Internet of Things, Challenges and Security issues: A Review

Aashaq Hussain Najar[1] ,Dhajvir Singh Rai[2], Saleem Yousuf Bhat[3]
[123]*Department of Computer Science And Engineering*
[123]*Uttarakhand Techinical University, PremNagar , Sudhowala, Dehradun, Uttarakhand ,India*

Abstract- The Internet of things is an emerging technology across the world, which helps to connect sensors, vehicles, hospitals, industries and consumers through internet connectivity, this type of architecture leads to smart cities, homes, agriculture and world and consists of a complex architecture because of the larger number of devices, link layer technology and services that are involved in the IoT system. However, security in IoT is most important parameter. Here we give an overview of the architecture of IoT with the help of smart world. Later, we will discuss the security challenges in IoT followed by the security measures in IoT and these all challenges could be research direction for future work in security for IoT.

Keywords- IOT Challenges, IOT Security issues, physical sensor connection, Security Policy Enforcement, IOT architecture.

I. INTRODUCTION

IoT mainly focuses of linking of various kinds of devices to the internet and even exchanges its data and feature helps us to monitor and control of real world and changes our daily lifestyle which was never available before, and with such a massive amount of devices, if we don't have set and organize security features on them properly, we will face unexperienced challenges on security issues[1] [6]. In order to overcome these security issues, we propose the on-demand security configuration technique that can configure required security functions and reorganize them without recreating device images[7] [10]. With the help of this approach, if there is a change on this security service, we can substitute the old modules for new ones without regenerating device image. Internet of things as the name suggests, is the connectivity of everyday devices with each other[1] [4]. With the advancement in technology numerous devices are using sensors, actuators, embedded computing and cloud computing[8]. This has enabled communication between devices. To put it simply, the Internet of Things enables devices (things) to interact and co-ordinate with each other thereby reducing human intervention in basic everyday tasks. To get a better understanding of IoT consider the scenario of a smart home[9]. As soon as the alarm rings it sends a signal to the coffee maker and the toaster, which automatically start doing their jobs without any human intervention. Thus, saving time and making our everyday tasks easy, this type of device communication is the Internet of Things. The IoT enables physical objects to see, hear, think and perform jobs by having them "speak" together, to share heterogeneous devices/applications has its own set of devices as well as with related services, is expected to happen autonomic and ad-hoc manner. In addition the services consequently,

II. RELATED WORK.

The security barriers in the Internet of Things will grow in an evolutionary contributions, rather than from a grand plan[3]. Security is a majority of IoT accessed by a third party easily. Thus there is a severe need to invade internet of things for future technology advancements [1]. Research into the IoT field is still in its early stage, and a standard definition of IoT is not yet available. IoT can be viewed from three perspectives. 1) Internet oriented 2) Things oriented 3) Semantic oriented. The first definition of Internet of Things was from a "Things oriented" perspective, where RFID tags were considered as things. It was defined as "The worldwide network of interconnected objects communication protocols". These definitions do not highlight the industrial view of IoT. Companies across the world are investing billions in the IoT to solve industrial problems (IoT). The IoT refers to industrial objects instrumented with sensors, automatically communicating over a network, without any human-to-human or human-to-computer interaction, to exchange information and take intelligent decisions with the support of advanced analytics.

III. IOT ARCHITECTURE:

The definition of things (as shown in fig.1) in IoT is very wide and includes a variety of physical elements. This network of a variety of objects can bring ample amount of challenges in developing applications and make existing challenges more difficult to tackle.

