ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 6, Issue 1 (Jan. - Mar. 2018)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2018)

Architecture, Technologies, Protocols, Applications, Security and Privacy of IOT

[I]S.Venkata Lakshmi, [II]N.Geetha, [III]B.Bharathi
[I,II,III]Asst. Professor, KMMITS, Tirupati, India

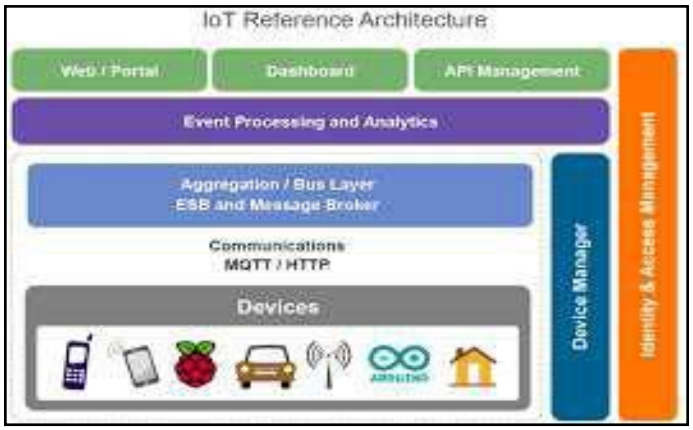
Abstract
The Internet of things is used for combining and covering the major aspects related to the extension of the Internet and Web into the phenomenon, by means of vast positioning of spatially distributed devices that contains embedded identification, sensing and/or actuation capabilities. Internet of Things (IoT) consists of a large number of connected objects that are communicating with each other. To discuss the Internet of things in wider sense and precedence on protocols, technologies, and application along with related issues. The main factor IoT concept is the integration of different technologies. The IoT is empowered by the hottest developments in smart sensors, communication technologies, and Internet protocols. Here we discuss IoT architecture and the technical aspect that relate to IoT. Then, give an overview of IoT technologies, protocols and applications and related issues with a comparison of other survey papers. Main enabling factor of this promising paradigm is the integration of several technologies and communication solutions. Identification and tracking technologies, wired and wireless sensor and activate networks, enhanced communication protocols and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.

Keywords
Internet of Things (IOT enabling technologies, security and privacy, and applications. IOT Architecture

I. Introduction

Nowadays, around two billion people around the world use the Internet for browsing the Web, sending and receiving emails, accessing multimedia content and services, playing games, using social networking applications and many other tasks. While more and more people will gain access to such a global information and communication infrastructure, another big leap forward is coming, related to the use of the Internet as a global platform for letting machines and smart objects communicate, dialogue, computer and coordinate. It is predictable that, within the next decade, the Internet will exist as a seamless fabric of classic networks and networked objects. Content and services will be all around us, always available, paving the way for new applications, enabling new ways of working; new ways of interacting; new ways of entertainment; new ways of living. In such a perspective, the conventional concept of the Internet as an infrastructure network reaching out to end-users terminals will fade, leaving space to a notion of interconnected ''smart'' objects forming pervasive computing environments. The term Internet of Things (IOT) has been known for last few years. In recent time, it's getting more attention due to the advancement of wireless technology. growing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea transportation, healthcare, industrial automation, and emergency response to natural and man-made disasters where human decision making is difficult. The IoT enables physical objects to see, hear, think and perform jobs by having them talk together, to share information and to coordinate decisions. The IoT transforms these objects from being traditional to smart by exploiting its underlying technologies such as ubiquitous and pervasive computing, embedded devices, communication technologies, sensor networks, Internet protocols and applications. A basic example of such objects includes thermostats and HVAC (Heating, Ventilation, and Air Conditioning) monitoring and control systems that enable smart homes. There are also other domains and environments in which the IoT can play a remarkable role and improve the quality of our lives. The IoT transforms these objects from being conventional to smart by manipulating its underlying technologies such as omnipresent and pervasive computing, embedded devices, communication technologies, sensor networks, protocols, and applications.

II. IOT Architecture



The Reference Model of IOT

In the vision of the Internet of Things, IoT-A wants to promote, a high level of interoperability needs to be reached at the communication level as well as at the service and the information level, going across different platforms, but established on a common grounding. The IoT-A project reckons that achieving those goals comes in two steps, first of all in establishing a common understanding of the IoT domain (hereafter called Reference Model), and second in providing to IoT system developers a common foundation for building interoperable IoT system Architectures (hereafter called Reference Architecture). A Reference Architecture (RA) can be

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

visualized as the "Matrix" that eventually gives birth ideally to all concrete architectures. For establishing such a Matrix, based on a strong and exhaustive analysis of the State of the Art, we need to envisage the superset of all possible functionalities, mechanisms and protocols that can be used for building such concrete architecture and to show how interconnections could take place between selected ones (as no concrete system is likely to use all of the functional possibilities). Giving such a foundation along with a set of design choices, based on the characterization of the targeted system w.r.t. various dimensions (like distribution, security, real-time, semantics,...) it becomes possible for a system architect to select the protocols, functional components, architectural options, ... needed to build their IoT systems.

The vision summarizes the rationale for providing an architectural reference model for the IoT. At the same time, it discusses underlying assumptions, such as motivations. It also discusses how the architectural reference model can be used, the methodology applied to the architecture modeling, and the business scenarios and stake-holders addressed. Business scenarios defined as requirements by stakeholders are the drivers of the architecture work.

