International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com, Special Issue 42 (AMBALIKA) (March 2017), PP.26-29

SECURITY & CHALLENGES FOR IOT DEPENDENT DEVICES- FUTURE DIRECTIONS OF M2M COMMUNICATION

[1] Manish Joshi, [2] Bramah Hazela, [3]Vineet Singh.
[1,2,3]Computer Science & Engineering Amity University, Uttar pradesh Lucknow
[1] manishjoshi0903@gmail.com, [2]bhazela@lko.amity.edu, [3]vsingh@lko.amity.edu.

***Abstract*— A new dimension in the internet world has emerged and provided the way of making our life easier by connecting various smart objects to the internet, enabling better performance and smooth functioning of the real time objects for the betterment and comfort of human race, and this I technology is called, "Internet of Things" . This paper aims to give the comprehensive view of the increasing need or dependency on IOT devices in the near future as well as various concerns associated with it i.e. improved security architecture that overcomes various security concerns specific to IOT devices, robust performance and various countermeasures proposed by different novel researches. This paper focuses on presenting different aspects of security principles, challenges with their proposed countermeasures and architectural frameworks to help in identifying the future directions for secure M2M communications.**

***Index Terms*—** Internet of Things (IoT), DTLS (Datagram Transport Layer Security), RFID, CoAP.

I. INTRODUCTION

M2M communication has been an industry buzzword for years and will soon provide us the connectivity to the physical world through smart homes, smart cars, automation networks etc. that focuses on providing information, enabling smart interaction through sensors. IoT is steadily evolving in order to process enormous amount of data generated ever year. This IoT technology promises the most lucrative and widespread interaction among humans or M2M. In the near future, smart devices, objects will interact with each other through sensors, gathering data, performing analysis that will result better and optimized results and various challenges are also considered like limited resources on field [1]. In order to secure the future of IoT, embedded security is proposed by the researcher in paper [2] to provide inbuilt security to the devices resulting software-hardware co-design architecture.Researchers [3] have discussed the growth of IoT devices in order to connect the whole world in more sophisticated way as compared to the other technologies, and IoT devices has become an utility with increased capabilities of sensing, actuations, communications and controls, resulting generating vast knowledge from huge data set. Application layer protocol of IoT i.e. CoAP (Constrained Application Layer Protocol) is responsible to retrieve data from sensory nodes, as it is complete and efficient communication protocol stack for data gathering and analysis from the sensor nodes in the field and the new alternative to CoAP is "CoAP observe" option which is used to retrieve the raw sensed data from the sensory nodes[4]

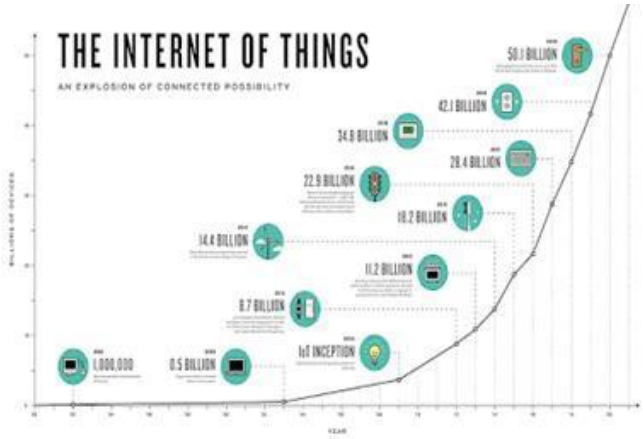

Fig. 1. Statistics showing explosion of connected IoT devices per year.