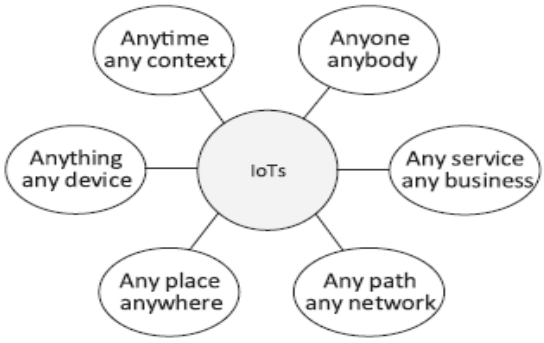

Fig.1: Definition of IoT

A middleware can offer common services for applications and ease application development by integrating heterogeneous computing and communications devices, and supporting interoperability within the diverse applications and services running on these devices. A number of operating systems have been developed to support the development of IoT middleware solutions. They reside in physical devices, and provide the necessary functionalities to enable service deployment[5]. The internet things is not a single technology, it's a concept in which most new things are connected and enabled such as street lights being networked and things like embedded sensors, image recognition functionality, augmented reality, near field communication are integrated into situational decision support, asset management and new services. These bring many business opportunities and add to the complexity of IoT [1].

Nowadays tremendous number of devices connected to the Internet and we can easily access and utilize one of them from personal gadgets to home appliances and even public services. According to estimation of surveys, by the year of 2020, we would be connected between 20 and 50 billion devices [2]. In this environment, we will encounter unexperienced security challenge if we don't prepare and configure proper security features in a robust way. Therefore, there are some research efforts to leverage these challenges on OS for IoT , configuration management and security updates [2]. According to surveys, lacking of security concern, many of them are very vulnerable and easily exploitable and even some are connectable through the Internet having several vulnerabilities [2]. For example, peeping at sleeping babies without authentication mechanisms is possible. In this paper we propose the on-demand security configuration technique that we can configure required security functions and reorganize them without recreating device image. We suggest security profile for constructing security functions and configuration map of them for reorganizing theirs combination of the device map without regenerating the device image. As we determine the security modules analyzing requests from the device's security profile, we can select appropriate these modules required for device's security service and create configuration map used for re-configuring them. With the help of this approach, if there is a change on this security service, we can substitute the old modules for new ones without regenerating device image.

IV. SECURITY THREATS ASSOCIATED WITH THE INTERNET OF THINGS

IoT security issues mainly consist of and are easily divided into two areas: virtual and physical threats. The physical threats increase as the things become more and more de-perimeterised. The virtual threats are closely coupled with the threats in any other IT-environment today and mainly consist of obtaining data and information (an asset) or taking control of the device itself. Additionally, applying the methods used for securing an IoT-environment are limited as many devices are constrained when it comes to performance and power. Since this thesis mainly concerns the concept of Information Security, the starting point of the threat analysis has been the asset itself, which is information (data). Nor has a threat agent been identified since this analysis considers more general threats rather than specific ones. By looking at the different points of attack it is easier to identify which threats are connected to IoT and also what vulnerabilities needs to be countered in order to secure each and every part in an IoT environment. The three identified points of attack are: the communication that occur between objects (IoT devices), the IoT devices themselves, and in the third case when a gateway is used, the central collection point of several sensors or a controller for several actuators. The Jericho Forum is a series of publication guides from The Open Group that defines principles when planning for a de-perimeterised future, which fits very well to the concept of IoT. De-parameterization includes protecting an organization's systems and data with a mixture of "secure" protocols, syst**e**ms, and data-level authentication with the absence of a specific boundary between the organization itself and the outside world. In relation to IoT this describes a scenario when an organization for example deploys weather sensors that collects information about wind, rainfall, etc. and send this information to the company's server or in some cases to a cloud to be retrieved later. Figure 2 illustrates such an environment.

