RESEARCH ARTICLE OPEN ACCESS

Internet of Things: Security Challenges and Solutions

Aravindha[1], Benson[2], Isaac Kevin[3]
[1,2,3](1st Year BCA, St Joseph's Evening College, Bangalore)

Abstract:

Internet of Things is simply the network of gadgets that can communicate with other devices in real time sharing some useful data. These devices can take the form of electronics, vehicles, home appliances, sensors etc... network connectivity enables these devices to communicate with each over a local network or exposed to the giant internet. Technology giants are in a race to become leading players of this revolutionary concept. This research paper explores and scrutinizes certain aspects on the security.

Keywords **— IoT, Internet of Things, IoT Issues, Security, Business Model, Solution**

I. INTRODUCTION

In this paper, the definition, statistics, predictions, current issues and security are introduced, and possible business models that can solve security issues. This study was conducted to analyse, scrutinize and possible improvements on the current business model and thereby expecting this study to contribute to the academic circles and related industries.

This applies to most of the Internet connected device, however, the paper focuses on security measures related to IoT. It's about the end to end processing aspects of the internet, where the features of application such as security are handled by end nodes of the network, client and server hardware. Security mechanisms, such as patching and updating which are considered at the manufacturing design rather than after device have been focused as well.

This paper is for an educated lay audience. The recommendations in this paper are for implementations by manufactures of IoT products, however they are also designed to be readable by nontechnical but well-educated lawmakers, corporate and governmental policy makers and participants in standard setting bodies.

II. IOT DEFINITION AND SECURITY PRINCIPLES

IoT or Internet of Things is simply a network of connected devices that can communicate by gathering and sharing useful data through sensors in real time. [1]

Figure 1: *IoT security chain for data protection.*

III. PREDICTION

In 2015 there were around 15.41 billion IoT devices which has grown to a whopping 20.35 billion in 2017. This number is expected to grow rapidly than ever. Starting from 2017 IoT business is projected to be worth more than 1 billion dollars. The following graph show the predictions for 2025 from 2017 consecutively. [2]

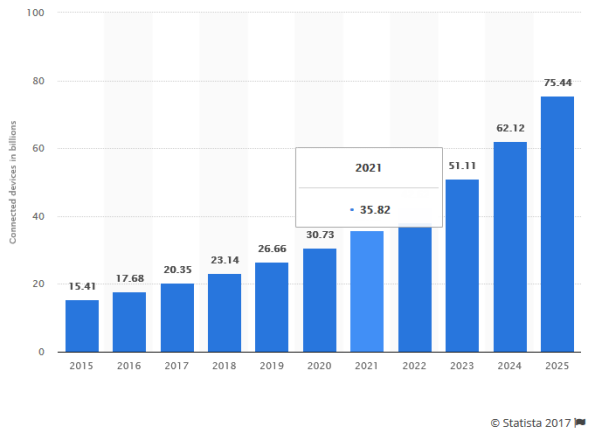

Figure 2: *IoT predictions in coming years.(Number of IoT devices in billions)*

IV. SECURITY

Security in information technology is the process of restricting unauthorized access to a hardware or software.

1. Are IoT devices secure?

The internet of the consists of many devices from small to large and from simple to complex. All of the devices are expanding and are connected to the internet, these devices are very different from your standard PC's or other consumer devices. Some of the devices are programmed specifically to perform a given task and many of the use operating systems like VxWorks,

MQX or INTEGRITY, or a stripped-down version of Linux. New software's to be installed on such devices need a specialized upgrading process or it is simply not supported. [3]

2. Current Issues in IoT

Security features is the major concern in IoT devices, there are many produces produced and sold with no basic security which resulted in serious harm to the consumers, both economic and otherwise, to general public. One such example includes the DVRs and IP cameras now recalled by Xiong Mai Technologies. As IoT devices snowballs out of control the harm caused may be even more worse in the future. [4]

Cost or benefits are not evaluated by corporate or individual consumers of IoT during the purchase properly, perhaps more expensive properly secured devices. If in case the danger caused by the devices does not affect the sellers or purchasers of the devices, but only the parties then there may be no worry about the device security for sellers or purchasers.

3. Security in IoT

Security in IoT is one of the major concerns in the current trend due to wide variety of devices that are versatile. Implementing security for wide range of devices is a tedious task. Security is a phenomenon that is inversely proportional to number of devices. I.e. more number of devices means less security.