Several trends have emerged over the past several years that are working together to shape the emerging IoT market:

- Rapid growth of data and analytics capabilities enabled by cloud computing
- Rapid growth in smart mobile devices
- Increasing interconnectivity between industrial, operational, and smart mobile devices
- Convergence of industrial and enterprise networks that enable applications such as video surveillance, smart meters, asset tracking, fleet management, digital health monitoring, and a host of other next-generation connected services.

III. Intigrate Technologies

Various technologies are involved implementing the idea of IOT. In this paper, we will focus on these. Radio frequency identification (RFID) Near Field Communication (NFC). Machine-to-Machine Communication (M2M)

A. Radio frequency identification (RFID) RFID system comprise of one or more readers and several RFID tags. It uses radio frequency electromagnetic fields to send data attached to it. 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 the line of sight comment RFID tag or label is very small microchip attached to an antenna in a compact package. The RFID tag comes in three configurations, Passive Reader Active Tag (PRAT), Active Reader Passive Tags (ARPT) and Active Reader Active Tag (ARAT). In ARAT, the reader is passive and receives the signal from the battery operated tag and its transmission range is from 1-2000 feet depends upon architecture. Secondly, most commonly used configuration, ARPT does not have onboard supplies, so it consumes the energy required to send data from the query signal sent by the RFID reader . The last one, ARAT have both the reader and tags active, and tags only awoke by the reader when it comes under the domain of reader.

B. Near Field Communication It is similar to RFID configuration. NFC can be made customer-oriented by integration of RFID reader into mobile phones. In addition, it is the type of radio communication between NFC mobile devices by connecting them together in the domain of another phone. It is short range, low power Smart Grid Application Bandwidth Latency Substation Automation 9.6-56 kbps 15-200 ms WASA 600 – 1500 kbps 15-200 ms Outage Management 56 kbps 2000 ms Distribution Automation 9.6-100 kbps 100 ms-2 sec Distributed Energy Resources 9.6-100 kbps 100 ms-2 sec Smart Meter Reading 10-100 kbps/meter 500 kbps/ concentrator 2000 ms Demand Response 14 – 100 kbps 500 ms/min Demand Side Management 14 – 100 kbps 500 ms/min Assets Management 56 kbps 2000 ms 382 wireless link that can send small amounts of data between two devices within the range of lying in the specific domain . NFC operates within the unlicensed Radio Frequency band of 13.56MHz. The typical range of NFC is 20m and mostly it depends on the size of the antenna in the device. The NFC technology can play a significant role in the future progress of IoT. It will enable to provide necessary tool to be wirelessly connected to other smart objects.

C. **Machine to Machine (M2M):**t refers to the communications between computers, embedded processors, smart sensors, actuators and mobile devices. This sort of communication is increasing these days. There are four components of M2M, that are sensing, heterogeneous access, information processing and applications & processing. In actual, M2M is a five-part structure that is as followsM2M Device: A device capable of replying to request for data contained within that device [16]. M2M Area Network (Device Domain): Provide connectivity between M2M Devices and M2M Gateways. M2M Gateway: Use M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network. M2M Communication Networks (Network Domain): Communications between the M2M Gateway(s) and M2M application. M2M Applications: Contains the middleware layer where data goes through various application services and is used by the specific business processing engines. M2M Applications: Contains the middleware layer where data goes through various application services and is used by the specific business processing engines. It has applications in different sectors like healthcare, smart robots, cyber transportation systems (CTS), manufacturing systems, smart home technologies, and smart grids.

IV. Applications

Applications of IoT are very diversified. Applications of IoT are increasing every day in many domains. Every day individual / industrial changes our needs and as per need, we use the Internet and hence Internet-of-Things. There are plenty of applications of IOT. In coming years, IOT will be more revolutionized because of the RFID, NFC, M2M and V2V communications.

A. Radio frequency Identification (RFID)

1) Smart parking

In recent time, smart parking sensors are attached in parking space to detect the arrival and departure of vehicles. It provides an efficient management solution which helps motorist to save time and fuel. It provides motorists with accurate information about parking spaces and keeps the traffic system smooth. It also enables the facility of deployment to book parking space directly from

the vehicle. It can also help to reduce CO2 emission and lessen the traffic jams .

2) Augments maps

Tourists augmented maps with tags allow NFC tag would enable the phones to search the information about places by connecting to web service. By this one will be able to search required information about hotels, restaurants, monuments, theater and the local attractions. This can be by hovering your mobile phone over the tag within its reading range so that the additional information about the marker can be displayed on the screen.

3) Logistics

By implementing IoT in retail chain monitoring has many advantages: RFIC and NFIC can be used to monitor every detail such as commodity details, purchasing of raw materials, production and sales of the product after sale service. With the help of IoT, one can track the inventory in the warehouse so that one can have information about stock, customer's satisfaction etc. and result in increased sales .

4) Data collection

If doctor becomes enable of having collection and transfer of data then it would help in reducing them, minimizing the data collection error, automated care, and routine auditing. It will also enable to transfer the previous health record of patients, which would result in an accuracy of the medication given by doctor.

5) Smart water supply

Wireless network system will enable to monitor the water supply and will help to ensure that there is the adequate water supply for the resident and business use. It will also help to discover if there is any water loss. In this way, water leakage problem would be discovered and help in water saving. Tokyo, for example, has calculated they save $170 million each year by detecting water leakage problems early . The system can report pipe flow measurement data regularly, as well as send automatic alerts if water use is outside of an estimated normal range. This allows a smart city to determine the location of leaking pipes and prioritize repairs based on the amount of water loss that could be prevented.383

6) Smart homes and offices

In recent time, human life is surrounded by thousands of electronic gadgets like microwave evens, refrigerators, heaters, air conditioners, fan, and lights.

