A Survey Report on: Security & Challenges in Internet of Things

Pratap Kumar[1] Rakesh Singh Kunwar[2] Alok Sachan[3]
[1]M. Tech (Cyber Security) [2]Ph. D. (Cyber Security) [3]M. Tech (Information Security)
[1,2]Department of Information Technology [3]Department of Computer Science and Engineering
[1,2]Raksha Shakti University, Ahmedabad [3]BIT Mesra, Ranchi

Abstract— In the era of computing technology, Internet of Things (IoT) devices are now popular in each and every domains like e-governance, e-Health, e-Home, e-Commerce, and e-Trafficking etc. Iot is spreading from small to large applications in all fields like Smart Cities, Smart Grids, Smart Transportation. As on one side IoT provide facilities and services for the society. On the other hand, IoT security is also a crucial issues.IoT security is an area which totally concerned for giving security to connected devices and networks in the IoT .As, IoT is vast area with usability, performance, security, and reliability as a major challenges in it. The growth of the IoT is exponentially increases as driven by market pressures, which proportionally increases the security threats involved in IoT The relationship between the security and billions of devices connecting to the Internet cannot be described with existing mathematical methods. In this paper, we explore the opportunities possible in the IoT with security threats and challenges associated with it.

Key words: Internet of Things (IoT), Challenges, Risk, Threats, Security

I. INTRODUCTION

The Internet of Things increasing preponderance of entities which is going to transform the real world objects into intelligent virtual and physical objects. In the era of present technology, the main aim of IoT is to unify everything in our real world under a common infrastructure andkeeping us informed of the state of the things. IoT devices include personal computers, PDAs, laptops, watches, tablets, smart phones and other hand-held embedded devices. IoT communication comes from computing machine and embedded sensor systems which is used in industrial machine-to-machine (M2M) communication like as smart city, smart energy grids, smart home and building automation. Generally, IoT products are old and unpatched embedded operating systems and software. To improve the security in IoT device which connects directly to the Internet, should network access restricted. The network segment should then be monitored to identify potential anonymous traffic, malicious activity and if there is a problem then take action over that. In December 2013, a researcher of Proof point (security firm) discovered the first IoT botnet. By the Proofpoint, more than 25 percent of the botnet was made up of peripheral devices other than computers, including smart watch, smart TVs,smart phone, baby monitors and other household appliances.

II. OPPORTUNITIES IN INTERNET OF THINGS

A. Smart Cities

By the McKinsey report Smart cities are the second or third largest target area for IoT ,with the project economic impact totaling somewhere between $1 trillion and $1.6 trillion by 2025. Many of the advantages of smart cities like as, ability to monitor and track the activities of citizens on a massive scale, These type of tracking of citizens raises serious issues regarding privacy and security. There are several systems within a city that could potentially to analyze the buying list of products so it is necessary to enforce standards for communications protocols.

B. Healthcare Things

An Internet of Healthcare Things (IoHT) can be a revolution in medicine, healthcare delivery and consumer health. Now it's working on Smart medical devices, including smartphones, watches, and other bio-based wearable's which are connected to IoHT, it can also provide improved, pervasive, cost-effective and personalized medical care. So, an IoHT can also improve hospitals, nursing homes, assisted living, and continuous care retirement communities in many ways.[19] [21][23].

C. Smart Homes

Smart homes have been a dream for decades but due to the lack of experiences and practical technology (e.g., low cost, easy-to-deploy, low maintenance, etc) has often limited large-scale deployments and mainstream adoption. There are over a 120 million homes in the U.S. and far fewer brand new homes are going to be built in the next couple decades. Finally interoperability in the home continues to be a barrier compared to other IoT domains (health, city) that provide more opportunities for professional system support and maintenance[19][23].

III. CHALLENGES /THREATS IN INTERNET OF THINGS

The Internet of Things (IoT) is the biggest revolution in the making in the IT industry. With the growth of special requirements in IoT, several challenges and potential threats also grow with time which are discussed below[2][3][4][5][6][7][8][12].

