R.M. COLLEGE OF ENGINEERING
KADAPA - 516 003. (A.P.)

Cc to:

The Management /Director / All Deans / All HODS/Staff / Students for information

The IQAC Cell for Documentation

K.S.R.M. COLLEGE OF ENGINEERING

(UGC - AUTONOMOUS)

Kadapa, Andhra Pradesh,India - 516003
Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu.
An ISO 14001:2004 & 9001: 2015 Certified Institution

Department of Electronics & Communication Engineering
Certificate Course on Internet of Things
Registered Student List

S. No.	Roll Number	Name of the Student	Year & Branch	Email address
1	179Y1A0462	KAMBHAM ADWAITH	Btech VI sem ECE	179Y1A0462@ksrmce.ac.in
2	179Y1A0498	PAMUDURTHI MANOJ KUMAR REDDY	Btech VI sem ECE	179Y1A0498@ksrmce.ac.in
3	189Y1A0401	ALLADI ANITHA (W)	Btech VI sem ECE	189Y1A0401@ksrmce.ac.in
4	189Y1A0402	ALLURI YADITHYA	Btech VI sem ECE	189Y1A0402@ksrmce.ac.in
5	189Y1A0403	ANDLURU PREM REDDY	Btech VI sem ECE	189Y1A0403@ksrmce.ac.in
6	189Y1A0404	ARAVA SHYAMDEEP	Btech VI sem ECE	189Y1A0404@ksrmce.ac.in
7	189Y1A0406	AVULA ADARSH KUMAR REDDY	Btech VI sem ECE	189Y1A0406@ksrmce.ac.in
8	189Y1A0407	AVULA NAGENDRABABU	Btech VI sem ECE	189Y1A0407@ksrmce.ac.in
9	189Y1A0408	AVULA SRIKANTH	Btech VI sem ECE	189Y1A0408@ksrmce.ac.in
10	189Y1A0409	BAIMUTHAKA MAHESH	Btech VI sem ECE	189Y1A0409@ksrmce.ac.in
11	189Y1A0410	BANDARI SAI HARSHA VARDHAN	Btech VI sem ECE	189Y1A0410@ksrmce.ac.in
12	189Y1A0411	BAREDDY JAGADEESH REDDY	Btech VI sem ECE	189Y1A0411@ksrmce.ac.in
13	189Y1A0412	BATHALA KOWSALYA (W)	Btech VI sem ECE	189Y1A0412@ksrmce.ac.in
14	189Y1A0413	BATIKERI VIJAYASREE (W)	Btech VI sem ECE	189Y1A0413@ksrmce.ac.in
15	189Y1A0414	BAYANABOINA REDDI SUBBARAYUDU	Btech VI sem ECE	189Y1A0414@ksrmce.ac.in
16	189Y1A0415	BEECHU CHETAN REDDY	Btech VI sem ECE	189Y1A0415@ksrmce.ac.in
17	189Y1A0416	BOGATHI HEMANTH KUMAR REDDY	Btech VI sem ECE	189Y1A0416@ksrmce.ac.in
18	189Y1A0417	BOGGALA CHANDRA SEKHAR	Btech VI sem ECE	189Y1A0417@ksrmce.ac.in
19	189Y1A0418	BOMMIREDDY LAKSHMI PRASANNA (W)	Btech VI sem ECE	189Y1A0418@ksrmce.ac.in
20	189Y1A0420	BONAMSETTY JAHNAVI (W)	Btech VI sem ECE	189Y1A0420@ksrmce.ac.in
21	189Y1A0468	KRISHNAM GANGA MAHESWAR REDDY	Btech VI sem ECE	189Y1A0468@ksrmce.ac.in
22	189Y1A0469	KUMBAGIRI MADHU PRIYA (W)	Btech VI sem ECE	189Y1A0469@ksrmce.ac.in
23	189Y1A0470	KUMMARA THANMAI (W)	Btech VI sem ECE	189Y1A0470@ksrmce.ac.in
24	189Y1A0471	KURAKU NAGESWARA RAO	Btech VI sem ECE	189Y1A0471@ksrmce.ac.in
25	189Y1A0472	KURRA MANJULA (W)	Btech VI sem ECE	189Y1A0472@ksrmce.ac.in
26	189Y1A0473	LAKKIREDDY SAIPRANAVARSHITHA (W)	Btech VI sem ECE	189Y1A0473@ksrmce.ac.in
27	189Y1A0474	MADARASU SAI KRISHNA	Btech VI sem ECE	189Y1A0474@ksrmce.ac.in

28	189Y1A0475	MALEPATI DEEPALI (W)	Btech VI sem ECE	189Y1A0475@ksrmce.ac.in
29	189Y1A0476	MALLELA HARIHARA NANDAN	Btech VI sem ECE	189Y1A0476@ksrmce.ac.in
30	189Y1A0477	MALLI SETTY DIVYA MALIKA (W)	Btech VI sem ECE	189Y1A0477@ksrmce.ac.in
31	189Y1A0478	MANGALA NAVEEN KUMAR	Btech VI sem ECE	189Y1A0478@ksrmce.ac.in
32	189Y1A0479	MANGALI ARUN KUMAR	Btech VI sem ECE	189Y1A0479@ksrmce.ac.in
33	189Y1A0480	MANGALI GIRINDRA KUMAR	Btech VI sem ECE	189Y1A0480@ksrmce.ac.in
34	189Y1A0481	MANGAMMAGARI SANDHYA (W)	Btech VI sem ECE	189Y1A0481@ksrmce.ac.in
35	189Y1A0482	MANJULA PAVANI (W)	Btech VI sem ECE	189Y1A0482@ksrmce.ac.in
36	189Y1A0483	MANJULA VENKATESHWARA	Btech VI sem ECE	189Y1A0483@ksrmce.ac.in
37	189Y1A0484	MANTRI REDDY AMRUTHA BHAVANI (W)	Btech VI sem ECE	189Y1A0484@ksrmce.ac.in
38	189Y1A0486	MEGADA SUNITHA (W)	Btech VI sem ECE	189Y1A0486@ksrmce.ac.in
39	189Y1A0487	MEKALA REVATHI (W)	Btech VI sem ECE	189Y1A0487@ksrmce.ac.in
40	189Y1A0488	MUDDALAPURAM SAI SURYA	Btech VI sem ECE	189Y1A0488@ksrmce.ac.in
41	189Y1A04D5	SHEELLA KRISHNA TEJA	Btech VI sem ECE	189Y1A04D5@ksrmce.ac.in
42	189Y1A04D6	SHREYA KAYANDE (W)	Btech VI sem ECE	189Y1A04D6@ksrmce.ac.in
43	189Y1A04D7	SIDDI ALTHAF	Btech VI sem ECE	189Y1A04D7@ksrmce.ac.in
44	189Y1A04D8	SINGAVARAM PAVAN SAI	Btech VI sem ECE	189Y1A04D8@ksrmce.ac.in
45	189Y1A04D9	SUDHAM ISWARYA (W)	Btech VI sem ECE	189Y1A04D9@ksrmce.ac.in
46	189Y1A04E0	SUNKESULA SIVA KUMARI (W)	Btech VI sem ECE	189Y1A04E0@ksrmce.ac.in
47	189Y1A04E1	SYED MOHAMMED TAHIR	Btech VI sem ECE	189Y1A04E1@ksrmce.ac.in
48	189Y1A04E2	TATAM SETTY NARAHAN DEEP GUPTA	Btech VI sem ECE	189Y1A04E2@ksrmce.ac.in
49	189Y1A04E3	THAMATAM GURU CHANDANA (W)	Btech VI sem ECE	189Y1A04E3@ksrmce.ac.in
50	189Y1A04E4	THIRUVEEDHULA BHAVANI (W)	Btech VI sem ECE	189Y1A04E4@ksrmce.ac.in
51	189Y1A04E5	THOTLI NAVYA (W)	Btech VI sem ECE	189Y1A04E5@ksrmce.ac.in
52	189Y1A04E6	UPPALURU SIVA SANKAR	Btech VI sem ECE	189Y1A04E6@ksrmce.ac.in
53	189Y1A04E7	UTTI SREE HARSHA	Btech VI sem ECE	189Y1A04E7@ksrmce.ac.in
54	189Y1A04E8	VADATHALA HARSHITH REDDY	Btech VI sem ECE	189Y1A04E8@ksrmce.ac.in
55	189Y1A04E9	VALASAPALLI ANNAMAYYA	Btech VI sem ECE	189Y1A04E9@ksrmce.ac.in
56	189Y1A04F0	VARRA PRAVALIKA (W)	Btech VI sem ECE	189Y1A04F0@ksrmce.ac.in
57	189Y1A04F1	VAYALPATI RAMANJANEYULU	Btech VI sem ECE	189Y1A04F1@ksrmce.ac.in
58	189Y1A04F2	VELLABOYINA CHANDAN SAI VAMSI KRISHNA	Btech VI sem ECE	189Y1A04F2@ksrmce.ac.in
59	189Y1A04F3	VELLALA NAGA RUCHITHA (W)	Btech VI sem ECE	189Y1A04F3@ksrmce.ac.in
60	189Y1A04F4	VEMA VISHNUVARDHAN	Btech VI sem ECE	189Y1A04F4@ksrmce.ac.in
61	189Y1A04F5	VEMPALLI RAM NARAYAN SASANK	Btech VI sem ECE	189Y1A04F5@ksrmce.ac.in

Coordinator

HOD

Professor & H.O.D.
Department of E.C.E.
K.S.R.M. College of Engineering
KADAPA - 516 003.

Principal

PRINCIPAL
K.S.R.M. COLLEGE OF ENGINEERING
KADAPA - 516 003. (A.P.)

Internet of Things

Course Objectives:

1. To understand the vision of IoT.
2. To understand IoT market perspective.
3. To study the data and knowledge management and use of devices in IoT technology.
4. To understand state of the art – IoT Architecture.
5. To study the real world IoT design constraints, industrial automation and commercial building automation in IoT.

Course Outcomes:

After learning the course the students should be able:

1. To interpret the vision of IoT from a global context.
2. To determine the market perspective of IoT.
3. To compare and contrast the use of devices, gateways and data management in IoT.
4. To implement state of the art architecture in IoT.
5. To illustrate the application of IoT in industrial automation and identify real world design constraints.

MODULE 1

INTRODUCTION: Internet of Things Promises–Definition– Scope–Sensors for IoT Applications–Structure of IoT– IoT Map Device

MODULE 2

IOT SENSORS: Industrial sensors – Description & Characteristics–First Generation – Description &Characteristics– Advanced Generation – Description & Characteristics–Integrated IoT Sensors – Description & Characteristics–Polytronics Systems – Description &Characteristics–Sensors' Swarm – Description & Characteristics–Printed Electronics – Description & Characteristics–IoT Generation Roadmap

MODULE 3

TECHNOLOGICAL ANALYSIS Wireless Sensor Structure–Energy Storage Module–Power Management Module–RF Module–Sensing Module

MODULE 4 - IOT DEVELOPMENT EXAMPLE

ACOEM Eagle – EnCana Push Button – NEST Sensor – Ninja Blocks -Focus on Wearable Electronics

MODULE 5 –

IOT PROJECTS : Creating the sensor project - Preparing Raspberry Pi/ ARM Cortex - Clayster libraries – Hardware Interacting with the hardware - Interfacing the hardware- Internal representation of sensor values - Persisting data - External representation of sensor values – Exporting sensor data - Creating the actuator project- Hardware - Interfacing the hardware - Creating a controller - Representing sensor values - Parsing sensor data – Calculating control states - Creating a camera - Hardware -Accessing the serial port on RaspberryPi/ ARM Cortex - Interfacing the hardware - Creating persistent default settings – Adding configurable properties - Persisting the settings - Working with the current settings -Initializing the camera

REFERENCE BOOKS:

1. Dr. Guillaume Girardin , Antoine Bonnabel, Dr. Eric Mounier, 'Technologies Sensors for the Internet of Things Businesses & Market Trends 2014 -2024',Yole Development Copyrights ,2014
2. Peter Waher, 'Learning Internet of Things', Packt Publishing, 2015
3. 3 Editors Ovidiu Vermesan Peter Friess, 'Internet of Things – From Research and Innovation to Market
4. 4 N. Ida, Sensors, Actuators and Their Interfaces, Scitech Publishers, 2014.

Professor & H.O.D.
Department of E.C.E.
K.S.R.M. College of Engineering
KADAPA - 516 003.

K.S.R.M. COLLEGE OF ENGINEERING

(UGC - AUTONOMOUS)

Kadapa, Andhra Pradesh, India - 516003

Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu.

An ISO 14001:2004 & 9001: 2015 Certified Institution

Department of Electronics & Communication Engineering

Certificate Course on Internet of Things

Schedule

S.No	Date	Time	Faculty	Topic
1	17/05/2021	3 PM to 5PM	Sri K.Pavan Kumar Sri N.Radha Krishna	Inauguration Introduction
2	18/05/2021	3PM to 5PM	Sri K.Pavan Kumar	MODULE I- INTRODUCTION: Internet of Things Promises–Definition– Scope–Sensors for IoT Applications–Structure of IoT– IoT Map Device
3	19/05/2021	3 PM to 5PM	Sri N.Radha Krishna	MODULE II- IOT SENSORS: Industrial sensors – Description & Characteristics–First Generation – Description &Characteristics
4	20/05/2021	3 PM to 5PM	Dr.S. L Prathapa Reddy	Advanced Generation – Description & Characteristics–Integrated IoT Sensors – Description & Characteristics–Polytronics Systems – Description &Characteristics
5	21/05/2021	3 PM to 5PM	Dr.S.L Prathapa Reddy Sri K.Pavan Kumar	Sensors' Swarm – Description & Characteristics–Printed Electronics – Description & Characteristics–IoT Generation Roadmap
6	22/05/2021	3 PM to 5PM	Dr.S.L Prathapa Reddy	MODULE III- TECHNOLOGICAL ANALYSIS Wireless Sensor Structure–Energy Storage Module–Power Management Module–RF Module–Sensing Module
7	24/05/2021	3 PM to 5PM	Dr.S.L Prathapa Reddy Sri K.Pavan Kumar	MODULE IV- IOT DEVELOPMENT EXAMPLE ACOEM Eagle – EnCana Push Button – NEST Sensor – Ninja Blocks -Focus on Wearable Electronics
8	25/05/2021	3 PM to 5PM	Dr.S.L Prathapa Reddy Sri N.Radha Krishna	MODULE V- IOT PROJECTS : Creating the sensor project - Preparing Raspberry Pi/ ARM Cortex - Clayster libraries – Hardware Interacting with the hardware - Interfacing the hardware- Internal representation of sensor values - Persisting data

9	26/05/2021	3 PM to 5PM	Dr.S.L Prathapa Reddy Sri K.Pavan Kumar	External representation of sensor values – Exporting sensor data - Creating the actuator project- Hardware - Interfacing the hardware -Creating a controller - Representing sensor values
10	27/05/2021	3 PM to 6PM	Dr.S.L Prathapa Reddy	Parsing sensor data – Calculating control states - Creating a camera - Hardware -Accessing the serial port on RaspberryPi/ ARM Cortex - Interfacing the hardware - Creating persistent default settings –
11	28/05/2021	3 PM to 6PM	Dr.S.L Prathapa Reddy Sri N.Radha Krishna	Parsing sensor data – Calculating control states - Creating a camera - Hardware -Accessing the serial port on RaspberryPi/ ARM Cortex - Interfacing the hardware - Creating persistent default settings –
12	29/05/2021	3 PM to 6PM	Dr.S.L Prathapa Reddy	Adding configurable properties - Persisting the settings - Working with the current settings -Initializing the camera
13	30/05/2021	3 PM to 6PM	Dr.S.L Prathapa Reddy Sri.K. Pavan Kumar Sri.N. Radha Krishna	Adding configurable properties - Persisting the settings - Working with the current settings -Initializing the camera

Coordinator

HOD

Professor & H.O.D.
Department of E.C.E.
K.S.R.M. College of Engineering
KADAPA - 516 003.

V. S. S. Murthy

Principal

PRINCIPAL
K.S.R.M. COLLEGE OF ENGINEERING
KADAPA - 516 003. (A.P.)

ACTIVITY REPORT

Certification Course

On

"Internet of Things"

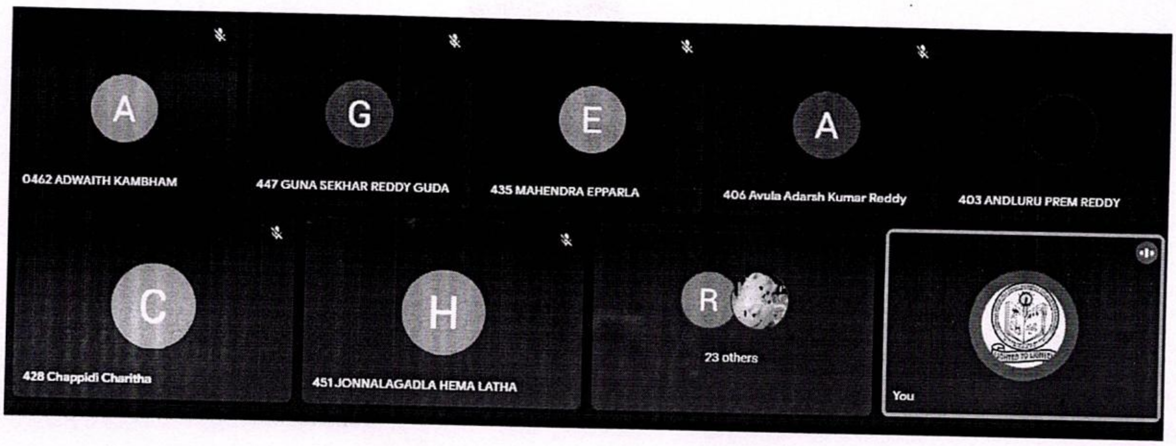
17/05/2021 to 30/05/2021

Target Group	:	Students
Details of Participants	:	61 Students
Coordinators	:	Sri K. Pavan Kumar, Asst. Professor Sri N. Radha Krishna, Asst. Professor
Organizing Department	:	Department of Electronics & Communication Engineering
Venue	:	Online mode (Google meet)

Description:

Certificate course on **"Internet of Things"** was organized by Dept. of ECE from 17-05-2021 to 30-05-2021 in online mode. Dr. S. L. Prathapa Reddy, Sri Pavan Kumar and Sri Radha Krishna acted as Course instructors. The main aim of the course is to create awareness on Internet of Things and its applications. Thirty Hours course was successfully completed and participation certificates were provided to the participants.

Photo :



Sri K. Pavan Kumar

Sri N. Radha Krishna

Coordinators

HoD

Professor & H.O.D.
Department of E.C.E.
K.S.R.M. College of Engineering
KADAPA - 516 003.

Principal

PRINCIPAL
K.S.R.M. COLLEGE OF ENGINEERING
KADAPA - 516 003. (A.P.)

K.S.R.M. COLLEGE OF ENGINEERING

UGC - Autonomous

Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu.
Kadapa, Andhra Pradesh, India– 516 003

Certificate Course on

Internet of Things

17/05/2021 to 30/05/2021

Organized by

DEPARTMENT OF
ELECTRONICS AND COMMUNICATION ENGINEERING

K.S.R.M. COLLEGE OF ENGINEERING

(UGC - AUTONOMOUS)

Kadapa, Andhra Pradesh,India - 516003

Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu.