V. Protocols

The Internet revolutionized how people communicate and work together. It ushered in a new era of free information for everyone, transforming life in ways that were hard to imagine in its early stages. But the next wave of the Internet is not about people. It's about intelligent, connected devices.

To interact successfully with the real world, these devices must work together with speeds, scales, and capabilities far beyond what people need or use. The Internet of Things (IoT) will change the world, perhaps more profoundly than today's human-centric Internet.

Protocol Overview

Devices must communicate with each other (D2D). Device data then must be collected and sent to the server infrastructure (D2S).

That server infrastructure has to share device data (S2S), possibly providing it back to devices, to analysis programs, or to people.

From 30,000 feet, the protocols can be described in this framework as:

MQTT: a protocol for collecting device data and communicating it to servers (D2S).

XMPP: a protocol best for connecting devices to people, a special case of the D2S pattern, since people are connected to the servers.

DDS: a fast bus for integrating intelligent machines (D2D).

AMQP: a queuing system designed to connect servers to each other (S2S).

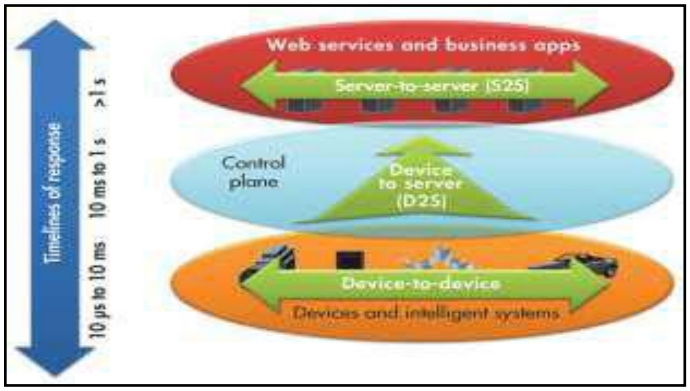


Fig. 2 : IOT Protocols Need to Address Response Time.

MQTT:

MQTT, the Message Queue Telemetry Transport, targets device data collection (Fig. 3). As its name states, its main purpose is telemetry or remote monitoring. Its goal is to collect data from many devices and transport that data to the IT infrastructure. It targets large networks of small devices that need to be monitored or controlled from the cloud.

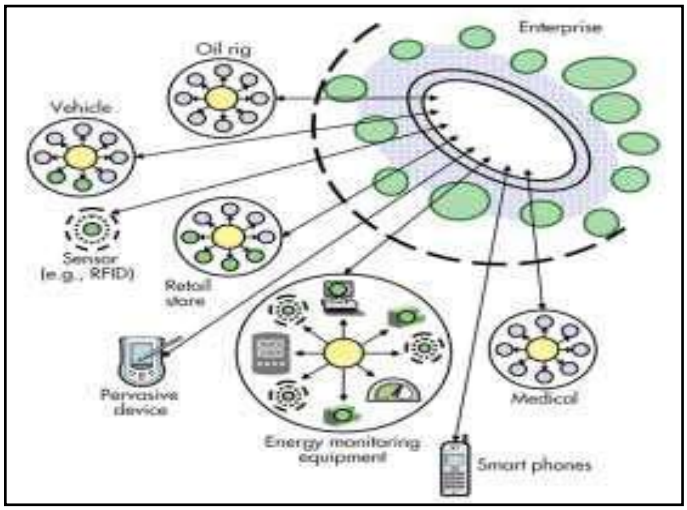


Fig. 3 : Message Queue Telemetry Transport (MQTT) implements a hub-and-spoke system

MQTT enables applications like monitoring a huge oil pipeline for leaks or vandalism. Those thousands of sensors must be concentrated into a single location for analysis. When the system finds a problem, it can take action to correct that problem. Other applications for MQTT include power usage monitoring, lighting

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

control, and even intelligent gardening. They share a need for collecting data from many sources and making it available to the IT infrastructure.

XMPP

XMPP was originally called "Jabber." It was developed for instant messaging (IM) to connect people to other people via text messages *(Fig. 4)*. XMPP stands for Extensible Messaging and Presence Protocol. Again, the name belies the targeted use: presence, meaning people are intimately involved.

VI. IOT Elements

Understanding the IoT building blocks helps to gain a better insight into the real meaning and functionality of the IoT. In the following sections we discuss six main elements needed to deliver the functionality of the IoT as illustrated in Fig. 4. Table II shows the categories of these elements and examples of each category.

A. Identification

Identification is crucial for the IoT to name and match services with their demand. Many identification methods are available for the IoT such as electronic product codes (EPC) and ubiquitous codes (uCode) . Furthermore, addressing the IoT objects is critical to differentiate between object ID and its address. Object ID refers to its name such as ―T1 for a particular temperature sensor and object's address refers to its address within a communications network. In addition, addressing methods of IoT objects include IPv6 and IPv4. 6LoWPAN provides a compression mechanism over IPv6 headers that make IPv6 addressing appropriate for low power wireless networks. Distinguishing between object's identification and address is imperative since identification methods are not globally unique, so addressing assists to uniquely identify objects. In addition, objects within the network might use public IPs and not private ones. Identification methods are used to provide a clear identity for each object within the network.

B. Sensing

The IoT sensing means gathering data from related objects within the network and sending it back to a data warehouse, database, or cloud. The collected data is analyzed to take specific actions based on required services. The IoT sensors can be smart sensors, actuators or wearable sensing devices. For example, companies like Wemo, revolve and Smart Things offer smart hubs and mobile applications that enable people to monitor and control thousands of smart devices and appliances inside buildings using their smart phones.

