ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

The Era of Internet of Thing's (IOT) and Its Challenges

Rohit P. Shirke, Manish U.Singh
Department of MCA, ASM's IMCOST
Mumbai, Thane-400604
University of Mumbai

Abstract- Rapid advancement in the field of technology has always put forwarded solution that made our life easier; it has left a strong impact on our lives changing the way we communicate, the way we work and the way we live. A small result of this evolution is, devices around us are also getting smarter and are getting more & more connected. Internet of thing's (IoT) originated from the human efforts to make every device around us connected. IoT is an approach that focuses on creating a smart network (environment) of connected devices that understands us & allows exchange of information with virtually any devices over internet anywhere at any time so as to deliver quality services that we never imagined before. In order to deliver such services IoT talks about giving more control on our lives to these devices. When such a smart network exists especially, which is deeply integrated with human lives we must have strong policies, procedures and standards in place which governs how these devices operates & at what extent they have controls on our lives. Ensuring security of this network is going to be a big challenge as breach to this network will result into many safety and security issues. This paper discusses some of the challenges that are likely to be faced before we move ahead, how some existing solutions can be utilized to tackle some problems, how fundamental concepts like PbD (Privacy by Design) can be helpful and more.

Keywords— IOT, Internet of things, Security, Privacy, Internet, PbD (Privacy by Design), M2M (Machine to Machine)

INTRODUCTION

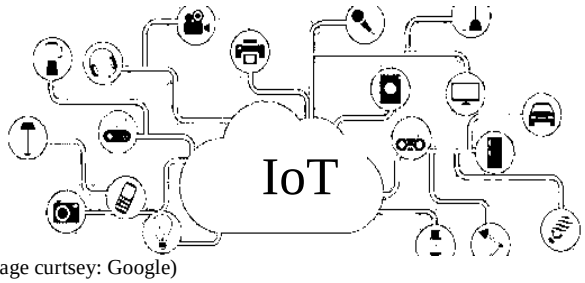
Iot came to reality as a future where a multitude of intelligent components (devices) collect and share data over global network (internet). This concept was termed as "Internet of Things" by British technology researcher Kevin Ashton in 1999.The upside is that we are able to do the things we never imagined before. But as with every good thing, there's a downside to IoT: It has brought many challenges that we never thought off, alternatively it is becoming an increasingly attractive target for cybercriminals. More connected devices mean more attack vectors and more possibilities for hackers to target us unless we move fast to address this rising security concern, else we'll soon be facing an inevitable disaster.

1. IoT& challenges:

1.1: IoT and security of local devices

IoT is growing at a dangerously fast pace, and researchers estimate that by 2020, the number of active wireless connected devices will exceed 40 billion. More devices mean more number of points of contact, means more Number of points of failures. Some of the more frightening vulnerabilities found on IoT devices have brought IoT security further up the stack of issues that need to be addressed quickly. In another development, it was proven that Internet-connected home appliances can be compromised, as well, and hackers can carry out any number of malicious activities, including taking control of the entertainment system, unlocking the doors or even shutting down the car in motion. Wearable's also can become a source of threat to our privacy, as Hackers can use the motion sensors embedded in smart watches to steal information we are typing, or they can gather health data from smart watch apps or health tracker devices we might be using. Some of the most worrisome cases of IoT hacks involve medical devices and can have detrimental perhaps fatal consequences on patients' health.

Fig: IoT Infrastructure.



(Image curtsey: Google)

IoT introduces a host of new devices, network traffic, and protocols. Large organizations are still figuring out

the security implications of mobile devices, cloud applications, and BYOD policies. These initiatives will look like child's play for now compared with the scale, capacity, and variability of IoT. As IoT devices grow and proliferate, they will require to ensure the devices that collect data and devices that perform analysis on this data must be secure from inside and outside boundaries of the IT system. Furthermore, IoT is going to be an extremely complex environment with a multitude of raw devices and communications protocols that security experts have little or no experience with.