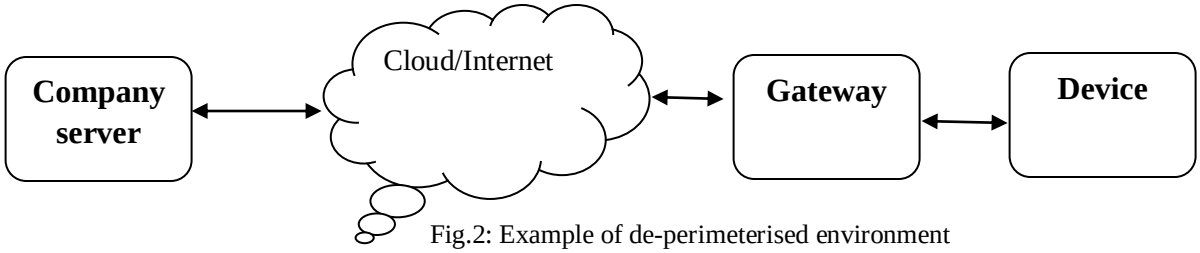

Fig.2: Example of de-perimeterised environment

To obtain Information Security in IoT it is required that systems and data are capable of protecting themselves *without* relying on basic network protection, such as firewalls. Firewalls effectively work as a perimeter to secure company resources from intruders, which in most cases are irrelevant for IoT. To simplify the deployment of more "things", these things

must be able to enforce their own security policy levels (for applications, network access, devices, and individuals) even in an un-trusted environment or network. Another requirement is that the security mechanisms are simple, scalable, and easy to manage which simplifies the determination of their limitations since not all solutions fit in all environments.

The various techniques required to embrace the de-perimeterised architecture are 1. Security policy enforcement system 2. Identity and rights management systems 3. Encryption of data

V. CONCLUSIONS

In this paper an attempt is made to highlight the various challenges in internet of things scenario considering the various application domains. We discussed the security issues associated with the smart home using IOT, vehicular technology, virtual reality etc. and carried out various security challenges to safeguard the important data obtained from number of internet connected smart sensors. The various security issues discussed in this work helps in proper sharing of information over physical connections without data interception. These techniques also helps in maintaining data integrity and breach less operation.

VI. REFERENCES

[1]. S.Vashi, J.Ram, J.Modi, S.Verma, Dr.C.Prakash ;"*Internet of Things",*International Confrence on IoT in Social, Mobile, Analyticas abd Cloud;pg-492-96;2017.

[2]. Mario Frustaci, Pasquale Pace, Gianluca Aloi ;"*Securing the IoT World: Issues and Prespectives*",IEEE Conference on standards for Communication and Networking(CSNS);pg-246-251;2017.

[3]. S.sridhar, Dr.S.Smys ;"*Intelligent Security framework for IoT Devices*",International Conference on Inventive systems and Control(ICISC);pg-1-5;2017.

[4]. S.N.Swamy, Prof. D.Jadhav, Proif. N. Kulkarni ;" *Security Threats in the Application layer in IoT Applications*", International Conference on I-SMAC;pg-477-80;2017.

[5]. S.Kumar K,S.Sahoo,A.Mahapatra, A.K.Swain,K.K.Mahapatra ;"*Security Enhancements to System on Chip Devices for IoT Preception Layer*",IEEE International Symposium on Nanoelectronic and information Systems;"pg-151-156;2017.

[6]. Shinsuke Tanaka, Kenzaburo Fujishim, Nodoka Mimura, Dr. Eng., Tetsuya Ohashi, Mayuko Tanaka;" *IoT System Security Issues and Solution Approaches*",Conference on IoT Security;pg-359-63;2016.

[7]. S.K.B V,Gnanasekaran T;"*A Systematic Study of Security Issues in Internet –of-Things(IoT)*",International Conference on I-SMAC;"pg-107-11;2017.

[8]. L.Singh Sayana, B. Kumar Joshi*;" SECURITY ISSUES IN INTERNET OF THINGS*", UGC Sponsored National Conference on Global Challenges – Role of Sciences & Technology in Imparting their Solutions;pg-1-8;2016.

[9]. D.Geneiatakis, I.Kounelis,R.Neisse, I.Nai-Fovino,G.Steri,G.Baldini;"*Security and Privacy Issues for an IoT based Smart Home"*,MIPRO Conference;pg-1292-97;2017.

[10]. Boheung Chung, Jeongyeo, and Youngsung Jeon ;"*On Demand Security Configuration for IoT Devices"*, ICTC,IEEE Conference;pg-1082-84;2016.

[11]. Nicolas Saklavos, I.D.Zaharakis*;" Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations",UGC Conference;pg-1-4;2016.*