Single Board Computers (SBCs) integrated with sensors and built-in TCP/IP and security functionalities are typically used to realize IoT products (e.g., Arduino Yun, Raspberry PI, Beagle Bone Black, etc.). Such devices typically connect to a central management portal to provide the required data by customers.

C. Communication

The IoT communication technologies connect heterogeneous objects together to deliver specific smart services. Typically, the IoT nodes should operate using low power in the presence of lossy and noisy communication links. Examples of communication protocols used for the IoT are WiFi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-Advanced. Some specific communication technologies are also in use like RFID, Near Field Communication (NFC) and *ultra-wide bandwidth* (UWB). RFID is the first technology used to realize the M2M concept (RFID tag and reader). The RFID tag represents a simple chip or label attached to provide object's identity. The RFID reader transmits a query signal to the tag and receives reflected signal from the tag, which in turn is passed to the database. The database connects to a processing center to identify objects based on the reflected signals within a (10 cm to 200 m) range . RFID tags can be active, passive or semi-passive/ active. Active tags are powered by battery while passive ones do not need battery. Semi-passive/active tags use board power when needed.

The NFC protocol works at high frequency band at 13.56 MHz and supports data rate up to 424 kbps. The applicable range is up to 10 cm where communication between active readers and passive tags or two active readers can occur .The UWB communication technology is designed to support communications within a low range coverage area using low energy and high bandwidth whose applications to connect sensors have been increased recently .

Another communication technology is WiFi that uses radio waves to exchange data amongst things within 100 m range WiFi allows smart devices to communicate and exchange information without using a router in some *ad hoc* configurations. Bluetooth presents a communication technology that is used to exchange data between devices over short distances using short-wavelength radio to minimize power consumption. Recently, the Bluetooth *special interest group* (SIG) produced Bluetooth 4.1 that provides Bluetooth Low Energy as well as high-speed and IP connectivity to support IoT . The IEEE 802.15.4 standard specifies both a physical layer and a medium access control for low power wireless networks targeting reliable and scalable communications.

LTE (Long-Term Evolution) is originally a standard wireless communication for high-speed data transfer between mobile phones based on GSM/UMTS network technologies. It can cover fast-travelling devices and provide multicasting and broadcasting services. LTE-A (LTE Advanced) [35] is an improved version of LTE including bandwidth extension which supports up to 100 MHz, downlink and uplink spatial multiplexing, extended coverage, higher throughput and lower latencies.

D. Computation

Processing units (e.g., microcontrollers, microprocessors, SOCs, FPGAs) and software applications represent the brain and the computational ability of the IoT. Various hardware platforms were developed to run IoT applications such as Arduino, UDOO, FriendlyARM, Intel Galileo, Raspberry PI, Gadgeteer, BeagleBone, Cubieboard, Z1, WiSense, Mulle, and T-Mote Sky.

Furthermore, many software platforms are utilized to provide IoT functionalities. Among these platforms, Operating Systems (RTOS) are vital since they run for the whole activation time of a device. There are several Real-Time Operating Systems (RTOS) that are good candidates for the development of RTOS-based IoT applications. For instance, the Contiki RTOS has been used widely in IoT scenarios. Contiki has a simulator called Cooja which allows researcher and developers to simulate and emulate IoT and wireless sensor network (WSN) applications [36]. TinyOS, LiteOS

Fig. 2: The IOT elements

and Riot OS also offer light weight OS designed for IoT environments. Moreover, some auto industry leaders with Google established the Open Auto Alliance (OAA) and are planning to bring new features to the Android platform to accelerate the adoption of the Internet of Vehicles (IoV) paradigm . Some features of these operating systems are compared in Table I.

TABLE 1 : COMMON OPERATING SYSTEMS USED IN IOT ENVIRONMENTS

Operating System	Language	Support	Minimum Memory (KB)	Event-based Programming	Multi-threading	Dynamic Memory
TinyOS	nesC		1	Yes	Partial	Yes
Contiki	C		2	Yes	Yes	Yes
LiteOS	C		4	Yes	Yes	Yes
Riot OS	C/C++		1.5	No	Yes	Yes
Android	Java		-	Yes	Yes	Yes

Cloud Platforms form another important computational part of the IoT. These platforms provide facilities for smart objects to send their data to the cloud, for big data to be processed in real-time, and eventually for end-users to benefit from the knowledge extracted from the collected big data. There are a lot of free and commercial cloud platforms and frameworks available to host IoT services

E. Services

Overall, IoT services can be categorized under four classes : Identity-related Services, Information Aggregation Services, Collaborative-Aware Services and Ubiquitous Services. Identity-related services are the most basic and important services that are used in other types of services. Every application that needs to bring real world objects to the virtual world has to identify those objects.

Information Aggregation Services collect and summarize raw sensory measurements that need to be processed and reported to the IoT application. Collaborative-Aware Services act on top of Information Aggregation Services and use the obtained data to make decision and react accordingly. Ubiquitous Services, however, aim to provide Collaborative-Aware Services *anytime* they are needed to *anyone* who needs them *anywhere*. With this categorization, we review some applications of the IoT in the following paragraphs. The ultimate goal of all IoT applications is to reach the level of ubiquitous services. However, this end is not achievable easily since there are a lot of difficulties and challenges that have to be addressed. Most of the existing applications provide identity-related, information aggregation, and collaborative-aware services. Smart healthcare and smart grids fall into the information aggregation category and smart home, smart buildings, intelligent transportation systems (ITS), and industrial automation are closer to the collaborative-aware category.