1.2: IoT makes the malware attack surface wider and deeper

In a survey it was found that nearly 40% of security professionals claim that network security is more difficult because malware can easily bypass traditional network security barriers (i.e., firewalls, IDS/IPS, etc.).Today ensuring the security of thousands of computer devices connected to internet worldwide is turning out as a major issue and there are many incidence in past that are enough evident to prove how worst the things can go, now imagine how the situation will be when billions of devices will be connected together to internet. The situation will be more tedious when we need to avoid the proliferation of malware on such huge network.This is not just the only issue that needs attention additionally this situation will be further impacted; For example, IoT powered devices will run small embedded operating systems and applications with little or no malware detection/prevention capabilities. This makes it even easier for cyber criminals to compromise the network.A single compromised device will open the door of millions of devices worldwide to attackers and no matter how much precautions taken for safety of mainframe computers, it will be of no use. Practically, A single vulnerable industrial controller, sensor, or thermostat could be compromised and then act as a beachhead for further malware proliferation and these are not just some worrisome concepts but many Critical vulnerabilities have been found in a wide range of IoT ready Devices, which could be leveraged by attackers to carry out a number of nefarious activities as some includes monitoring live feeds, changing camera settings and authorizing other users to remotely view and control the monitor.

1.3: Physical and physiological risks:

IoT not just introduces privacy and security related risks but more frightening physical and physiological risks as it is more about bringing machines closure to humans. IoT introduces some really worrisome risks as organizations Monitor and take actions based on IoT infrastructure. For example, a cyber-adversary could, Use IoT to shut down transportation systems, compromise automobiles, destroy industrial components, or alter medical devices. These threats aren't theoretical some real-world examples includes: Stuxnet was used to disrupt atomic research in Iran; researchers demonstrated how to hack an Insulin pump at the 2013 Black Hat security conference; and hackers have proven that it is possible to take control of critical automobile mechanisms, including steering and brakes controls. one of the most recent example includes a recent experiments of IoT with driverless car. Researchers has shown taking controls of a vehicle in motion in mid-way by taking control of critical engine and breaking system of vehicle imagine how worst the thing would have gone if it was a real scenario with car being a public transport vehicle or a personal vehicle stopped on a busy highway.

1.4: Neutrality principle in IoT

IoT not just brings security and privacy related concerns but some challenges that are related to conceptual implementation of IoT one of them being "Neutrality". Neutrality means ensuring transparency and lack of specific actions that promote one actor or perspective over others. In the development of the IoT, there are a number of things to which neutrality principle should apply including forming, operating, operating within and the evolution of the IoT. Neutrality has an impact in terms of privacy and data protection as some specific actions can lead to exposure to personal data (e.g. Packet sniffing). The formation of IoT must be done on the basis of some solid rules/standards as standards have an important role to play in forming the IoT and it is also essential to ensure that all actors to have an equal access to the standards making process for the IoT. Considering the today's situation where multiple technologies are separated by their own environment as a result of multiple standards. As everyone among them will dive into IoT there will of course be many simultaneous standards making activities, distributed not only by technologies and applications but also geographically. Coordination of standards development, without constraining freedom to innovate, will promote efficient development of IoT infrastructure and consequently applications, services and devices. To ensure that IoT is not monetized by some players in the markets a similar approach of development to the manner in which global coordination of Machine to machine (M2M) standard being considered within the Global System for

communication (GSC) has to be applied for further IoT development.

