International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 15, 2019 (Special Issue)

Internet of things a communication perspective

[1]Shwetha. S [2]Sabarmathi G
[1]BCA, Christ Academy Institution for Advanced Studies, Bengaluru
shwethasujendra1097@gmail.com
[2]Asst.Professor, Christ Academy Institution for Advanced Studies, Bengaluru
sabarmathi@caias.in

I. Abstract— The term internet of things is used as an umbrella keyword for converging various aspects related to the extension of the internet and web into the physical realm by the means of the widespread deployment of spatially distributed devices with embedded identification sensing capabilities. Internet of things in visions a future in which digital and physical entities can be linked by the mean of appropriate information and communication technologies.

II. Keywords—Internet of Things, communication, internet, smart device, cloud, network.

III. INTRODUCTION

In today world the most important in thing is Internet . A man day starts with internet and end with Internet . If one has to learn or to communicate they take the help of internet which has dragged us towards the Internet . mostly internet is used to let other now about all things happening around us either it might be an event or any other information we want. The content and the services are always available paving new ways of interaction , new ways of working ,new ways of living . internet infrastructure is always reaching out to the end users leaving a space for the notion of interconnected “smart “object forming pervasive computing environment . this always gives rise to a new opportunities for information and communication technologies (ict)sectors passing new ways to services application able to leverage the interconnection of physical and virtual realms

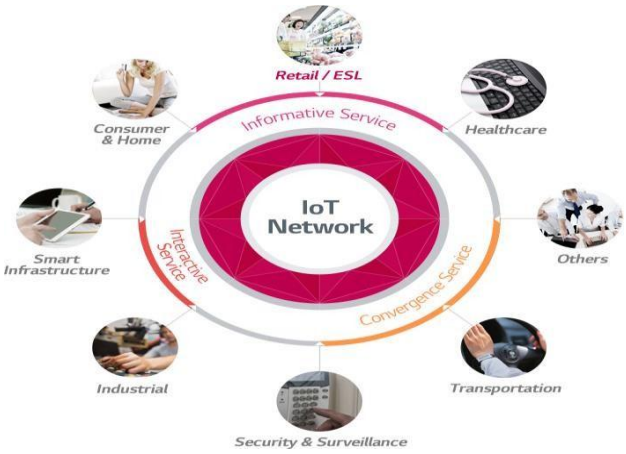
IV. VISION

The Internet and mobile technologies are considered as the biggest revolution for mankind since the industrial revolution two centuries ago. The IoT will be a further step in this "information-age" revolution with immense implications,

V. BUILDING BLOCKS OF INTERNET

The Internet of Things (IoT) is about interconnecting embedded systems, bringing together two evolving technologies: wireless connectivity and sensors. These connected embedded systems are independent microcontroller-based computers that use sensors to collect data. These IoT systems are networked together usually by a wireless protocol such as WiFi, Bluetooth, 802.11.4, or a custom communication system. The networking protocol is selected based on the distribution of nodes and the amount of data to be collected.
This data is sent over the network to the main hub or computer. This main computer collects and analyzes the data, storing it in memory and even making system decisions based on the results of the analysis.
Crucial to modern IoT nodes is the need for security with some form of data encryption, the most common being AES256. This security is critical for helping the microcontroller perform a secure boot, insuring that the core is running the code is meant to run. Encryption security is also used to encrypt the data transmitted over the network, insuring that it is viewed only by those systems authorized

The internet of thing is emerging as a new trend in shaping the development of technologies in ict sector at large .this shift from an internet is used for main concept of iot in communication mainly to build three pillar that is firstly to be identifiable , secondly to communicate and thirdly to interact either which build a good network of interconnected objects among themselves. Smart objects from entities traditionally considered I network system .and such entities into a global network system question the architecture and algorithm principles at the basics of the designs of internet as we know . the inclusion of devices with only very basic communication and computing capability ,from the conceptual stand pint indeed iot is about entities acting as provided and /or consumer of data related to the physical world .this mainly focus on the data and information rather end to end communication.



A. Abbreviations and Acronyms

Iot : internet of things

To have a very good network system security is very much necessary where it represents a critical components for enabling the widespread adoption of iot technology and application without guarantee in terms of system level confidentially, authenticity and privacy relevant stake holder are unlikely to adopt iot solution on a large scale . now it is all secure and safe in almost networking
Which involves three things require innovative approach is data confidentially , privacy and trust which represents a critical component for enabling the widespread adoption of iot technologies and applications .

Unique Security Challenges of IoT Devices

IoT devices tend to differ from traditional computer and computing devices in important ways that challenge security: Many Internet of Things devices, such as sensors and consumer items, are designed to be deployed at a massive scale that is orders of magnitude beyond that of traditional Internet-connected devices.