Earlier we just had very few devices such as computers and mobiles to secure, now that we are seeing a world with wide variety of devices that can connect to internet such as television, vehicles, home appliances etc. It would be much more difficult to secure several of these devices until the manufacturer has implemented rock solid security to these devices and consumers have knowledge of keeping these devices updated and upgraded.

Since these devices are connected to another if any one devices compromises security then it might pave way for hackers to exploit other devices. Since these devices gather our personal

information and data is exchanged with corporate giants who are well known to spy on our data. Can we trust this data on their sceptical servers?

On the other hand, we know that Technology giants are in a race to become lead players in this revolutionary concept. [5]Their main goal is to become a primary hub for this growing market. To become one such entity they obviously focus less on security. Well, you might be thinking is this true?

Yes, it is, as an example let's consider Apple s iPhone X, their latest phone that has top notch Bio Metric security through facial recognition technology which is a combination several other secure technologies. They presented it as the most secure phone in the current trend. On a second thought, it's an amazing technology we should applause for. But it has already made front pages on several news articles that it is not as secure as they thought. Wired, an online news magazine has brief post "Hackers say they've broken face id a week after iPhone X release" The hackers made use of 3D printed face masks to break into the devices. It was bit hard but it's possible.

If this is the current state of our security, Imagine the type of security that may arise soon for thousands of such devices. Are we ready for such rapid growth? [6]

V. SOLUTION

The IoT is not just a device connected to the internet, It's a complex and rapidly growing and evolving system. To find solution to certain problem we must look in big data and artificial intelligence to understand and analyse risks and come up with effective security solutions

Our main aim is to protect the public and consumers, so we must develop proper security practices which must be well defined by the technical professionals and policy makers. Due to different conditions, it is not possible to set a standard rule for IoT security.

However, we can still describe few general set of principles, security measures which are widely accepted by professionals and are necessary. These are just suggestions not that any measure is better or superior to any other.

1. HARWARE SECURITY

A. Tamper Resistant Hardware

Some IoT gadgets may work constantly unattended and not subject to the security inferred by this regular, coordinate human perception. While it is best to keep gadgets generally disengaged with the goal that only a couple of assigned people have physical access, particularly for totally unattended gadgets, so making them tamper-proof will be worthwhile. This type of endpoint solidifying can help piece potential interlopers from achieving information. It may likewise safeguard against a programmer, purchasing and after that weaponing gadgets.

The physical security of endpoints can incorporate, for instance, little basic plastic gadgets, port locks and camera covers, which bolt out USB and Ethernet ports and cover webcam. Port locks help anticipate undesirable malware coming in. Some tamper-resistive methodologies cripple the gadget when it is altered. As a best practice, secure endpoint solidifying likely infers a layered approach that expects attackers to go around an assortment of obstructions intended to ensure the gadget and its information from illegal access and utilize. [7]

B. To Perform dynamic testing

It is essential that IoT gadgets experience exhaustive testing, and set up least standard for security. Static testing isn't planned or intended to discover vulnerabilities that exist in the off-the-rack parts, for example, processors and memory into which might be a part of the generally speaking application.

2. NETWORK SECURITY

C. By Using Strong Authentication

IoT gadgets should not utilize simple to-figure username/secret code, for example, administrator/administrator. Also, these Gadgets should not utilize default credentials that are same over various gadgets and must exclude indirect accesses and troubleshoot mode settings (secret credentials created by the device's programmers) because numerous gadgets can be hacked if once speculated. [8]

Every gadget ought to have an interesting default username/secret code, maybe imprinted on its packaging, and ideally resettable by the client. Passwords ought to be enlightened enough to oppose taught speculating thus called brute force strategies.

We recommend Two-factor authentication (2FA) where ever possible, which requires a client to utilize both their code and another validation form that does not depend on client information, for example, an irregular code produced by means of SMS content informing. Context-aware authentication (CAA) is practiced for IoT application, otherwise called adaptive authentication, which utilize relevant data and machine-learning calculations to persistently assess danger of malice without bother to the client by requesting authentication. On the off chance if the hazard is high, at that point the subscriber (or hacker) would be requested a multi-factor token to keep approaching. [9]

D. By Using Strong Encryption and Secure Protocols

Regardless of whether gadget passcode is secure, communication between gadget may be hackable. There are many different protocols or conventions in the IoT, that includes Bluetooth, Wi-Fi, Z-Wave, 6LoWPAN, Thread, ZigBee, NFC, Sigfox, Neul, and Lora WAN. Depending upon the convention and on accessible figuring assets, a gadget might be pretty much ready to utilize solid encryption. Producers ought to analyse their circumstance on a case-by-case premise and utilize the most grounded encryption conceivable, ideally IPsec as well as TLS/SSL.