1.5: IoT Applications network autonomy and security

Ensuring the autonomy and along with the security of the devices is another challenge that needs to be tackled. The need for ensuring network autonomy and security can be different, and it will depend on considerations of the impact of dependence on a service or infrastructure that is temporarily not available or the compromised security. Whether or not an application is the extension of a physical infrastructure is therefore only a secondary consideration. The Internet of Things involves an increasing number of smart interconnected devices and sensors (e.g. cameras, biometric and medical sensors) that are often non-intrusive, transparent and invisible. For such systems or devices the autonomy is something that never gets accounted as the communication among these devices as well as with related services, is expected to happen anytime, anywhere to serve its purpose also, the communication among these devices frequently done in a wireless, autonomic and ad-hoc manner, ensuring a fluid and decentralized communication among them being the needs of the systems design consequently lead to turning the security barriers in IoT to become much thinner. It also becomes much simpler to search, collect, process, and store personal information and peep into people's privacy. Finally, concern is rising that control over personal information is increasingly getting out of the hands of peoples. Obviously, this goes beyond the risks people are currently used with, leading to new security requirements and to a general requirement / obligation of transparency and accountability when delivering IoT services. In general, applications with and without extensions to the physical infrastructure can have needs for autonomous operations and strong security implementations. A database of nuclear secrets, a hospital patient monitoring system and computer-controlled brakes in a car may all require significant care in their own respects. As IoT will grow it is perhaps likely that advances in machine-to-machine networking, there will be more applications that have security or autonomy requirements. This is natural, as IT technology expands to additional application areas. The requirements from applications do differ, however, and there should be no forcing of all applications to comply with the toughest requirements providing that they are enough secure to the identified risks. As IoT is based on Machine to Machine Communication, Autonomous operation will be needed in many applications. It can consist of autonomous operation of individual home appliances or of self-organizing networks. It is important to ensure that any individual device or even the entire network is not dependent on some remote service that may become unavailable at times. Naturally there are also many applications where the ability to communicate outside a single network is crucial, and such applications cannot be entirely independent of the rest of the worldwide networks. Issues with security, configuration, and autonomous operation should be addressed through the normal technical mechanisms and proper network design. Some areas, such as autonomous operation, are still active research domains and the solutions for specific situations are evolving.

1.6: Ensuring Fair Spectrum access for IoT (Lets just not monetize IoT)

The IoT will have a very wide range of devices acting as data sources and a very wide range of services acting as source for IoT data. At the heart of the IoT is the principle of connecting mundane everyday devices – sensors & actuators, monitoring devices and appliances – and mining the flows of data they produce to synthesize information which fuels innovative services that leads to a better future. The issue of fair access to the infrastructure requires connecting technologies and implementing policies to ensure that fair access is enabled in all aspects of the IoT infrastructure. Connectivity technologies may be a function of the type of device and will operate over many different media e.g. fixed and mobile communications systems or wireless communication, especially short-range wireless, technologies. For optimum development of the IoT, the resources necessary for connectivity must be unbiased. Communications technologies for both fixed and mobile devices should enable reliable connectivity at low cost for even the simplest of devices. A chosen spectrum for IoT devices depends on the application but must satisfy the demands of the propagation environment, provide sufficient bandwidth for the application and the number of devices requiring service; it requires the needs to be harmonized to allow large market development and support for applications across the globe. A simple example is Asia is currently at a disadvantage in regards to some other regions because of the lack of a 900MHz IS&M band (because of cellular deployments) which is available in countries like USA and Australia. For a

future ready IoT we need a solid and globally acceptable infrastructure that is not biased and based on fair sharing principles.

2. Moving from IoT to Secure IoT

2.1: Taking Primary Precaution Measures

Today to ensure a safe and secure IoT environment we must start taking the steps some initial steps can be ensuring the gateways to this "information globe" to secure ,we must ensure the safety of gateways that connect IoT devices to company and manufacturer networks as well as the every small devices being part of the system. IoT devices are always connected and always on in contrast to human-controlled devices, they go through a one-time authentication process, which can make them perfect sources of infiltration into private networks. Therefore, more security needs to be implemented on these gateways to improve the overall security of the system. There also must be a sound plan for installing new security updates on IoT devices. Each consumer will likely soon own hundreds of inter-connected devices. The idea of manually installing updates on so many devices is matter of discussion and beyond the scope, also having them automatically pushed by manufacturers is also a risky business. Proper safeguards must be put in place to prevent updating interfaces from becoming security holes themselves.

