iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** II **Month of publication:** February

DOI: http://doi.org/10.22214/ijraset.2019.2142

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue II, Feb 2019- Available at www.ijraset.com

Internet of Things (IoT) Technologies - A Study

Linguberi Sravani[1], Shaik Nasreen[2]
[1, 2]UG Student, Department of EEE, GMR Institute of Technology, Rajam.

Abstract: This paper discusses about the internet of things and its technologies. Internet of things is newly developed in smart sensors, Communication, agricultural technology, Medical Technology, Industrial and household appliances. It is designed in a way to work without presence of human. In future years of IoT is to create the main hub between the various Technologies by connecting smart physical objects together and form different applications along related issues.
Keywords: Internet of things (IoT), Intricate technologies

I. INTRODUCTION

In the coming years IoT is expected to be one of the main hub in various technologies. IoT is mainly by using smart phone problems directly to drive without any external or human presence. The life of potential user can become easy and comfortable by adopting various Technologies based on IoT in addition it has dramatic effect on domestic sphere, such as living smart homes, smart cars etc IoT is the uniquely with the network and capable of sharing information with or without human interaction. For the domestic purposes rapidly increases in the better management mechanisms are developing in IoT. It creates a crucial demand to implement smart home applications focusing on consuming energy efficient in residential buildings. New connection of smart home interference the different applications has more realistic and more energy efficient smart home. The home automation is widely used for central controlling of lighting, heating, ventilation and air conditioning and security. IoT is mainly used for the monitoring systems and controlling system in industries.

II. INTRICATE TECHNOLOGIES

Various technologies are involves implementing the idea of IOT. In this paper we will focus on these technology.

1) Radio frequency Identification (RFID)
2) Near Field Communication (NFC)
3) Machine-to-Machine Communication (M2M)
4) Vehicle-to-Vehicle Communication (V2V)

A. Radio Frequency Identification (RFID)

RFID system comprise two or more readers and several RFID tags. The attached data is send by using radio frequency electromagnetic fields. The tags that are attached to it, stored data electronically which can be read by RFID when it comes in the proximity of the reader comments. RFID allows monitoring objects in real time, without the need of being in line of sight comment RFID tag or label is very small microchip attached to an antenna in a compact package. Different types of frequencies like low frequency (LF), high frequency (HF), ultrahigh frequency (UHF) and super high frequency (SHF) bands etc. are used in RFID technology. The ultrahigh frequency (UHF) band RFID has been attractive to industrial services, goods flow tracking, manufacturing industries, logistic distribution, and the bioengineering applications. The another RFID band known as the super high frequency (SHF) RFID performs high-speed tracking, and thus, it can be used for traffic toll collection and the goods management.

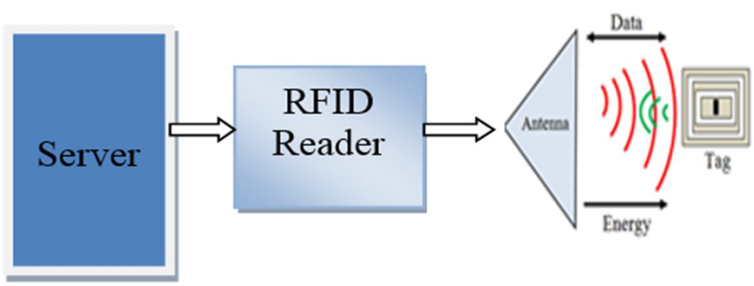


Fig. 1 Block diagram of RFID technology

The channel communication between the RFID tag and the RFID reader is not secure because they exchange data or information through wirelessly and an adversary could intercept the data easily. But the communication channel between the RFID read and the server is secure because a secure channel is established between them through a pre-shared secret key and some security mechanism.

