The Internet of Things (IoT) Needs to Become a Reality in IT world

Dr .I.Lakshmi
Assistant Profsssor, Department of Computer Science,
Stella Maris College, Chennai-600086.

Abstract
We're entering another period of registering innovation that many are calling the Internet of Things (IoT). Machine to machine, machine to framework, machine to condition, the Internet of Everything, the Internet of Intelligent Things, keen frameworks—call it what you need, yet it's going on, and its potential is gigantic. We see the IoT as billions of savvy, associated "things" (a kind of "general worldwide neural system" in the cloud) that will envelop each part of our lives, and its establishment is the insight that implanted handling gives. The IoT is involved savvy machines interfacing and speaking with different machines, items, situations and foundations. Accordingly, gigantic volumes of information are being produced, and that information is being prepared into helpful activities that can "order and control" things to make our lives a lot simpler and more secure—and to decrease our effect on the earth. The imagination of this new time is endless, with stunning potential to enhance our lives. What does the IoT need to end up a reality? In this white paper, Free scale and ARM accomplice to answer that question.

INTRODUCTION

Depending on WHO you sit down with, the Internet of Things (IoT) is outlined in numerous ways that, and it encompasses many aspects of life—from connected homes and cities to connected cars and roads (yes, roads) to devices that track an individual's behaviour and use the knowledge collected for "push" services. Some mention one trillion Internet-connected devices by 2025 and define mobile phones as the "eyes and ears" of the applications connecting all of these connected "things." Depending on the context, others give examples that ar less phone-centric, speak of a class of devices that don't exist nowadays or purpose to Google's augmented-reality sensible glasses as a sign of things to return. Everyone, however, thinks of the IoT as billions of connections (a sort of "universal world neural network" within the cloud) that may include each side of our lives. All of this public discussion suggests the IoT is finally becoming a hot topic among the thought media. Many recent articles purpose to the IoT as the interaction and exchange of knowledge (lots of it) between machines and objects, and now there ar product definitions reflective the same thought. Hence, from a technology perspective, the IoT is being defined as sensible machines interacting and act with alternative machines, objects, environments and infrastructures, resulting in volumes {of knowledge|of knowledge|of information} generated and process of that data into helpful actions that may "command and control" things and create life a lot of easier for personalities … the same as the planet visualised within the Nineteen Seventies cartoon The Jetsons, only higher. Estimates of the future market size of the IoT cover a broad vary, but most pundits agree it can dwarf the other market. In mature markets today, the ultimate, pervasive consumer device is a transportable. Consider your own menage, and count the number of mobile phones you presently have. Then count the number of windows, doors, electrical outlets, lights, appliances and heating and AC units you have. You'll quickly see why the IoT market will surpass the mobile phone market, at least within the western world. A quick net search highlighted the subsequent example use cases/applications below consideration:

- Machine-to-machine communication
- Machine-to-infrastructure communication
- Telehealth: remote or real-time pervasive observance of patients, diagnosis and drug delivery Continuous observance of, and firmware upgrades for, vehicles
- Asset tracking of product on the move
- Automatic traffic management
- Remote security and control
- Environmental monitoring and management
- Home and industrial building automation
- "Smart" applications, including cities, water, agriculture, buildings, grid, meters, broadband, cars, appliances, tags, animal