An ISO 14001:2004 & 9001: 2015 Certified Institution

Department of Electronics & Communication Engineering

Certificate Course on Internet of Things

Attendance Sheet

S.No	Roll Num	Name of the Student	17/05/2021	18/05/2021	19/05/2021	20/05/2021	21/05/2021	22/05/2021	24/05/2021	25/05/2021	26/05/2021	27/05/2021	28/05/2021	29/05/2021	30/05/2021
1	179Y1A0462	KAMBHAM ADWAITH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	179Y1A0498	PAMUDURTHI MANOJ KUMAR REDDY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	189Y1A0401	ALLADI ANITHA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	189Y1A0402	ALLURI YADITHYA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	189Y1A0403	ANDLURU PREM REDDY	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	✓
6	189Y1A0404	ARAVA SHYAMDEEP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	189Y1A0406	AVULA ADARSH KUMAR REDDY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	189Y1A0407	AVULA NAGENDRABABU	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9	189Y1A0408	AVULA SRIKANTH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	189Y1A0409	BAIMUTHAKA MAHESH	✓	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
11	189Y1A0410	BANDARI SAI HARSHA VARDHAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
12	189Y1A0411	BAREDDY JAGADEESH REDDY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
13	189Y1A0412	BATHALA KOWSALYA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	189Y1A0413	BATIKERI VIJAYASREE (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
15	189Y1A0414	BAYANABOINA REDDI SUBBARAYUDU	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
16	189Y1A0415	BEECHU CHETAN REDDY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

17	189Y1A0416	BOGATHI HEMANTH KUMAR REDDY	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
18	189Y1A0417	BOGGALA CHANDRA SEKHAR	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
19	189Y1A0418	BOMMIREDDY LAKSHMI PRASANNA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
20	189Y1A0420	BONAMSETTY JAHNAVI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
21	189Y1A0468	KRISHNAM GANGA MAHESWAR REDDY	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓
22	189Y1A0469	KUMBAGIRI MADHU PRIYA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
23	189Y1A0470	KUMMARA THANMAI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
24	189Y1A0471	KURAKU NAGESWARA RAO	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
25	189Y1A0472	KURRA MANJULA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
26	189Y1A0473	LAKKIREDDY SAIPRANAVARSHITHA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
27	189Y1A0474	MADARASU SAI KRISHNA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
28	189Y1A0475	MALEPATI DEEPALI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
29	189Y1A0476	MALLELA HARIHARA NANDAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
30	189Y1A0477	MALLI SETTY DIVYA MALIKA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
31	189Y1A0478	MANGALA NAVEEN KUMAR	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
32	189Y1A0479	MANGALI ARUN KUMAR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
33	189Y1A0480	MANGALI GIRINDRA KUMAR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
34	189Y1A0481	MANGAMMAGARI SANDHYA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
35	189Y1A0482	MANJULA PAVANI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
36	189Y1A0483	MANJULA VENKATESHWARA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
37	189Y1A0484	MANTRI REDDY AMRUTHA BHAVANI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
38	189Y1A0486	MEGADA SUNITHA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
39	189Y1A0487	MEKALA REVATHI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
40	189Y1A0488	MUDDALAPURAM SAI SURYA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
41	189Y1A04D5	SHEELLA KRISHNA TEJA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
42	189Y1A04D6	SHREYA KAYANDE (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
43	189Y1A04D7	SIDDI ALTHAF	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
44	189Y1A04D8	SINGAVARAM PAVAN SAI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
45	189Y1A04D9	SUDHAM ISWARYA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
46	189Y1A04E0	SUNKESULA SIVA KUMARI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
47	189Y1A04E1	SYED MOHAMMED TAHIR	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
48	189Y1A04E2	TATAM SETTY NARAHAN DEEP GUPTA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
49	189Y1A04E3	THAMATAM GURU CHANDANA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
50	189Y1A04E4	THIRUVEEDHULA BHAVANI (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
51	189Y1A04E5	THOTLI NAVYA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
52	189Y1A04E6	UPPALURU SIVA SANKAR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
53	189Y1A04E7	UTTI SREE HARSHA	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
54	189Y1A04E8	VADATHALA HARSHITH REDDY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓

55	189Y1A04E9	VALASAPALLI ANNAMAYYA	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
56	189Y1A04F0	VARRA PRAVALIKA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
57	189Y1A04F1	VAYALPATI RAMANJANEYULU	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
58	189Y1A04F2	VELLABOYINA CHANDAN SAI VAMSI KRISHNA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
59	189Y1A04F3	VELLALA NAGA RUCHITHA (W)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
60	189Y1A04F4	VEMA VISHNUVARDHAN	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
61	189Y1A04F5	VEMPALLI RAM NARAYAN SASANK	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓

Coordinator

HOD

Professor & H.O.D.
Department of E.C.E.
K.S.R.M. College of Engineering
KADAPA - 516 003.

Principal

PRINCIPAL
K.S.R.M. COLLEGE OF ENGINEERING
KADAPA - 516 003. (A.P.)

K.S.R.M. COLLEGE OF ENGINEERING

UGC - Autonomous

Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu.
Kadapa, Andhra Pradesh, India– 516 003

Certificate Course on

INTERNET OF THINGS PHASE II

17/05/2021 to 30/05/2021

Organized by

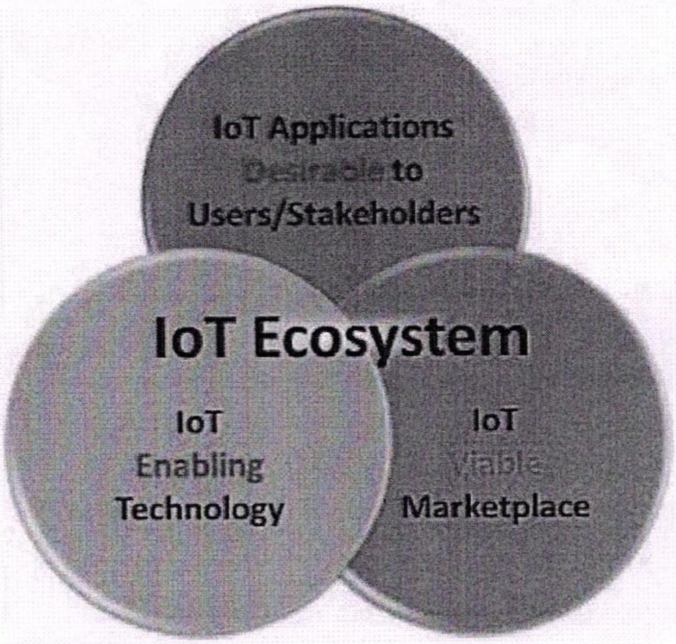
DEPARTMENT OF
ELECTRONICS AND COMMUNICATION ENGINEERING

Unit 1

FUNDAMENTALS OF IoT

1. INTRODUCTION TO IoT

- Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life in unimaginable ways.
- We are now entering an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web.
- One year after the past edition of the Clusterbook 2012 it can be clearly statedthat the Internet of Things (IoT) has reached many different players and gainedfurther recognition. Out of the potential Internet of Things application areas,Smart Cities (and regions), Smart Car and mobility, Smart Home and assistedliving, Smart Industries, Public safety, Energy & environmental protection,Agriculture and Tourism as part of a future IoT Ecosystem (Figure 1.1) haveacquired high attention.



IoT Ecosystem.

- We are entering an era of the "Internet of Things" (abbreviated as IoT).There are 2 definitions: First one is defined by Vermesan and second by Pe˜na-L´opez
  1. The Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators.
  2. Another is the Internet of Things is defined as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object.

Text Books:

1. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017
2. Internet of Things – A hands-on approach, Arshdeep Bahga, Vijay Madisetti, Universities Press, 2015
3. Internet of Things: Architecture, Design Principles And Applications, Rajkamal, McGraw Hill HigherEducation

Reference Books:

1. The Internet of Things – Key applications and Protocols, Olivier Hersent, David Boswarthick, Omar Elloumi and Wiley, 2012 (for Unit2).
2. "From Machine-to-Machine to the Internet of Things – Introduction to a New Age of Intelligence",Jan Ho¨ ller, VlasiosTsiatsis, Catherine Mulligan, Stamatis, Karnouskos, Stefan Avesand. David Boyle and Elsevier, 2014.
3. Architecting the Internet of Things,Dieter Uckelmann, Mark Harrison, Michahelles and Florian (Eds), Springer,2011.
4. Recipes to Begin, Expand, and Enhance Your Projects, 2nd Edition,Michael Margolis,Arduino Cookbook and O"Reilly Media,2011.

Course Outcomes:

At the end of this course, students will be able to

- Understand the basics of IoT.
- Implement the state of the Architecture of an IoT.
- Understand design methodology and hardware platforms involved in IoT.
- Understand how to analyze and organize the data.
- Compare IOT Applications in Industrial & realworld.

- We use these capabilities to query the state of the object and to change its state if possible.
- In common parlance, the Internet of Things refers to a new kind of world where almost all the devices and appliances that we use are connected to a network.
- We can use them collaboratively to achieve complex tasks that require a high degree of intelligence.
- For this intelligence and interconnection, IoT devices areequipped with embedded sensors, actuators, processors, andtransceivers.
- IoT is not a single technology; rather it is anagglomeration of various technologies that work together intandem.
- Sensors and actuators are devices, which help in interactingwith the physical environment.
- The data collected by thesensors has to be stored and processed intelligently in order toderive useful inferences from it.
- Note that we broadly definethe term *sensor*; a mobile phone or even a microwave ovencan count as a sensor as long as it provides inputs about itscurrent state (internal state + environment).
- An *actuator* is adevice that is used to effect a change in the environment suchas the temperature controller of an air conditioner.
- The storage and processing of data can be done on theedge of the network itself or in a remote server.
- If any preprocessingof data is possible, then it is typically done at eitherthe sensor or some other proximate device.
- The processeddata is then typically sent to a remote server.
- The storageand processing capabilities of an IoT object are also restrictedby the resources available, which are often very constraineddue to limitations of size, energy, power, and computationalcapability.
- As a result the main research challenge is toensure that we get the right kind of data at the desired levelof accuracy.
- Along with the challenges of data collection, and handling, there are challenges in communication aswell.
- The communication between IoT devices is mainlywireless because they are generally installed at geographicallydispersed locations.
- The wireless channels often have high rates of distortion and are unreliable.
- In this scenario reliablycommunicating data without too many retransmissions is animportant problem and thus communication technologiesare integral to the study of IoT devices.
- We can directly modify the physical world through actuators or we may do something virtually. For example,we can send some information to other smart things.

- The process of effecting a change in the physical world is often dependent on its state at that point of time. This is called *context awareness*. Each action is taken keeping in consideration the context because an application can behave differently in different contexts.
- For example, a person may not like messages from his office to interrupt him when he is on vacation. Sensors, actuators, compute servers, and the communication network form the core infrastructure of an IoT framework. However, there are many software aspects that need to be considered.
- First, we need a middleware that can be used to connect and manage all of these heterogeneous components. We need a lot of standardization to connect many different devices.
- The Internet of Things finds various applications in health care, fitness, education, entertainment, social life, energy conservation, environment monitoring, home automation, and transport systems.

1.2 TECHNOLOGIES INVOLVED IN IOT DEVELOPMENT: INTERNET/WEB AND NETWORKING BASICS OSI MODEL

- Networking technologies enable IoT devices to communicate with other devices, applications, and services running in the cloud.
- The internet relies on standardized protocols to ensure communication between heterogeneous devices is secure and reliable.
- Standard protocols specify rules and formats that devices use to establish and manage networks and transmit data across those networks.
- Networks are built as a "stack" of technologies. A technology such as Bluetooth LE is at the bottom of the stack.
- While others such as such as IPv6 technologies (which is responsible for the logical device addressing and routing of network traffic) are further up the stack. Technologies at the top of the stack are used by the applications that are running on top of those layers, such as message queuing technologies.
- This article describes widely adopted technologies and standards for IoT networking. It also provides guidance for choosing one network protocol over another. It then discusses key considerations and challenges related to networking within IoT: range, bandwidth, power usage, intermittent connectivity, interoperability, and security.

NETWORKING STANDARDS AND TECHNOLOGIES

- The Open Systems Interconnection (OSI) model is an ISO-standard abstract model is a stack of seven protocol layers.
- From the top down, they are: application, presentation, session, transport, network, data link and physical. TCP/IP, or the Internet Protocol suite, underpins the internet, and it provides a simplified concrete implementation of these layers in the OSI model.

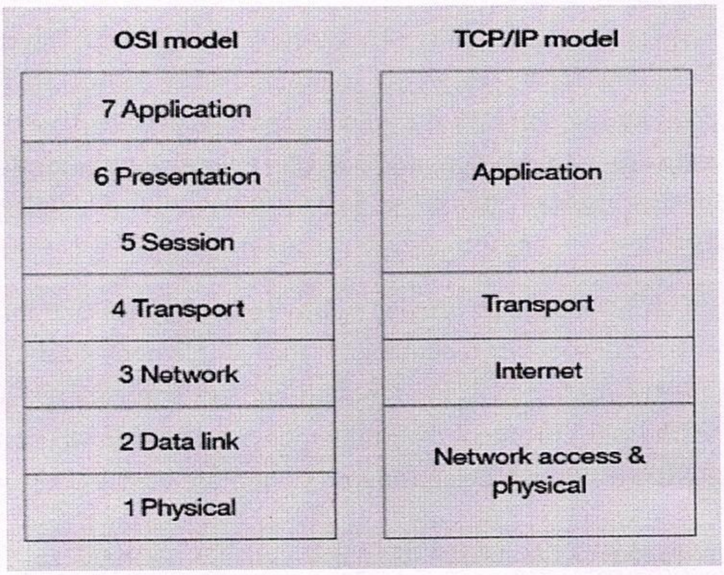


Figure 1. OSI and TCP/IP networking models

The TCP/IP model includes only four layers, merging some of the OSI model layers:

- **Network Access & Physical Layer**

  This TCP/IP Layer subsumes both OSI layers 1 and 2. The physical (PHY) layer (Layer 1 of OSI) governs how each device is physically connected to the network with hardware, for example with an optic cable, wires, or radio in the case of wireless network like wifi IEEE 802.11 a/b/g/n). At the link layer (Layer 2 of OSI), devices are identified by a MAC address, and protocols at this level are concerned with physical addressing, such as how switches deliver frames to devices on the network.

- **Internet Layer**

  This layer maps to the OSI Layer 3 (network layer). OSI Layer 3 relates to logical addressing. Protocols at this layer define how routers deliver packets of data between source and destination hosts identified by IP addresses. IPv6 is commonly adopted for IoT device addressing.

- **Transport Layer**

  The transport layer (Layer 4 in OSI) focuses on end-to-end communication and provides features such as reliability, congestion avoidance, and guaranteeing that packets will be delivered in the same order that they were sent. UDP (User Datagram protocol) is often adopted for IoT transport for performance reasons.

- **Application Layer**

  The application layer (Layers 5, 6, and 7 in OSI) covers application-level messaging. HTTP/S is an example of an application layer protocol that is widely adopted across the internet.

Although the TCP/IP and OSI models provide you with useful abstractions for discussing networking protocols and specific technologies that implement each protocol, some protocols don't fit neatly into these layered models and are impractical. For example, the Transport Layer Security (TLS) protocol that implements encryption to ensure privacy and data integrity of network traffic can be considered to operate across OSI layers 4, 5, and 6.

NETWORK ACCESS AND PHYSICAL LAYER IOT NETWORK TECHNOLOGIES

IoT network technologies to be aware of toward the bottom of the protocol stack include cellular, Wifi, and Ethernet, as well as more specialized solutions such as LPWAN, Bluetooth Low Energy (BLE), ZigBee, NFC, and RFID.

NB-IoT is becoming the standard for LPWAN networks, according to Gartner. This IoT for All article tells more about NB-IoT.

The following are network technologies with brief descriptions of each:

- **LPWAN**
  (Low Power Wide Area Network) is a category of technologies designed for low-power, long-range wireless communication. They are ideal for large-scale deployments of low-power IoT devices such as wireless sensors. LPWAN technologies include LoRa (LongRange physical layer protocol), Haystack, SigFox, LTE-M, and NB-IoT (Narrow-Band IoT).
- **Cellular**
  The LPWAN NB-IoT and LTE-M standards address low-power, low-cost IoT communication options using existing cellular networks. NB-IoT is the newest of

these standards and is focused on long-range communication between large numbers of primarily indoor devices. LTE-M and NB-IoT were developed specifically for IoT, however existing cellular technologies are also frequently adopted for long-range wireless communication. While this has included 2G (GSM) in legacy devices (and currently being phased out), CDMA (also being retired or phased out), it also includes 3G, which is rapidly being phased out with several network providers retiring all 3G devices. 4G is still active and will be until 5G becomes fully available and implemented.

- **Bluetooth Low Energy (BLE)**

  BLE is a low-power version of the popular Bluetooth 2.4 GHz wireless communication protocol. It is designed for short-range (no more than 100 meters) communication, typically in a star configuration, with a single primary device that controls several secondary devices. Bluetooth operates across both layers 1 (PHY) and 2 (MAC) of the OSI model. BLE is best suited to devices that transmit low volumes of data in bursts. Devices are designed to sleep and save power when they are not transmitting data. Personal IoT devices such as wearable health and fitness trackers, often use BLE.

- **ZigBee**

  ZigBee operates on 2.4GHz wireless communication spectrum. It has a longer range than BLE by up to 100 meters. It also has a slightly lower data rate (250 kbps maximum compared to 270 kbps for BLE) than BLE. ZigBee is a mesh network protocol. Unlike BLE, not all devices can sleep between bursts. Much depends on their position in the mesh and whether they need to act as routers or controllers within the mesh. ZigBee was designed for building and home automation applications. Another closely related technology to ZigBee is Z-Wave, which is also based on IEEE 802.15.4. Z-Wave was designed for home automation. It has been proprietary technology, but was recently released as a public domain specification.
- **NFC**

  The near field communication (NFC) protocol is used for very small range communication (up to 4 cm), such as holding an NFC card or tag next to a reader. NFC is often used for payment systems, but also useful for check-in systems and smart labels in asset tracking.
- **RFID**

  RFID stands for Radio Frequency Identification. RFID tags store identifiers and data. The tags are attached to devices and read by an RFID reader. The typical range of RFID is less than a meter. RFID tags can be active, passive, or assisted passive. Passive tags are ideal for devices without batteries, as the ID is passively read by the reader. Active tags periodically broadcast their ID, while assisted passive tags become active when RFID reader is present. **Dash7** is a communication protocol that uses active RFID that is designed to be used within Industrial IoT applications for secure long-range communication. Similar to NFC, a typical use case for RFID is tracking inventory items within retail and industrial IoT applications.

- **Wifi**
  Wifi is standard wireless networking based on IEEE 802.11a/b/g/n specifications. 802.11n offers the highest data throughput, but at the cost of high-power consumption, so IoT devices might only use 802.11b or g for power conservation reasons. Although wifi is adopted within many prototype and current generation IoT devices, as longer-range and lower-power solutions become more widely available, it is likely that wifi will be superseded by lower-power alternatives.
- **Ethernet**
  Widely deployed for wired connectivity within local area networks, Ethernet implements the IEEE 802.3 standard. Not all IoT devices need to be stationery wireless . For example, sensor units installed within a building automation system can use wired networking technologies like Ethernet. Power line communication (PLC), an alternative hard-wired solution, uses existing electrical wiring instead of dedicated network cables.

INTERNET LAYER IOT NETWORK TECHNOLOGIES

Internet layer technologies (OSI Layer 3) identify and route packets of data. Technologies commonly adopted for IoT are related to this layer, and include IPv6, 6LoWPAN, and RPL.

- **IPv6**
  At the Internet layer, devices are identified by IP addresses. IPv6 is typically used for IoT applications over legacy IPv4 addressing. IPv4 is limited to 32-bit addresses, which only provide around 4.3 billion addresses in total, which is less than the current number of IoT devices that are connected, while IPv6 uses 128 bits, and so provides 2^{128} addresses (around 3.4×10^{38} or 340 billion billion billion billion) addresses. In practice, not all IoT devices need public addresses. Of the tens of billions of devices expected to connect via the IoT over the next few years, many will be deployed in private networks that use private address ranges and only communicate out to other devices or services on external networks by using gateways.
- **6LoWPAN**
  The IPv6 Low Power Wireless Personal Area Network (6LoWPAN) standard allows IPv6 to be used over 802.15.4 wireless networks. 6LoWPAN is often used for wireless sensor networks, and the Thread protocol for home automation devices also runs over 6LoWPAN.

- **RPL**

  The Internet Layer also covers routing. IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is designed for routing IPv6 traffic over low-power networks like those networks implemented over 6LoWPAN. RPL (pronounced "ripple") is designed for routing packets within constrained networks such as wireless sensor networks, where not all devices are reachable at all times and there are high or unpredictable amounts of packet loss. RPL can compute the optimal path by building up a graph of the nodes in the network based on dynamic metrics and constraints like minimizing energy consumption or latency.