3. DATA SECURITY

E. Secure Sensitive Data

The essential thought of IoT is to interface regular items by means of Internet. IoT gadgets give benefits that are discoverable by other IoT gadgets. A large portion of the conventions release sensitive and personally identifiable information(PII,) like user's name or data that might be linkable to an individual, like a gadget's host name. This data can be connected to other data sources to target them. Administration components and verification conventions are required with the goal that exclusive approved customers can find the gadget.

4. SCRUTINIZING SOULTION

IoT seems be having an exponential growth, and we all know that exponential growth will have severe consequences. Can we slow down a little bit and put some ground rules before we launch a new IoT device every few months? We need to take a step back and think, Do I really need this device to be connected on the internet. For example; A washing machine connected to the internet through an app. [10] Is it really required? Majority of the people operate on their washing while staying at home so there is no point in checking the status of the washing machine though an app from office. It does not make any sense at all. Just because IoT is a buzzing word now doesn't mean that we need to re-invent a new device that can connect to the internet.

Security Giant "Kaspersky" had release a blog post called "Internet of crappy things" which exposes the vulnerability that IoT carries with it. It's astonishing to read that most of the home appliances were easily hacked and could be misused. Instead of IoT solving a problem it introduces several more problems to bear with. Quoting Kaspersky's very own tweet

"There is a flood of appliances which are connected without a though whether it's necessary or not #theSAS2015" [11]

Release of new IoT products frequently outdates the older devices and paves way for hackers easily exploit them. Instead we should regulate the new releases of these new devices and their software's and focus on providing long term support and robust security. If not "Internet of Things" may get a fancy rename as "Internet of Insecure Things"

VI. CONCLUSION

Over the last few years, this emerging area for the IoT has been attracting the great interest, and will retain for the years to come. despite fast evolution, we're nevertheless facing new problems and intense challenges. in this paper, we concisely reviewed protection in the IoT, and analysed protection traits and requirements in various different aspects.

Then, we discussed the status in this area from encryption mechanism, communication protection, protecting sensor records, and encryption set of rules. At closing we summarize numerous challenges. All in all, the improvement of the IoT will deliver greater severe safety problems, which can be usually the point of interest and the number one project of the studies.

REFERENCES

[1] "Gemalto.com," 2006-2017. [Online]. Available: https://www.gemalto.com/iot/iot-security. [Accessed November 2017].

[2] L. Columbus, "www.Forbes.com," 27 November 2016. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#6c001de9292d. [Accessed November 2017].

[3] G. Wood, "Patching the Internet of Things (IoT) Software Update.," 26 June 2016. [Online]. Available: https://www.ietf.org/blog/2016/07/patching-the-internet-of-things-iot-software-update-workshop-2016/. [Accessed November 2017].

[4] G. A. F. George Corser, "Internet of Things (IoT) Security Best Practices," February 2017. [Online]. Available: https://www.academia.edu/32053241/Internet_Of_Things_Iot_Security_Best_Practices._IEEE_Community-led_White_Paper. [Accessed November 2017].

[5] BanafaAhmed, "iot.ieee.org," March 2017. [Online]. Available: https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot. [Accessed November 2017].

[6] A. RAZANI, "readwrite.com," 16 July 2016. [Online]. Available: https://readwrite.com/2016/07/14/iot-and-problems-the-concerns-that-arise-with-iot-pt2/. [Accessed November 2017].

[7] "BITAG Report," November 2016. [Online]. Available: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

[8] "Strategic Principles for Securing (IoT)," 15 November 2016. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf. [Accessed November 2017].

[9] "The Statistics Portal," 2017. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed Novermber 2017].

[10] S. WARREN, "www.thenextweb.com," [Online]. Available: https://thenextweb.com/contributors/2017/05/31/iot-brings-us-future-whole-lot-problems/. [Accessed November 2017].

[11] A. Drozhzhin, 19 February 2015. [Online]. Available: https://www.kaspersky.com/blog/internet-of-crappy-things/7667/. [Accessed November 2017].