A. Confidentiality and Encryption

Each and every device or node in the IoT can act as a potential risk. Preserving confidentiality of the data and its integrity must be maintaining during the transmission of data. Sometime due to poor encryption and backdoor security mechanisms, transmitted data is not secured against unauthorized interference or it can be capture and misuse by the attacker during transmission across the network.

B. Trust and Data Integrity

During transmission messages send from sender to receiver can be spoof and false data can be send. This problem is exist in several IoT devices which suddenly become connected. So, security must be built into the architectural design of these IoT devices and systems to enable trust in both the hardware and integrity of the data.

C. Data Collection, Protection and Privacy

IoT provide several facilities which directly easier everyday lives by boosting efficiency and productivity of businesses with employees. Using IoT in such a fashion have both pros and cons. In one side, the data collected will help us make effective and smarter decisions. But on the other side, it impacts the privacy expectations. If connected device which collect the data is compromised, then it will undermine the trust in the IoT.

D. Mobility

Mobility is one of the eminent attributes of the IoT devices, where the devices hyper connected to the network without prior configuration. So it is necessary to develop mobility springy security algorithms for the IoT devices.

E. Identifying & Implementing Security Controls

In digital world, redundancy is critical; if one product fail, another is there to capture. Similarly concept of layered security works, but it is notable thing to see how well enterprises can keep security and manage the redundancy. The biggest challenges for enterprises is to identifying where security controls are needed for this emerging breed of internet-connected devices and then implementing these controls effectively.

F. Modular Hardware and Software Components

It is very important part in which security must be considered and implemented in every domain of IoT to maintain and control the parts or modules of Internet-connected devices. The major problem is that the attackers unfortunately compromise the supply chain of IoT devices, after implanting malicious code and other vulnerabilities they exploit all the devices have been implemented in an enterprise environment. It may prove necessary to adopt a security paradigm

G. Resource Constraints

Every peripheral IoT devices are resource constrained. i.e, they need computational resources, onboard memory, energy, bandwidth etc. In open environment these nodes accessible physically, so easily be cloned and tampered.

H. Resource and Service Discovery

In Iot large number of end devices are deployed in the field therefore, most of the Iot devices can function autonomously with the requirement. They also acquire and use the required services which are useful for the connection. So, coordinators in an IoT deployment must implement resource and service directories that can be queried on a public interface. Due to distributed architecture in nature, all the data is spread over clouds. So without proper security measures it may lead to information leakage and user privacy issues.

As there are several challenges and threats spread which effect the IoT, some of these threats are listed in table below which display on different attack based on threats or challenges:

Challenges/ Threats	Spoofing	Tempring	Repudiation	Information leakage	DOS	Elevation of Privilage	MITM	user privacy	Reply attack	Cloning of nodes
Heterogeneity	High	Low	Low	Low	Low	Low	High	Low	Low	Low
Connectivity	Low	Low	Low	Low	High	Low	High	Low	Low	Low
Mobility	High	Low	High	Low	High	Low	High	Low	Low	Low
Addressing and Identification	High	Low	High	Low	Low	High	Low	Low	Low	Low
Resource constraints	Low	High	Low	High	High	Low	Low	High	Low	Low
Resource and service	High	Low	Low	Low	High	Low	Low	High	Low	Low

Table 1: various attack based on threats in IoT

IV. SECURITY IN INTERNET OF THINGS

According to SANS technology, we collect information as respect to security, challenge and an opportunity for new ways of thinking about ecologies of security [17] shown in fig1. Whereas in fig 2, The threat of IoT listed in different aspect would be, the most difficulty patching thing (31%) in embedded operating systems and applications. Malware and any infection through virus it cited as (26%), with the concern being that IoT devices would end up spreading malware into the enterprise. Denial of service attack on things(13%) and sabotage and destruction of connected Things (12%) were also concern.