Smart home [43] IoT services contribute to enhancing the personal life-style by making it easier and more convenient to monitor and operate home appliances and systems (e.g., air conditioner, heating systems, energy consumption meters, etc.) remotely. For example, a smart home can automatically close the windows and lower the blinds of upstairs windows based on the weather forecast. Smart homes are required to have regular interaction with their internal and external environments . The internal environment may include all the home appliances and devices that are Internet-connected while the external environment consists of entities that are not in control of the smart home such as smart grid entities.

Smart buildings connect *building automation systems* (BAS) to the Internet . BAS allows to control and manage different building devices using sensors and actuators such as HVAC, lighting and shading, security, safety, entertainment, etc. Furthermore, BAS can help to enhance energy consumption and maintenance of buildings. For example, a blinking dishwasher or cooling/heating system can provide indications when there is a problem that needs to be checked and solved. Thus, maintenance requests can be sent out to a contracted company without any human intervention.

Intelligent transportation systems (ITS) or *Transportation Cyber-Physical Systems* (T-CPS) represent integration between computation and communication to monitor and control the transportation network. ITS aims to achieve better reliability, efficiency, availability and safety of the transportation infrastructure. ITS employs four main components, namely: vehicle subsystem (consists of GPS, RFID reader, OBU, and communication), station subsystem (road-side equipment), ITS monitoring center and security subsystem. Moreover, connected vehicles are becoming more important with the aim to make driving more reliable, enjoyable and efficient [48, 49]. For instance, Audi became the first automaker with a license for self-driving in Nevada. Google is another pioneer in this area . Also, in December 2013, Volvo announced its self-driving car to drive

Smart healthcare plays a significant role in healthcare applications through embedding sensors and actuators in patients and their medicine for monitoring and tracking purposes. The IoT is used by clinical care to monitor physiological statuses of patients through sensors by collecting and analyzing their information and then sending analyzed patient‘s data remotely to processing centers to make suitable actions. For example, Masimo Radical-7 monitors the patient‘s status remotely and reports that to a clinical staff. Recently, IBM utilized RFID technology at one of OhioHealth’s hospitals to track hand washing after checking each patient [56-58]. That operation could be used to avoid infections that cause about 90,000 deaths and losing about $30 billion annually.

Smart grids utilize the IoT to improve and enhance the energy consumption of houses and buildings. Employing the IoT in smart grids helps power suppliers to control and manage resources to provide power proportionally to the population increase. For example, smart grids use the IoT to connect millions or billions of buildings‘ meters to the network of energy providers. These meters are used to collect, analyze, control, monitor, and manage energy consumption. The IoT enables energy providers to improve their services to meet consumers‘needs. Also, utilizing the IoT in the smart grid reduces the potential failures, increases efficiency

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

and improves quality of services.
smart city which could be seen as an application of ubiquitous services, aims to improve the quality of life in the city by making it easier and more convenient for the residents to find information of interest . In a smart city environment, various systems based on smart technologies are interconnected to provide required services (health, utilities, transportation, government, homes and buildings).

F. Semantics

Semantic in the IoT refers to the ability to extract knowledge smartly by different machines to provide the required services. Knowledge extraction includes discovering and using resources and modeling information. Also, it includes recognizing and analyzing data to make sense of the right decision to provide the exact service . Thus, semantic represents the brain of the IoT by sending demands to the right resource. This requirement is supported by Semantic Web technologies such as the Resource Description Framework (RDF) and the Web Ontology Language (OWL). In 2011, the *World Wide Web consortium* (W3C) adopted the *Efficient XML Interchange* (EXI) format as a recommendation.

VII. Building Blocks and Technologies of The IOT

IoT Elements		Samples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, , LTE-A
Computation	Hardware	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, Smart Phones
	Software	OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc.)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)
Semantic		RDF, OWL, EXI

VIII. Security and Privacy

A. Security Features of IoT

I. *Confidentiality*: Confidentiality can ensure that the data is only available to authorized users throughout the process, and cannot be eavesdropped or interfered by non-authorized users. In IoT, confidentiality is an important security principle, because a large number of measurement devices (RFID, sensors, etc.) can integrated in IoT. Thus, it is critical to ensure that the data collected by a measurement device will not reveal secure information to its neighboring devices. To achieve great confidentiality, enhanced techniques, including secure key management mechanisms, and others should be developed and used .

II. *Integrity*: Integrity can ensure that the data cannot be tampered by intended or un-intended interference during the data delivery in communication networks, ultimately providing the accurate data for authorized users. Integrity is important for IoT, because if IoT applications receive forged data or tampered data, erroneous operation status can be estimated and wrong feedback commands can be made, which could further disrupt the operation of IoT applications. To achieve acceptable integrity, enhanced secure data integrity mechanisms (false data filtering schemes, etc.) should be developed and applied .

III. *Availability*: Availability can ensure that the data and devices are available for authorized users and services when-ever the data and devices are requested. In IoT, services are commonly requested in real-time fashion, and services cannot be scheduled and provided if the requested data cannot be delivered in a timely manner. Thus, availability is also an important security principle. One of the most serious threats to availability is the denial-of-service (DoS) attack, and enhanced techniques (secure and efficient routing protocols, etc.) should be studied and applied to ensure availability in IoT .

IV. Identification and Authentication: Identification can ensure that non-authorized devices or applications cannot be connected to IoT, and authentication can ensure that the data delivered in networks are legitimate, and the devices or applications that request the data are legitimate as well. In IoT, identifying and authenticating each data and object is difficult, because a large number of diverse objects comprise an IoT. Thus, designing efficient mechanisms to deal with the authentication of objects or things is critical in IoT .