1) *RFID Tag:* A tag is consists of an antenna, a microchip and a dedicated hardware for cryptographic operations. It can store the secret data for authentication and it communicates with the RFID reader. Usually, the RFID tags computing capacity and memory storage are very limited. RFID tags could be divided into three types:
   a) Passive tag.
   b) Semi active tag.
   c) Active tag.
2) *Passive Tag:* The passive tag gets power through wireless signals or radio signals from the reader. It is depend external device. It is highly used due its cost is less as compare to the other tags. The semi-active tag is equipped with a small battery and gets power from it. The passive and the semi-active tags use backscatter modulation to send messages to the RFID reader. The active tag is independent and it is equipped with a small battery and a radio transceiver. It can communicate directly with the reader.
3) *RFID Reader:* An RFID reader is composed of a radio transmitter or transponder, a radio receiver, a control unit, and a memory unit. Memory unit is to store the information which is received from RFID tags. The main function of an RFID reader is to enable the RFID tag and the server to exchange messages or data information between each other and achieve mutual authentication. Usually, the RFID tag computing capacity is lesser compared to that of the RFID reader's.
4) *Server:* A server is a trusted entity. To achieve the goal of mutual authentication, when the system is set up then the stores of all the RFID tags Identification information is in its database. The server could determine the validity of the tag by using the stored identification information. Usually computing capability and memory capacity are high in the server's. [D. He and S. Zeadally, 2015]

There are a number of frequency bands assigned to this technology such as SHF band of 5.72–5.87Ghz UHF band (840–960 MHz),microwave-frequency bands (2.4 Hz–2.48 GHz), whose Utilities are governed by the local regulations of a nation. There is the need of integrating this technology to the various wireless standards to make the RFID system automated. In any wireless system, the antenna is the RF-front end which plays a crucial role in the system operation and performance. Using an omnidirectional antenna we can investigate the RFID automation platform. Circular polarized (CP) and LP-based reader antennas readers are used in the RFID. Multi-standard reader antenna to integrate the RFID system to various networking infrastructure needed for the IOT applications.

Wideband reader antenna working at three RFID bands 840–960 MHz, 2.40–2.48 GHz, and 5.72–5.87 GHZ matched to 50-_ port characteristic impedance is proposed. In the lower band, the −10Db impedance bandwidth of the antenna extends over 697–1000 MHz which encompasses various multi-standard services like TV broadcasting, global standard for mobile communications (GSM), and long-term evolution (LTE) bands for 4G and 5G communications. To integrate the RFID reader to the IOT infrastructures, a switching/multiplexing schematic using the various communication modules is proposed.

RFID is highly desired to extract power from the signal transmitted by a reader instead of using battery to power-up RFID tags. Passive RFID tags commonly utilize two different coupling techniques are to extract power from reader's signal.

a) Inductive
b) Radiative

Inductive coupling supports a short communication range of a few centimeters, while radiative coupling can extend the communication range to a few meters. The available power for a tag decreases rapidly with its distance from reader. Thus, a transponder has to be within a short range from reader to extract the required power for its internal circuits from the signal transmitted by reader.

The available power for a UHF tag at several meters from reader is in the range of microwatts.

A passive RFID transponder converts the induced voltage across its antenna to a dc voltage using rectifier to activate its control circuit and memory. The tag internal circuits have to be optimized for power efficiency due to the limited available power. To extract maximum power from the reader signal by a tag, matching circuits are required.

[A.Attaran and R. Rashidzadeh, 2016]

B. Near Field Communication (NFC)

Near Field Communication (NFC) is a set of standards for portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually not greater than 10 cm. NFC standards cover communications protocols and data exchange formats. NFC are designed based on existing radio frequency identification (RFID). Link addresses of NFC devices are not physically fixed values, so this give negative influences to IP networking; especially, connection continuity. [Y. Choi et.al.2017]

NFC provides a short span of wireless communication between two NFC enabled devices or an NFC enabled device and an NFC chip (also known as an NFC tag or sensor), without the need for an internet connection. Most Android smartphones and tablets are NFC enabled, and can be programmed to read and react to NFC tags. Hence, applications written for exploiting Androids NFC capabilities can lead to a product that is expected to be attractive to a large number of customers. [H. Saeed et.al, 2016]

NFC technology enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC complements many popular consumer level wireless technologies, by utilizing the main elements in existing standards for contact less card technology. [Y.Honget.al, 2015]

Fig. 4 Near field communication device

NFC is a contactless communication standard based on RFID technology that operates at a radio frequency of 13.56 MHz. In addition to eavesdropping, also other types of attacks such as man-in-the-middle, denial-of-service or replay attacks can be applied to unsecured NFC communication Despite these potential issues, NFC is used in various domains due to its intuitive device coupling mechanism that is easy to understand for humans.[T.Ulz,T.Pieberet.a', 2017].

