Security in Internet of Things Systems

M. Shankar Lingam
Research Scholar, DOS in Business Administration,BIMS, Manasagangothri, University of Mysore, Mysore, India

Dr. A. M. Sudhakara
Director, Centre for Information Science & Technology (CIST) and Systems Manager & Head, University Computer Center, Manasagangothri, University of Mysore Mysore-570006

Abstract: **Technology is the backbone of economy.**
In today's world, one can observe a change in the paradigmatic approach to information technology which advocates Innovation, Internet of Things, Social, Mobility, Analytics and Cloud services have emerged as the fastest growing verticals, which will shape the future of the IT and Electronics sector growth in the country. Policies have to be considered and notified, preferably together or in close succession, so as to give a holistic picture of what the Country wants to achieve and how. These Policies are based on 4 Pillars – Infrastructure, Human Capital, Incentives and Good Governance.

Keywords: IoT, Devices, Policies

1. INTRODUCTION

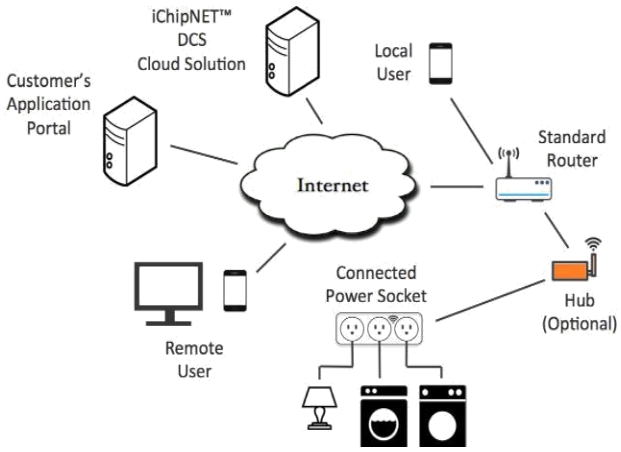
Internet of Things (IoT): The basic notion

The Internet of Things (IoT) is all about the internet-based informationarchitecture, which facilitatessecured exchange of items and services. In other words, IoT enables exchange of "things" using secured network infrastructure by connecting physical objects and their knowledge representation. The major advantage of IoT is total transparency and transaction efficiency in a global supply-chain networks. As defined by Haller, Karnouskos and Schroth, IoT is a system that unifies physical objects and information and communication networks and advocates the participation of smart objects in business processes. Secured IoT services are gradually evolving for the past a year or so.

Similar to distributed computing, grid computing and cloud computing IoT could also be viewed as a possible ubiquitous computing wherein the entire information space would turn out to be a smart environment that observes, detects, adapts and collate various objects.

Every physical object could be made smart to interact and communicate with other objects using the tenets of IoT. There is no need to produce smart objects anymore, but it is possible to make every object smart.

One can quote many examples to highlight this concept of IoT and its uses. A cell phone can interact with any other object like a car, a refrigerator, an umbrella, even a chair and a pen. Object to object interaction could be on a half-duplex mode or in a full-duplex mode. The concept of IoT is not directly linked to humans because human beings are not things. However, human beings could indeed observe, control and derive benefits from IoT. Already available technologies like RFID, GPS, barcodes and so on could be effectively used in the development of IoT.



Block Diagram of IOT

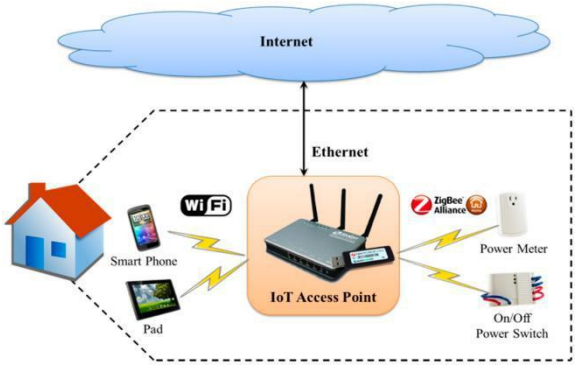
Under the smart city plan of the Government of India, one can visualize the constructive use of IoT almost in every walk of life. Pentagram Research Centre Private Limited, a Hyderabad based company along with the help of Avatar MedVision US LLC, NC, a US based company has propose very recently three initiatives namely Digital Food Initiative, Digital Health Initiative and Digital Security Initiative which would work on certain advanced tenets of IoT (Ref: www.pentagramresearch.com). These three initiatives are framed on certain key aspects of smart cities, to be precise, smart country. Some of them are listed below.