Paper is organized in different sectons: 1st Section defines the introduction part while vision of IoT is explained in Section 2, 3rd Section is considered to be the part of discussing architectural evolution in IoT, Section 4 discusses the future applications, Section 5 is all about security challenges and Section 6 finally concludes the paper

II. VISION OF IOT

inter device collaboration with internet under iot vision enables smart communication within objects using various sensory nodes and actuators. vision of iot enables us to provide the various opportunities in the multitude of area. it also specifies the vision of secure iot in coming future in order to avoid any disintegration of security architecture, because transmission of highly sensitive information can cause security breach. emerging trends of smart devices improves people lives through both automation and smart decision based on the facts and stats analyzed through the devices [8]. internet of Things can be understood as the dispersed power to control the objects and people's lives through remote monitoring and automation. IoT can be the next big thing for improving healthcare system for the humanity, as it enables us

to remotely monitor the patient's health and it can help us to analyze the patient's condition

through web browser. In paper [11], simulation softwares like 6LoWPAN protocol stack and ContikiOS are used to perform this task of attaining remote health monitoring deployability

ratio in real. Researcher [12] have envisioned python based implementation of CoAP protocol i.e. CoAPthon, it is an open source python based open library and used through through easy to use programming interface. Researcher [19] has not only defined the importance and evolution of IoT in today's].

III. ARCHITECTURE

Researcher[7] have proposed an effective deployable architectural model that helps in monitoring and tracking of patients with the help of smart SHS architecture for better functioning. Researcher[16] have proposed a better deployable model for implementing in various healthcare systems. DTLS over CoAP is proposed as a deployable architecture. Researcher [13][10] have proposed DTLS/TLS[17] based schemes that relies on various certificates provided along with the authentication process to work in limited resource with better performance and efficiency and DTLS also helps in reducing the risk of DOS attacks. Researcher [24] investigates the performance of "AuthLite", which is a novel authentication approach and it is a key management scheme with conventional pre-shared key mode while maintaining its lightweight feature. Research [15] have mentioned the use of security principles that should be enforced to each layer.

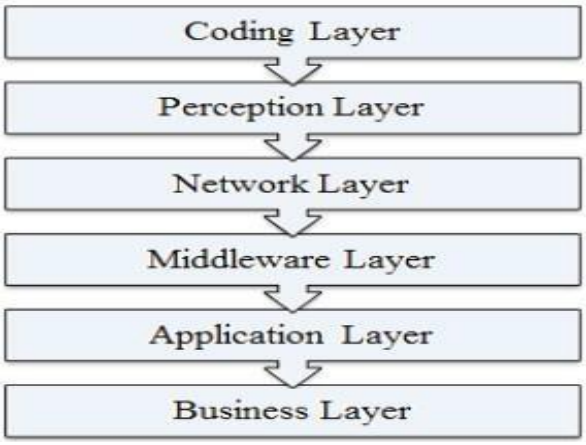

Fig. Layered Architectural overview with different layers.

In the above layered architecture, different layered approach is used to define the functionality. *Coding layer* is responsible for identifying the objects through their object ID, *perception*

IV. APPLICATIONS

Internet of Things have come with wide variety of applications which are smart, productive and efficient as compared to existing technologies. Internet of things is basically providing the idea of enhancing technological advancement by enabling the mutual interaction among devices and these collaborative approaches to

connect various devices through internet will create wide range of innovative applications [26]. Concept of Google car is another world, but has also defined the secure way of using IoT with considering all privacy parameters. With this approach, researcher has defined IoT using MQTT protocol. Researcher [5] have demonstrated an important application layer protocol CoAP, with new formatted SCoAP, as a version of IoT that runs through various protocols used in web browsers. IoT CAD security techniques [6] are another visionary aspect for IoT security that can evolve various IoT security concers using different IoT counters.

layer consists of field sensors deployed in different forms called as RFID tags etc., *network layer* make use of information and transfers it to the processing systems using communication protocols like Wifi, Bluetooth etc., *middleware layer* includes processing of information received from sensor devices using cloud computing while application and business layer is responsible for developing smart homes and various business models respectively [25]. Researcher [22] have proposed the architecture in which algorithms that need to be tested among different environmental variables and to enable developers, so that various adjustments can be made to have better overview of the performance of the algorithm for better security of the Internet of Things (IoT).