APPLICATION LAYER IOT NETWORK TECHNOLOGIES

HTTP and HTTPS are ubiquitous across internet applications, which is true also within IoT, with RESTful HTTP and HTTPS interfaces widely deployed. CoAP (Constrained Application Protocol) is like a lightweight HTTP that is often used in combination with 6LoWPAN over UDP. Messaging protocols like MQTT, AMQP, and XMPP are also frequently used within IoT applications:

- **MQTT**

  Message Queue Telemetry Transport (MQTT) is a publish/subscribe-based messaging protocol that was designed for use in low bandwidth situations, particularly for sensors and mobile devices on unreliable networks.
- **AMQP**

  Advanced Message Queuing Protocol (AMQP) is an open standard messaging protocol that is used for message-oriented middleware. Most notably, AMQP is implemented by RabbitMQ.
- **XMPP**

  The Extensible Messaging and Presence Protocol (XMPP) was originally designed for real-time human-to-human communication including instant messaging. This protocol has been adapted for machine-to-machine (M2M) communication to implement lightweight middleware and for routing XML data. XMPP is primarily used with smart appliances.

Your choice of technologies at this layer will depend on the specific application requirements of your IoT project. For example, for a budget home automation system that involves several sensors, MQTT would be a good choice as it is great for implementing messaging on devices without much storage or processing power because the protocol is simple and lightweight to implement.

IOT NETWORKING CONSIDERATIONS AND CHALLENGES

When you consider which networking technologies to adopt within your IoT application, be mindful of the following constraints:

- Range
- Bandwidth
- Power usage
- Intermittent connectivity
- Interoperability
- Security

Range

Networks can be described in terms of the distances over which data is typically transmitted by the IoT devices attached to the network:

- **PAN(PersonalAreaNetwork)**
  PAN is short-range, where distances can be measured in meters, such as a wearable fitness tracker device that communicates with an app on a cell phone over BLE.
- **LAN(LocalAreaNetwork)**
  LAN is short- to medium-range, where distances can be up to hundreds of meters, such as home automation or sensors that are installed within a factory production line that communicate over wifi with a gateway device that is installed within the same building.
- **MAN (Metropolitan Area Network)**
  MAN is long-range (city wide), where distances are measured up to a few kilometers, such as smart parking sensors installed throughout a city that are connected in a mesh network topology.
- **WAN (Wide Area Network)**
  WAN is long-range, where distances can be measured in kilometers, such as agricultural sensors that are installed across a large farm or ranch that are used to monitor micro-climate environmental conditions across the property.

Your network should retrieve data from the IoT devices and transmit to its intended destination. Select a network protocol that matches the range is required. For example, do not choose BLE for a WAN application to operate over a range of several kilometers. If transmitting data over the required range presents a challenge, consider edge computing. Edge computing analyzes data directly from the devices rather than from a distant data center or elsewhere.

Bandwidth

Bandwidth is the amount of data that can be transmitted per unit of time. It limits the rate at which data can be collected from IoT devices and transmitted upstream. Bandwidth is affected by many factors, which include:

- The volume of data each device gathers and transmits
- The number of devices deployed
- Whether data is being sent as a constant stream or in intermittent bursts, and if any peak periods are notable

The packet size of the networking protocol should match up with the volume of data typically transmitted. It is inefficient to send packets padded with empty data. In contrast, there are overheads in splitting larger chunks of data up across too many small packets. Data transmission rates are not always symmetrical (that is, upload rates might be slower than download rates). So, if there is two-way communication between devices, data transmission needs to be factored in. Wireless and cellular networks are traditionally low bandwidth, so consider whether a wireless technology is the right choice for high-volume applications.

Consider whether all raw data must be transmitted. A possible solution is to capture less data by sampling less frequently. Thus, you'll capture fewer variables and may filter data from the device to drop insignificant data. If you aggregate the data before you transmit it, you reduce the volume of data transmitted. But this process affects flexibility and granularity in the upstream analysis. Aggregation and bursting are not always suitable for time-sensitive or latency-sensitive data. All of these techniques increase the data processing and storage requirements for the IoT device.

Power usage

Transmitting data from a device consumes power. Transmitting data over long ranges requires more power than over a short range. You must consider the power source – such as a battery, solar cell, or capacitor – of a device and its total lifecycle. A long and enduring lifecycle will not only provide greater reliability but reduce operating cost. Steps may be taken to help achieve longer power supply lifecycles. For example, to prolong the battery life, you can put the device into sleep mode whenever it is idle. Another best practice is to model the energy consumption of the device under different loads and different network conditions to ensure that the device's power supply and storage capacity matches with the power that is required to transmit the necessary data by using the networking technologies that you adopted.

Intermittent connectivity

IoT devices aren't always connected. In some cases, devices are designed to connect periodically. However, sometimes an unreliable network might cause devices to drop off due to connectivity issues. Sometimes quality of service issues, such as dealing with interference or channel contention on a wireless network using a shared spectrum. Designs should incorporate intermittent connectivity and seek any available solutions to provide uninterrupted service, should that be a critical factor for IoT landscape design.

Interoperability

Devices work with other devices, equipment, systems, and technology; they are interoperable. With so many different devices connecting to the IoT, interoperability can be a challenge. Adopting standard protocols has been a traditional approach for maintaining interoperability on the Internet. Standards are agreed upon by industry participants and avoid multiple different designs and directions. With proper standards, and participants who agree to them, incompatibility issues, hence interoperability issues may be avoided.

However, for the IoT, standardization processes sometimes struggle to keep up with innovation and change. They are written and released based on upcoming versions of standards that are still subject to change. Consider the ecosystem around the technologies: Are they widely adopted? Are they open versus proprietary? How many implementations are available?

Using these questions to plan your IoT networks help plan better interoperability for a more robust IoT network.

Security

Security is a priority. Selection of networking technologies that implement end-to-end security, including authentication, encryption, and open port protection is crucial. IEEE 802.15.4 includes a security model that provides security features that include access control, message integrity, message confidentiality, and replay protection, which are implemented by technologies based on this standard such as ZigBee.

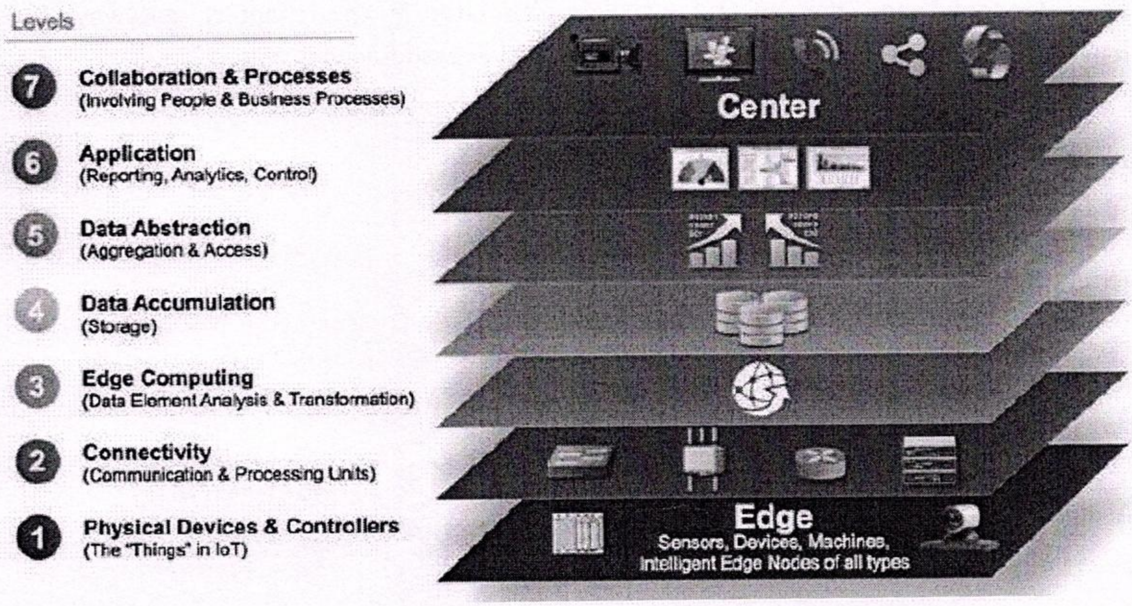
Consider the following factors in shaping a secure and safe IoT network:

- **Authentication**
  Adopt secure protocols to support authentication for devices, gateways, users, services, and applications. Consider using adopting the X.509 standard for device authentication.

- **Encryption**
  If you are using wifi, use Wireless Protected Access 2 (WPA2) for wireless network encryption. You may also adopt a Private Pre-Shared Key (PPSK) approach. To ensure privacy and data integrity for communication between applications, be sure to adopt TLS or Datagram Transport-Layer Security (DTLS), which is based on TLS, but adapted for unreliable connections that run over UDP. TLS encrypts application data and ensures its integrity.
- **Port protection**
  Port protection ensures that only the ports required for communication with the gateway or upstream applications or services remain open to external connections. All other ports should be disabled or protected by firewalls. Device ports might be exposed when exploiting Universal Plug and Play (UPnP) vulnerabilities. Thus, UPnP should be disabled on the router.

The IoT World Forum (IoTWF) Standardized Architecture

In 2014 the IoTWF architectural committee (led by Cisco, IBM, Rockwell Automation, and others)published a seven-layer IoT architectural reference model. While various IoT reference models exist, theone put forth by the IoT World Forum offers a clean, simplified perspective on IoT and includes edgecomputing, data storage, and access. It provides a succinct way of visualizing IoT from a technicalperspective. Each of the seven layers is broken down into specific functions, and security encompassesthe entire model. Figure belowdetails the IoT Reference Model published by the IoTWF.



As shown in Figure 2-2, the IoT Reference Model defines a set of levels with control flowing from thecenter (this could be either a cloud service or a dedicated data center), to the edge, which includessensors, devices, machines, and other types of intelligent end nodes. In general, data travels up the stack,originating from the edge, and goes northbound to the center. Using this reference model, we are able toachieve the following:

- Decompose the IoT problem into smaller parts
- Identify different technologies at each layer and how they relate to one another
- Define a system in which different parts can be provided by different vendors
- Have a process of defining interfaces that leads to interoperability
- Define a tiered security model that is enforced at the transition points between levels

The following sections look more closely at each of the seven layers of the IoT Reference Model.

Layer 1: Physical Devices and Controllers Layer

The first layer of the IoT Reference Model is the physical devices and controllers layer. This layer is hometo the "things" in the Internet of Things, including the various endpoint devices and sensors that send andreceive information. The size of these "things" can range from almost microscopic sensors to giantmachines in a factory. Their primary function is generating data and being capable of being queriedand/or controlled over a network.

Layer 2: Connectivity Layer

In the second layer of the IoT Reference Model, the focus is on connectivity. The most important functionof this IoT layer is the reliable and timely transmission of data. More specifically, this includestransmissions between Layer 1 devices and the network and between the network and informationprocessing that occurs at Layer 3 (the edge computing layer).As you may notice, the connectivity layer encompasses all networking elements of IoT and doesn't reallydistinguish between the last-mile network (the network between the sensor/endpoint and the IoT gateway,discussed later in this chapter), gateway, and backhaul networks. Functions of the connectivity layer aredetailed in Figure 2-3.

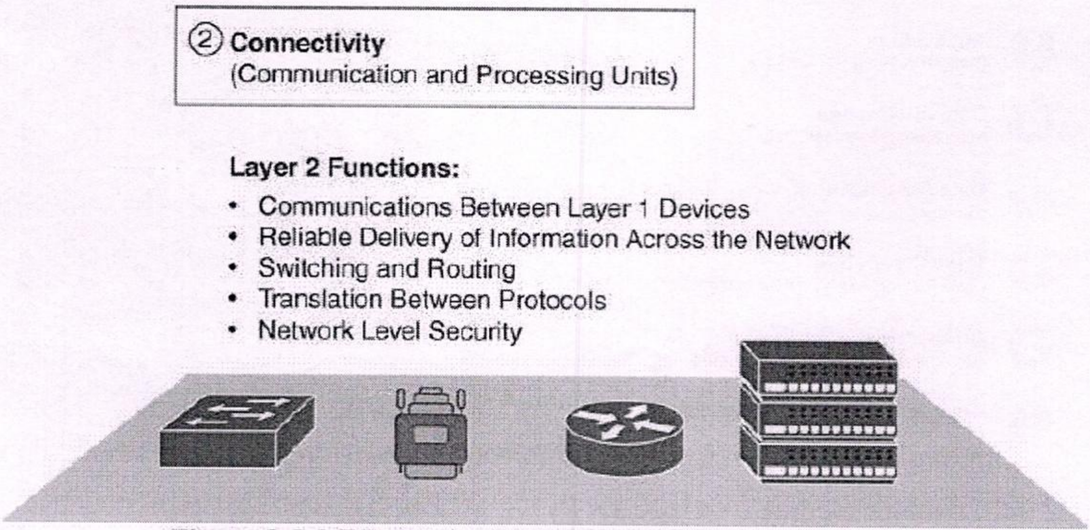


Figure 2-3 *IoT Reference Model Connectivity Layer Functions*

Layer 3: Edge Computing Layer

Edge computing is the role of Layer 3. Edge computing is often referred to as the "fog" layer and isdiscussed in the section "Fog Computing," later in this chapter. At this layer, the emphasis is on datareduction and converting network data flows into information that is ready for storage and processing byhigher layers. One of the basic principles of this reference model is that information processing is initiated
as early and as close to the edge of the network as possible. Figure 2-4 highlights the functions handledby Layer 3 of the IoT Reference Model.

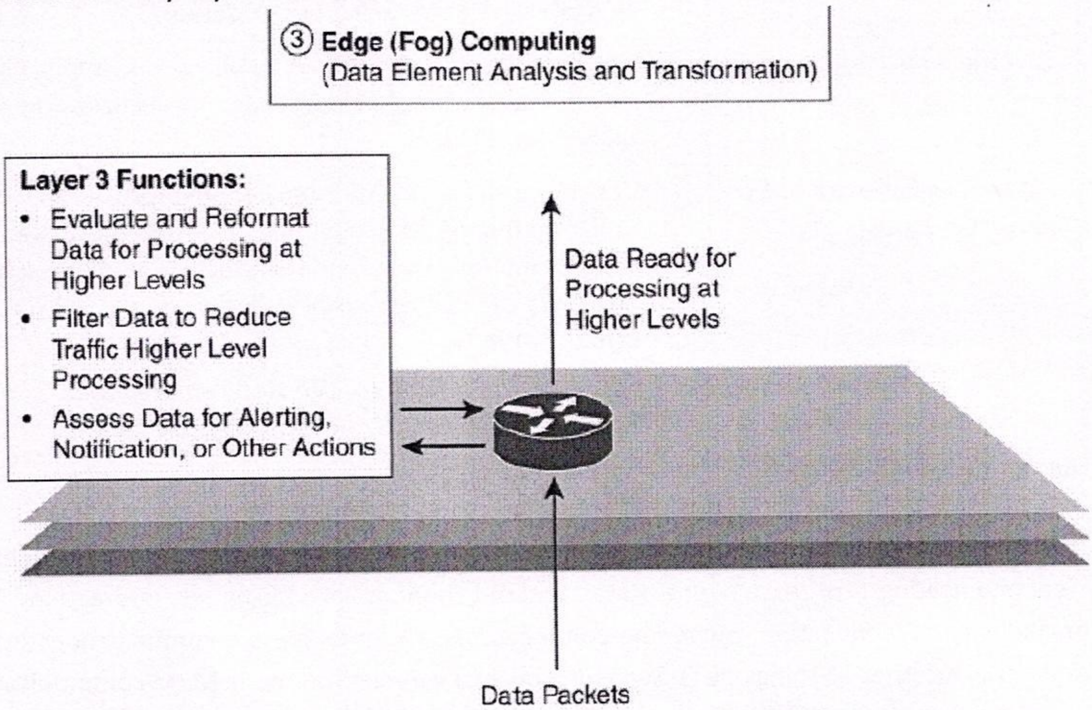


Figure 2-4 *IoT Reference Model Layer 3 Functions*

Another important function that occurs at Layer 3 is the evaluation of data to see if it can be filtered oraggregated before being sent to a higher layer. This also allows for data to be reformatted or decoded,making additional processing by other systems easier. Thus, a critical function is assessing the data to seeif predefined thresholds are crossed and any action or alerts need to be sent.

Upper Layers: Layers 4–7

The upper layers deal with handling and processing the IoT data generated by the bottom layer. For thesake of completeness, Layers 4–7 of the IoT Reference Model are summarized in Table 2-2.

IoT Reference Model Layer	Functions
Layer 4: Data accumulation layer	Captures data and stores it so it is usable by applications when necessary. Converts event-based data to query-based processing.
Layer 5: Data abstraction layer	Reconciles multiple data formats and ensures consistent semantics from various sources. Confirms that the data set is complete and consolidates data into one place or multiple data stores using virtualization.
Layer 6: Applications layer	Interprets data using software applications. Applications may monitor, control, and provide reports based on the analysis of the data.
Layer 7: Collaboration and processes layer	Consumes and shares the application information. Collaborating on and communicating IoT information often requires multiple steps, and it is what makes IoT useful. This layer can change business processes and delivers the benefits of IoT.

Table 2-2 *Summary of Layers 4-7 of the IoTWF Reference Model*

M2M Communication

Machine-to-machine communication, or M2M, is exactly as it sounds: two machines "communicating," or exchanging data, without human interfacing or interaction. This includes serial connection, powerline connection (PLC), or wireless communications in the industrial Internet of Things (IoT). Switching over to wireless has made M2M communication much easier and enabled more applications to be connected.

In general, when someone says M2M communication, they often are referring to cellular communication for embedded devices. Examples of M2M communication in this case would be vending machines sending out inventory information or ATM machines getting authorization to despense cash.

As businesses have realized the value of M2M, it has taken on a new name: the Internet of Things (IoT). IoT and M2M have similar promises: to fundamentally change the way the world operates. Just like IoT, M2M allows virtually any sensor to communicate, which opens up the possibility of systems monitoring themselves and automatically responding to changes in the environment, with a much reduced need for human involvement. M2M and IoT are almost synonymous—the exception is IoT (the newer term) typically refers to wireless communications, whereas M2M can refer to any two machines—wired or wireless—communicating with one another.

Traditionally, M2M focused on "industrial telematics," which is a fancy way of explaining data transfer for some commercial benefit. But many original uses of M2M still stand today, like smart meters. Wireless M2M has been dominated by cellular since it came out in the mid-2000's with 2G cell networks. Because of this, the cellular market has tried to brand M2M as an inherently cellular thing by offering M2M data plans. But cellular M2M is only one subsection of the market, and it shouldn't be thought of as a cellular-only area.

How M2M Works

As previously stated, machine-to-machine communication makes the Internet of Things possible. According to Forbes, M2M is among the fastest-growing types of connected device technologies in the market right now, largely because M2M technologies can connect millions of devices within a single network. The range of connected devices includes anything from vending machines to medical equipment to vehicles to buildings. Virtually anything that houses sensor or control technology can be connected to some sort of wireless network.

This sounds complex, but the driving thought behind the idea is quite simple. Essentially, M2M networks are very similar to LAN or WAN networks, but are exclusively used to allow machines, sensors, and controls, to communicate. These devices feed information they collect back to other devices in the network. This process allows a human (or an intelligent control unit) to assess what is going on across the whole network and issue appropriate instructions to member devices.

M2M Applications

The possibilities in the realm of M2M can be seen in four major use cases, which we've detailed below:

1. MANUFACTURING

Every manufacturing environment—whether it's food processing or general product manufacturing—relies on technology to ensure costs are managed properly and processes are executed efficiently. Automating manufacturing processes within such a fast-paced environment is expected to improve processes even more. In the manufacturing world, this could involve highly automated equipment maintenance and safety procedures.

For example, M2M tools allow business owners to be alerted on their smartphones when an important piece of equipment needs servicing, so they can address issues as quickly as they arise. Sophisticated networks of sensors connected to the Internet could even order replacement parts automatically.

2. HOME APPLIANCES

IoT already affects home appliance connectivity through platforms like Nest. However, M2M is expected to take home-based IoT to the next level. Manufacturers like LG and Samsung are already slowly unveiling smart home appliances to help ensure a higher quality of life for occupants.