farming and the environment, to name a few

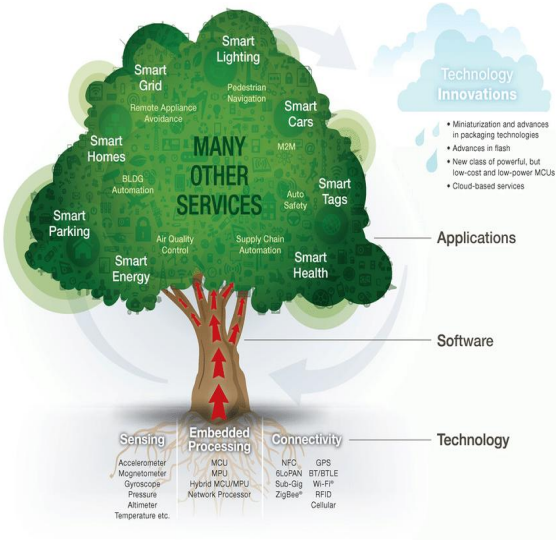

Fig1: The IoT: Different Services, Technologies, Meanings for Everyone

Making Things Smart

Do an IoT-related web pursuit, and you'll rapidly see the abuse of the expression "brilliant." So, what does it extremely mean when something is shrewd, and what makes a protest keen? For instance, how might a fridge or a toaster stove that hasn't been viewed as keen turned into a savvy apparatus? Today, we are seeing the jolt of our general surroundings. Any fabricated great presently incorporates an inserted processor (normally a microcontroller, or MCU), alongside UIs, that can include programmability and deterministic "order and control" usefulness. The jolt of the world and the inescapability of installed preparing are the keys to making objects "shrewd." Your old toaster that mechanically controlled the shade of your toast presently has a MCU in it, and the MCU controls the shade of your toast. The toaster finishes its undertaking all the more reliably and dependably, and on the grounds that it is presently a savvy toaster, it can speak with you electronically utilizing its touchpad or switches. After a gadget ends up savvy through the mix of implanted preparing, the following sensible advance is remote correspondence with the keen gadget to help make life less demanding. For instance, on the off chance that I am running late at the workplace, would I be able to turn on my home lights for security reasons utilizing my workstation or cell phone? Correspondence ability and remote manual control lead to the subsequent stage … how would I robotize things and, in view of my settings and with complex cloud-based handling, get things going without my mediation? That is a definitive objective of some IoT applications. Furthermore, for those applications to interface with and use the Internet to accomplish this objective, they should initially progress toward becoming "savvy" (join a MCU/implanted processor with a related one of a kind ID) at that point associated and, at last, controlled. Those capacities would then be able to empower another class of administrations that makes life simpler for their clients. For the system, refined cloud-based handling requires another age of correspondences processors that can monitor those associated gadgets, speak with them and make an interpretation of their usefulness into helpful administrations … all with nonlinear enhancement to their execution and proficiency. The test will be to manufacture secure systems that stay aware of interest, while all the while decreasing vitality utilization and cost of hardware. This will require a wide range of developments, well past the upgrades Moore's law can convey.

Application Categories

How about we take a gander at a few classes for IoT-related applications. While there are actually several applications being considered and distinguished by various ventures, they can be arranged in a basic, consistent manner.

Class One

Class one includes the possibility of a large number of heterogeneous "mindful" and interconnected gadgets with one of a kind IDs cooperating with different machines/articles, framework, and the physical condition. In this classification, the IoT to a great extent plays a remote track, order, control and course (TCC&R) job. Likewise with all parts of the IoT, wellbeing and security are principal. These applications are not about information mining of individuals' practices (along the lines of "elder sibling viewing") yet rather they stretch out the mechanization and machine-to-machine (M2M), machine-to-framework (M2I) and machine-to-nature (M2N) correspondences that can help disentangle individuals' lives.

Class Two

The second classification is tied in with utilizing the information that gets gathered by the end hubs (brilliant gadgets with detecting and availability capacity) and information digging for patterns and practices that can produce valuable promoting data to make extra business. Charge card organizations and

enrolment shopping clubs as of now track and utilize individuals' conduct, to a degree, to concoct offers that may advance steady deals. Presently, the inquiry is how far will this information mining go? Utilize cases could incorporate a store following which passageways you visited, where you invested the most energy inside those paths and even what kind of things you lifted and perused. This situation is effortlessly conceivable utilizing a cell phone's GPS capacity, RFID and savvy labels in stores and remote labels. The outcome could be as straightforward as giving email offers or "push" administrations at the purpose of offer. Or on the other hand, it could go further, with your vehicle insurance agency following your driving propensities and spots made a trip to allot chance factors that assistance decide your month to month premium, for instance. You can perceive how this class can turn into an elusive slant and how the IoT can empower information gathering in each part of one's regular daily existence and appoint a "classification" to a man … with charming or horrendous outcomes. When others wind up mindful of the setting related with an element, a man or a gathering (henceforth, knowing character, area, action and time), to what degree can that information be utilized, and to what degree should the substance, individual or gathering have a say in how that information gets utilized? This second classification, particularly, goads talks about protection, security, administration and the social obligation that joins such a "mindful," associated world. This paper is centered around class one—explicitly, the innovations and gadgets required to empower the IoT for TCC&R purposes.

IoT Use Cases

At the point when gadgets can detect and impart by means of the Internet, they can go past nearby implanted handling to access and exploit remote super-registering hubs. This enables a gadget to run progressively advanced investigations, settle on complex choices and react to nearby needs immediately, frequently with no human mediation required. How about we investigate the most widely recognized utilize cases for the IoT. Unavoidable Remote Tracking/Monitoring and (if necessary) Command,

Control and Routing (TCC&R)

This alludes to remote following/checking and, if necessary, direction, control and steering capacities for undertakings and procedures today typically done physically, or, whenever done remotely, that require extra foundation. For instance, in many homes today, it's a manual procedure to kill on and certain lights, set temperature zones and kill on and a clothes washer. Later on, entryways, windows, electrical outlets, apparatuses and numerous different kinds of independent hardware will progress toward becoming "savvy" with a remarkable ID. Those savvy gadgets would then be able to be associated by means of wired or remote correspondence, enabling a client to screen his or her home remotely, change settings on a fridge or clothes washer and control family errands through a PC or cell phone. Actually, there are a few administrations offered today by security or Internet specialist co-ops to do precisely that, however on an a lot littler scale and with less capacities than we hope to find later on.