2.2: Industries & Secure IoT

The silver lining to IoT security is that, previously ignored has now become an issue of high concern. Now security firms and manufacturers are joining hands to help secure the IoT world before it spins out of control. Several efforts are being led to tackle major disasters before they come to reality. A precursor to them being Few real life incidents like the Jeep Cherokee hack, which automaker Fiat scrambled with and to have the problem fixed, quickly issued a safety recall for 1.4 million cars and trucks in U.S. to install a security update patch. The whole episode also served as a wakeup call for the entire IoT industry. Simple solution as enable advanced digital security and life-cycle management via encryption of data and access-control limitation to sensitive information. It's not about ensuring the safety of systems but Also of concern are huge repositories where IoT data is being stored, which can become attractive targets for corporate hackers and industrial spies who rely on big data to make profits. In the wake of massive data leaks and data theft cases we've seen in recent years, industry is putting more effort to secure IoT-related data to ensure the privacy of consumers and the functionality of businesses and corporations. Companies like Microsoft are also entering the fray, and has started promising solutions such as Bit Locker encryption to the Windows Os' introduced by Microsoft and Secure Boot technology, for IoT devices and platforms such as the Raspberry Pi. This can be crucial to secure on-device data. Simple solutions as secure boot developed by members of the PC industry to help make sure that your PC boots using only software that is trusted by the PC manufacturer can be of great help as Its Implementation can prevent device hijacking.

2.3: Securing the data mountains

Today millions of Post shared on social networking and other blogging& information delivery sites which collect millions of tons of data daily, this information will soon be integrated with IoT devices, surely analysis to this information will help to deliver better services E.g. Face book's graph search technology can actually figure out a person from a group picture based on Facial Coordinates but such implementations also rises serious security concerns over privacy. If some further implementation ask to incorporate home appliances to this analysis then the results are going to Also of concern are huge repositories where IoT data is being stored, which can become attractive targets for corporate hackers and industrial spies who rely on big data to make profits. In the wake of massive data breaches and data theft cases we've seen in recent years, more effort needs to be made to secure IoT-related data to ensure the privacy of consumers and the functionality of businesses and corporations. With a surge of new devices comes a virtual explosion of data. According to IDC , from 2005 to 2020 the digital universe will grow by a factor of 300 from 130 Exabyte's to more than 5,200 gigabytes for every man, woman, and child in 2020. Between now until 2020, the digital universe will double every two years. Protecting the IoT, data, and privacy is a shared responsibility. Industry collaboration but not competition will accelerate broader ecosystem support by aligning current computing-industry standards with the world's most widely adopted security ecosystem for a secure environment of future ready system that deliver services as we never imagined before.

2.4: Device Certificates for Authentication

Device authentication so far has proven to be a strong and effective approach since its inception even after some of the past obligation of breaches. The approach simply suggests to Authenticate IoT devices and encrypts data transmitted throughout IoT systems and networks. Additionally a great advantage of this approach is it is well tested and proven solution in recent years and the infrastructure needed is already present so very little efforts are needed to align with the current needs of IoT.

Why to utilize existing PKI solution?

- PKI is the trusted security solution for protecting system, consumer and personal data.
- PKI provides the highest level of authentication and encryption to ensure data integrity for IoT devices.
- PKI systems provide the components required to manage the provisioning and management process of device certificates and keys throughout a device's lifecycle.
- PKI security allows for a variety of deployment approaches and this makes PKI the most flexible solution for securing IoT devices.
- PKI's existing infrastructure of identity vetting completed by publicly trusted and audited Certificate Authorities provides the necessary foundation for IoT organization authentication.

Simple solutions as Ensuring the Roots of Trust and Code Protection will allow us to be assured about the Systems safety, it suggest to simply verify that all code running on each IoT device is authorized for that device, and protected by a strong Root of Trust.