- As a result, the potential quantity of interconnected links between these devices is unprecedented. Further, many of these devices will be able to establish links and communicate with other devices on their own in an unpredictable and dynamic fashion. Therefore, existing tools, methods, and strategies associated with IoT security may need new consideration.
- Many IoT deployments will consist of collections of identical or near identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics. For example, a communication protocol vulnerability of one company's brand of Internet-enabled light bulbs might extend to every make and model of device that uses that same protocol or which shares key design or manufacturing characteristics.
- Many Internet of Things devices will be deployed with an anticipated service life many years longer than is typically associated with high-tech equipment. Further, these devices might be deployed in circumstances that make it difficult or impossible to reconfigure or upgrade them; or these devices might outlive the company that created them, leaving orphaned devices with no means of long-term support. These scenarios illustrate that security mechanisms that are adequate at deployment might not be adequate for the full lifespan of the device as security threats evolve. As such, this may create vulnerabilities that could persist for a long time. This is in contrast to the paradigm of traditional computer systems that are normally upgraded with operating system software updates throughout the life of the computer to address security threats. The long-term support and management of IoT devices is a significant security challenge.

- The subscript for the permeabilit The Internet of Things (IoT) is about interconnecting embedded systems, bringing together two evolving technologies: wireless connectivity and sensors. These connected embedded systems are independent microcontroller-based computers that use sensors to collect data. These IoT systems are networked together usually by a wireless protocol such as WiFi, Bluetooth, 802.11.4, or a custom communication system. The networking protocol is selected based on the distribution of nodes and the amount of data to be collected.
- Many IoT devices are intentionally designed without any ability to be upgraded, or the upgrade process is cumbersome or impractical. For example, consider the 2015 Fiat Chrysler recall of 1.4 million vehicles to fix a vulnerability that allowed an attacker to wirelessly hack into the vehicle. These cars must be taken to a Fiat Chrysler dealer for a manual upgrade, or the owner must perform the upgrade themselves with a USB key. The reality is that a high percentage of these autos probably will not be upgraded because the upgrade process presents an inconvenience for owners, leaving them perpetually vulnerable to cybersecurity threats, especially when the automobile appears to be performing well otherwise.
- Many IoT devices operate in a manner where the user has little or no real visibility into the internal workings of the device or the precise data streams they produce. This creates a security vulnerability when a user believes an IoT device is performing certain functions, when in reality it might be performing unwanted functions or collecting more data than the user intends. The device's functions also could change without notice when the manufacturer provides an update, leaving the user vulnerable to whatever changes the manufacturer makes.

- Some IoT devices are likely to be deployed in places where physical security is difficult or impossible to achieve. Attackers may have direct physical access to IoT devices. Anti-tamper features and other design innovations will need to be considered to ensure security
- Some IoT devices, like many environmental sensors, are designed to be unobtrusively embedded in the environment, where a user does not actively notice the device nor monitor its operating status. Additionally, devices may have no clear way to alert the user when a security problem arises, making it difficult for a user to know that a security breach of an IoT device has occurred. A security breach might persist for a long time before being noticed and corrected if correction or mitigation is even possible or practical. Similarly, the user might not be aware that a sensor exists in her surroundings, potentially allowing a security breach to persist for long periods without detection.
- • Early models of Internet of Things assume IoT will be the product of large private and/or public technology enterprises, but in the future "Build Your own Internet of Things" (BYIoT) might become more commonplace as exemplified by the growing Arduino and Raspberry Pi60 developer communities. These may or may not apply industry best practice security standards.

VI. APPLICATIONS OF INTERNET OF THINGS

1) A. Smart home

Smart Home clearly stands out, ranking as highest Internet of Things application on all measured channels. More than 60,000 people currently search for the term "Smart Home" each month. This is not a surprise. The IoT Analytics company database for Smart Home includes 256 companies and startups. More companies are active in smart home than any other application in the field of IoT. The total amount of funding for Smart Home startups currently exceeds $2.5bn. This list includes prominent startup names such as Nest or AlertMe as well as a number of multinational corporations like Philips, Haier, or Belkin.

2) B. Wearables

Wearables remains a hot topic too. As consumers await the release of Apple's new smart watch in April 2015, there are plenty of other wearable innovations to be excited about: like the Sony Smart B Trainer, the Myo gesture control, or LookSee bracelet. Of all the IoT startups, wearables maker Jawbone is probably the one with the biggest funding to date. It stands at more than half a billion dollars!