Fig:2 Remote Patient Monitoring

Asset pursuit

An extension of these types of services is quality pursuit, which these days is done via barcode and a spread of manual steps, but in the future can leverage good tags, near-field communication (NFC) and RFID to globally track all kinds of objects, interactively. The word geo-tagged is now being used by some corporations to sit down with this category of applications. In a future scenario, a user would be able to use Google Earth to trace something with associate RFID tag. Alternatively, your refrigerator may keep track of your smart-tagged groceries and tell your cell phone app you're low on a definite item. If your bag of frozen vegetables can have a good tag, other objects such as valuable cars, jewellery and purses may too, and they can be tracked via the net and additionally make the most of a spread of obtainable web-based applications. Some telehealth-related services also belong in this class. Process

management and improvement this is once varied categories of sensors (with or while not exploit capabilities) square measure used for observation and to produce information thus a method will be controlled remotely. This could be as straightforward because the use of cameras (the sensing nodes during this example) to position boxes of varied sizes on a conveyor belt thus a label machine will properly apply labels to them. This task can be worn out real time by causation the info to a foreign laptop, analyzing it and bringing a command back to the line thus varied management actions will be taken to enhance the method … with none human intervention.

Resource Allocation and Optimization

The smart energy market provides associate ideal example of this use case. The term "smart energy" has been used in many ways, but it primarily refers to accessing info concerning energy consumption and reacting to the info to optimize the allocation of resources (energy use). In the case of a household, for example, once the residents know they've been exploitation their laundry machine throughout peak hours once the grid is most forced and therefore the price of electricity is at premium, they could change their behaviour and wash their laundry throughout nonpeak hours, saving money and serving to the utility company cope with the height demand.

Context-aware Automation and Decision improvement

This category is the most fascinating, as it refers to monitoring unknown factors (environmental, interaction between machines and infrastructures, etc.) associated having machines make selections that square measure as "human-like" as potential … solely better! Here's an example that will facilitate illustrate this: "In a traffic collision turning away system (TCAS), when 2 airplanes approach every alternative on a collision path, the 'machines' in the two airplanes take over. The system first sends associate perceptible warning to the pilots concerning the danger ahead, while at the same time communication between the 2 planes and deciding however every plane ought to move to avoid a collision. The assumption is that if the 2 pilots square measure warned and are on top of things to form fast selections, they can each arrange to build turns that may still cause a crash." There are a whole host of latest technologies accessible these days and in development that might permit vehicles to speak with one another further like a central management unit. These smart vehicles additionally may sense the road, traffic signs and lane markers and, using GPS and a communication link, avoid incoming traffic, avoid accidents around a curve or, in conjunction with the central control unit, avoid going over a distressed bridge on the verge of collapse. Remote patient monitoring is another example relevant to this use case. For instance, imagine associate implantable sensing node that tracks statistics associated sends a signal relating to an abnormal readout for an senior patient. If the patient doesn't respond by taking a medication, the node could place associate emergency decision to a contact from a list, and, if there's no answer, call a second contact, and finally, if no answer, contact a monitoring clinic or quickly offer alternative emergency help. Another example is continuous monitoring of chronic diseases to facilitate doctors confirm best treatments, with minimal human intervention.

- Requirements common to all of the utilization cases on top of include:
- Sensing and data assortment capability (sensing nodes)
- Layers of local embedded process capability (local embedded process nodes)
- Wired and/or wireless communication capability (connectivity nodes)
- Software to automate tasks and alter new categories of services
- Remote network/cloud-based embedded process capability (remote embedded processing nodes)
- Full security across the signal path

In the factory automation example (applying labels to boxes), a camera detects information exploitation a charge-coupled device (CCD) device (sensing node), the collected data is then communicated to associate embedded processor/controller (embedded process node) exploitation wired or wireless communication technology (connectivity node), a decision is created by the remote server (remote embedded process node) and communicated (connectivity node), which causes a mechanical action to take place that corrects things. A context-aware automation associated call improvement example may be a wise automobile exploitation its active safety system (sensing node) in conjunction with image process cameras (sensing nodes) that communicates with an embedded processor (embedded process node) within the center stack of the automobile to form an acceptable decision relating to danger ahead. Or, the vehicle may leverage its inbuilt GPS and wide-area-network

(WAN) wireless communication capability (connectivity node) to pass on info to a central process server on the network/in the cloud (remote embedded process node) that could then build the automobile awake to the data it had simply received from the sensors on a bridge (sensing node) that was being pounded by flood waters and losing its structural integrity, guiding the car to a completely different route to avoid danger.