V. *Privacy*: Privacy can ensure that the data can only be controlled by the corresponding user, and that no other user can access or process the data. Unlike confidentiality, which aims to encrypt the data without being eavesdropped and interfered by non-authorized users, privacy ensures that the user can only have some specific controls based on received data and cannot infer other valuable information from the received data. Privacy is considered as one of important security principles due to a large number of devices, services, and people sharing the same communication network in IoT.

VI. *Trust*: Trust can ensure the aforementioned security and privacy objectives to be achieved during the interactions among different objects, different IoT layers, and different applications. The objectives of trust in IoT can be divided as trust between each IoT layer, trust between devices, and trust between devices and applications. With trust, security and privacy can be enforced. Trust management systems should be designed to implement these trust objectives in IoT.

B. Security

In this section, security challenges in each layer of IoT architecture are presented in detail. In SoA based IoT, he service layer is established via extracting the functionality of data services in the network layer and the application layer. Thus, security challenges in the service layer can be attributed to challenges in the network and the application layers. In the following, only security challenges in the perception layer, the network layer, and the application layer are presented.

Perception Layer: As the main purpose of the perception layer in IoT is to collect data, the security challenges in this layer focus on forging collected data and destroying perception devices, which are presented below.

(i) Node Capture Attacks: In a node capture attack, the adversary can capture and control the node or device in IoT via physically replacing the entire node, or tampering with the hardware of the node or device. If a node is compromised by the node capture attack, the important information (group communication key, radio key, matching key, etc.) can be exposed to the adversary. The adversary can also copy the important information associated with the captured node to a malicious node, and then fake the malicious node as an authorized node to connect to the IoT network or system. This attack is denoted as the node replication attack. A node capture attack can incur a serious impact on the network. To defend against the node capture attack, effective schemes to monitor and detect malicious nodes need to be studied.

(ii) Malicious code Injection Attacks: In addition to the node capture attack, the adversary can control a node or a device in IoT by injecting malicious code into the memory of the node or device, which is denoted as the malicious code injection attack . The injected malicious code not only can perform specific functions, but can also grant the adversary access into the IoT system, and even gain the full control of the IoT system. To defend against the malicious code injection attack, effective code authentication schemes need to be designed and integrated into IoT .

(iii) False Data Injection Attacks: With the captured node or device in IoT, the adversary can inject false data in place of normal data measured by the captured node or device, and transmit the false data to IoT applications. After receiving the false data, IoT applications can return erroneous feedback commands or provide wrong services, which further affect the effectiveness of IoT applications and networks. To defend against such a malicious attack, techniques (false data filtering schemes, etc.), which can efficiently detect and drop the false data before the data is received by the IoT applications, need to be designed.

(iv) Replay Attacks (or Freshness Attacks): In IoT, the adversary can use a malicious node or device to transmit to the destination host with legitimate identification information, which has been received by the destination host.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final make the malicious node or device obtain the trust of IoT .Replay attack is commonly launched in authentication process to destroy the validity of certification. To mitigate the replay attack, techniques (secure time stamp schemes, etc.) should be designed and developed in IoT .

(v) *Cryptanalysis Attacks and Side Channel Attacks*: A cryptanalysis attack can use the obtained cipher text or plaintext to infer the encryption key being used in the encryption algorithm [158]. Nonetheless, the efficiency of cryptanalysis attack is low. To improve the efficiency, new attacks, namely the side channel attacks, can be introduced by the adversary. For example, in the side channel attack investigated in IoT the adversary could deploy some techniques on the encryption devices in IoT to obtain the encryption key, which is used in IoT for encrypting data and decrypting data. One of the typical side channel attacks is the timing attack, in which the adversary can obtain the encryption key by analyzing the time information required to execute the encryption algorithm. To mitigate the side channel attack, efficient and secure encryption algorithms and key management schemes need to be developed in IoT

(vi) Eavesdropping and Interference: Because most of devices in IoT will communicate via wireless networks, vulnerability lies in the fact that information delivered in wireless links can be eavesdropped by non-authorized users. To deal with eavesdropping, secure encryption algorithms and key management schemes are required. The adversary can also send noise data or signal to interfere with the information delivered in wireless links. To ensure the accuracy and timely delivery of data, effective secure noise filtering schemes are required to filter the noise data and restore original data .

(vii) Sleep Deprivation Attacks: In IoT, most devices or nodes have low power ability. To extend the life cycle of the devices and nodes, devices or nodes are programmed to follow a sleep routine to reduce the power consumption .Nonetheless, the sleep deprivation attack can break the programmed sleep routines and keep device or nodes awake all the time until they are shut down. To extend the life cycle of these devices and nodes, the energy harvest scheme can be one possible solution, in which devices and nodes can harvest energy from the external environment. In addition, other techniques, like secured duty-cycle mechanism to mitigate the sleep deprivation attack, need to be studied in IoT.

2) Network Layer: As the main purpose of the network layer in IoT is to transmit collected data, the security challenges in this layer focus on the impact of the availability of network resources. Also, most devices in IoT are connected into IoT networks via wireless communication links. Thus, most security challenges in this layer are related to wireless networks in IoT.