1. IoT enabled corporate farming
2. IoT enabled transportation of things and people
3. IoT enabled Farm-To-Home (FTH) distribution system
4. IoT enabled power distribution system
5. IoT enabled health care
6. IoT enabled security measures
7. IoT enabled governance

2. Implementation of IoT

Internet of Things (IoT) is implemented in three stages

1. Implant of suitable sensors on things and allocation of addresses for them
2. Software for sensor data collection and consolidation
3. Data transmission and decision making using expert systems



Many countries(Korea, Denmark, Switzerland and USA) have already taken initiative to implement IoT enabled infrastructure and services. The steps to be taken for the implementation of IoT are outlined in the following.

1. Investment in the fundamental R&D plays a significant role in this context.
2. Manufacturing of sensors for various data collection is of paramount importance.
3. Multi-sensor fusion techniques have to be seriously looked into
4. Formatting of raw data using big data analytics methods are to be studied.
5. Machine learning techniques have to be developed for decision making purposes.
6. Training of human resource in this area is to be viewed seriously.
7. Policy making in government and private sectors is important in integrating networks.
8. A commercial outlook has to be given to the entire initiative for its own survival.

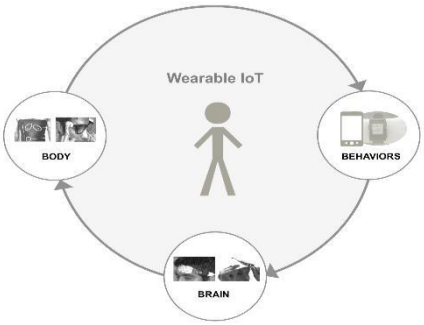
3. Applications of IoT and Challenges

Some of the applications of IoT are briefly described in the following:

Wearable Technology & Personalized ealthcare

Wearable technology that can collect data, from monitoring physical activity, and give real-time responses is the future of personalized healthcare. Wearable devices can read temperatures, heart-rate, test blood and monitor movement disorders, and even release medication.

Within five years, biometric information pertaining to human beings would be available in the network so that devices and various physical objects would warn and advise human beings for corrective measures based on situation related biometric information.



The Connected Home

Home automation is a decade old paradigm which will play a significant role in connecting all homes in a city and all cities in a country. Based on the current trend, users will soon be able to control all home electronics with just their phone. Studies show people are now using technology daily for longer periods than they spend sleeping, as the ability to multi-task activities easily with smart phones and tablets increases. This level of remote control and access in the palm of your hand allows users to conserve energy in their home, even when they are not there. The ease of doing this with a simple interface, connecting multiple devices and programs, will be beneficial not only to individuals for saving money but could also have an environmental impact in reducing energy use and ultimately climate change. A smart lock does not require a wireless connection, and users will still be able to use their low-tech keys. A signal from a smartphone app would open the door. Homeowners can send these digital keys to friends and relatives through the app, and delete them as and when required.

Security and Privacy Challenges

Most countries have no laws that specifically mention IoT devices, so general privacy laws -- many of which went on the books before anyone had heard of the term 'IoT' -- apply when a company wants to collect data from users.