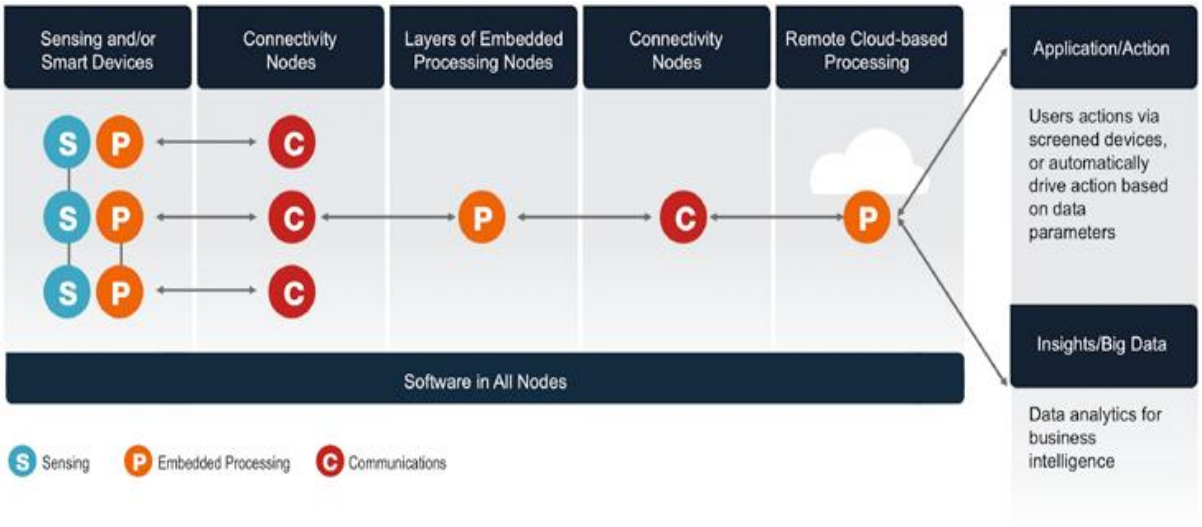

Fig3: Functional read of web of Things Technologies

Building Blocks of the IoT

Sensing Nodes

The types of sensing nodes required for the IoT vary wide, depending on the applications concerned. Sensing nodes could embrace a camera system for image monitoring; water or gas flow meters for good energy; Associate in Nursing ranging |measuring device vision once active safety is needed; RFID readers sensing the presence of an object or person; doors and locks with open/close circuits that indicate a building intrusion; or a easy measuring system measurement temperature. The bottom line is that there may be many alternative sorts of sensing nodes, depending on the applications. Who may forget the heat-seeking mechanical bugs that unbroken track of the population of a building in the flick Minority Report? Those mechanical bugs represent potential sensing nodes of the longer term. These nodes will all carry a distinctive ID and may be managed individually via an overseas command and control topology. Use cases exist today in that a Smartphone with RFID and/or NFC and GPS practicality will approach individual RFID/NFC-enabled "things" in a very building, communicate with them and register their physical locations on the network. Hence, RFID and NFC will have a place in remote registration, and, ultimately, command and control of the IoT.

Layers of Local Embedded process Nodes

Embedded processing is at the heart of the IoT. Local process capability is most typically provided by MCUs, hybrid microcontrollers/microprocessors (MCUs/MPUs) or integrated MCU devices, which will give the "real-time" embedded process that's a key demand of most IoT applications. Use cases vary significantly, and fully addressing the time period embedded process perform needs a scalable strategy (using a scalable family of devices), as one size won't fit all. In the home automation example, depending on the scale or form of residence, requirements may vary from a easy network to a additional advanced structure with stratified, nested sub networks controlled at different levels. For example, in a single-family home, all windows, doors, electrical outlets and/or electrical instrumentality and thermostats may have easy embedded managementlers that communicate with a master MCU/MPU hybrid device for command and control of the entire house. In turn, this master device can communicate via the web with a range of "clients," from the security service provider and different service suppliers to portals which will provide the home-owner access to remotely management all of those connected "things." In an living accommodations building, the same idea will be extended, with an even additional advanced superimposed network hierarchy that features apartment-level command and management, as well

as floor level and building-level command and control.

There are a few necessities that create associate degree MCU ideal to be used within the IoT.