(i) Denial-of-Service (DoS) Attacks: DoS attacks can consume all of the available resources in IoT by attacking network protocols or bombarding the IoT network with massive traffic, rendering the services of IoT systems unavailable. The DoS attack is considered to be one of the most common attacks, and represents an attack category, which can result in the services of IoT systems being unavailable. Thus, DoS attacks can be generated by attack schemes, including Ping of Death, TearDrop, UDP flood, SYN flood, Land Attack, etc.. To defend against DoS attacks, attacking schemes need to be carefully investigated first, and then the efficient defensive schemes to mitigate attacks need be developed to secure IoT systems.

(ii) Spoofing Attacks: The purpose of spoofing attacks is for the adversary to gain full access to the IoT system, and send malicious data into the system. In IoT, examples of spoofing attacks include IP spoofing RFID spoofing etc. In an IP

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

spoofing attack, the adversary can spoof and record the valid IP address of other authorized devices in the IoT, and then access the IoT system to send malicious data with the obtained valid IP address, making malicious data appear to be valid. In a RFID spoofing attack, the adversary can spoof and record the information of a valid RFID tag, and then send malicious data with this valid tag ID to the IoT system. Secure trust management, identification and authentication can be possible solutions to defend against the spoofing attack .

Sinkhole Attacks: In a sinkhole attack, a compromised device or node claims exceptional capabilities of power, computation, and communication, such that more neighboring devices or nodes will select the compromised device or node as the forwarding node in data routing process because of the appealing capabilities. By doing this, the compromised device or node can increase the amount of data obtained before its delivered in the IoT system. Notice that a sinkhole attack not only can break the confidentiality of delivered data, but also can be a fundamental step to launch additional attacks (DoS attack, etc.). To defend against the sinkhole attack, techniques such as secure multiple routing protocols need to be studied and applied .

(iii) *Wormhole Attacks*: Wormhole attack can be launched by two cooperative malicious devices or nodes in IoT, in which the two malicious devices in different locations can exchange routing information with private links to achieve a false one-hop transmission between them, even if they are located far away from each other . In a wormhole attack, because the forwarding hops are reduced, more data will be delivered through these two malicious devices or nodes. With access to more delivereddata, the wormhole attack can lead to the similar damage as sinkhole attack. To defend against wormhole attack, there are some possible defensive techniques. One technique is to modify the routing protocols to enhance the security in the route selection process , while other techniques involve deploying secure hardware (GPS, directed antenna, etc.).

(iv) *Man in the Middle Attack*: In a man in the middle attack, a malicious device controlled by the adversary can be virtually located between two communicating devices in IoT . By stealing the identify information of the two normal devices, the malicious device can be a middle device to store and forward all data, which is communicated between these two normal devices, while the two normal devices cannot detect the existence of the malicious device, and instead believe that they directly communicate with each other. The man in the middle attack can violate the confidentiality, integrity, and privacy of restricted data in IoT through monitoring, eavesdropping, tampering and controlling the communication between the two normal devices. Unlike malicious node capture attacks that need to physically tamper with the hardware of devices, the man in middle attack can be launched by only relying on the communication protocols used in IoT networks. Se-cure communication protocols and key management schemes, which can ensure the identify and key information of normal devices not be leaked to the adversary, can be efficient defense techniques to protect against the attack .

(v) *Routing Information Attacks*: Routing information attacks focus on the routing protocols in IoT systems, in which the routing information can be manipulated and resent by the adversary to create route loops in the data transmission of the network, leading to the extension of source paths and the increase of end-to-end delay in IoT networks . To defend against the routing information attack, secure routing protocols and trust. management to establish secure links among devices in IoT and ensure the identifying information and IP addresses not to be leaked to the adversary are possible techniques to be used.

(vi) *Sybil Attacks*: In a sybil attack, a malicious device, namely a sybil device, can claim several legitimate identities and impersonate them in IoT systems . Be-cause a sybil device has several legitimate identities, false data sent by the sybil device can be easily accepted by their benign neighboring devices. Also, routes that select sybil devices as forwarding nodes may consider that several different intersected paths are determined, but, in fact only one path is determined and all transmitted data needs to go through the sybil device, in which jamming and DoS can be used. To defend against sybil attacks, secure identification and authentication mechanisms need to be developed for IoT systems .

(vii) *Unauthorized Access*: RFID is an important enabling technology in IoT. Nonetheless, as a large number of RFID-based devices are integrated in IoT, and most of the RFID tags lack proper authentication mechanisms, RFID tags can be accessed and the information stored in tags can be obtained, modified, and deleted by the adversary . Thus, authorization access and authentication mechanisms for RFID-based devices in IoT is a challenge in need of further development .

3) *Application Layer:* The main purpose of the application layer is to support services requested by users. Thus, challenges in the application layer focus on the software attacks. Here, several possible challenges in the application layer of IoT are presented below.

i) *Phishing Attack*: In phishing attacks, the adversary can obtain the confidential data of users, such as identification and passwords, by spoofing the authentication credentials of users via the infected e-mails and phishing websites. Secure authorization access, and identification and authentication can mitigate phishing attacks. Nonetheless, the most efficient way is for users themselves to always be vigilant while surfing online. This becomes an issue as most of devices in IoT are machines, which may lack of such intelligence.

ii) *Malicious Virus/worm*: A malicious virus/worm is another challenges to IoT applications . The adversary can infect the IoT applications with alicious self-propagation attacks (worms, Trojan Horse, etc.), and then obtain or tamper with confidential data. Reliable firewall, virus detection, and other defensive mechanisms need to be deployed to combat malicious virus/worm attacks in IoT applications .