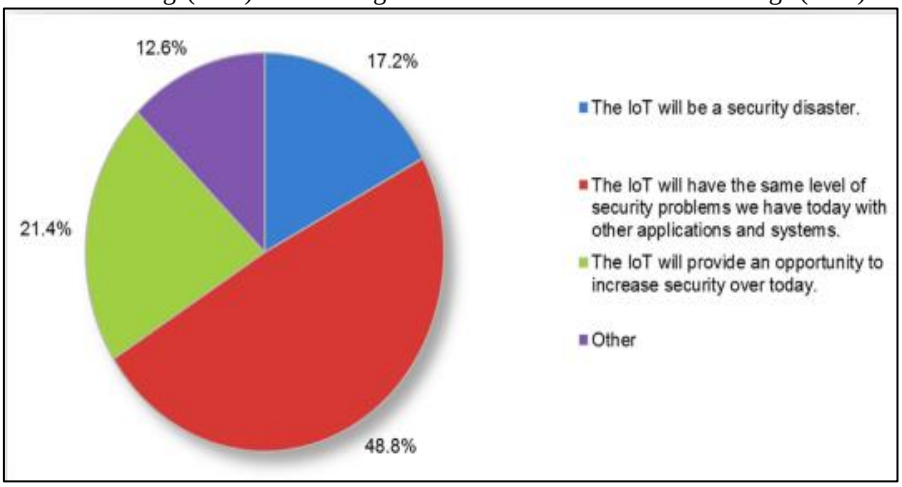

Fig. 1: Perception about IoT Security[17]

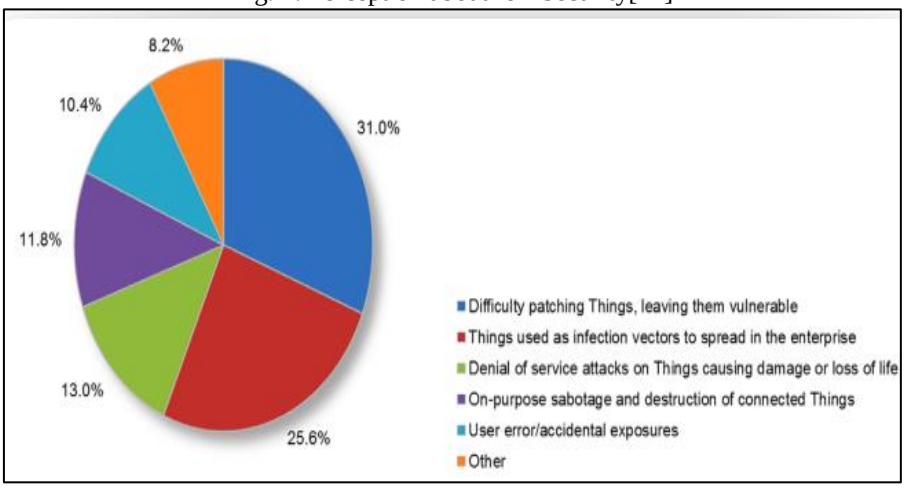

Fig. 2: Threats to the Internet of Things[17]

A. Risk in IoT

Internet connection as the riskiest aspect of the IoT devices because for consumer power constraints and also guarantee security. As per sans technology Command and control channels to the devices (24%), with concerns about device operating systems (11%) and firmware (9%) rounding out the list. Organizations using IoT will need to add more security in IoT applications need to configuration and patch management maintenance.

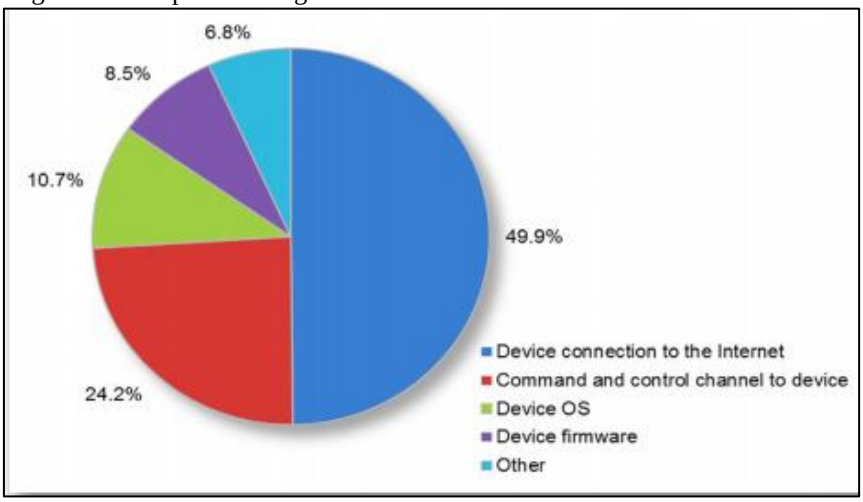

Fig. 3: Greatest Risk in IoT[17].