- **Energy efficiency:** First and foremost, the MCU needs to be energy-efficient. In many cases, the sensing nodes are battery-operated satellite nodes, so a low-power specification is a basic demand. For example, an MCU in a battery-operated thermostat that wakes up once each jiffy to visualize the temperature and regulate the AC supported its findings must consume as very little power as doable to attenuate battery replacement. Integrated circuit (IC) designers have some ways to scale back power consumption, including low-leakage method technologies, best-in-class low-power non-volatile memory/flash memory technologies, architectural innovations and numerous duration schemes. For battery operated nodes, all of those techniques are required to realize the bottom doable power consumption.
- **Embedded architecture with a made computer code ecosystem:** The big variety of potential IoT applications wants a computer code development atmosphere that ties along the applications, the command, control and routing process and the security of the node and system. While the importance of computer code in MCU solutions has raised throughout the past few years, for MCUs supporting the IoT, even more computer code, tools and enablement will be required. A broad ecosystem with simply accessible support is key to enabling the event of embedded process nodes and IoT applications.
- **Portfolio breadth that enables computer code scalability:** the flexibility to utilise computer code and leverage existing computer code investment may be a key success issue for corporations developing IoT applications. Software utilise permits the speedy rollout of multi-layered architectures (in that the embedded processor is tasked with totally different layers and levels of trailing, command, control and routing functions). Portfolio breadth that cost-effectively enables totally different levels of performance and a sturdy mixture of I/O interfaces: the range of things to be controlled within the IoT, along with the various use cases, the number of things in a very micro-network, totally different levels of service needed and different interfaces in a heterogeneous atmosphere can cause the requirement for various tiers of devices, with diverse I/Os needed for the numerous applications. A "one size fits all" approach will not be cost- or performance-optimized enough to satisfy the requirements of this market.
- **Cost-effectiveness:** As with the other market, mass adoption will not present itself till a particular worth purpose for the solutions is reached. Like all other systems, the overall cost is that the add of the components of the system and the price of the services needed for the system. The overall system cost should be cheap for the paradigm shift to require hold in way of life, so product price is a terribly relevant issue.
- **Quality and reliability:** Unlike your mobile phone, laptop or different electronic device that you simply might modification each 2 years, product life cycles in the industrial market are a minimum of 10-15 years. Even inside a home, certain devices, such as thermostats, aren't changed that typically. When you add the automotive market to the combination, more rigorous reliableness necessities and harsh environmental conditions should be supported. Hence, quality, reliability and longevity necessities for these markets ar keys to the success of the IoT paradigm shift. Although shifting the bulk of industrial quality processing and analysis to remote supercomputing nodes within the network cloud is offered and permits the native nodes "live longer" (not become obsolete as fast), there is still a balance between what proportion local vs. remote processing can be required. This is especially vital for time-critical applications that like native process.
- **Security:** For the local embedded process node at the physical layer, there are a selection of crypto logical engines and security accelerators to support encoding (e.g. DES, AES, etc.) and authentication (e.g. SHA, etc.). Additional layers of security computer code, as well as best practices associated with boot-up routines,

are among the selection of security approaches accessible.

Wired and Wireless Communication Capability

The role of the communication node is to transfer information gathered by the sensing nodes and processed by native embedded process nodes to the destinations known by the local embedded processing nodes. And, once the data is remotely processed and new commands ar generated, the communication node brings back the new commands to the local embedded process nodes to execute a task. Sometimes this may be as easy as sensing a electric refrigerator door being left open supported energy use, and after analyzing the information, automatically closing the door via a mechanical mechanism or generating a warning for the homeowners' "home automation app." Or, it could be as subtle as communication to associate degree autonomous vehicle to avoid associate degree accident.