C. Machine-to-Machine Communication

Machine-to-Machine Communication (M2M) communication has emerged as a promising technology enabling billions of multipurpose devices, namely machine-type communication (MTC) devices can capability to communicate with each other without human intervention. Applications are like smart grids for intelligent monitoring, control and efficient delivery ery of electricity to consumers, smart cities, for increasing security, green energy, and intelligent parks, smart Healthcare systems intelligent transportation systems [B.W.Khoueiry et.al, 2016]

M2M communications is an emerging communication paradigm that provides ubiquitous connectivity between devices along with an ability to communicate autonomously requiring no human intervention. M2M communications acts as an enabling technology for the practical realization of IoT. IoT is envisioned as "a global network of connected devices having identities and virtual personalities operating in smart spaces and using intelligent interfaces to communicate within social, environmental, and user contexts".

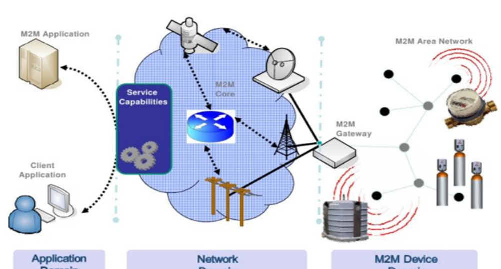


Fig. 5: Layout of M2M communication
Source: ETSI

Generally, M2M networks can be divided into two broad domains: 1) capillary M2M and2) cellular M2M networks. Capillary M2M networks, M2M devices form a device area network wherein connectivity is pro- vided through short-range communication technologies (such as ZigBee and Wi-Fi). Wide area connectivity is provided through a gateway. Capillary M2M networks are generally characterized by a huge number of low-cost and low-complexity devices, requirements of high energy efficiency and reliability, unplanned deployments, high packet loss ratios, use of low power link layer technologies, etc.

This type of networks is also referred to as low power networks in cellular M2M networks, M2M devices are equipped with embedded SIM cards and have the ability of communicating autonomously with the cellular network like a normal user equipment. Cellular M2M has uniquely characteristics of small data transmissions, mostly mobile-originated (uplink) traffic, little or no mobility of devices, service requirements of high energy efficiency, etc. [A.Aijaz. Et.al, 2015]

Smart city supported by MTC devices with interconnected users, surveillance systems, traffic lights, vehicles, roads, railways, sensor devices, and servers via telecommunication infrastructures

First the number of devices that are connected and maintained by one AP is usually large in an M2M communication network. It is highly likely that the large number of devices share limited network resources such as spectrum and time slot. If the network is designed for the highly congested industrial, scientific and medical (ISM) radio band, the coexistence problem needs to be studied. Meanwhile, for the licensed radio band deployment scenarios, the operating cost of using the spectrum also influences the design.

Second, the energy consumption of M2M communication network devices is usually constrained. Wireless devices must operate on their own batteries for years instead of days. This constraint poses design challenges on both the physical (PHY) layer and media access control (MAC) layer protocols. Therefore, while on the one hand low Tx power and high receiver sensitivity are expected, on the other hand, the channel access mechanism must be energy aware, minimizing the energy consumption.

Third, it is likely that one network supports M2M communication devices with ability to generate and process different traffic patterns. Under this scenario, the MAC scheme of the network must be adaptive to the different traffic types to achieve energy efficiency while maintaining their QOS requirement. [H. Wang et,al. 2017]

III. CONCLUSION

Generally, the design of the enabling technologies for a wide variety of low power and long range M2M communication networks is challenging.