For example, an M2M-capable washing machine could send alerts to the owners' smart devices once it finishes washing or drying, and a smart refrigerator could automatically order groceries from Amazon once its inventory is depleted. There are many more examples of home automation that can potentially improve quality of life for residents, including systems that allow members of the household to remotely control HVAC systems using their mobile devices. In situations where a homeowner decides to leave work early, he or she could contact the home heating system before leaving work to make sure the temperature at home will be comfortable upon arrival.

3. HEALTHCARE DEVICE MANAGEMENT

One of the biggest opportunities for M2M technology is in the realm of health care. With M2M technology, hospitals can automate processes to ensure the highest levels of treatment. Using devices that can react faster than a human healthcare professional in an emergency situation make this possible. For instance, when a patient's vital signs drop below normal, an M2M-connected life support device could automatically administer oxygen and additional care until a healthcare professional arrives on the scene. M2M also allows patients to be monitored in their own homes instead of in hospitals or care centers. For example, devices that track a frail or elderly person's normal movements can detect when he or she has had a fall and alert a healthcare worker to the situation.

4. SMART UTILITY MANAGEMENT

In the new age of energy efficiency, automation will quickly become the new normal. As energy companies look for new ways to automate the metering process, M2M comes to the rescue, helping energy companies automatically gather energy consumption data, so they can accurately bill customers. Smart meters can track how much energy a household or business uses and automatically alert the energy company, which supplants sending out an employee to read the meter or requiring the customer to provide a reading. This is even more important as utilities move toward more dynamic pricing models, charging consumers more for energy usage during peak times.

A few key analysts predict that soon, every object or device will need to be able to connect to the cloud. This is a bold but seemingly accurate statement. As more consumers, users, and business owners demand deeper connectivity, technology will need to be continually equipped to meet the needs and challenges of tomorrow. This will empower a wide range of highly automated processes, from equipment repairs and firmware upgrades to system diagnostics, data retrieval, and analysis. Information will be delivered to users, engineers, data scientists, and key decision-makers in real time, and it will eliminate the need for guesswork.

The Value Of M2M

Growth in the M2M and IoT markets has been growing rapidly, and according to many reports, growth will continue. Strategy Analytics believes that low power, wide-area network (LPWAN) connections will grow from 11 million in 2014 to 5 billion in 2022. And IDC says the market for worldwide IoT solutions will go from $1.9 trillion in 2013 to $7.1 trillion in 2020.

Many big cell operators, like AT&T and Verizon, see this potential and are rolling out their own M2M platforms. Intel, PTC, and Wipro are are all marketing heavily in M2M and working to take advantage of this major industry growth spurt. But there is still a great opportunity for new technology companies to engage in highly automated solutions to help streamline processes in nearly any type of industry. We're certain we'll see a huge influx of companies who begin to innovate in this area in the next five years.

However, as the cost of M2M communication continues to decrease, companies must determine how they will create value for businesses and customers. In our mind, the opportunity and value for M2M doesn't lie in the more traditional layers of the communication world. Cell carriers and hardware manufacturers, for example, are beginning to look into full-stack offerings that enable M2M and IoT product development. We strongly believe value lies in the application side of things, and the growth in this industry will be driven by smart applications from this point forward.

Companies shouldn't think about IoT or M2M for the sake of IoT or M2M. Instead, they should focus on optimizing their business models or providing new value for their customers. For example, if you're a logistics company like FedEx or UPS, you have obvious choices for automated logistics decisions made by machines. But if you're a retailer, the transition to automation may not be as obvious. It's one thing to think of a "cool" automated process—say, creating advertising that is automatically tied to a specific customer through the use of M2M technology—but before you move forward with the process, you have to consider the value you're getting out of it. How much does it cost to implement? Will any company considering a move into the IoT space needs to understand what its business model is, how it will make money, and how it will provide value for customers or internal processes.

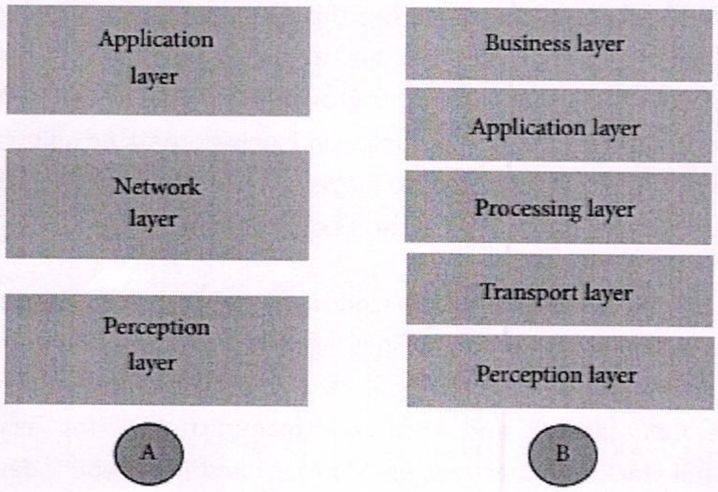
Architecture of IoT

Figure below has three layers, namely, the perception, network, and application layers.

(i) The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.

(ii) The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.

(iii) The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.



The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the fivelayer architecture, which additionally includes the processing and business layers [3–6]. The five layers are perception, transport, processing, application, and business layers (see Figure 1). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

(i) The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

(ii) The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.

(iii) The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

Core IoT Functional Stack

The IoT network must be designed to support its unique requirements and constraints. This section provides an overview of the full networking stack, from sensors all the way to the applications layer.

The Core IoT Functional Stack IoT networks are built around the concept of "things," or smart objects performing functions and delivering new connected services. These objects are "smart" because they use a combination of contextual information and configured goals to perform actions. These actions can be self-contained (that is, the smart object does not rely on external systems for its actions); however, in most cases, the "thing" interacts with an external system to report information that the smart object collects, to exchange with other objects, or to interact with a management platform. In this case, the management platform can be used to process data collected from the smart object and also guide the behavior of the smart object. From an architectural standpoint, several components have to work together for an IoT network to be operational: "Things" layer: At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed. Communications network layer: When smart objects are not self-contained, they need to communicate with an external system. In many cases, this communication uses a wireless technology. This layer has four sublayers: Access network sublayer: The last mile of the IoT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa. The sensors connected to the access network may also be wired. Gateways and backhaul network sublayer: A common communication system organizes multiple smart objects in a given area around a common gateway. The gateway communicates directly with the smart objects. The role of the gateway is to forward the collected information through a longer-range medium (called the backhaul) to a headend central station where the information is processed. This information exchange is a Layer 7 (application) function, which is the reason this object is called a gateway. On IP networks, this gateway also forwards packets from one IP network to another, and it therefore acts as a router. Network transport sublayer: For communication to be successful, network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect and media to use. IoT network management sublayer: Additional protocols must be in place to allow the headend applications to exchange data with the sensors. Examples include CoAP and MQTT.

Application and analytics layer: At the upper layer, an application needs to process the collected data, not only to control the smart objects when necessary, but to make intelligent decision based on the information collected and, in turn, instruct the "things" or other systems to adapt to the analyzed conditions and change their behaviors or parameters. The following sections examine these elements and help you architect your IoT communication network.

Layer 1: Things: Sensors and Actuators Layer

Most IoT networks start from the object, or "thing," that needs to be connected.From an architectural standpoint, the variety of smart object types, shapes, and needs drive the variety of IoT protocols and architectures. There are myriad ways to classify smart objects. One architectural classification could be:

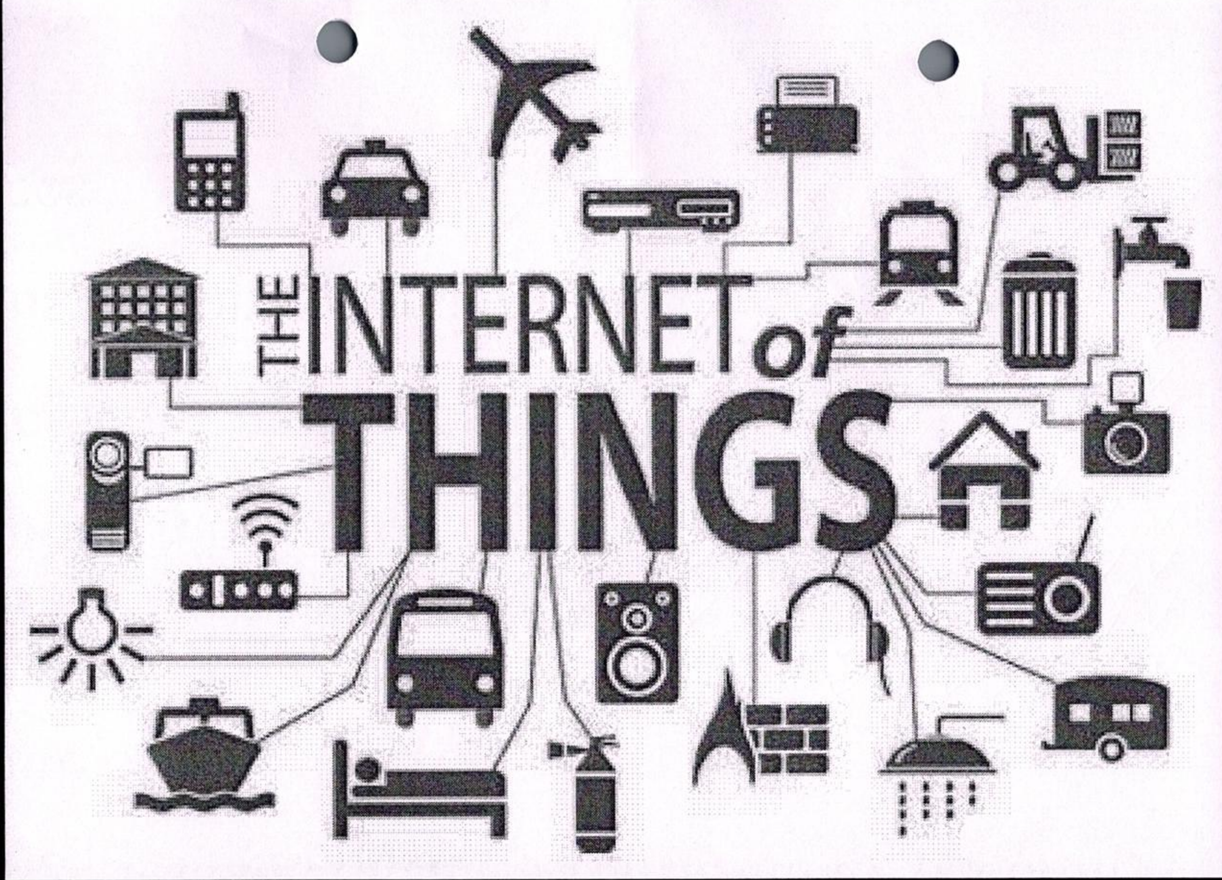
- **Battery-powered or power-connected:** This classification is based on whether the object carries its own energy supply or receives continuous power from an external power source. Battery- powered things can be moved more easily than line-powered objects. However, batteries limit the lifetime and amount of energy that the object is allowed to consume, thus driving transmission range and frequency.
- **Mobile or static:** This classification is based on whether the "thing" should move or always stay at the same location. A sensor may be mobile because it is moved from one object to another (for example, a viscosity sensor moved from batch to batch in a chemical plant) or because it is attached to a moving object (for example, a location sensor on moving goods in a warehouse or factory floor). The frequency of the movement may also vary, from occasional to permanent. The range of mobility (from a few inches to miles away) often drives the possible power source.
- **Low or high reporting frequency:** This classification is based on how often the object should report monitored parameters. A rust sensor may report values once a month. A motion sensor may report acceleration several hundred times per second. Higher frequencies drive higher energy consumption, which may create constraints on the possible power source (and therefore the object mobility) and the transmission range.
- **Simple or rich data:** This classification is based on the quantity of data exchanged at each report cycle. A humidity sensor in a field may report a simple daily index value (on a binary scale from 0 to 255), while an engine sensor may report hundreds of parameters, from temperature to pressure, gas velocity, compression speed, carbon index, and many others. Richer data typically drives higher power consumption. This classification is often combined with the previous to determine the object data throughput (low throughput to high throughput). You may want to keep in mind that throughput is a combined metric. A medium-throughput object may send simple data at rather high frequency (in which case the flow structure looks

continuous), or may send rich data at rather low frequency (in which case the flow structure looks bursty).

- **Report range:** This classification is based on the distance at which the gateway is located. For example, for your fitness band to communicate with your phone, it needs to be located a few meters away at most. The assumption is that your phone needs to be at visual distance for you to consult the reported data on the phone screen. If the phone is far away, you typically do not use it, and reporting data from the band to the phone is not necessary. By contrast, a moisture sensor in the asphalt of a road may need to communicate with its reader several hundred meters or even kilometers away.
- **Object density per cell:** This classification is based on the number of smart objects (with a similar need to communicate) over a given area, connected to the same gateway. An oil pipeline may utilize a single sensor at key locations every few miles. By contrast, telescopes like the SETI Colossus telescope at the Whipple Observatory deploy hundreds, and sometimes thousands, of mirrors over a small area, each with multiple gyroscopes, gravity, and vibration sensors.

Layer 2: Communications Network Layer

Once you have determined the influence of the smart object form factor over its transmission capabilities (transmission range, data volume and frequency, sensor density and mobility), you are ready to connect the object and communicate. Compute and network assets used in IoT can be very different from those in IT environments. The difference in the physical form factors between devices used by IT and OT is obvious even to the most casual of observers. What typically drives this is the physical environment in which the devices are deployed. What may not be as inherently obvious, however, is their operational differences. The operational differences must be understood in order to apply the correct handling to secure the target assets. Temperature variances are an easily understood metric. The cause for the variance is easily attributed to external weather forces and internal operating conditions. Remote external locations, such as those associated with mineral extraction or pipeline equipment can span from the heat of the Arabian Gulf to the cold of the Alaskan North Slope. Controls near the furnaces of a steel mill obviously require heat tolerance, and controls for cold food storage require the opposite. In some cases, these controls must handle extreme fluctuations as well. These extremes can be seen within a single deployment. For example, portions of the Tehachapi, California, wind farms are located in the Mojave Desert, while others are at an altitude of 1800 m in the surrounding mountains. As you can imagine, the wide variance in temperature takes a special piece of hardware that is capable of withstanding such harsh environments. Humidity fluctuations can impact the long-term success of a system as well. Well heads residing in the delta of the Niger River will see very different conditions from those in the middle of the Arabian Desert. In some conditions, the systems could be exposed to direct liquid contact such as may be found with outdoor wireless devices or marine condition deployments. Less obvious are the operating extremes related to kinetic forces. Shock and vibration needs vary based on the deployment scenario. In some cases, the focus is on low-amplitude but constant vibrations, as may be expected on a bushing-mounted manufacturing system. In other cases, it could be a sudden acceleration or deceleration, such as may be experienced in peak ground acceleration of an earthquake or an impact on a mobile system such as high-speed rail or heavy-duty earth moving equipment. Solid particulates can also impact the gear. Most IT environments must contend with dust build-up that can become highly concentrated due to the effect of cooling fans. In less-controlled IT environments, that phenomenon can be accelerated due to higher concentrations of particulates. A deterrent to particulate build-up is to use fanless cooling, which necessitates a higher surface area, as is the case with heat transfer fins. Hazardous location design may also cause corrosive impact to the equipment. Caustic materials can impact connections over which power or communications travel. Furthermore, they can result in reduced thermal efficiency by potentially coating the heat transfer surfaces. In some scenarios, the concern is not how the environment can impact the equipment but how the equipment can impact the environment. For example, in a scenario in which volatile gases may be present, spark suppression is a critical design criterion. There is another class of device differentiators related to the external connectivity of the device for mounting or industrial function. Device mounting is one obvious difference between OT and IT environments. While there are rack mount environments in some industrial spaces, they are more frequently found among IT type assets. Within industrial environments, many compute and communication assets are placed within an enclosed space, such as a control cabinet where they will be vertically mounted on a DIN (Deutsches Institut für Normung) rail inside. In other scenarios, the devices might be mounted horizontally directly on a wall or on a fence. In contrast to most IT-based systems, industrial compute systems often transmit their state or receive inputs from external devices through an alarm channel. These may drive an indicator light (stack lights) to display the status of a process element from afar. This same element can also receive inputs to initiate actions within the system itself. Power supplies in OT systems are also frequently different from those commonly seen on standard IT equipment. A wider range of power variations are common attributes of industrial compute components. DC power sources are also common in many environments. Given the criticality of many systems, it is often required that redundant power supplies be built into the device itself. Extraneous power supplies, especially those not inherently mounted, are frowned upon, given the potential for accidental unplugging. In some utility cases, the system must be able to handle brief power outages and still continue to operate.



Internet of Things (IoT)

Plan of Presentation

- What is Internet of Things?
- How IoT Works?
- Current Status & Future Prospect of IoT
- Knowledge Management – From Data to Wisdom
- The Future of IoT
- The Potential of IoT
- Few Applications of IoT
- Technological Challenges of IoT
- Criticisms & Controversies of IoT
- References

What is IoT?

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.

"**Things**," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist fire-fighters in search and rescue operations.

These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.

History of IoT

The concept of the Internet of Things first became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications. R

Radio-frequency identification (RFID) was seen as a prerequisite for the IoT at that point. If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes, bluetooth, and digital watermarking.

How IoT Works?

Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include:

- ***Communication and cooperation***
- ***Addressability***
- ***Identification***
- ***Sensing***
- ***Actuation***
- ***Embedded information processing***
- ***Localization***
- ***User interfaces***

How IoT Works?

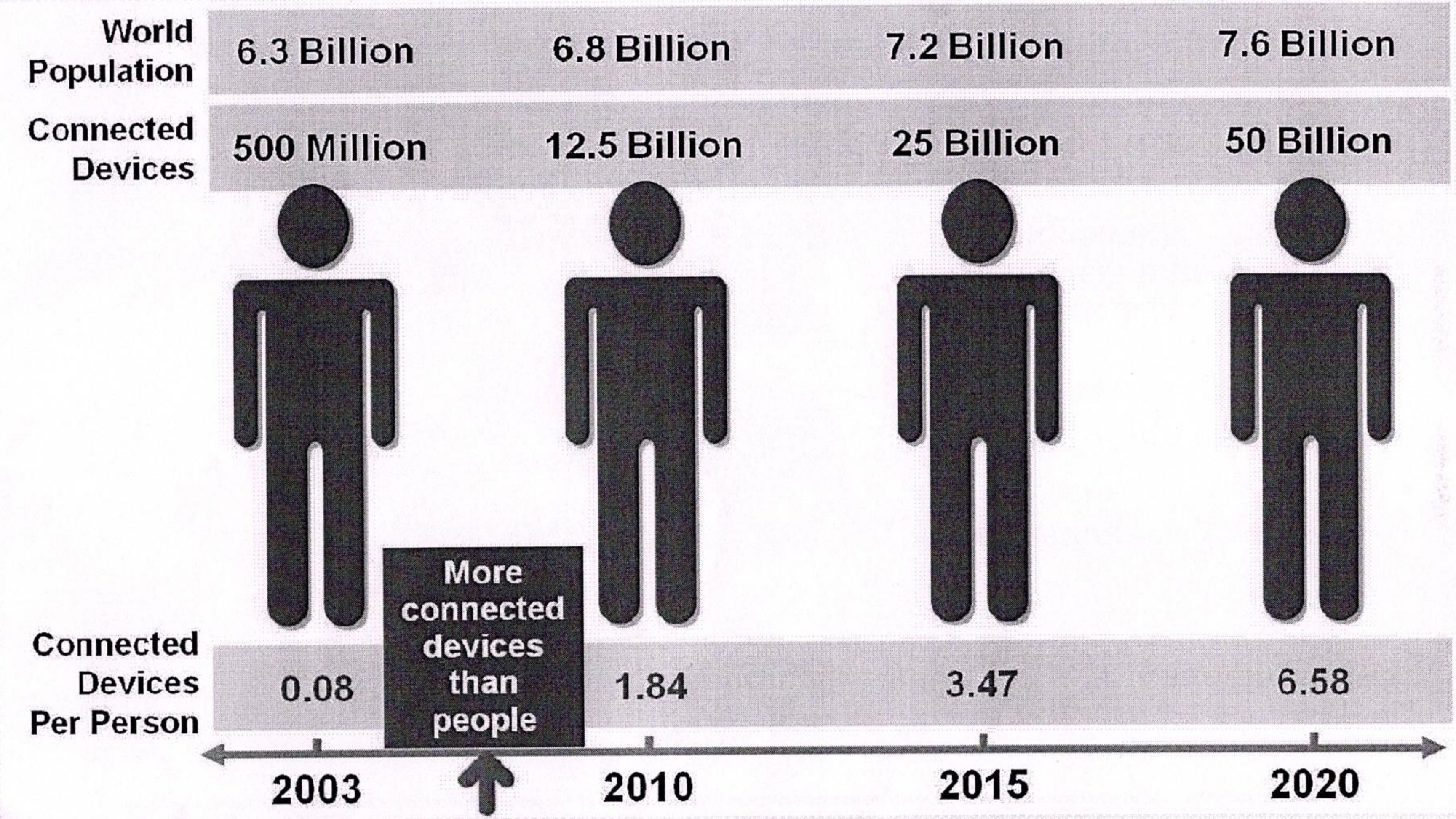
RFI D	Senso r	Smart Tech	Nano Tech
To identify and track the data of things	To collect and process the data to detect the changes in the physical status of things	To enhance the power of the network by devolving processing capabilities to different part of the network.	To make the smaller and smaller things have the ability to connect and interact.