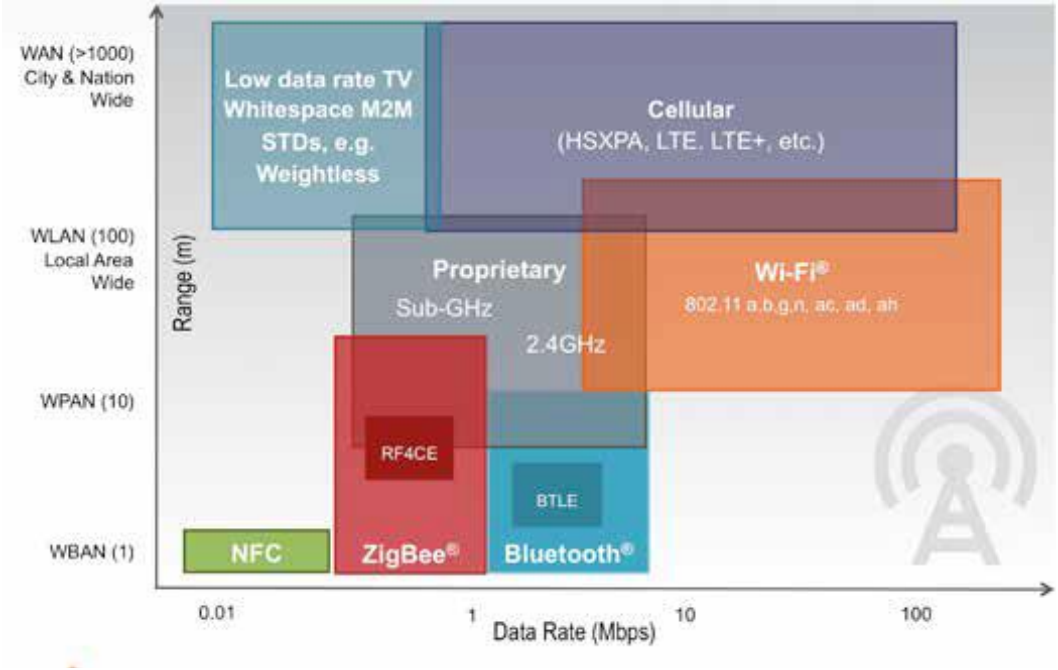

Fig4:4 Today's Wireless Landscape

Utilize cases could change definitely, yet what is basic to these direction and control correspondence joins is that they regularly just need to convey couple of kilobytes of information for some random hub, except if high-transmission capacity picture preparing or video information is included. The IoT will incorporate all parts of one's regular daily existence, thus there is no restriction to the separations for which direction and control correspondence can/will be utilized. To show signs of improvement comprehension of the elements of this portion, how about we make a stride back and take a gander at the different correspondence topologies that exist today, from remote body territory arrange (WBAN) to wide zone organize (WAN), and the majority of the alternatives in the middle. If you somehow managed to configuration wired and remote advances for the IoT starting from the earliest stage, you could possibly wind up with the interchanges scene as we probably am aware it today. Be that as it may, a significant number of the organizations advertising remote and wired arrangements are situating their items as "the correspondence motor of decision" for the IoT advertise. The IoT will likewise include the idea of remote sensor and actuator systems (WSANs), which are systems that contain detecting and installed handling hubs that can control their condition. Similarly as with any developing business sector, a progress period before framework streamlining happens and innovations turn out to be more qualified for the end IoT-related applications is likely. In light of run of the mill item life cycles and the job of programming, it is protected to state that if an innovation grabs hold in an IoT portion now, that innovation (or an upgraded to-reason adaptation of it) will be set up for in any event the following five to eight years. There are some fight lines officially drawn that might harden. For instance, it appears just as Bluetooth® Low Energy (BTLE) is being embraced by the medicinal services industry for

versatile therapeutic and way of life gadgets. Then again, the fight among ZigBee® and low-control Wi-Fi® advancements for modern control and robotization has quite recently started. Administrators are direly searching for new income streams, and machine-to-machine correspondence and area based administrations appear to be great puts down to make a wager. Both can utilize existing framework and are particularly a piece of the rising IoT advertise.

Correspondence Technologies

Real volumes for the IoT market will probably not occur for another 10-12 years, and, around then, the correspondences innovations might be totally not quite the same as those being viewed as today, or new modifications of existing gauges may have developed. Wi-Fi technologists as of now are dealing with 802.11ah (Wi-Fi on ISM groups underneath 1 GHz) to tailor it for framework autonomous specially appointed, work systems administration and longer-go control of sensor systems. On the other hand, there could be fresh out of the box new advances more qualified for specific parts of IoT correspondence that uproot the current principles for the IoT. For instance, administrators may choose their profitable range is too valuable to use for WAN-based order and control administrations and they rather need to utilize an alternate innovation. Or then again, a problematic remote system innovation like what Weightless (weightless.org/) is creating may grab hold. One thing about the network needs of things to come IoT showcase is clear—it is so various, vast and cost-cognizant that a scope of various advancements will be required (conceivably including WAN, LAN, WPAN, WBAN, and so forth.), and one size won't fit all. Necessities for correspondence capacities are nearly equivalent to for implanted preparing hubs:

- Cost-viability
- Low control
- Quality and unwavering quality
- Security

	NFC	RFID	Blue-tooth®	Blue-tooth® LE	ANT	Proprietery (Sub-GHz & 2.4 GHz)	Wi-Fi®	ZigBee®	Z-wave	KNX	Wireless HART	6LoWPAN	WiMAX	2.5–3.5 G
Network	PAN	PAN	PAN	PAN	PAN	LAN	LAN	LAN	LAN	LAN	LAN	LAN	MAN	WAN
Topology	P2P	P2P	Star	Star	P2P, Star, Tree Mesh	Star, Mesh	Star	Mesh, Star, Tree	Mesh	Mesh, Star, Tree	Mesh, Star	Mesh, Star	Mesh	Mesh
Power	Very Low	Very Low	Low	Very Low	Very Low	Very Low to Low	Low-High	Very Low	Very Low	Very Low	Very Low	Very Low	High	High
Speed	400 Kbs	400 Kbs	700 kbs	1 Mbs	1 Mbs	250 kbs	11-100 Mbs	250 kbs	40 Kbs	1.2 Kbps	250 kbs	250 Kbs	11-100 Mbs	1.8-7.2 Mbs
Range	<10 cm	<3 m	<30 m	5-10 m	1-30 m	10-70 m	4-20 m	10-300 m	30 m	800 m	200 m	800 m (Sub-GHz)	50 km	Cellular network
Application	Pay, get access, share, initiate service, easy setup	Item tracking	Network for data exchange, headset	Health and fitness	Sports and fitness	Point to point connectivity	Internet, multimedia	Sensor networks, building and industrial automation	Residential lighting and automation	Building automation	Industrial sensing networks	Senor networks, building and industrial automation	Metro area broadband Internet connectivity	Cellular phones and telemetry
Cost Adder	Low	Low	Low	Low	Low	Medium	Medium	Medium	Low	Medium	Medium	Medium	High	High

Table1: Communication Technologies

'Box-level' View of IoT Building Blocks

If we convert the building blocks of the IoT from simple nodes to a box/product-level view, we end up with sensing/edge nodes that use PAN/BAN/LAN types of communications topologies, connected to gateways with different levels of hierarchy. These gateways, in turn, communicate to the cloud via WAN communication technology. Once connected to the cloud through an access network, data will be routed through a server for application/action, as well as big data analysis.