Malicious Scripts: Malicious scripts represent the scripts that are added to software, modified in software, and deleted from software with the purpose of harming the system functions of IoT . Because all IoT applications are connected to the Internet, the adversary can easily fool the customers in running malicious scripts (java attack applets, active-x scripts, etc.) when requesting services through the Internet. Malicious scripts can pose the leakage of confidential data and even a complete system shut down. To defend against malicious scripts, effective script detection techniques, including honey

pot techniques, static code detection, and dynamic action detection, need to be deployed in IoT systems.

C. Privacy

In general, all of the massive data collected and used in IoT should go through the following three steps: (i) data collection, (ii) data aggregation and (iii) data mining and analytics . Particularly, data collection is enacted to sense and collect the status data of objects in IoT, data aggregation integrates an amount of related data into a comprehensive information, and data mining and analytics extract the potential value of integrated comprehensive information for special applications in IoT . Although data collection, data aggregation, and data mining and analytics can provide a number of services to our daily lives, the privacy issues of the data in these steps are raised in IoT as well. Privacy, as a new challenge in IoT, can lead to property loss, and even compromise human safety . For example, in the smart grid, if the adversary obtains the private data of the energy consumption of customers, he or she can infer the time when users are in the home or out of home, and conduct theft or other damage to users with a probability. Thus, privacy-preserving mechanisms need to be developed to ensure private data not to be leaked to the adversary in IoT.

Based on different data processing steps, privacy-preserving mechanisms can be divided into three categories: (i) privacy preservation in data collection , (ii) privacy preservation in data aggregation, and (iii) privacy preservation in data mining and analytics . As the privacy in data collection, data mining, and data analytics can be greatly preserved by various techniques (encryption, key management, etc.), a majority of the existing efforts on privacy preservation in IoT focus on data privacy in data aggregation.

In data aggregation, the relevant data could be processed in several different locations, and thus it is difficult to achieve privacy preservation through traditional encryption mechanisms. Thus, several privacy-preserving mechanisms have been developed that focused on data aggregation, and can be divided into the following categories: (i) anonymity-based privacy preservation , (ii) encryption-based privacy preservation , and (iii) perturbation-based privacy preservation. Particularly, in anonymity-based privacy preservation, several related anonymity tech-niques (K-anonymity, L-diversity, T-closeness, etc.) were used in the data aggregation process to preserve the privacy of identification information . In addition, traffic analysis techniques could affect anonymous communication systems .In encryption-based privacy preservation, several encryption techniques (homomorphism encryption, commitment mechanism, secret sharing, zero-knowledge proof, etc.) were used in the data aggregation to ensure data not to be eavesdropped by adversaries [39]. Nonetheless, existing encryption techniques can only achieve the confidentiality on data transmission and may not work well on privacy preservation. In perturbation-based privacy preservation, perturbation-based techniques (data customization, data sharing, random noise injection, etc.) were used in data aggregation to perturb raw data, achieving privacy preservation [48], however, the utilization of data could hinder the application of this technique in the IoT.

Due to the great performance by directly operating on raw data, perturbation-based privacy preserving schemes are highly popular techniques used in IoT. Nonetheless, most of perturbation-based privacy preserving achieves great performance via reducing the utility of the data. With low utility, data may not, or may only partially, support services requested by IoT applications. Thus, the design of privacy preserving schemes with great data utility remains great challenges on data privacy preservation in IoT for future research.

IX. Conclusion

A comprehensive review of IoT has been presented, including architectures, enabling technologies, and security and privacy issues, as well as the integration of fog/edge computing and IoT to support diverse applications. Particularly, the relationship and difference between IoT and CPS has been clarified at the outset. Possible architectures for IoT have been discussed, including the traditional three-layer architecture and the SoA-based four-layer architecture. Based on the SoA based IoT architecture, enabling technologies in layers (perception layer, network layer, and service layer) have been detailed, respectively. In addition, to secure IoT, potential security and privacy issues that could affect the effectiveness of IoT, and their potential solutions, have been presented. To investigate the fog/edge computing-based IoT, the relationship between IoT and fog/edge computing and related issues have been discussed. Furthermore, several applications, including the smart grid, smart transportation, and smart cities, are presented to show how fog/edge computing-based IoT to be implemented in real-world applications. The main purpose of this survey is to provide a clear, comprehensive, and deep understanding of IoT and its integration with fog/edge computing, outlining the breadth of topics that IoT entails, and highlighting areas that remain unresolved, in an effort to further promote the development of IoT.

References

[1]. D. Evans, "The internet of things: How the next evolution of the internet is changing everything," CISCO White Paper, 2011.

[2]. L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

[3]. R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference On, 2012, pp. 257-260.

[4]. J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Comput. Syst., vol. 29, pp. 1645-1660, 2013.

[5]. P. Lopez, D. Fernandez, A. J. Jara and A. F. Skarmeta, "Survey of internet of things technologies for clinical environments," in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference On, 2013, pp. 1349-1354.

[6]. D. Yang, F. Liu and Y. Liang, "A survey of the internet of things," in Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010), 2010, pp. 358-366.

[7]. Fosstrak: open source rfid software platform. Avaliable : https:// fosstrak.github.io/ . Google self-driving car. In http:// www.google.com/ selfdrivingcar/ how/ .

[8]. Ieee standard for local and metropolitan area networks: Overview and architecture. IEEE Std 802-2001 (Revision of IEEE Std 802-1990), pages 1–48, February 2002.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[9]. S. H. Ahmed, G. Kim, and D. Kim. Cyber physical system: Archi-tecture, applications and research challenges. In Proc. of 2013 IFIP Wireless Days (WD), November 2013.

[10]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4):2347–2376, Fourthquarter 2