The Structure of IoT

The IoT can be viewed as a gigantic network consisting of networks of devices and computers connected through a series of intermediate technologies where numerous technologies like RFIDs, wireless connections may act as enablers of this connectivity.

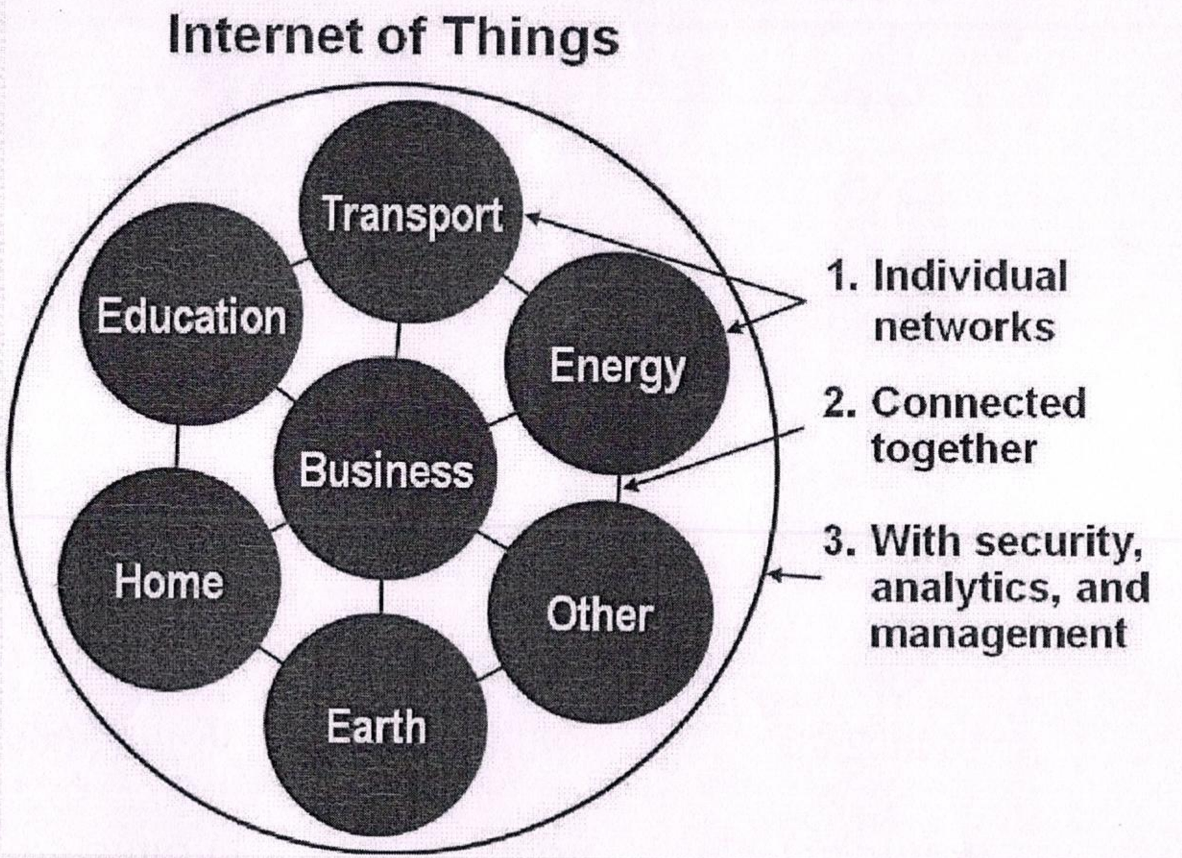
- ***Tagging Things* :** Real-time item traceability and addressability by ***RFID***s.
- ***Feeling Things* : *Sensors*** act as primary devices to collect data from the environment.
- ***Shrinking Things* :** *M*iniaturization and ***Nanotechnology*** has provoked the ability of smaller things to interact and connect within the "things" or "smart devices."
- ***Thinking Things* : *Embedded intelligence*** in devices through sensors has formed the network connection to the Internet. It can make the "things" realizing the intelligent control.

Current Status & Future Prospect of IoT



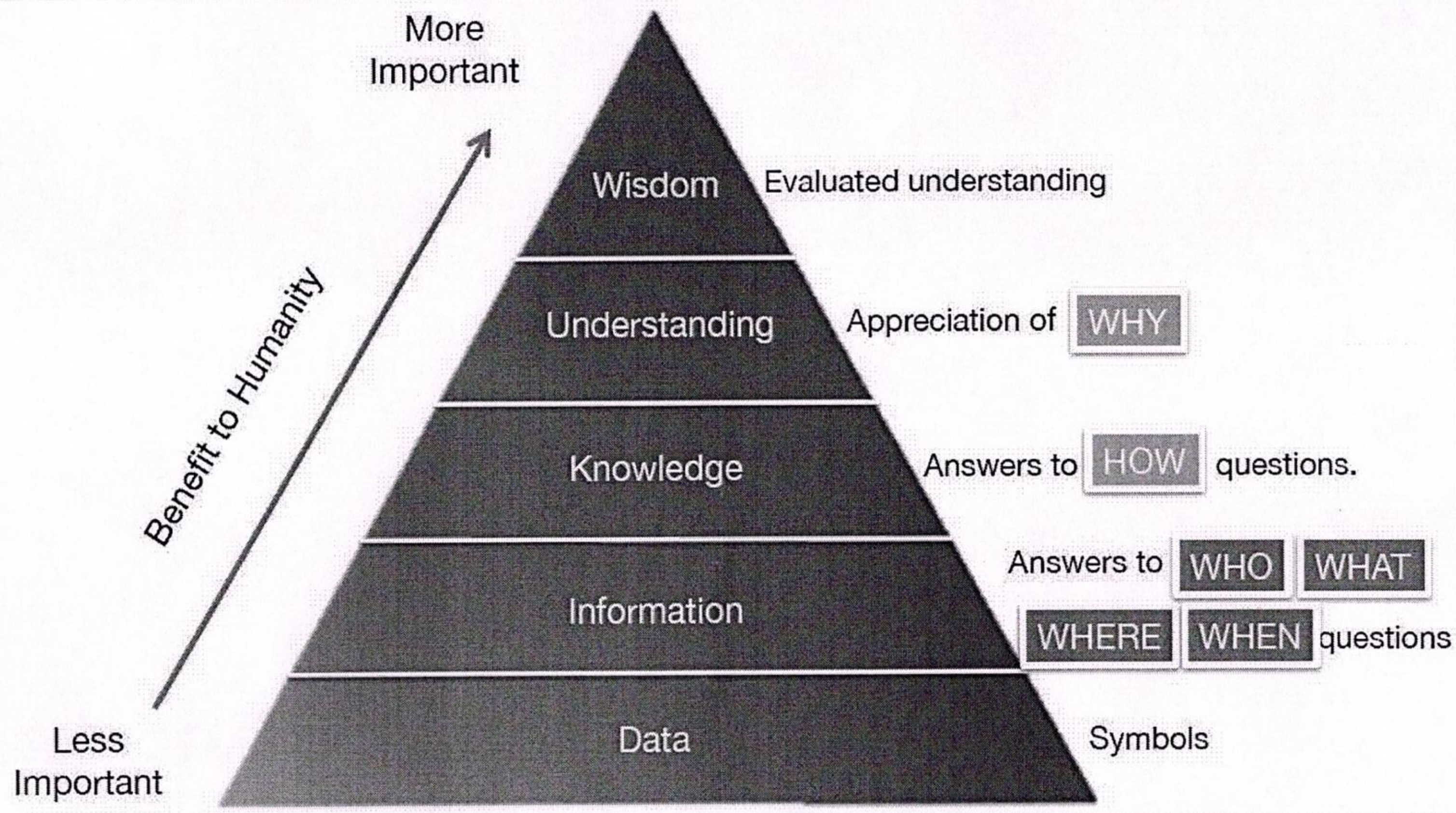
"Change is the only thing permanent in this world"

IoT as a Network of Networks:



These networks connected with added security, analytics, and management capabilities. This will allow IoT to become even more powerful in what it can help people achieve.

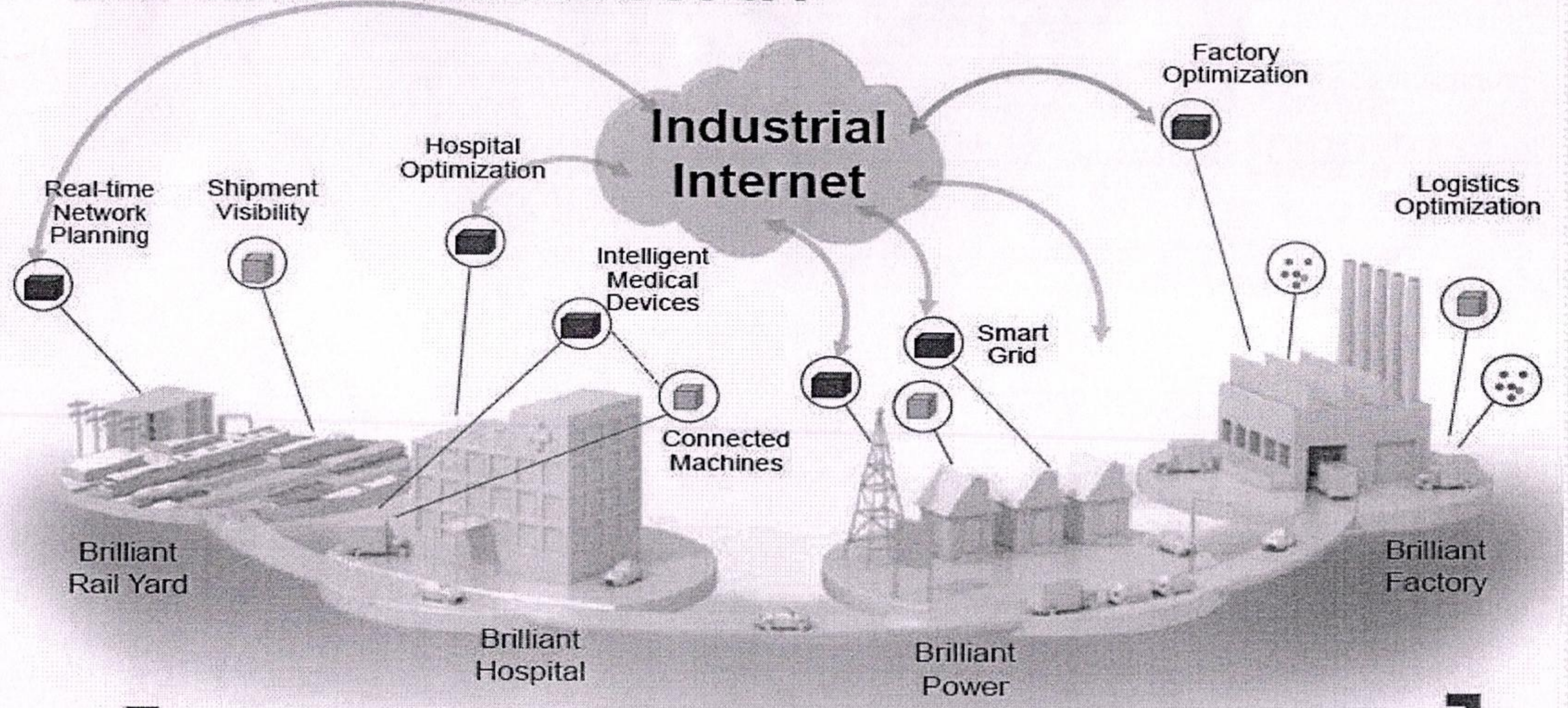
Knowledge Management – Turning Data into Wisdom



The more data that is created, the better understanding and wisdom people can obtain.

The Future of IoT

What happens when 50B Machines become connected?



[OT is virtualized -------- Analytics become predictive ---- Employees increase productivity

Machines are self healing & automated -------- Monitoring and maintenance is mobilized] 6

"The Sky's not the limit. It's only the beginning with IoT."

The Potential of IoT

Value of Industrial Internet is huge

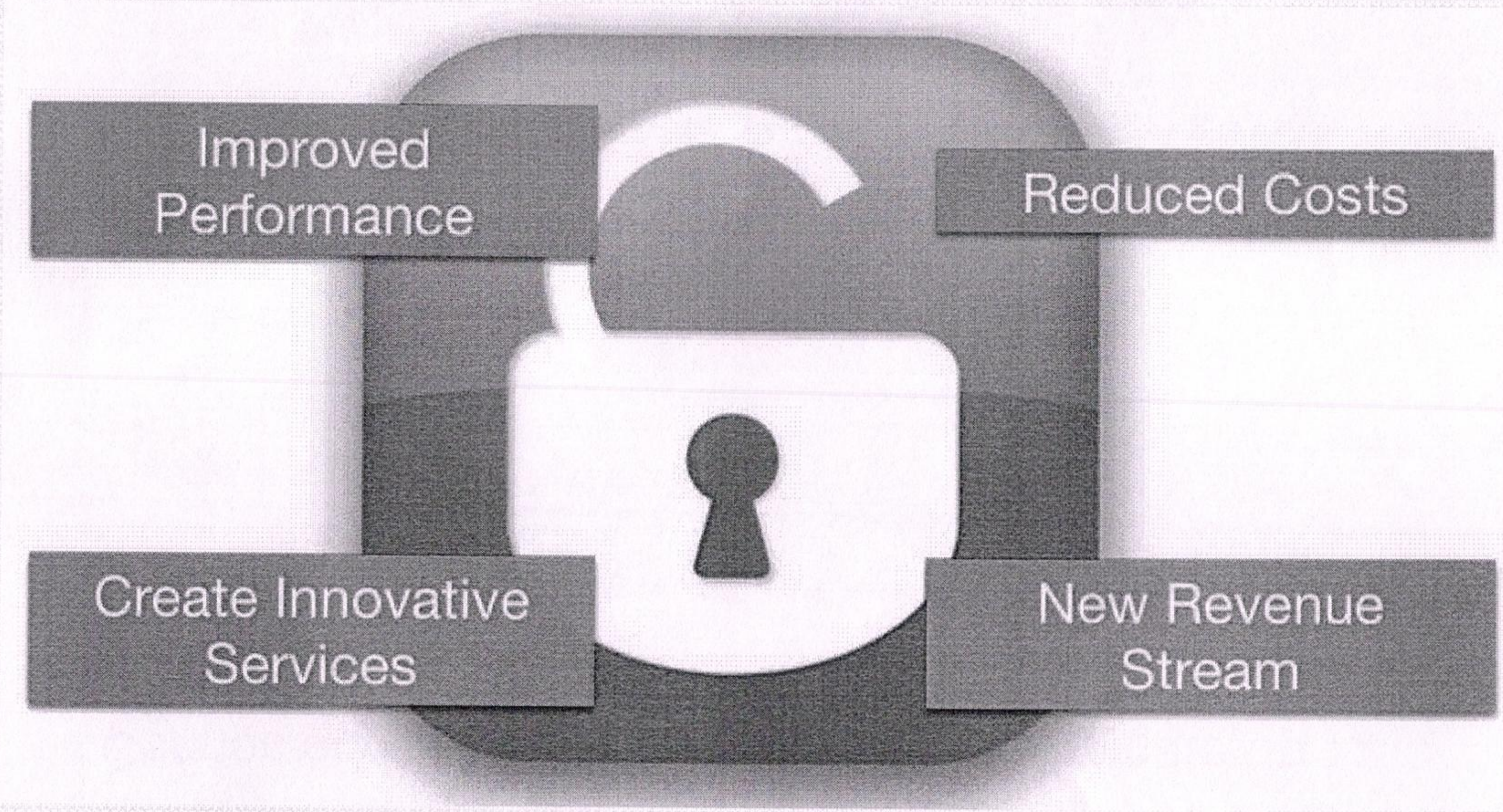
Connected machines and data could eliminate up to $150 billion in waste across industries

Industry	Segment	Type of savings	Estimated value over 15 years (Billion nominal US dollars)
Aviation	Commercial	1% fuel savings	$30B
Power	Gas-fired generation	1% fuel savings	$66B
Healthcare	System-wide	1% reduction in system inefficiency	$63B
Rail	Freight	1% reduction in system inefficiency	$27B
Oil and Gas	Exploration and development	1% reduction in capital expenditures	$90B

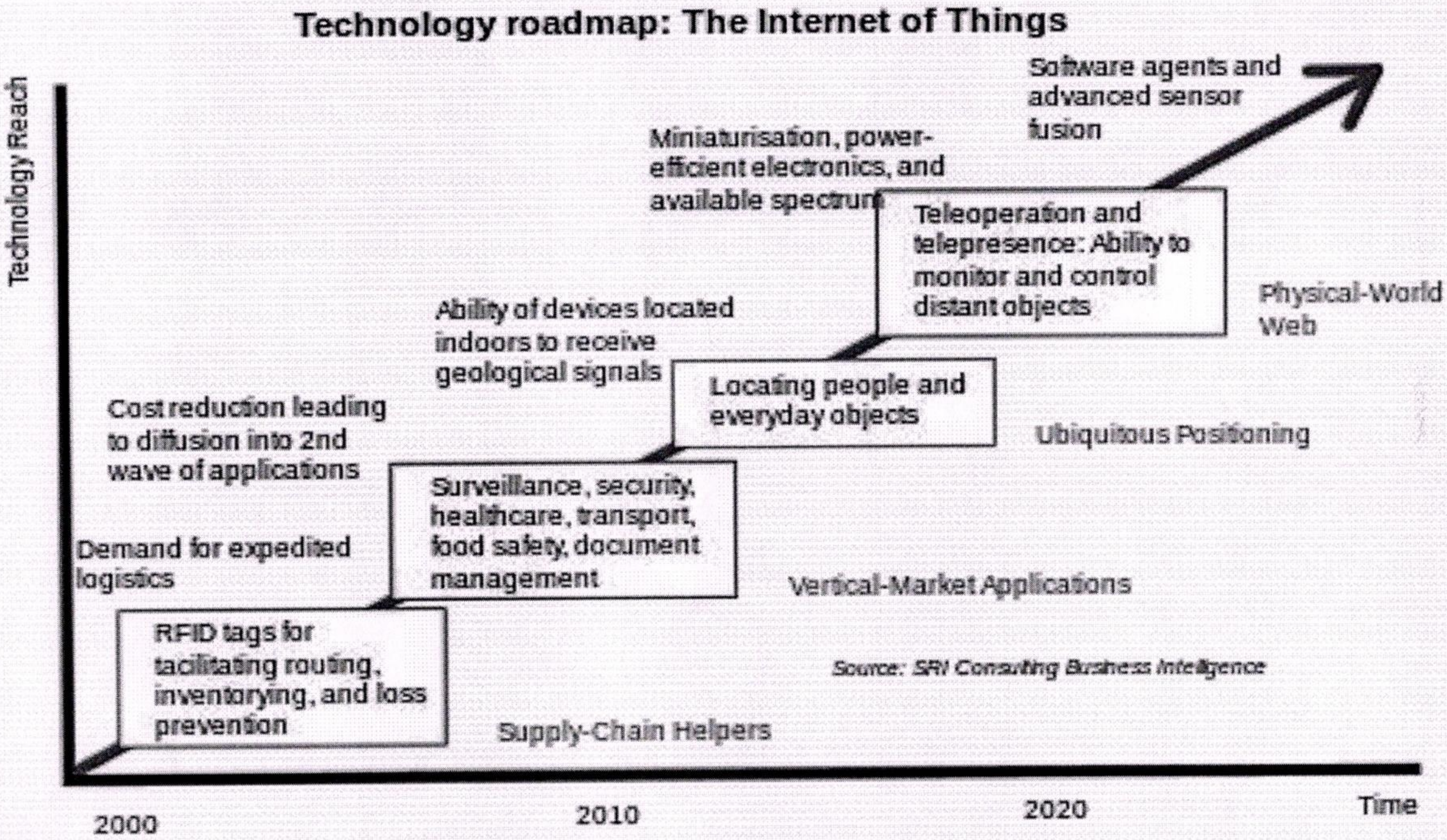
Note: Illustrative examples based on potential one percent savings applied across specific global industry sectors. Source: GE estimates

GE's estimates on potential of just ONE percent savings applied using IoT across global industry sectors.