V. SECURITY CHALLENGES

Hardware malfunctioning is one of the biggest challenges that can affect the integrity of the IoT security. In order to simultaneously persist various trojan and modifies side channel analysis attacks, these vulnerabilities can be prevented through the proposed method of dynamic permutation, as it makes more difficult to find the key of cryptographic algorithms and generates the bar against loosing integrity of the IoT security [23][21] and security vulnerabilities like identity theft etc. are also discussed in [20]. Advanced congestion control algorithms like CoCoA, developed to maximize throughput and minimizing packet loss is also proposed in order to counter the problem of congestion in limited resource IoT functioning[18]. Health Sector is also facing various security issues in IoT wearable devices and monitoring systems used in smart healthcare facilities like privacy, digital forensics, computation, communication and trusted sensing,[14] as these variable factors are susceptible to tampering, as these data must pass through secure channel in order to prevent the data tampering and modifications. A human interactive system that works takes visual as an input, for analyzing various complex security loopholes in IoT infrastructure [9].

showcasing of upcoming IoT applications with real time traffic [29].

A. Smart Agricultural Techniques:

Working together of IoT with cloud computing generates powerful computing tools to make a better agricultural information cloud with the combined power of cloud computing with IoT. RFID and its sensing techniques are required to achieve the various parameters in collecting large amount of data and then

analyzing it with agricultural information cloud [27].

Smart Healthcare Services: Internet of Things is spreading its wings in the healthcare sector by providing newly improved and smart healthcare services with the help of growing IoT technology i.e. RFID sensing, RFID field can be applied to the healthcare services, so that monitoring and assessing patient's current health stats for the better treatment of the disease. This paper [30] proposes deployment of RFID locator to improve the quality of healthcare services.

B. Smart Traffic Management*:*

Various Smart sensing technologies like GPS, RFID and EPC are used in order to provide effective all weather smart traffic management through the use of IoT technology. It is a complete automation in traffic monitoring system for better functioning.

CONCLUSION

In a nutshell, we can say that Internet of Things has presented us an eye opening fact about the future of connecting people and the machines together for the betterment and comfort of human race. In this paper, we have reviewed various present applications of this technology where M2M interaction plays an important role in the successful deployment of this technology. IOT has commendable applications in various fields with the better version in terms of deploy ability, reliability and performance. We have also discussed the projected future or vision of IoT in the coming years with the highest growth rate in the market. In this projected path of IOT, it has also defined that various security challenges are on its way that also exposes the vulnerabilities behind this new technology.

REFERENCES

[1] Yen-Kuang Chen, "Challenges and Opportunities of Internet of Things", in IEEE, 2012, pp. 384-387

[2] Sachin Babar, Antonietta Stango, Neeli Prasad, Jaydip Sen and Ramjee Prasad, "Proposed Embedded Security Framework for Internet of Things (IoT)", in IEEE, 2011, pp. 1-3

[3] John A. Stankovic, "Research Directions for the Internet of Things", in IEEE Internet of Things Journal, Vol. 1,No.1, February 2014, pp.3,8

[4] Richard Mietz, Philipp Abraham, and Kay Romer, "High-level States with CoAP: Giving Meaning to Raw Sensor Values to Support IoT Applications", in IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)Symposium on Public Internet of Things Singapore, 21–24 April 2014, pp.1,6

[5] Nam K Giang, Minkeun Ha and Daeyoung Kim, "SCoAP: An Integration of CoAP Protocol With Web- based Application", in Globecom 2013 - Symposium on Selected Areas in Communications, 2013, pp. 2648

[6] Teng Xu, James B. Wendt, and Miodrag Potkonjak, "Security of IoT Systems: Design Challenges and Opportunities", in IEEE 2014, pp. 418,423

[7] Luca Catarinucci, Danilo de Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone, "An IoT-Aware Architecture for Smart Healthcare Systems", in IEEE Internet of Things Journal, December 2015, pp. 515

[8] Rajendra Billure, Varun M Tayur and Mahesh V, "Internet of Things - A Study on the Security Challenges", in IEEE 2015, pp. 247

[9] Panagiotis Sarigiannidis, Eirini Karapistoli and Anastasios A. Economides, " VisIoT: A Threat Visualisation Tool for IoT Systems Security", in IEEE IC 2015, pp. 2633.