2.5: Solving problem at Conceptual level

2.5.1 Ensuring a Fair Utilization of resources

To prevent monetizing of IoT by industry and ensuring a fair utilization few fair solutions are:

- Mandate adequate spectrum resources for device connectivity technology.
- Ensure regulations to promote equitable use of the spectrum resource
- Satisfy the operating requirements of IoT devices and applications
- Harmonize these resources across global regions as far as possible to promote technology interoperability leading to global scale efficiencies.

Supportive spectrum policies will stimulate innovation via investment in new device communications technologies, improved efficiency in medium use and increased reliability in communications leading to reduced device power consumption, increased device operational lifetime and reduction in total costs. Continuous data sensing devices will be the powerhouse providing raw data to the IoT for myriad data mining applications, transportation medical, environmental.As there will be many different – as yet unknown - technologies and applications that will connect to the IoT. This may be described by a layered model. In order to ensure a maximum level of interoperability, it may be necessary to define the interoperability requirements both from a communication and from a data perspective at one or more of these levels based on internationally agreed protocols. From a public policy perspective ensuring a minimum level of interoperability may be considered relevant to Promote competition to avoid that simple measure can be followed as:

Self-regulation: Simply allowing the approach to become de-facto standard can be helpful. The advantage of self-regulation is that the market will find the optimum. Stakeholders, whether or not assembled in international standardization bodies, will agree on the levels of interoperability and protocols. However, a potential disadvantage of this policy option may be the rice of a large number of competing, incompatible or incomplete implementations, none of which will gain sufficient critical mass in the short to medium term.

Using soft law approach: The advantage of soft law approach is that it will clarify what are the requirements for interoperability to be seen as desirable from IoT architecture. it can be helpful as it will get the guidance from current developments. Potential disadvantages of this policy option may be that –conflict of interest of market may affect further developments. Also for this policy option it is required that there is clarity which requirements to the IoT architecture/protocols are already covered by existing solutions.

Co-regulation law: An another approach can be co-regulation law, where the regulator body/ governments set high-level objectives to be obtained and leave's it to recognized bodies in the field to bring out the best solution among them.

The Binding law: The binding law is based on prescribing the architecture and protocols through regulation/directive. But the risk of approach is that it will stifle innovation: At this moment it is not possible to predict which technologies and applications will be part of the internet of things. A further risk of prescribing interoperability at any level of detail is that it

may disturb the working of the market and that there will be insufficient (commercial) incentive to develop and introduce new technology.

2.5.2. Implementing Security at Design Level

Privacy by Design (PbD):

(Privacy by Design) The concept originated from a report on "Privacy-enhancing technologies" by team of the Information and Privacy Commissioner of Ontario, the Netherlands Organization for Applied Scientific Research, the Dutch Data Protection Authority, and Canada in 1995. It is a process focused on user control and freedom of choice regarding how and when to share personal data Privacy by design is an approach that focuses on implantation of security at the design level. It argues to consider security from the point of view of human values. The theme talks about protecting the human values getting compromised in M2M communication. It simply suggest some principle, simply adhering to these principle throughout the development process of a system for IoT will bring a level of safety in System. The Principles are as follows

Principles:

- **Being Proactive not reactive for security**: The principle of being Proactive simply suggest, consider implementing security at the core rather than at last. Make the system secure by its design. Why not to ensure the system to be ready to handle all likely to be security related challenges.
- **Ensure Privacy as core**: The principle of Privacy suggest, ensure privacy of the user as the central approach to design. As the IoT coming to reality to deliver service to feed our need then they must respect our privacy first.
- **Privacy embedded into design of Systems**-it asks to consider privacy as integrated component of system design rather than a separate discipline. Simply designing the system and then later thinking about how to add security measures should be avoided.
- **Implement full functionality**: Using Security as a base model for development should not result into preventing further improvements in system. Being implementing the system with likely features and later improvising it would leave loopholes in already implemented safety solutions to ensure the security of that system.
- **End-to-end security** – Ensure the security to data right from the moment data enter into system to moment data leaves the system. Let's just not allow the unsecured data freely move along the transport lines. Encryption is something that will serve the purpose.
- **Make sure System is truly transparency** – the privacy implemented system must not implement any methodologies that any how result into preventing the transparency of the system.
- **User privacy at the top**– The user should be central to designing process for the system. Ensuring any changes made to system must not result into breach to security and privacy of the user and user data.