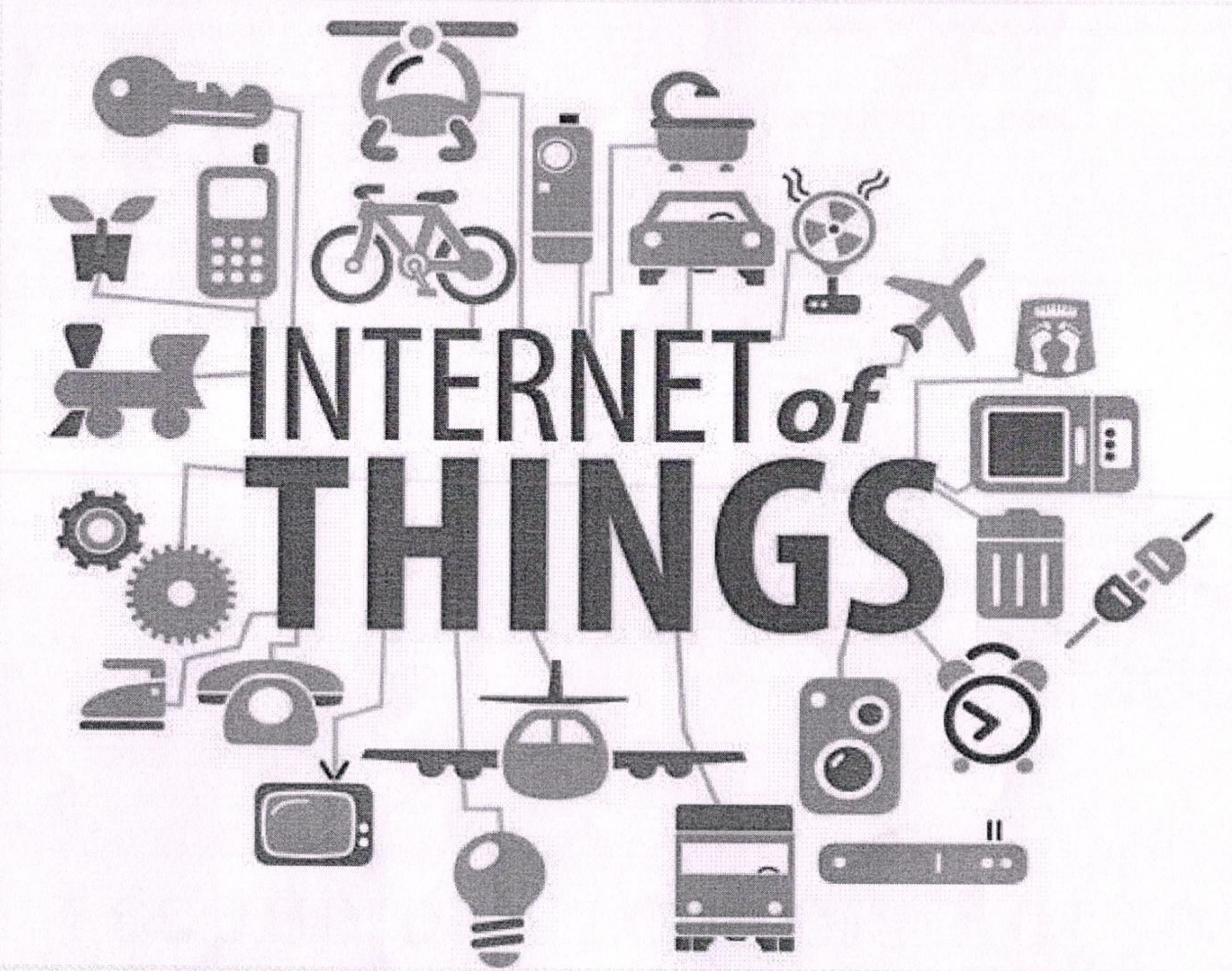
Unlock the Massive potential of IoT



Technology roadmap of IoT



Applications of IoT



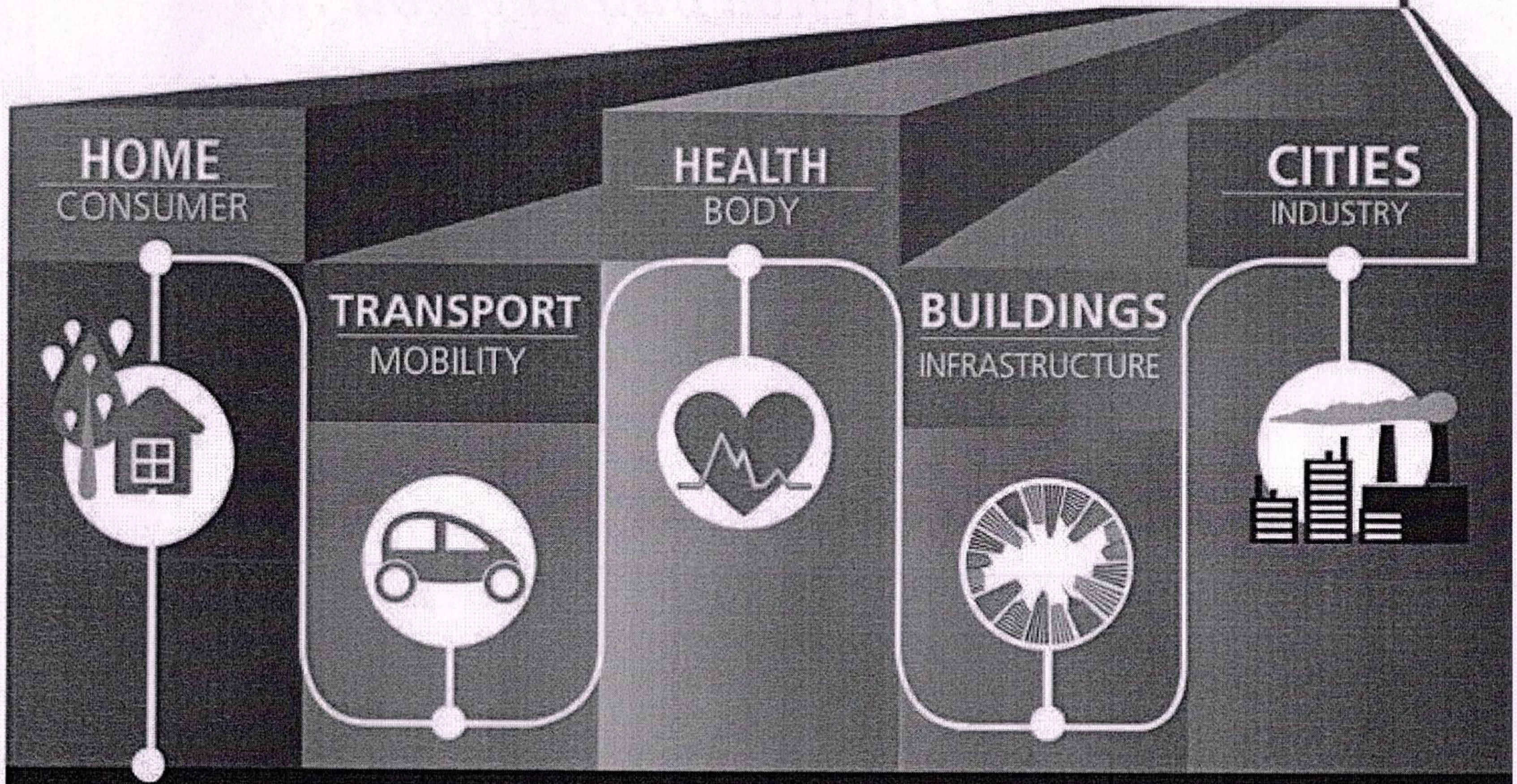
"The Ultimate Goal of IOT is to Automate Human Life."

Few Applications of IoT

- ✔ Building and Home automation
- ✔ Manufacturing
- ✔ Medical and Healthcare systems
- ✔ Media
- ✔ Environmental monitoring
- ✔ Infrastructure management
- ✔ Energy management
- ✔ Transportation
- ✔ Better quality of life for elderly
- ✔ … … …

You name it, and you will have it in IoT!

TO ➡ DIVERSE APPLICATIONS



Home / Consumer
Light bulbs
Security
Pet Feeding
Irrigation Controller
Smoke Alarm
Refrigerator
Infotainment
Washer / Dryer
Stove
Energy Monitoring

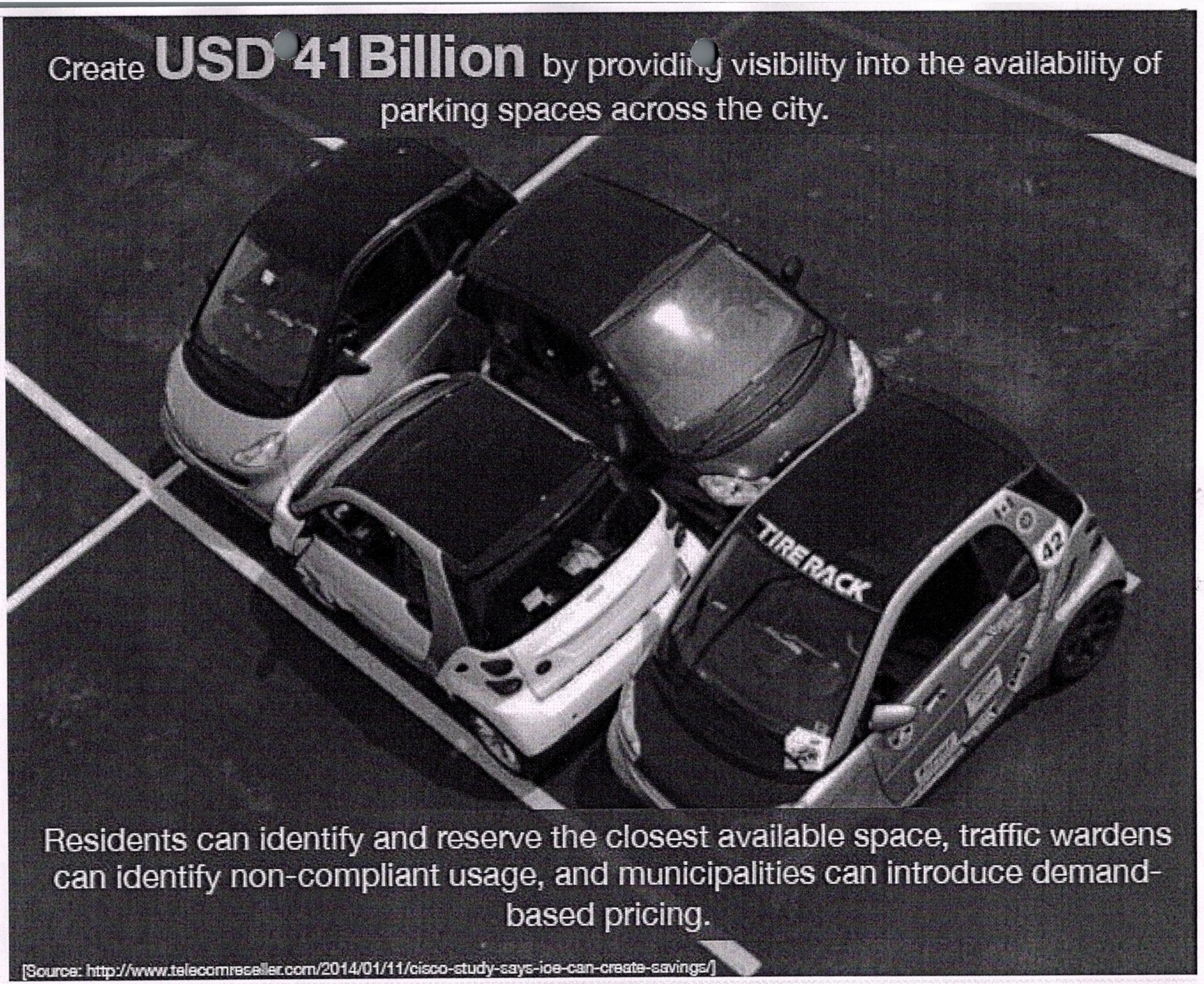
Transport / Mobility
Traffic routing
Telematics
Package Monitoring
Smart Parking
Insurance Adjustments
Supply Chain
Shipping
Public Transport
Airlines
Trains

Health / Body
Patient Care
Elderly Monitoring
Remote Diagnostic
Equipment Monitoring
Hospital Hygiene
Bio Wearables
Food sensors

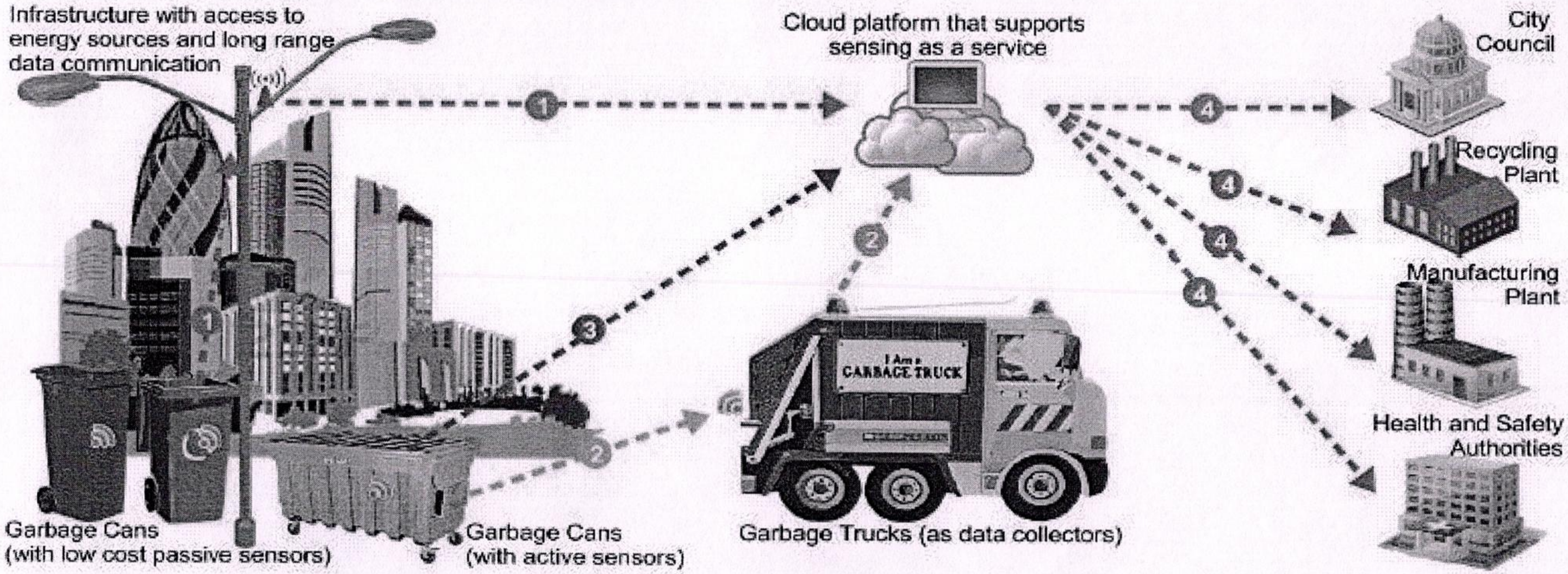
Buildings / Infrastructure
HVAC
Security
Lighting
Electrical
Transit
Emergency Alerts
Structural Integrity
Occupancy
Energy Credits

Cities / Industry
Electrical Distribution
Maintenance
Surveillance
Signage
Utilities / Smart Grid
Emergency Services
Waste Management

Smart Parking

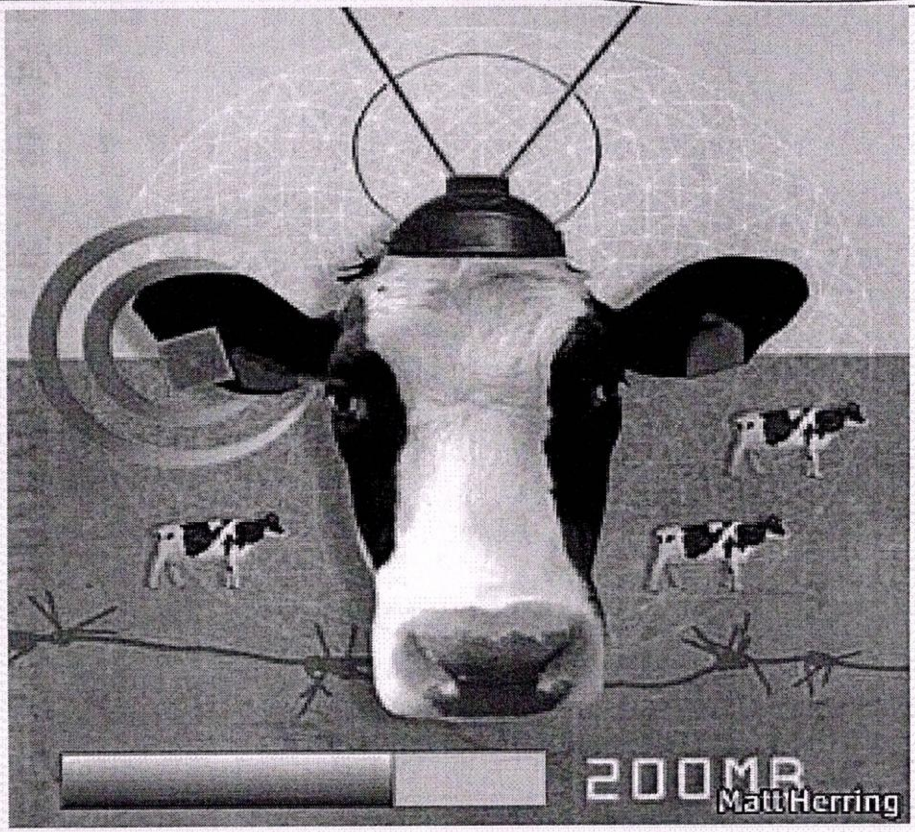


Efficient Waste Management in Smart Cities Supported by the Sensing-as-a-Service



[Source: "Sensing as a Service Model for Smart Cities Supported by Internet of Things", Charith Perera et. al., Transactions on Emerging Telecommunications Technology, 2014]

Sensors in even the holy cow!



In the world of IoT, even the cows will be connected and monitored. Sensors are implanted in the ears of cattle. This allows farmers to monitor cows' health and track their movements, ensuring a healthier, more plentiful supply of milk and meat for people to consume. On average, each cow generates about 200 MB of information per year.

Of course, we know nothing remains static, especially when it comes to the Internet. Initiatives and advances, such as Cisco's Planetary Skin, GE's Industrial Internet, HP's central nervous system for the earth (CeNSE), and smart dust, have the potential to add millions—even billions—of sensors to the Internet.

As cows, water pipes, people, and even shoes, trees, and animals become connected to IoT, the world has the potential to become a better place.