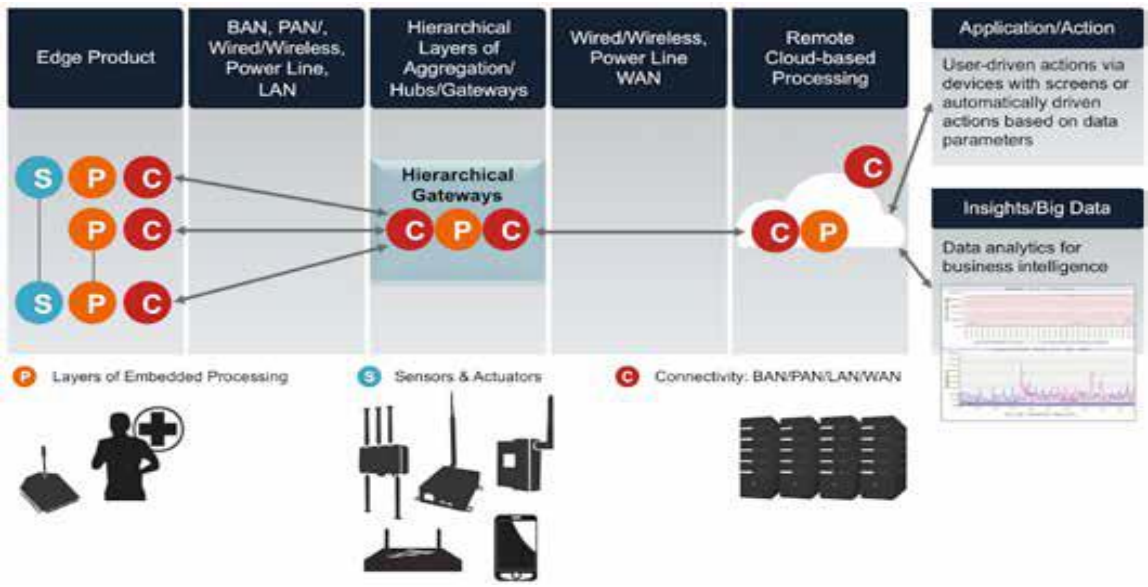

Fig:5 'Box-level' View of IoT Building Blocks

Software to Automate Tasks

Getting all segments of the IoT to communicate and work together is key to the success of the Technology rollout and that means deploying a lot of software (and middleware) that will enable various heterogeneous devices to talk with each other and the infrastructure around them. For example, in a smart meter application, an analog front end (AFE) reads the meter and the MCU manages the meter to interpret and push the data through the communication pipe, which will be communicating with the house on one end and the curb side on the other end. While most developers have a clear view of the software architecture from a device, communication pipe and application profile perspective, the service-level fabric must also be considered for a given application. In this configuration, the sensing node (here the AFE) is using an embedded processing (MCU) node to translate and transmit the data through the communication functions to the central embedded processing node in the house, as well as one on the curb side. A lot of middleware software is needed to enable this interaction to happen reliably, with the services delivered seamlessly. Remote Embedded Processing Nodes

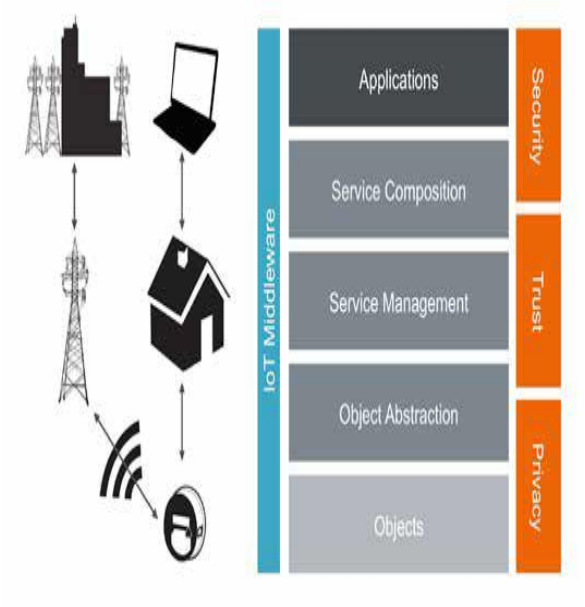

Fig:6 Software Service Fabric for Metering Application

(access to cloud computing) Since there are not yet industry-wide IoT best practices agreed upon and deployed, many component providers are approaching the connection between devices and the cloud as a connection to their niche cloud, as opposed to the cloud. Some companies promote that all devices will be "dumb nodes," with all processing and decision-making done within "their cloud." Alternatively, some believe only minimal access to the cloud for basic Internet related services will be required, with most of the "thinking" done locally. The architecture and building blocks of the IoT as described in this paper allow for a number of different approaches, which will likely be necessary

due to the wide variety of use cases and configurations anticipated. That flexibility will be needed to optimize system-level performance. So, why does software get such a big headline? Software enables the various services the IoT will provide. Services are the means by which the IoT will address certain needs. Those needs could exist today, or they may be things we don't yet realize we need, but someday we'll wonder why we never had them before. Many people forget that until 20 years ago, most of us lived without mobile phones and didn't see a need for them, but now they are the most personal gadget owned by people in the western world. Along those lines, some IoT services will address needs easily identifiable today (e.g. asset tracking, smart energy, etc.), but others are yet to be defined.