[10] Angelo Capossele, Valerio Cervo, Gianluca De Cicco and Chiara Petrioli, " Security as a CoAP resource: an optimized DTLS implementation for the IoT", IEEE ICC 2015, pp.549

[11] Dejana Ugrenovic, Gordana Gardasevic, "CoAP protocol for Web-based monitoring in IoT healthcare applications", 23rd Telecommunications forum TELFOR 2015, pp. 79,82

[12] G. Tanganelli, C. Vallati and E. Mingozzi, "CoAPthon: Easy Development of CoAP-based IoT Applications with Python", in IEEE 2015, pp.1

[13] Gl´ederson Lessa dos Santos, Vin´ıcius Tavares Guimar˜aes, Guilherme da Cunha Rodrigues, Lisandro Zambenedetti Granville and Liane Margarida Rockenbach Tarouco, " A DTLS-based Security Architecture for the Internet of Things", in 20th IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 809-815

[14] Ebrahim AL Alkeem, Chan Yeob Yeun and M. Jamal Zemerly, "Security and Privacy Framework for Ubiquitous Healthcare IoT Devices", in 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), 2015, pp.70,74.

[15] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul and Imran Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", in 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), 2015, pp. 336- 341

[16] Shu-yuan Ge, Seung-Man Chun, Hyun-Su Kim and Jong-Tae Park, "Design and Implementation of Interoperable IoT Healthcare System Based on International Standards", in 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 1

[17] Pascal Urien, "Innovative DTLS/TLS Security Modules Embedded in SIM Cards for IoT Trusted and Secure Services", in 13th IEEE Annual Consumer Communication and Networking Conference (CCNC), 2016, pp. 1

[18] Rahul Bhalerao, Sridhar Srinivasa Subramanian and Joseph Pasquale, "An Analysis and Improvement of Congestion Control in the CoAP Internet-of-Things

[19] Surapon Kraijak, Panwit Tuwanut, "A SURVEY ON IOT ARCHITECTURES, PROTOCOLS, APPLICATIONS, SECURITY, PRIVACY, REAL-WORLD IMPLEMENTATION AND FUTURE TRENDS" in King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, pp. 1,6

[20] Florent Bruguier, Pascal Benoit, Lionel Torres and Lilian Bossuet, "Hardware Security: from Concept to Application", in 2016 European Union, 2016, pp. 1

[21] Subha Koley, Prasun Ghosal, "Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions", in IEEE Computer Societyx, 2015, pp. 517, 520

[22] Jaya Dofe, Jonathan Frey, and Qiaoyan Yu, "Hardware Security Assurance in Emerging IoT Applications", in IEEE, 2016, pp. 2050-2053

[23] Arijit Ukil, Soma Bandyopadhyay, Abhijan Bhattacharyya, Arpan Pal and Tulika Bose, "Auth-Lite: Lightweight M2MAuthentication Reinforcing DTLS for CoAP" in IEEE International Conference on Pervasive Computing and Communications Work in Progress, 2014, pp. 215-219

[24] Reem Abdul Rahman, Babar Shah, "Security Analysis of IoT Protocols: A Focus in CoaP", in 3rd ME International Conference on Big Data and Smart City, 2016, pp. 1-6

Protocol", in 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 1

[25] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal, "A Review on Internet of Things (IoT), in International Journal of Computer Applications, Volume 113 - No. 1, March 2015, pp. 1,5

[26] R. Abdmeziem, D.Tandjaoui, "Internet of Things: Concept, Building blocks, Applications and Challenges, Computers and Society, Cornell University"

[27] F.TongKe, "Smart Agriculture Based on Cloud Computing and IoT," in Journal of Convergence Information Technology (JCIT), Jan'13

[28] L.Xiao, Z.Wang, "Internet of Things: A New Application for Intelligent Traffic Monitoring System," in JOURNAL OF NETWORKS, 2011

[29] "What we're driving at," Google Official Blog. It can be accessed at:http://googleblog.blogspot.com/2010/10/what-were- drivingat.html

[30] P.Fuhrer, D.Guinard, "Building a Smart Hospital using RFID technologies"