V. SECURITY DEVICE LIFE CYCLE

Security is the major concern in IoT Security must be addressed throughout the device lifecycle, from the initial design to till operational environment.

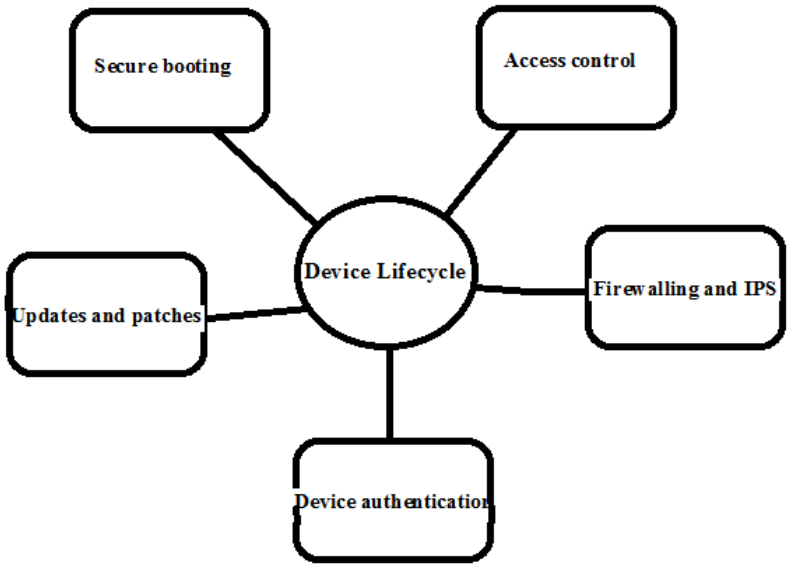

Fig. 4: IOT Security Device Life Cycle

A. Secure Booting

When power is introduced into the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital signatures. A digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to run on that device, and signed by the entity that authorized it, but the device still needs protection from various run-time threats and malicious intentions.

B. Access Control

Access control is applied in different forms of resource that controls built into the operating system limit the privileges of device components and applications so they access only the resources. It is important to understand that device-based access control mechanisms are correspondent to network-based access control systems i.e. even if intruder able to steal corporate credentials to gain access to a network, only limited information will open to access.

C. Device Authentication

When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data Just as user authentication allows a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area.

D. Firewalling and IPS

The device needs a firewall or the packet inspection capability to control traffic that is destined to terminate at the device .Embedded devices have unique protocols, For instance, the every smart energy grid must has its own set of rules and protocols governing how devices talk to each other . The network appliances must take care of it but it mainly need to filter the specific data bound to terminate on that device in a way that makes optimal use of the limited computational resources available.

E. Updates and Patches

Once the devices is in the field performing critical operation or services and are dependent on security patches to protect against the inevitable vulnerability that escapes into the wild. In IoT software updates and security patches must be delivered in a way that conserves the limited bandwidth.

VI. FUTURE WORK

In the future, the Internet of Things is likely to combine the virtual and physical worlds together such a way that it makes difficult to understand. As a security and privacy perspective, the predicted pervasive of sensors and devices such as home, the car and wearable and ingestible, poses particular challenges. Physical objects in our everyday lives, share our observations and detect the feature particular to detect.

VII. CONCLUSION

In this paper, we have surveyed the most important security aspects of the Internet of Things with focus on the security and challenges concern with the IoT. As the IoT comes with the different opportunity, due to outgrow the number of personal computers and even mobile phones by several orders of magnitude. It also raises different types of challenges.

REFERENCES

[1] OETZEE, Louis; EKSTEEN, Johan "The Internet of Things - promise for the future? An introduction" IST-Africa Conference 2011 , Issue Date: 11-13 May 2011
[2] Xu, Teng; Wendt, James B.; Potkonjak, Miodrag "Security of IoT systems: Design challenges and opportunities" Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on , Issue Date: 2-6 Nov. 2014
[3] Fink, G.A.; Zarzhitsky, D.V.; Carroll, T.E.; Farquhar, E.D "Security and privacy grand challenges for the Internet of Things" Collaboration Technologies and Systems (CTS), 2015 International Conference on, Issue Date: 1-5 June 2015
[4] S.S.; Tripathy, S.; Chowdhury, A.R "Design challenges and security issues in the Internet of Things" Region 10 Symposium (TENSYMP), 2015 IEEE, Issue Date: 13-15 May 2015
[5] Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. "Security and privacy challenges in industrial Internet of Things"Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, Issue Date: 8-12 June 2015
[6] Billure, R.; Tayur, V.M.; Mahesh, V. "Internet of Things - a study on the security challenges" Advance Computing Conference (IACC), 2015 IEEE International, Issue Date: 12-13 June 2015
[7] Hossain, M.M.; Fotouhi, M.; Hasan, R. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things" Services (SERVICES), 2015 IEEE World Congress on, Issue Date: June 27 2015-July 2 2015
[8] Matharu, G.S.; Upadhyay, P.; Chaudhary, L. "The Internet of Things: Challenges & security issues"Emerging Technologies (ICET), 2014 International Conference on, Issue Date: 8-9 Dec. 2014
[9] Axelrod, C.W. "Enforcing security, safety and privacy for the Internet of Things" Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, Issue Date: 1-1 May 2015
[10] Li, Lan " Study on security architecture in the Internet of Things" Measurement, Information and Control (MIC), 2012 International Conference on , Issue Date: 18-20 May 2012
[11] XuXiaohui "Study on Security Problems and Key Technologies of the Internet of Things"Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on, Issue Date: 21-23 June 2013
[12] G.S.; Upadhyay, P.; Chaudhary, L. "The Internet of Things: Challenges & security issues" Emerging Technologies (ICET), 2014 International Conference on, Issue Date: 8-9 Dec. 2014
[13] Harald Bauer, Mark Patel, and Jan Veira "Internet of Things: Opportunities and challenges for semiconductor companies"Article by McKinsey'soctober 2015
[14] http://www.forbes.com/sites/davelewis/2014/09/16/security-and-the-internet-of-things/
[15] Madakam, S. ,Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications,3, 164-173. doi: 10.4236/jcc.2015.35021.
[16] Wind River System white paper "Security In The Internet Of Things" 2015
[17] John Pescatore "Securing the Internet of Things Survey" A SANS Analyst Survey: January 2014
[18] Carolyn Marsan "The Internet of Things: an overview" Internet Society October 2015
[19] Rajeev Alur, Emery Berger, Ann W. Drobnis, Limor Fix, Kevin Fu, Gregory D. Hager, Daniel Lopresti, KlaraNahrstedt, Elizabeth Mynatt, Shwetak Patel, Jennifer Rexford, John A. Stankovic, and Benjamin Zorn "Systems Computing Challenges in the Internet of Things" computing community consortium(ccc), Issue Date: September 22, 2015
[20] JayavardhanaGubbi ,RajkumarBuyya , SlavenMarusic , MarimuthuPalaniswami "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions" by buyya 2012
[21] Sir Mark Walport "The Internet of Things: making the most of the Second Digital Revolution" UK Government Chief Scientific Adviser 2014
[22] http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security
[23] Tavis C. McCourt, DanielToomey, SimonLeopold, GeorgiosKyriakopoulos,AlexanderSklar,Brian Peterson "The Internet of Things: A Study in Hype, Reality, Disruption, and Growth"U.S. Research Published by Raymond James & Associates, , Issue Date : January 24, 2014
[24] Dave Evans "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" by postscapes Issue Date: July 09, 2012