"With a trillion sensors embedded in the environment—all connected by computing systems, software, and services—it will be possible to hear the heartbeat of the Earth, impacting human interaction with the globe as profoundly as the Internet has revolutionized communication." - Peter Hartwell, Senior Researcher, HP Labs.

"How much more IoT can do is only left to your imagination"

Internet of Things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances.

Integration with the Internet implies that devices will use an IP address as a unique identifier. However, due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use IPv6 to accommodate the extremely large address space required.

Objects in the IoT will not only be devices with sensory capabilities, but also provide actuation capabilities (e.g., bulbs or locks controlled over the Internet).

On the other hand, IoT systems could also be responsible for performing actions, not just sensing things. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favourite products, or even location of items that they need, which their fridge has automatically conveyed to the phone.

Additional examples of sensing and actuating are reflected in applications that deal with heat, electricity and energy management, as well as cruise-assisting transportation systems. Other applications that the Internet of Things can provide is enabling extended home security features and home automation.

IOT Application Scenario Shopping

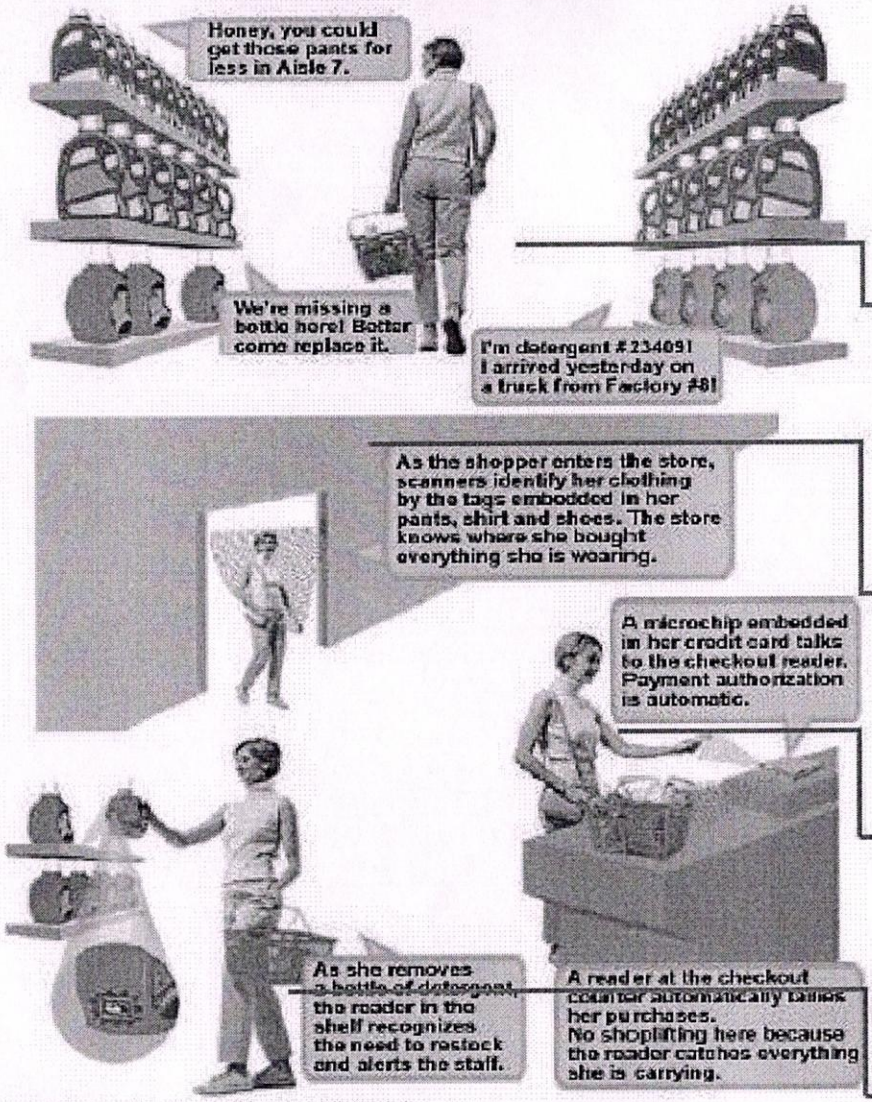


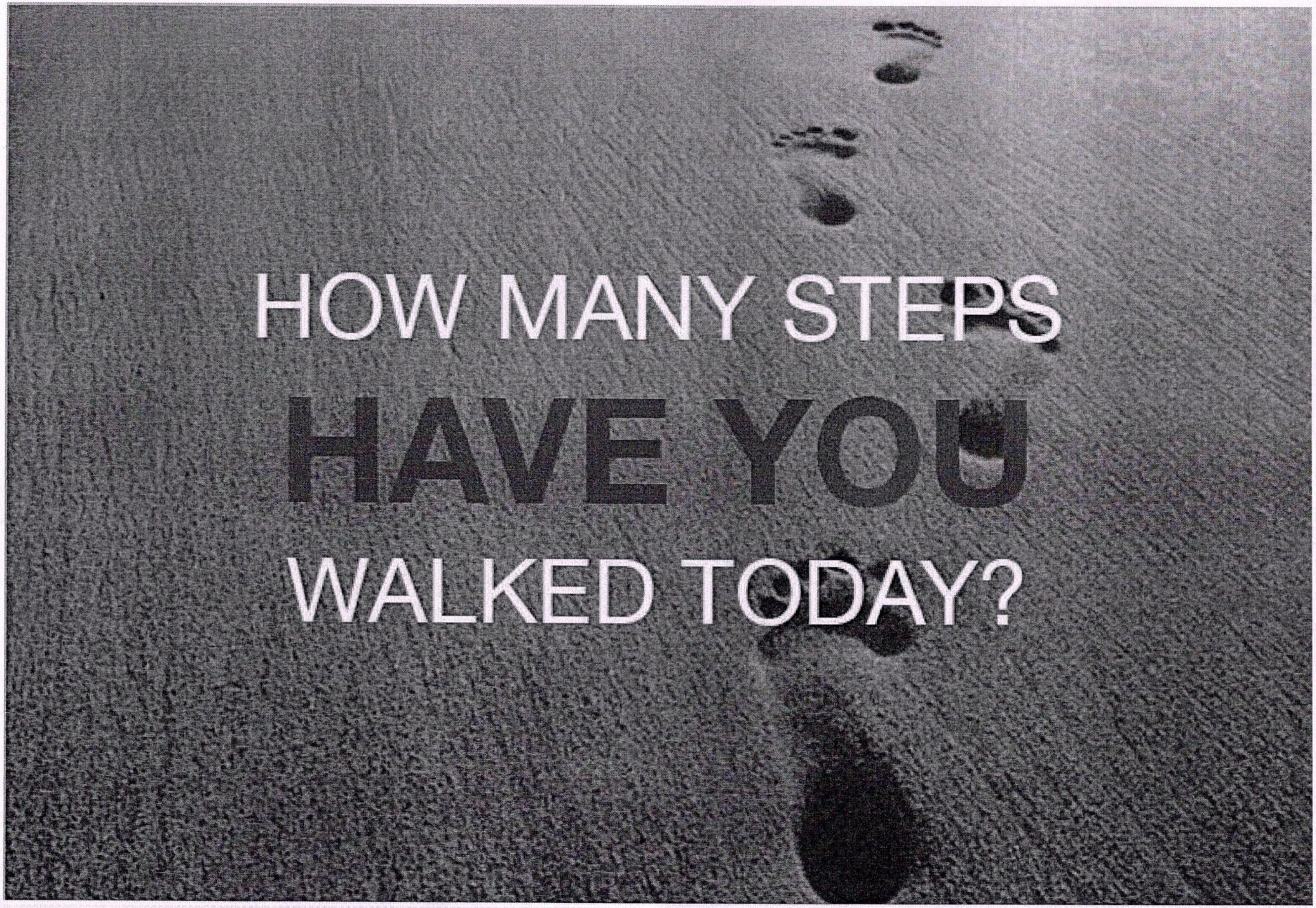
Illustration by Lisa Knouse Braiman for Forbes

(2) When shopping in the market, the goods will introduce themselves.

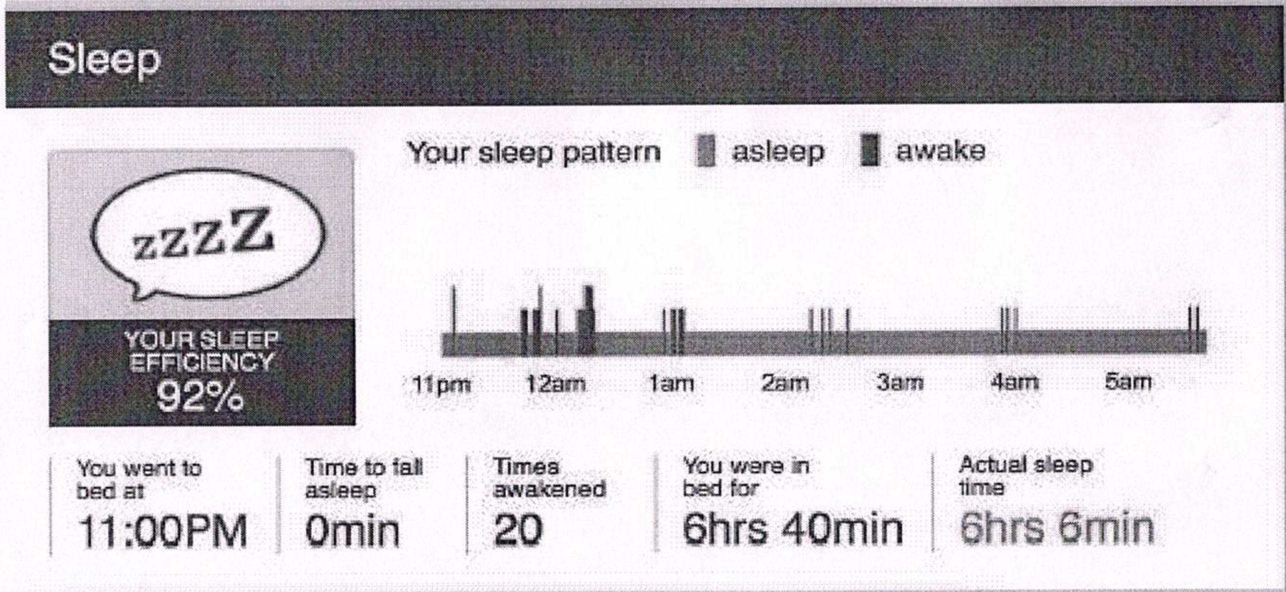
(1) When entering the doors, scanners will identify the tags on her clothing.

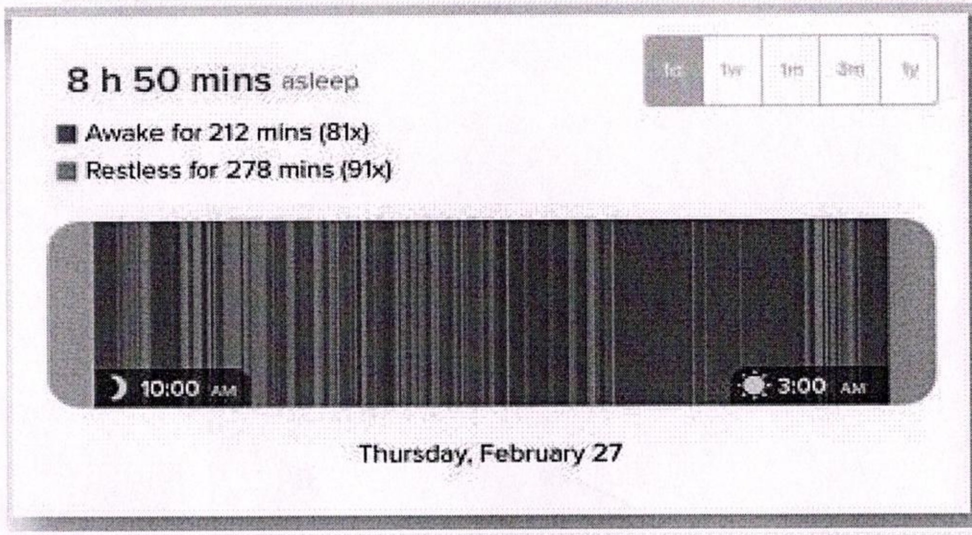
(4) When paying for the goods, the microchip of the credit card will communicate with checkout reader.

(3) When moving the goods, the reader will tell the staff to put a new one.


HOW MANY STEPS
HAVE YOU
WALKED TODAY?

How Well Do I Sleep?

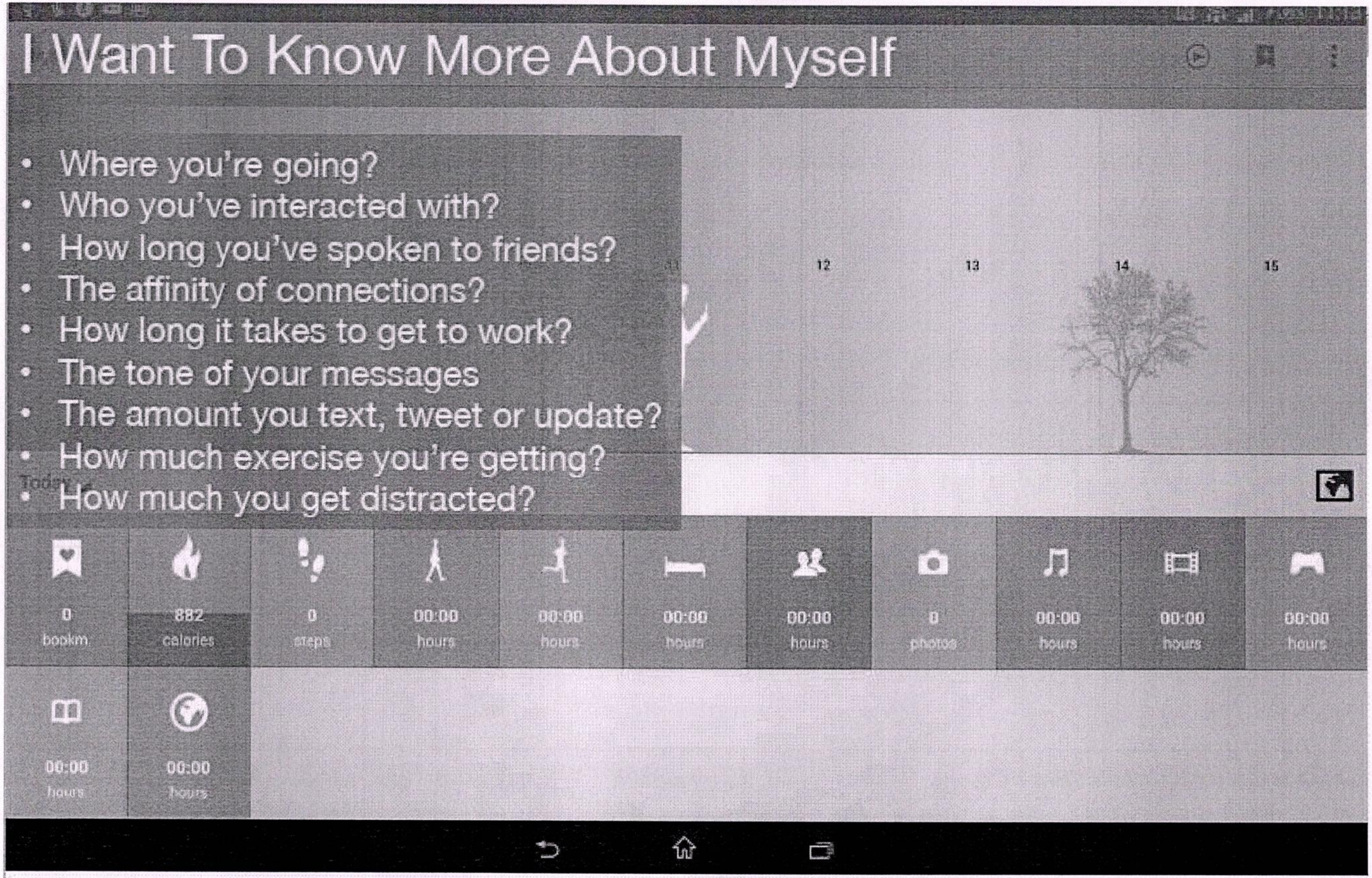




fitbit flex
Wireless Activity + Sleep Wristband

I Want To Know More About Myself

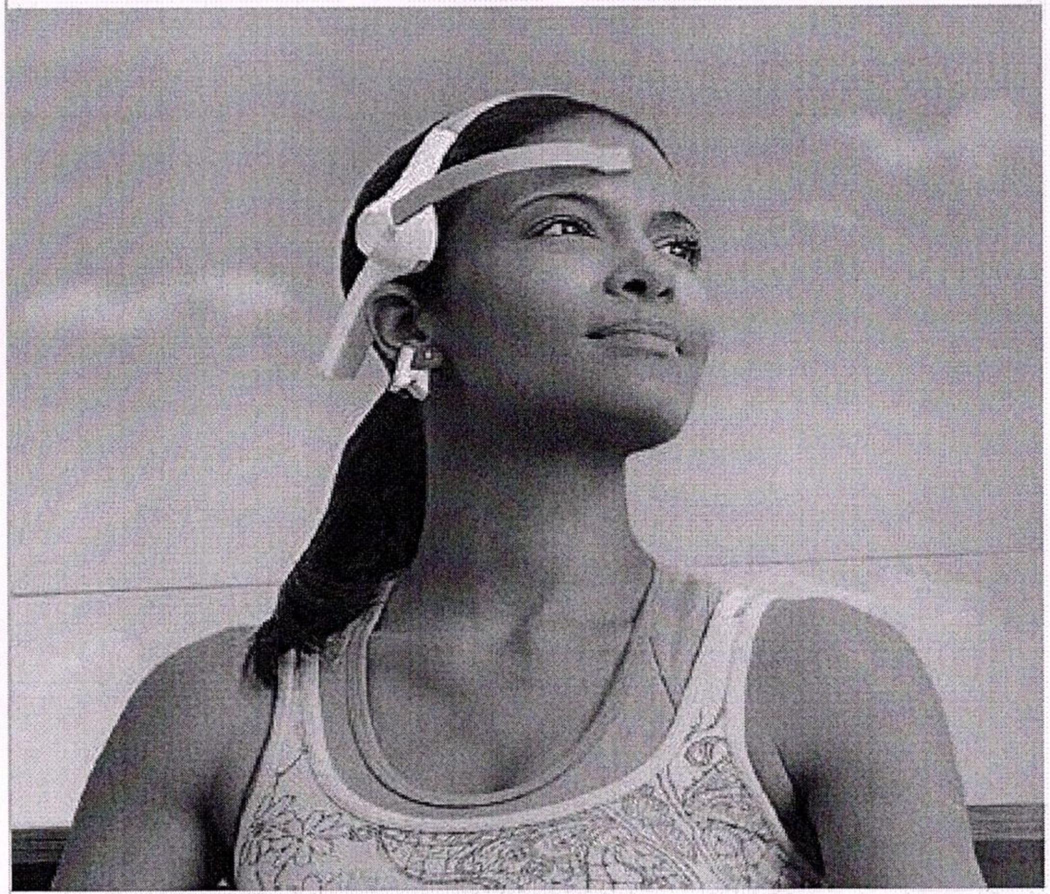
- Where you're going?
- Who you've interacted with?
- How long you've spoken to friends?
- The affinity of connections?
- How long it takes to get to work?
- The tone of your messages
- The amount you text, tweet or update?
- How much exercise you're getting?
- How much you get distracted?



Can Internet of Things (IOT) Help Us To Know More About Ourselves?

IoT helps you in LIFE LOGGING

Thought Controlled Computing



The flagship product, MindWave, is a headset that can log into your computer using just your thoughts. Researchers recently used the EEG headset to develop a toy car that can be driven forward with thought.

NeuroSky's smart sensors can also track your heart rate and other bodily metrics and can be embedded in the next generation of wearable devices.

"We make it possible for millions of consumers to capture and quantify critical health and wellness data," Yang (CEO of Softbank) said. Softbank is the funder.