These privacy laws vary from country to country, which can be a challenge. For example, U.S.-based companies used to be able to easily collect data from users in the EU, where data privacy laws are stricter, if they were certified under a program called Safe Harbor. But late last year, the EU declared Safe Harbor invalid. So, said Kate Lucente, a US attorney who works with data privacy issues, "companies have had to scramble to put some backup mechanism in place to make the data transfers legal."

As the changeover from closed networks to open enterprise networks is rapidly advancing, and the use of smart devices is surging, many fears have been raised for the security of data. As the reliance on IoT technologies becomes more widespread, and our dependence on interconnected devices grows, how will we effectively monitor and protect personal information and public safety?

The prime objective of IoT is to develop an autonomous world order in which human
interference would be reduced to a large extent. Devices and things could be smart, possibly smarter than human beings but they are not bound by emotions. Alternatively, human beings function mostly on emotions and hence any system in which human beings play a role is susceptible for corruption and misuse. This amounts to saying that any autonomous system with human beings as a part, poses threat to the integrity of the system. So, the biggest challenge in IoT based system is security breach that may lead to chaos and catastrophe.

SMART CITIES

A smart city is an urban development vision to integrate multiple information and communication technology (ICT) solutions in a secure fashion to manage a city‟s assets

– the city‟s assets include, but not limited to, local departments information systems, schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services. The goal of building a smart city is to improve quality of life

by using technology to improve the efficiency of services and meet residents‟ needs. ICT allows city officials to interact directly with the community and the city infrastructure and to monitor what is happening in the city, how the city is evolving, and how to enable a better quality of life. Through the use of sensors integrated with real-time monitoring systems, data are collected from citizens and devices - then processed and analyzed. The information and knowledge gathered are keys to tackling inefficiency.

Here, then, are the top 10 smart cities on the Planet:

1. Vienna.
2. Toronto.
3. Paris
4. New York
5. London
6. Tokyo
7. Berlin
8. Copenhagen
9. Hong Kong
10. Barcelona

The Indian Government's plan of developing 100 smart cities in the country, for which Rs. 7,060 crores has been allocated in the current budget could lead to a massive and quick expansion of IoT in the country. Also, the launch of the Digital India Program of the Government, which aims at

„transforming India into digital empowered society and knowledge economy‟ will provide the required impetus for development of the IoT industry in the country. The various initiatives proposed to be taken under the Smart City concept and the Digital India Program to setup Digital Infrastructure in the country would help boost the IoT industry. IoT will be critical in making these cities smarter.

More than fifty per cent of the world‟s population currently lives in cities and the need to make future cities more intelligent and connected has never been greater. How can future cities be better designed to benefit healthcare, education, transport and energy needs? – is a fundamental question.

Future smart cities would turn out to be „flexible‟ when natural and environmental situations are also taken into account while designing IoT enabled smart cities. A decision made for the dynamics of a smart city in a particular season need not be the same for another season. Moreover, an expert system based automatic control over the dynamics of future smart cities is a white space for researchers and city planners.

Emerging Trends & Opportunities in the IoT

Albeit the fact that work is in progress pertaining to sensor development and big data analytics, it is far more important that fundamental research is initiated in areas like environmental engineering, prediction of natural calamities in disaster prone areas and post calamity damage control. Manufacturing will become more efficient with better supply chain management; healthcare will be impacted by increased patient surveillance; agriculture will be enhanced by monitoring crops and controlling growing conditions; our environmental data will be captured and controlled to decrease air pollution; and water leakages will be detected using sensor devices, to name a few.

Security in the current Internet of Things is not as good at it ought to be. This thesis shows some glaring flaws in existing products, which is often created because of oversight from the developers, as the constraints existing in IoT requires a more thorough thought-process than is normal in desktop computing. Due to limited power, bandwidth and processing power, everything needs to get stripped down to the bare minimum, while still maintaining good security properties.