REFERENCE

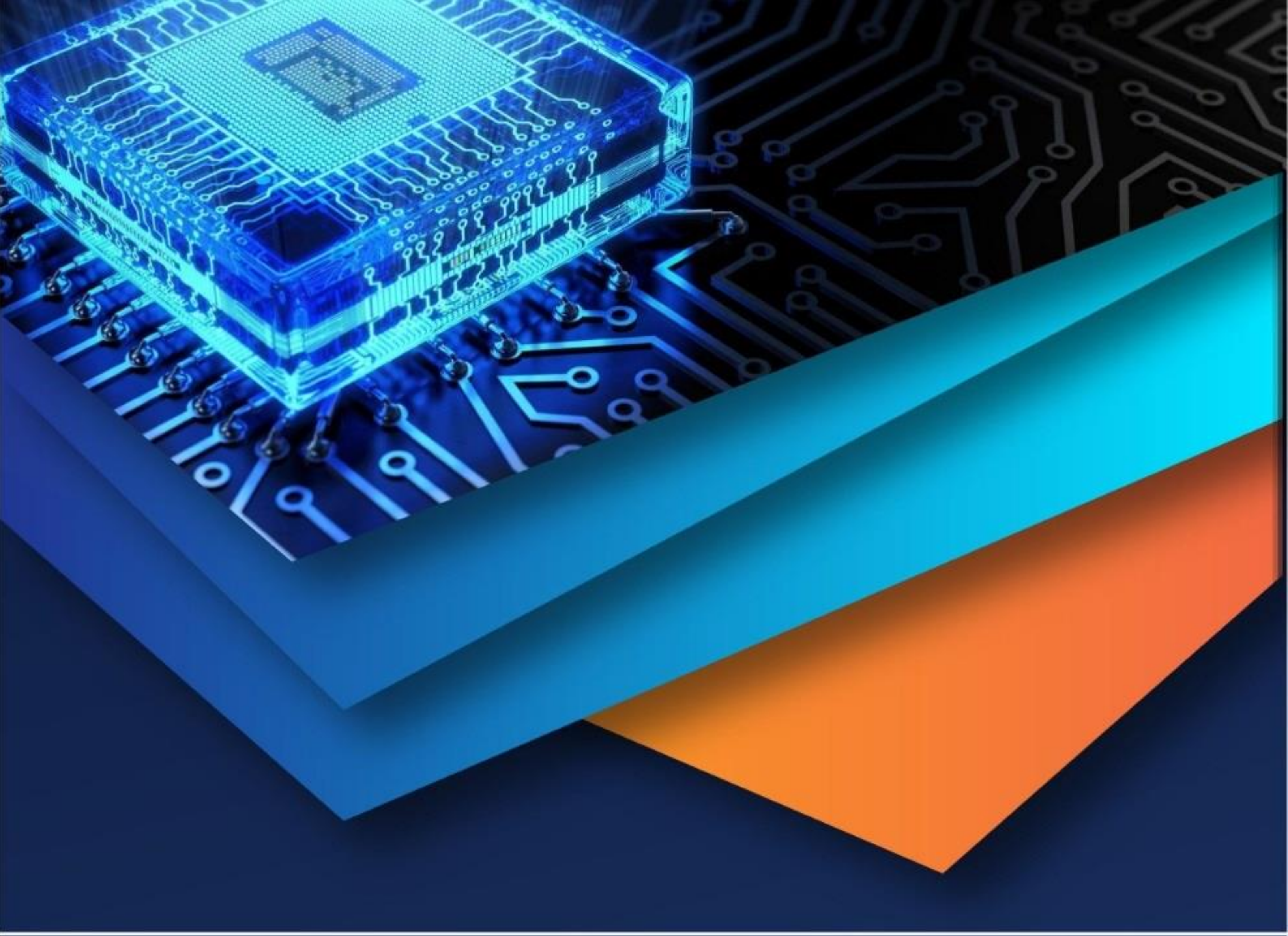
[1] Attaran and R. Rashidzadeh, "Chipless Radio Frequency Identification Tag for IoTApplications," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1310-1318, Dec.2016. Doi: 10.1109/JIOT.2016.2589928

[2] Y.Choi,Y.Choi, D.Kim and J.Park, “Scheme to guarantee IP continuity for NFC_based IOT networking ,” 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, 2017. pp.695-698. Doi:10.23919/ICACT.2017.7890182

[3] H. Saeed, A. Shouman, M. Elfar, M. Shabka, S. Majumdar and C. Horng-Lung,"Near-field communication sensors and cloud-based smart restaurant managementsystem," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA,2016, pp. 686-691.

[4] Y.Hong,Y.choi, M. Shin and J.Youn, “ Analysis of design space and use case in ipv6 over NFC for resource-conference on Information and communication Technology Convergence (ICTC), Jeju , 2015, pp.1009-1012.

[5] T.Ulz, T.Pieber, A. Holler, S. Haas and C. Ster, “ Secured and Easy-to-Use NFC- Based Device Configuration for the Internet of things ,” in EEE Journal of Radio Frequency Identication , vol.1,no.1, pp. 75-84, march 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY