IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Cyber Security Challenges In IoT

S.Dharini Iswarya[1], K.Priyadharshini[2], R.Minakumari[3], S.Anbazhaki[4]

II MCA , Anjalai Ammal Mahalingam Engineering College,Kovilvenni[1-4]

Abstract: Nowadays, the evolution of the world of the Internet of Thing is promising the explosion of a number of devices connected to the Internet. According to Cisco analysts (Evans, 2011), in 2015 there were more than 25 billion devices connected and with a projection of more than 50 billion devices connected by 2020. Also, the new business model that the Internet of Things technologies enable are manufacturing a super-fast increase of machine-to-machine communications. This is a real market innovation moment that opens up a lot chances for enterprises and, generally speaking, for the entire society.[1] Inherently, it increases dramatically the security problems, which could discomfit a sizeable part of Internet of Things' potential benefits that McKinsey valuates at approximately $4 trillion. Indeed, a recent survey by HP reports that the 70% of devices contain defenselessness. The intent of this segment is to give an overview of present trends about cyber security involvement and a glimpse of what the future of the Internet of Things will convey.

Keywords: Security, Internet of Things,Cyber-attack, Security threats, Secure Reprogrammable Networks.

1.INTRODUTION

The great flow of connected devices in the IoT has created excessive demand for robust security in response to the growing demand of millions or perhaps billions of connected devices and utility worldwide.The number of threats is rising daily, and attacks have been on the increase in both number and complexity[2]. Security has been defined as a process to protect an object against environment damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed According to fizz there is no thing as the secure state of any object, actual or not, because no such object can ever be in a perfectly secure state and still be useful. Information technology (IT) has exposed the user to a huge data bank of information regarding everything and anything. Recent reports encourage that the revolutionary is also getting supplied to utilize cyber space to carryout terrorist attacks.[3] The possibility of such attacks in future cannot be denied. Terrorism related to cyber is popularly known as cyber security.

2. LITERATURE SURVEY

Noura Aleisa and Karen Renaud: The Internet of Things' potential for major solitude invasion is a concern. This paper reports on a methodical literature review of privacy-preserving solutions appearing in the research literature and in the media. We analysed planned solutions in terms of the techniques they deployed and the coverage to which they contented hub space to yourself ideology.

N. R. Prasad: Internet of Things is the incorporation of a multiplicity of technology. The Internet of Things incorporate visibly and faultlessly large number of an assortment of end systems, providing open access to preferred facts for digital services. Internet of things is a shows potential research in import, industry, and education application.

R. Moskowitz, P. Jokela: The Internet of Things (IoT) is an conservatory of the Internet in which large numbers of things, including sensors, actuators and processors, in addition to human users, are network and able to provide high decision data on their milieu and implement a extent of control over it. It is still at an early juncture of progress, and many problems/research challenge must be solved before it is far and wide adopt.

Tobias Heer, Oscar Garci: Morchon:A direct understanding of the phrase Internet of Things refers to the use of ordinary Internet protocol for the human to thing or thingto thing announcement in rooted networks. Although the securitydesires are well predictable in this sphere of influence,it is motionless not fully unwritten how accessible IP security protocols and constructions can be deploy

Henrik Stein: Organisations are going all the way through a big adjust in the way they activate, the technique they suppose and the approach they occupation. This revolutionize is being hard-pressed by major industrial general digitalization, cloud and mobile, intellectual big data and analytics and behavioral social conversions that are distressing the total selling With the materialization of stronger and more pervasive cybersecurity threats, organisational leaders cannot be in a wait and watch mode.

3. SECURITY IN IOT DEVICES AND SERVICES

Ensuring the security entails protecting both IoT devices and servicesfrom unauthorized access from within the devices and externally. Securityshould look after the services, hardware resources, information and data,both in changeover and

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

storage. In this section, we identified three key problems with IoT devices and services: data confidentiality, privacy and trust. [4]Data confidentiality represents a elementary problem in IoT devices and services. This requires addressing two important aspects: first, access control and authorization mechanism and second authentication and identity management (IdM) mechanism.. Access control entails controlling access to resources by granting or denying means using a wide array of criteria. Authorization and access control are important to establishing a secure connection between a number of devices and services.[5] The main issue to be dealt with in this scenario is making access control rules easier to create, understand and manipulate.

4. THE CHALLENGES OF IOT CYBERSECURITY

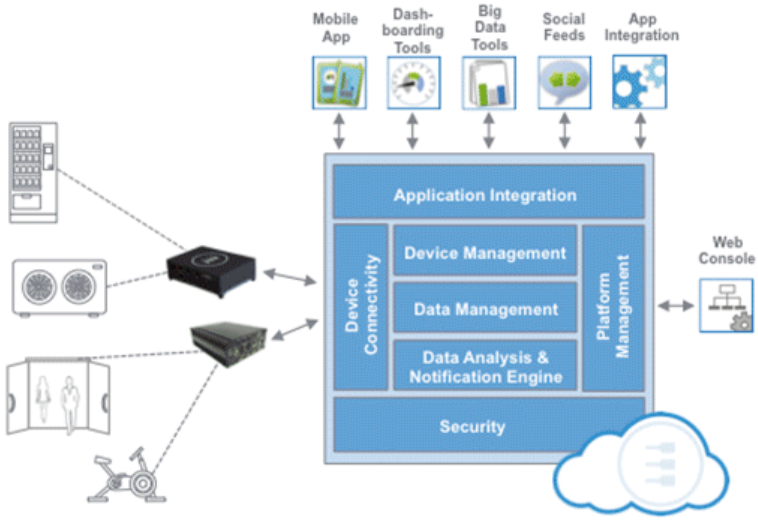
Due to the constant evolution of these technologies, it is very difficult to know what the scope of the advance of IoT will be on services in the future. However, what we can hazard a guess at is the large amount of cyber security and user information problems that may be affected.[6]The relevance of IoT technology as a target for possible threats that compromise cybersecurity and privacy come mainly from the fact that this technology uses and depends on everyday items.

5. SUMMARY OF RISKS AND WEAKNESSES

Currently, IoT technology presents a series of risks and vulnerabilities that can be summarised as follows[7]:

- **Limited resources:** the majority of IoT devices have limited capacities in terms of processing, memory and power, thus advanced security measures cannot be efficiently applied.
- **Complexed ecosystem:** The security fears have worsened now that the IoT cannot be seen as a collection of autonomous devices, but fairly as a rich, diverse and wide ecosystem that includes aspects such as devices, communications, interfaces and people.
- **Low cost:** in some cases, manufacturers may be inclined to limit security elements so as to guarantee a low cost, therefore the product's security is not able to protect it against certain types of IoT attacks.
- **Lack of experience:** This is a fairly new field and as such there is a lack of experts in IoT cybersecurity that have a background in threats or problems that allow for putting the previous lessons learned into practice regarding this technology.
- **Security failures in the device's design and its exploitation:** the most common practice is that manufacturers concentrate on reducing the launch time of the products, sometimes neglecting the phase where they design essential cybersecurity elements (encrypting of transmitted information, access controls, etc.). In many cases this is due to the need to launch before competitors do.
- **Lack of control and asymmetry of the information:** the user is often not aware of the treatment of data carried out by devices with sensorization technology. The conventional mechanisms used to obtain the users' consent are considered as "low quality" consent due to the fact that on many occasions they are based on the lack of information that the user receives regarding the subsequent treatment of the personal details they are providing

Security against efficiency: when balancing the optimisation of the device's hardware resources with the security requirements that these devices require, a variety of challenges arise for manufacturers.[8] Due to the fact that time pressures when commercialising IoT products are greater than in other fields, this sometimes causes limitations in the efforts to develop secure devices.



5.1 Source of cyber security for the IOT challenges and issues

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

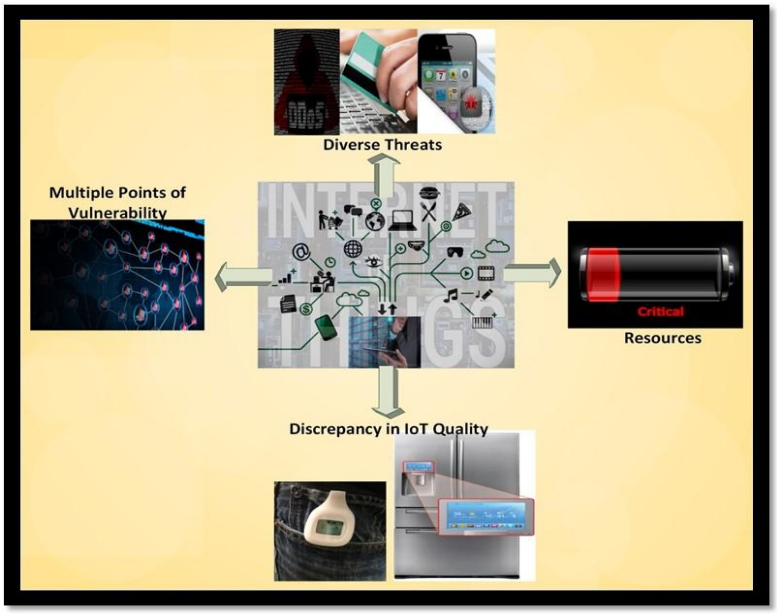
6. CONSTRAINTS AND HETEROGENEOUS COMMUNICATION

In the following we for a short time discuss the resource constraints of IoT devices and the consequences for the use of Internet Protocols in the IoT domain.

Tight resource-constraints: The IoT is a resource-forced network that relies on loss and low-bandwidth channels for communication between small nodes, relating to CPU, memory, and energy budget.[9] These characteristics directly impact the terrorization to and the design of security protocols for the IoT domain. First, the use of small packets (e.g., IEEE 802.15.4 supports 127-byte sized packets at the physical layer) may result in fragmentation of larger packets of security protocols.

DoS resistance: The firm memory and processing constraints of things naturally alleviate resource exhaustion attacks. Especially in unattended T2T communication, such attacks are difficult to observe before the service becomes unavailable (e.g., because of battery or memory exhaustion). since a DoS countermeasure, DTLS, IKEv2, HIP, and Diet HIP execute return reusability checks based on a cookie method to delay the enterprise of state at the responding host awaiting the address of the initiate host is verified.[11]

6.1 Common Security Characteristics of IoT Products:



6.1.1. Source of security characteristics of IoT

Conforming to a grand number of educational policy in the IoT globe convey in a different array of possible security risks.A few of these risks are fixed fear for regular computers·For instance, new smart TVs that allow users to side the Internet, [10]]purchase other "Things, and carve up photos via social networks may well put data stored or transmit through the TV at risk." receptive bank card information, passwords, and personal data that can smooth the progress of identity theft are some types of in sequence attackers can get their hands on.

CONCLUSION

Internet-of-Things (IoT) has generally been agreed to the foundation for digital economy; and cyber security is always a big fear when mission critical applications are built on top of IoT. In this paper, we fight that one root problem for IoT security is the lack of the careful notion of "Identity" in the Internet-of-Things. To solve the identity problem, we propose a new information.Different from the "Identity" of a user, this new information stack puts a strong emphasis on situational information, which is predictable to be imprecise and noisy. With the expectation of using multi-factor authentication in IoT security, we survey on attribute based authentication and analyze the pros and cons of current techniques to support IDoT. It is hope that by granting this deep understanding, IDoT can be addressed in a more systematic and effective way.There is a trend toward more simplicity and regulation over cyber security. Security Directive and General Data Protection Regulation, will reinforce the obligations for organizationsImprove deliver and efficiency of exis-ng services and products Innova-ve new services will emerge Policy and regulatory are needed Infrastructure; coverage and quality Skills; use and development of services..

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey,"*Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
[2] S. Andreev and Y. Koucheryavy, "Internet of things, smart spaces, andNext generation networking," *Springer, LNCS*, vol. 7469, p. 464, 2012.
[3] J. S. Kumar and D. R. Patel, "Asurvey on internet of things: Security andprivacy issues," *International Journal of Computer Applications*, vol. 90,no. 11, pp. 20–26, March 2014, published by Foundation of ComputerScience, New York, USA.
[4] A. Stango, N. R. Prasad, and D. M. Kyriazanos, "A threat analysismethodology for security evaluation and enhancement planning,"in *Emerging Security Information, Systems and Technologies, 2009.SECURWARE'09. Third International Conference on*. IEEE, 2009,pp. 262–267.
[5] D. Jiang and C. ShiWei, "A study of information security for m2m ofiot," in *Advanced Computer Theory and Engineering (ICACTE), 20103rd International Conference on*, vol. 3. IEEE, 2010, pp. V3–576
[6]C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306, December2005. Updated by RFC 5282.
[7]T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version1.2. RFC 5246, August 2008. Updated by RFCs 5746, 5878.
[8] T. Phelan. Datagram Transport Layer Security (DTLS) over the Datagram Con-gestion Control Protocol (DCCP). RFC 5238, May 2008.
[9] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol.RFC 5201 (Experimental), April 2008.
[10] R. Moskowitz, P. Jokela, T. Henderson, and T. Heer. Host Identity Protocol Version 2. draft-ietf-hip-rfc5201-bis-03 (Work in progress), October 2011.