Ares which started to include the principle of Privacy by Design includes surveillance cameras in mass transit systems, biometrics used in casinos and gaming facilities, smart meters and smart grids, mobile communications, near-field Communications, RFID and sensor technologies, redesigning ID geo-location, remote healthcare, and big data and analytics. Even though the Privacy by Design Concept look simple and yet applicable, researchers are also working on the application/ Implementation perspective of these principles. As we all are aware about no solution to a problem can be concluded as a final solution but being remaining prepared for an expected challenge with a solution is always is safe play. PbD may appear to be very theoretical today but as we move ahead toward the Era of IoT no one knows it might become an integral concept for the development of future IoT ready Systems.

Conclusions

The Internet of Things is closer to being implemented than the average person would think. Most of the necessary technological advances needed for it have already been in market, and some manufacturers and agencies have already begun implementing a small-scale version of it. The true challenges about IoT are the impact it will have on the legal, ethical, security and social fields. Workers could potentially abuse it, hackers could potentially access it, corporations may not want to share their data, and individual people may not like the complete absence of privacy. For these reasons, the Internet of Things may very well be pushed back longer than it truly needs to be unless sound solutions are in place to tackle challenges it brings.

Acknowledgement

We thank our colleagues from **IMCOST** who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.
We thank our director Prof. Ramesh Mahadik and our guide mentor Miss. Sheeba Jamesfor their valuable guidance and support throughout the entire documentations.

References

[1] Denis Kozlov, JariVeijalainen, Yasir Ali - Security and privacy threats in IoT (2012)
[2] Springer New York 20th Tyrrhenian Workshop on Digital Communications (2010)
[3] Wikipedia (Privacy By Design)Data Protection In Internet Of Things Era (Steven Kester and Stephen Pattison)
[4] A.Cavoukian. (2011, January) Privacy by Design: The 7 Foundational Principles, Revised Version.
[5] IoT6 D2.2, "Distributed IPv6-based Security, Privacy, Authentication and QoS".
[6] Neisse, R.; Doerr, J., "Model-based specification and refinement of usage control policies," Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on , vol., no., pp.169,176, 10-12 July 2013, doi: 10.1109/PST.2013.6596051.
[7] E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryp- toschemes for data concealment in wireless sensor networks," in *Proc. of IEEE ICC'06*. IEEE, September 2006, pp. 2288–2295.
[8] G. Yajun, W. Yulin, "Establishing Trust Relationship in Mobile Ad-Hoc Network," Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on , vol., no., pp.1562-1564, 21-25 Sept. 2007.
[9] Uckelman, D., Harrison, M., and Michahelles, F. (eds.) 2011. Architecting the Internet of Things. Springer-Verlag Berlin Heidelberg.
[10] LeneSørensen and Knud Erik Skouby (eds.), "User scenarios 2020 – a worldwide wireless future", OUTLOOK - Visions and research directions for the Wireless World, Wireless World Research Forum, No4, July 2009.
[11] Ramachandran, A., Singh, L., Porter, E. and Nagle, F., 'Exploring Re-identification Risks in Public Domains', Proceedings of the Tenth Annual International Conference on Privacy, Security and Trust (PST), 2012, pp.35–42, 2012.
[12] EDPS (European Data Protection Supervisor). 2010. Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design). OJ C 280, 16.10.2010.

1. **Mr. Rohit Pandurang Shirke- Currently pursuing Master of Computer Application Degree (Third Year) at ASM's Institute of Management & Computer Studies (IMCOST), Thane, Mumbai-400604**
2. **Mr. Manish Upendra Singh- Currently pursuing Master of Computer Application Degree (Third Year) at ASM's Institute of Management & Computer Studies (IMCOST), Thane, Mumbai-400604**