[Source: http://venturebeat.com/2013/11/04/next-step-for-wearables-neurosky-brings-its-smart-sensors-to-health-fitness/]

TECHNOLOGICAL CHALLENGES OF IoT

At present IoT is faced with many challenges, such as:

- Scalability
- Technological Standardization
- Inter operability
- Discovery
- Software complexity
- Data volumes and interpretation
- Power Supply
- Interaction and short range communication
- Wireless communication
- Fault tolerance

"Big Data is not magic. It doesn't matter how much data you have if you can't make sense of it."

Criticisms and Controversies of IoT

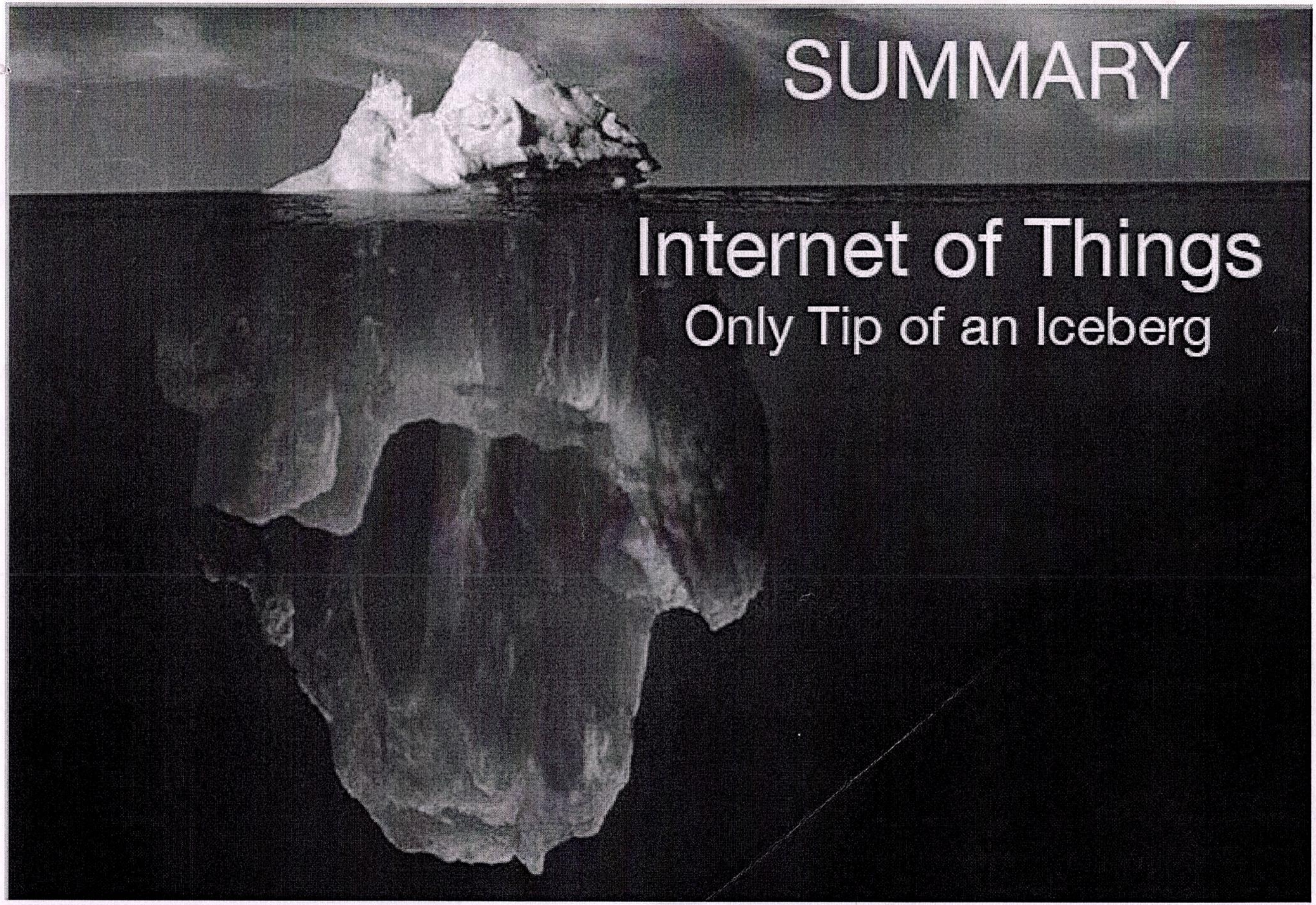
Scholars and social observers and pessimists have doubts about the promises of the ubiquitous computing revolution, in the areas as:

- Privacy
- Security
- Autonomy and Control
- Social control
- Political manipulation
- Design
- Environmental impact
- Influences human moral decision making

THANK YOU

References

1. www.google.com
2. https://en.wikipedia.org/wiki/Internet_of_Things
3. Cisco whitepaper, "The Internet of Things" - How the Next Evolution of the Internet Is Changing Everything, by Dave Evans, April 2011.
4. GE cloud expo 2014, "Industrial Internet as a Service", by Shyam Varan Nath, Principal Architect.
5. Dr. Mazlan Abbas, MIMOS Berhad, Wisma IEM, Petaling Jaya


SUMMARY
Internet of Things
Only Tip of an Iceberg

K.S.R.M. COLLEGE OF ENGINEERING

UGC - AUTONOMOUS
KADAPA, AP – 516 005

Certificate of Completion

This is to certify that

Mr/Ms. V. Vishnu Vardhan

Bearing the Roll No 189Y1A04F4

has Succesfully completed certification course on

Internet of things

From 17/05/2021 to 30/05/2021, Organized by Department of

ECE

Coordinator   Head Of Department   V. S. S. Murthy Principal

K.S.R.M. COLLEGE OF ENGINEERING

UGC - AUTONOMOUS

KADAPA , AP – 516 005

Certificate of Completion

This is to certify that

Mr/Ms. A Prem Reddy

Bearing the Roll No 189Y1A0403

has Succesfully completed certification course on

Internet of Things

From 17/05/2021 *to* 30/05/2021 *, Organized by Department of*

ECE

Coordinator

Head Of Department

V. S. S. Murthy

Principal

K.S.R.M. COLLEGE OF ENGINEERING

UGC - AUTONOMOUS

KADAPA , AP – 516 005

Certificate of Completion

This is to certify that

Mr/Ms. S. Iswarya

Bearing the Roll No 189Y1A04D9

has Succesfully completed certification course on

Internet of things

From 17/05/2021 to 30/05/2021 , Organized by Department of

ECE

Coordinator

Head Of Department

V. S. S. Murthy

Principal

K.S.R.M. COLLEGE OF ENGINEERING

(UGC - AUTONOMOUS)

Kadapa, Andhra Pradesh, India - 516003

Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu.

Department of Electronics & communication Engineering

Feedback Form

S.No.	Email addrtess	Name of the student	Year & Semester	Branch	Roll Num	Is the course content met your expectation	Is the lecture sequence well planned	The contents of the course is explained with examples	Is the level of course high	Is the course exposed you to the new knowledge and practices	Is the lecturer clear and easy to understand	Rate the value of course in increasing your skills	Any issues
1	179Y1A0462@ksrmce.ac.in	KAMBHAM ADWAITH	B.Tech VIsem	ECE	179Y1A0462	Yes	Yes	Agree	Agree	Strongly agree	4	5	Nothing
2	179Y1A0498@ksrmce.ac.in	PAMUDURTHI MANOJ KUMAR	B.Tech VIsem	ECE	179Y1A0498	Yes	Yes	Agree	Agree	Strongly agree	5	5	Nothing
3	189Y1A0401@ksrmce.ac.in	ALLADI ANITHA (W)	B.Tech VIsem	ECE	189Y1A0401	Yes	Yes	Agree	Agree	Strongly agree	4	5	Good
4	189Y1A0402@ksrmce.ac.in	ALLURI YADITHYA	B.Tech VIsem	ECE	189Y1A0402	Yes	Yes	Agree	Agree	Strongly agree	5	5	nothing
5	189Y1A0403@ksrmce.ac.in	ANDLURU PREM REDDY	B.Tech VIsem	ECE	189Y1A0403	Yes	Yes	Agree	Agree	Strongly agree	5	5	Good
6	189Y1A0404@ksrmce.ac.in	ARAVA SHYAMDEEP	B.Tech VIsem	ECE	189Y1A0404	Yes	Yes	Agree	Agree	Strongly agree	4	5	very good
7	189Y1A0406@ksrmce.ac.in	AVULA ADARSH KUMAR REDDY	B.Tech VIsem	ECE	189Y1A0406	Yes	Yes	Strongly agree	Agree	Strongly agree	4	3	Nothing

8	189Y1A0407@ksrmce.ac.in	AVULA NAGENDRABABU	B.Tech VIsem	ECE	189Y1A0407	Yes	Yes	agree	Agree	Strongly agree	4	4	no
9	189Y1A0408@ksrmce.ac.in	AVULA SRIKANTH	B.Tech VIsem	ECE	189Y1A0408	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	Nothing
10	189Y1A0409@ksrmce.ac.in	BAIMUTHAKA MAHESH	B.Tech VIsem	ECE	189Y1A0409	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	Good
11	189Y1A0410@ksrmce.ac.in	BANDARI SAI HARSHA VARDHAN	B.Tech VIsem	ECE	189Y1A0410	Yes	Yes	Agree	Agree	Strongly agree	5	4	Good
12	189Y1A0411@ksrmce.ac.in	BAREDDY JAGADEESH REDDY	B.Tech VIsem	ECE	189Y1A0411	Yes	Yes	agree	Agree	Strongly agree	5	5	Good
13	189Y1A0412@ksrmce.ac.in	BATHALA KOWSALYA (W)	B.Tech VIsem	ECE	189Y1A0412	Yes	Yes	agree	Agree	Strongly agree	3	5	Good
14	189Y1A0413@ksrmce.ac.in	BATIKERI VIJAYASREE (W)	B.Tech VIsem	ECE	189Y1A0413	Yes	Yes	agree	Agree	Strongly agree	5	4	very good
15	189Y1A0414@ksrmce.ac.in	BAYANABOINA REDDI	B.Tech VIsem	ECE	189Y1A0414	Yes	Yes	agree	Agree	Strongly agree	4	4	very good
16	189Y1A0415@ksrmce.ac.in	BEECHU CHETAN REDDY	B.Tech VIsem	ECE	189Y1A0415	Yes	Yes	agree	Agree	Strongly agree	5	4	very good
17	189Y1A0416@ksrmce.ac.in	BOGATHI HEMANTH KUMAR REDDY	B.Tech VIsem	ECE	189Y1A0416	Yes	Yes	agree	Agree	Strongly agree	3	5	no
18	189Y1A0417@ksrmce.ac.in	BOGGALA CHANDRA SEKHAR	B.Tech VIsem	ECE	189Y1A0417	Yes	Yes	agree	Agree	Strongly agree	4	5	nithing
19	189Y1A0418@ksrmce.ac.in	LAKSHMI PRASANNA (W)	B.Tech VIsem	ECE	189Y1A0418	Yes	Yes	Strongly agree	Agree	Strongly agree	4	5	Good
20	189Y1A0420@ksrmce.ac.in	BONAMSETTY JAHNAVI (W)	B.Tech VIsem	ECE	189Y1A0420	Yes	Yes	Strongly agree	Agree	Strongly agree	4	4	Good
21	189Y1A0468@ksrmce.ac.in	KRISHNAM GANGA MAHESWAR REDDY	B.Tech VIsem	ECE	189Y1A0468	Yes	Yes	Strongly agree	Agree	Strongly agree	4	3	Good
22	189Y1A0469@ksrmce.ac.in	KUMBAGIRI MADHU PRIYA (W)	B.Tech VIsem	ECE	189Y1A0469	Yes	Yes	agree	Agree	Strongly agree	4	4	Good
23	189Y1A0470@ksrmce.ac.in	KUMMARA THANMAI (W)	B.Tech VIsem	ECE	189Y1A0470	Yes	Yes	agree	Agree	Strongly agree	5	4	Good

24	189Y1A0471@ksrmce.ac.in	KURAKU NAGESWARA RAO	B.Tech VIsem	ECE	189Y1A0471	Yes	Yes	Strongly agree	Agree	Strongly agree	5	4	Good
25	189Y1A0472@ksrmce.ac.in	KURRA MANJULA (W)	B.Tech VIsem	ECE	189Y1A0472	Yes	Yes	agree	Agree	Strongly agree	5	5	Good
26	189Y1A0473@ksrmce.ac.in	LAKKIREDDY SAIPRANAVARSHITHA (W)	B.Tech VIsem	ECE	189Y1A0473	Yes	Yes	agree	Agree	Strongly agree	5	5	Nothing
27	189Y1A0474@ksrmce.ac.in	MADARASU SAI KRISHNA	B.Tech VIsem	ECE	189Y1A0474	Yes	Yes	agree	Agree	Strongly agree	5	5	no
28	189Y1A0475@ksrmce.ac.in	MALEPATI DEEPALI (W)	B.Tech VIsem	ECE	189Y1A0475	Yes	Yes	agree	Agree	Strongly agree	3	4	no
29	189Y1A0476@ksrmce.ac.in	MALLELA HARIHARA NANDAN	B.Tech VIsem	ECE	189Y1A0476	Yes	Yes	Strongly agree	Agree	Strongly agree	3	4	no
30	189Y1A0477@ksrmce.ac.in	MALLI SETTY DIVYA MALIKA (W)	B.Tech VIsem	ECE	189Y1A0477	Yes	Yes	Strongly agree	Agree	Strongly agree		5	no
31	189Y1A0478@ksrmce.ac.in	MANGALA NAVEEN KUMAR	B.Tech VIsem	ECE	189Y1A0478	Yes	Yes	Strongly agree	Agree	Strongly agree	5	4	nothing
32	189Y1A0479@ksrmce.ac.in	MANGALI ARUN KUMAR	B.Tech VIsem	ECE	189Y1A0479	Yes	Yes	agree	Agree	Strongly agree	5	5	Nothing
33	189Y1A0480@ksrmce.ac.in	MANGALI GIRINDRA KUMAR	B.Tech VIsem	ECE	189Y1A0480	Yes	Yes	agree	Agree	Strongly agree	5	4	no
34	189Y1A0481@ksrmce.ac.in	MANGAMMAGARI SANDHYA (W)	B.Tech VIsem	ECE	189Y1A0481	Yes	Yes	agree	Agree	Strongly agree	5	4	Nothing
35	189Y1A0482@ksrmce.ac.in	MANJULA PAVANI (W)	B.Tech VIsem	ECE	189Y1A0482	Yes	Yes	agree	Agree	Strongly agree	5	4	Good
36	189Y1A0483@ksrmce.ac.in	MANJULA VENKATESHWARA	B.Tech VIsem	ECE	189Y1A0483	Yes	Yes	agree	Agree	Strongly agree	5	5	Good
37	189Y1A0484@ksrmce.ac.in	MANTRI REDDY AMRUTHA BHAVANI	B.Tech VIsem	ECE	189Y1A0484	Yes	Yes	agree	Agree	Strongly agree	5	5	Good
38	189Y1A0486@ksrmce.ac.in	MEGADA SUNITHA (W)	B.Tech VIsem	ECE	189Y1A0486	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	Good

39	189Y1A0487@ksrmce.ac.in	MEKALA REVATHI (W)	B.Tech VIsem	ECE	189Y1A0487	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	Good
40	189Y1A0488@ksrmce.ac.in	MUDDALAPURAM SAI SURYA	B.Tech VIsem	ECE	189Y1A0488	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	Good
41	189Y1A04D5@ksrmce.ac.in	SHEELLA KRISHNA TEJA	B.Tech VIsem	ECE	189Y1A04D5	Yes	Yes	agree	Agree	Strongly agree	4	4	Good
42	189Y1A04D6@ksrmce.ac.in	SHREYA KAYANDE (W)	B.Tech VIsem	ECE	189Y1A04D6	Yes	Yes	agree	Agree	Strongly agree	4	5	Good
43	189Y1A04D7@ksrmce.ac.in	SIDDI ALTHAF	B.Tech VIsem	ECE	189Y1A04D7	Yes	Yes	agree	Agree	Strongly agree	4	5	Good
44	189Y1A04D8@ksrmce.ac.in	SINGAVARAM PAVAN SAI	B.Tech VIsem	ECE	189Y1A04D8	Yes	Yes	agree	Agree	Strongly agree	3	5	Good
45	189Y1A04D9@ksrmce.ac.in	SUDHAM ISWARYA (W)	B.Tech VIsem	ECE	189Y1A04D9	Yes	Yes	agree	Agree	Strongly agree	3	5	Nothing
46	189Y1A04E0@ksrmce.ac.in	SUNKESULA SIVA KUMARI (W)	B.Tech VIsem	ECE	189Y1A04E0	Yes	Yes	Strongly agree	Agree	Strongly agree	2	5	Nothing
47	189Y1A04E1@ksrmce.ac.in	SYED MOHAMMED TAHIR	B.Tech VIsem	ECE	189Y1A04E1	Yes	Yes	agree	Agree	Strongly agree	2	5	very good
48	189Y1A04E2@ksrmce.ac.in	NARAHAN DEEP GUPTA	B.Tech VIsem	ECE	189Y1A04E2	Yes	Yes	agree	Agree	Strongly agree	4	5	very good
49	189Y1A04E3@ksrmce.ac.in	THAMATAM GURU CHANDANA (W)	B.Tech VIsem	ECE	189Y1A04E3	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	very good
50	189Y1A04E4@ksrmce.ac.in	THIRUVEEDHULA BHAVANI (W)	B.Tech VIsem	ECE	189Y1A04E4	Yes	Yes	Strongly agree	Agree	Strongly agree	4	5	nothing
51	189Y1A04E5@ksrmce.ac.in	THOTLI NAVYA (W)	B.Tech VIsem	ECE	189Y1A04E5	Yes	Yes	agree	Agree	Strongly agree	4	5	Good
52	189Y1A04E6@ksrmce.ac.in	UPPALURU SIVA SANKAR	B.Tech VIsem	ECE	189Y1A04E6	Yes	Yes	agree	Agree	Strongly agree	4	5	Good
53	189Y1A04E7@ksrmce.ac.in	UTTI SREE HARSHA	B.Tech VIsem	ECE	189Y1A04E7	Yes	Yes	agree	Agree	Strongly agree	4	5	nothing

54	189Y1A04E8@ksrmce.ac.in	VADATHALA HARSHITH REDDY	B.Tech VIsem	ECE	189Y1A04E8	Yes	Yes	agree	Agree	Strongly agree	4	5	nothing
55	189Y1A04E9@ksrmce.ac.in	VALASAPALLI ANNAMAYYA	B.Tech VIsem	ECE	189Y1A04E9	Yes	Yes	agree	Agree	Strongly agree	4	5	nothing
56	189Y1A04F0@ksrmce.ac.in	VARRA PRAVALIKA (W)	B.Tech VIsem	ECE	189Y1A04F0	Yes	Yes	agree	Agree	Strongly agree	4	5	Good
57	189Y1A04F1@ksrmce.ac.in	VAYALPATI RAMANJANEYULU	B.Tech VIsem	ECE	189Y1A04F1	Yes	Yes	agree	Agree	Strongly agree	5	5	Good
58	189Y1A04F2@ksrmce.ac.in	CHANDAN SAI VAMSI KRISHNA	B.Tech VIsem	ECE	189Y1A04F2	Yes	Yes	agree	Agree	Strongly agree	5	5	very good
59	189Y1A04F3@ksrmce.ac.in	VELLALA NAGA RUCHITHA (W)	B.Tech VIsem	ECE	189Y1A04F3	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	very good
60	189Y1A04F4@ksrmce.ac.in	VEMA VISHNUVARDHAN	B.Tech VIsem	ECE	189Y1A04F4	Yes	Yes	Strongly agree	Agree	Strongly agree	5	5	nothing
61	189Y1A04F5@ksrmce.ac.in	VEMPALLI RAM NARAYAN SASANK	B.Tech VIsem	ECE	189Y1A04F5	Yes	Yes	agree	Agree	Strongly agree	5	5	no

Coordinator

HOD
Professor & H.O.D.
Department of E.C.E.
K.S.R.M. College of Engineering
KADAPA - 516 003.

V. S. S. Murthy
Principal
PRINCIPAL
K.S.R.M. COLLEGE OF ENGINEERING
KADAPA - 516 003. (A.P.)