Full Security Across the Entire Signal Path

Some people bundle this topic within the software portion of the IoT, but it deserves the attention of a separate category. Without a solid security mechanism for all of the IoT building blocks mentioned above, the IoT will not be as pervasive as it is anticipated to become. When we say security, we really mean security of information—the information that gets passed around by various parts of the system and is context- and service-dependent. For example, knowing the location of a person could be considered a good thing if the person was lost. However, if that person felt his or her privacy was being compromised, knowing the location information could be considered a bad thing.

Here's what we mean by secure information:

- Information needs to be available when needed: This is the most basic level of security. If the information regarding an intruder in your house gets sent to the police station the next day, that information loses its value. The assurance that the services and their underlying infrastructure can process, store and deliver the data when and where it's needed is the first aspect of a secure system. In certain cases, redundant infrastructure needs is required to ensure this will happen.
- Information needs to be confidential: Hence, the owner of the information decides which authorized people, groups or organizations can access it. Safeguarding the information obtained by IoT services is critical, or those services will lose the users' trust. Mechanisms must be put in place to ensure confidentiality of the information exchanged. This is a tough balancing act, as there are a whole host of IoT-related services designed to leverage data mining and generate push services. The "opt out" mechanism for such services would be subject to the governance of the IoT.
- The integrity of data needs to be assured: Assurance that the information is accurate, authentic, timely and complete is key. Unless the data can be trusted and relied upon, it cannot be used for its intended purposes, and the entire service paradigm around that data will break down. The security of the system is as good as the last threat it was able to prevent, and, as soon as it gets broken, one needs to implement new ways of making it secure again. If the recent hacking of credit card and personal information from reputable outlets on the Internet is any indication of the challenges facing IoT services, the Internet security infrastructure available today is inadequate to manage IoT services. During the summer of 2010, malware targeted electronic process control systems for the first time instead of the traditional credit cards and personal information. The Stuxnet Trojan horse worm that attacked Siemens process control systems at nuclear plants demonstrated incredible levels of sophistication and showed the potential damage that could be done to undermine the security of the IoT.
- Device-level Security: There are different types (MCU, hybrid MCU/MPU, integrated MCUs, etc.) and layers of embedded processing at various nodes of the IoT, and for any device to be considered smart so it can be connected to the Internet, it must incorporate an embedded processor. Embedded processors are going to be pervasive in the IoT, and they'd better be very secure. MCUs are vulnerable during their boot-up process, when software is executed from programmable memory using the code stored in the read-only memory (ROM) or non-volatile memory (NVM)/flash memory. During this process, expert hackers can break the routine and hack the system in a variety of ways. Many new technologies are rolling out to address

the security issues related to passive attacks (e.g. glitching) and invasive attacks (e.g. UV attacks), but more are likely necessary. The intent of the IoT is to put smart devices on a sort of universal neural net, controlling them remotely. Hence, each of these identifiable objects (billions of them) can introduce a threat to the overall system. With such potential for disaster, are there best practices engineers can learn to enhance the security of MCUs in an IoT system? By now it should be clear that networks of the future will connect more objects, machines and infrastructure to a global neural network of cloud-based services than they will connect people. A tsunami of data and services will affect the way we live, well beyond the changes experienced when the Internet first arrived and changed the way people network and communicate with each other. At the heart of the IoT are layers of embedded processing, from the most remote satellite sensing node to the core of the network. The diversity of services being planned for the IoT means no one company can develop full solutions and supporting IoT-based innovations. IoT-based innovations will require a broad, rich ecosystem of partner companies working together to bring IoT-based services to the market. An open (non-proprietary) platform (ARM.com) that allows all partners working together to use the same baseline technologies is key to making the IoT happen.

Conclusion

The pervasiveness of embedded processing is already happening everywhere around us. At home, appliances as mundane as your basic toaster now come with an embedded MCU that not only sets the darkness of the piece of toast to your preference, but also adds functional safety to the device. Your refrigerator has started talking to you and keeping track of what you put in it. There are energy-aware HVAC systems that can now generate a report on the activity in your house and recommend ways to reduce your energy consumption. The electrification of vehicles has already started happening, and in just a few years from now, each car will contain >50 percent more electronics than it did just five years ago. The cars of the future will indeed be able to drive themselves. Similar changes are also happening in other aspects of our lives … in factories, transportation, school systems, stadiums and other public venues. Embedded processing is everywhere. Connecting those smart devices (nodes) to the web has also started happening, although at a slower rate. The pieces of the technology puzzle are coming together to accommodate the Internet of Things sooner than most people expect. Just as the Internet phenomenon happened not so long ago and caught like a wildfire, the Internet of Things will touch every aspect of our lives in less than a decade. Are you ready for it?

/