Summary

Security is an oversight in many projects. Using examples from previous research, and conducting unique analysis on existing products, it is shown that many developers more or less ignores everything related to security (BMW, HomeEasy, Sonos), or creates their own cryptographic algorithms with clear flaws (Eye-Fi, OSGP smartgrid). To ensure that the future of IoT is secure, this thesis aims to make developers think about the limitations that exists, and provide solutions to the problems that will occur
when designing a device for the Internet of Things. Securing the Internet of Things is important to consumers. Through previous research it is shown exactly how devastating not focusing on the security of IoT devices can be, with the majority of consumers (62
%) “feeling completely violated and extremely angry to the point where I would take action.”. Close to half (48%) of all consumers would hold the manufacturer responsible if a flaw was to be found in the system, showing the obvious economical risks taken by not securing a device properly. Some of the topics of challenges presented are common in information security, but poses new challenges because of the unique constraints. Securing an IT system requires confidentiality, integrity, and authorization. Where this usually is handled by libraries like OpenSSL and using TLS into desktop computers, deciding on an encryption, authentication and signature algorithm is not as easy as calling a different method. The limited power, bandwidth and processing capabilities will require a thorough thought process to decide how to both efficiently, and effectively secure a device.

The other challenges are more specific to the Internet of Things. In regular desktop computing, an advanced user interface is usually available, and physical loss of a device during use is relatively uncommon. IoT devices will on the other hand usually have a really limited user interfaces, and will often be placed in exposed areas and used in situations with high physical stress.

Security should be a consideration through the whole project. Long before the first prototype PCB-design is sent

to the factory, key decisions on security should have been decided. These include how keys should be distributed to each device, if hardware-acceleration should be used, how updates can be handled, if A public key infrastructure is a viable solution for the device, what type of cryptographic algorithms should be used, etc.

Future Work

The Internet of Things is a relatively new concept in terms of optimized protocols and security, and thus there is a lot of work for the future. The most pressing issue is simplifying the use of security in IoT for developers without thorough knowledge of IT security. Designing and implementing security in protocols that is simple for developers to use is a must for the future of IoT. Speed and cryptographic strength is especially important in the Internet of Things.

As devices in the Internet of Things are constrained devices, efficient implementations of cryptographic algorithms is especially important to keep the cryptographic strength at an acceptable level.

The Internet of Things is an ever-changing area that will continue to change in the future. While the recommendations in this thesis are made with assumptions for the future of IoT, and encompassing many different solutions, one will have to re-examine the recommendations with large changes in the market. But as many cryptographic properties will always be existing and important, most of the recommendations will be the same for all foreseeable future.

4. CONCLUSION

Internet of Things (IoT) is the future of the world order and western countries have already initiated various plans and programs in this regard. As usual India is lagging behind them and now is the time for the country to start thinking in this direction.

This is an act of togetherness and integrity and the central and state governments should take note of this and provide plans and facilities to various governmental and private industries. Common man should also be educated accordingly.

ACKNOWLEDGEMENT

The authors acknowledge support extended by My Guide Dr. A. M. Sudhakara, Director, CIST, University of Mysore, Mysore and

Messer‟ s Pentagram Research Centre Private Limited, Hyderabad for their extensive technical support in making this paper worth presenting as a contributed paper.

REFERENCES:

[1] Sophie Curtis, Director of Marketing at RE•WORK
[2] http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf.
[3] Draft Policy on Internet of Things, Department of Electronics & Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India
[4] http://siliconangle.com/blog/2014/03/21/most-influential-countries-for-the-internet-of-things/ by Mellisa Tolentino | Mar 21, 2014 |
[5] https://arc.applause.com/2015/12/02/internet-of-things-growth-developing-countries/
[6] ZDNet Korea (zdnet.co.kr)
[7] www.aponline.gov.in/apportal/Downloads/2016ITC_M S3.pdf
[8] Rolf H. Weber, Romana Weber - Internet of Things.pdf by Springer Publications Security in Internet of Things Systems by Christian Dancke Tuen, Norwegian University of Science and Technology.
[9] The Internet of Things: An Overview by Karen Rose, Scott Eldridge, Lyman Chapin