3) C. Smart City

Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fueled by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

4) D. Smart grids

Smart grids is a special one. A future smart grid promises to use information about the behaviors of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity. 41,000 monthly Google searches highlights the concept's popularity. However, the lack of tweets (Just 100 per month) shows that people don't have much to say about it.

5) E. Industrial internet

The industrial internet is also one of the special Internet of Things applications. While many market researches such as Gartner or Cisco see the industrial internet as the IoT concept with the highest overall potential, its popularity currently doesn't reach the masses like smart home or wearables do. The industrial internet however has a lot going for it. The industrial internet gets the biggest push of people on Twitter (~1,700 tweets per month) compared to other non-consumer-oriented IoT concepts.

6) F. Connected car

The connected car is coming up slowly. Owing to the fact that the development cycles in the automotive industry typically take 2-4 years, we haven't seen much buzz around the connected car yet. But it seems we are getting there. Most large auto makers as well as some brave startups are working on connected car solutions. And if the BMWs and Fords of this world don't present the next generation internet connected car soon, other well-known giants will: Google, Microsoft, and Apple have all announced connected car platforms.

7) G. ConnectedHealth(Digitalhealth/Telehealth/Telemedicine)

Connected health remains the sleeping giant of the Internet of Things applications. The concept of a connected health care system and smart medical devices bears enormous potential not just for companies also for the well-being of people in general. Yet, Connected Health has not reached the masses yet. Prominent use cases and large-scale startup successes are still to be seen. Might 2015 bring the breakthrough?

8) H. Smart retail

Proximity-based advertising as a subset of smart retail is starting to take off. But the popularity ranking shows that it is still a niche segment. One LinkedIn post per month is nothing compared to 430 for smart home.

9) I. Smart supply chain

Supply chains have been getting smarter for some years already. Solutions for tracking goods while they are on the road, or getting suppliers to exchange inventory information have been on the market for years. So while it is perfectly

logic that the topic will get a new push with the Internet of Things, it seems that so far its popularity remains limited.

10) J. Smart farming

Smart farming is an often overlooked business-case for the internet of Things because it does not really fit into the well-known categories such as health, mobility, or industrial. However, due to the remoteness of farming operations and the large number of livestock that could be monitored the Internet of Things could revolutionize the way farmers work. But this idea has not yet reached large-scale attention. Nevertheless, one of the Internet of Things applications that should not be underestimated. Smart farming will become the important application field in the predominantly agricultural-product exporting countries ..

example applications are

. At home

- To track down the lost key
- Make sure that the oven is off
  light our home in a new way

Our city

- To keep our city calm
- To avoid driving in circles
- Receive pollution warnings

Industry

- Maintain and repair
- Keeps track of all the assets
- Maintain quality and consistency

The environment

- Tracks the water level
- Help protect wildlife
- Monitor pollution level

CONCLUSION

The internet of things may represent the big leap ahead in the ict sector through the massive deployment of embedded device . it is like a new gate way opened for the new exciting direction for both research and business field . the iot umbrella concept comprises all these aspects , based on the paradigms of computing and communication anywhere ,anytime , and by anything . the internet of things is unlikely to arise as a brand new class of system . we envision an incremental development path , along which iot technologies will be progressively employed to extend existing ict systems applications , providing additional functionalities related to the ability of interacting with the physical realms . when we look at todays state of the art technologies , we get a clear indication of how the iot will be implemented on a universal level in the coming years . in the next few years , addressing the challenges will be powerful driving force for networking and communication research in all the fields where a clear legislative framework ensuring the right of privacy and security levels for all users are implemented that will contain much higher quantity of data and will be more interactive and intelligent

References

[1] M . Weiser , the computer for the 21 century , Sci am .(1991) 94-100
[2] V . Raghunath , S . Ganeriwal , M Srinivas , emerging techniques for long live wireless sensor networks ,IEEE communication . (2006)
[3]I.akyilidiz , F.Brunetti , C . Blazquz , Nano networking : a communication paradigm compute . netw .52 (12)(2008)

[4] H . Liu , M . Bolic , A. nayak , I . Stojmenovic , taxonomi and challenges as the intergration of RFID and wireless sensor network , IEEE network 22(2008)

[5] L . Zhang , Z . Wang , integration of RFID into wireless sensor networks : architecture , oppurtunities and challenging networks .

[6] https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-

[7] http://www.mouser.in/applications/internet-of-_ _ things-block-diagram/

[8] Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions Jayavardhana Gubbi,a Rajkumar Buyya,b* Slaven Marusic,aMarimuthu Palaniswamia aDepartment of Electrical and Electronic Engineering, The University of Melbourne, Vic - 3010, Australia bDepartment of Computing and Information Systems, The University of Melbourne, Vic - 3010, Australia

[9] http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#32a1df946828