A review paper on

Enhanced Security and Challenges in Embedded System Integrated with IoT

K.Pradeep [1]
Research Scholar
k.pradeep423@gmail.com

Dr.R.Prasanthi [2]
Dean Associate (R&D)
rprasanthi@cutmap.ac.in

Dr M. Murali [3]
Dean (R&D)
muralitejas@cutmap.ac.in

Centurion University of Technology and Management, Andhra Pradesh [1, 2, 3]

Abstract - Internet of things (IoT) is a new model of connectivity where all objects are communicate with each other with very little or no human intervention. To achieve this, system designers focus not only on the traditional design constraints but also on the latest trends such as security and privacy. IOT consists unique constraints in terms of connectivity, computational power and energy efficiency, which make it significantly different from those contemplated by the canonical doctrine of security in distributed systems. In this paper, various security issues are discussed with the integration of IOT.

Index Terms -IoT, Power Consumption, Embedded devices.

I.INTRODUCTION

Internet of this (IoT) is emerging technology and latest trends in embedded technologies and all these IoT components are integrated with the internet and every component is interconnected in IoT. We can estimate that future of the IoT devices that are embedded with the various environments that will generate the huge amount of data. This data is stored in the correct format and it is useful for further usage.

In IoT, various components are integrated with the number of devices such as mobile users, software vendors, access technology suppliers, and so on. Many applications in IoT are very powerful and networks are executed in preparing, usage home automation, industrial management, agriculture, and health sectors. In the next generation, the IoT can be seen differently and this is connected to the people with the various components with the sensors. Many types of sensors are used to manage the various applications. Security is most widely used IoT devices to prevent the attacks from the various attackers. All the IoT devices are smart devices and these are connected to the internet.

In IoT the complicated issues are increasing day by day because of the security challenges that are facing various

K.Pradeep[1], Faculty member in the Department of ECE, Baba Institute of Technology and Sciences, Visakhapatnam, AP, INDIA.

issues in the networks. IoT networks are more complex and integrated with the huge amount of data is generated by the various devices. IoT integrated with the embedded devices provide the huge security and this is used to prevent the security for the overall components. One disadvantage with the IoT devices are various attacks can be possible to have the intrusion within the devices [1]. If the security is compromised by the components used such as nodes, many hackers can get the control on the compromised nodes and these are used as medium for the attackers to enter into the IoT devices and may damage the overall network.

In this paper, we have discussed the variety of efforts to secure IoT networks and security attacks and vulnerabilities briefly depicted above. The IoT security challenges mainly fall under privacy, cryptographic framework, secure routing and forwarding, localization and tracking, profiling, resilience management in IoT and DoS, and insider attack detection in IoT. Furthermore, we have identified and discussed open issues and challenges in each of the domains mentioned above.

II. LITERATURE SURVEY

The author in [3] explained about the security upgrades in IoT in several application areas. Many key factors for the security necessities for savvy home frameworks are talked about. Likewise, the authors recommended an inexpensive security design for IoT. The important infrastructure is chosen to be the foremost fitting for asset obliged gadgets and for top framework accessibility. This design actualizes advanced administration calculations on a sensibly amazing processor and may work basic shrewd home capacities. Apart from entryway design, different models are examined for IoT are middleware and cloud engineering. Two advances are examined in this work are auto configuration support upgrading framework security and programmed update of framework to stay up continuous secure framework.

Many efforts are developing security for IoT by proficient information labeling through DSC (Data Stream Control) labels are often found in [4]. The detected information is labeled with security properties that let believed control get to hooked in to affect ability. Due to the asset prerequisite of IoT, labeling is over the cost effective, and this work examines the concerns about labeling asset compelled IoT. Four considerations of protection touchy IoT applications including physical association, detecting significant information, disseminated execution, and helpless sensors are lit up which makes DSC information label achievable for

security conservation. Apart from these four, there are two additional properties of such applications that are associated activity and slanted label utilize that make usage of DSC information labels tons simpler.

Many innovations for IoT security provisioning, for instance, RFID is found in [6] with definite conversation on danger investigation of RFID framework segments. RFID innovation is viewed as useful for following and keeping load of things. The author used RFID to empower IoT with mechanical and social issues must be considered.

In [7], authors have proposed a Host Identity Protocol (HIP) and Multimedia Internet Keying convention empowering secure system with the system during a safe way along overseeing keys utilizing a key administration component. HIP use open key cryptography to offer particular ID for IoT gadgets. Moreover, the authors have enhanced HIP to have key administration support.

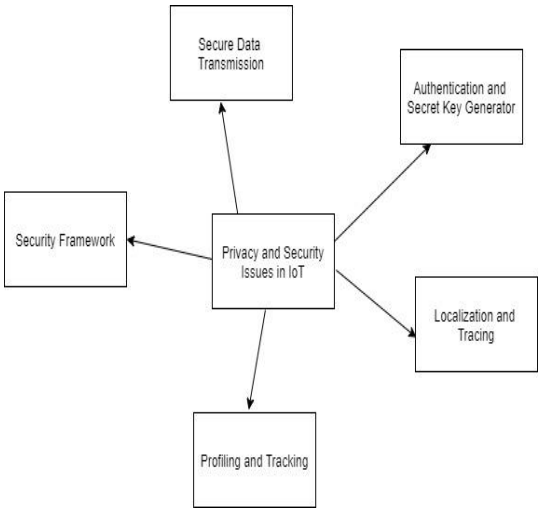

Figure I: Security Issues in IoT

III. SECURITY ISSUES IN IoT

Various IoT Security issues and solutions are discussed:

(1) Profiling and Tracking: The Internet of Things (IoT) is a system of related computing devices, digital machines, objects or people that are provided with unique identifiers and the ability to transfer data over a network without requiring physical interaction**.**

The problem in the logistics industry faces is tracking of the fleet. IoT in particular makes Vehicle Tracking solutions a lot more efficient, economy and automated. There can be n number of use cases for IoT and one of them is fleet management system. Present-day vehicle tracking system can be used for fuel, load, temperature monitoring and RFID integration and so on.

(2) Localization and Tracking: One among the many difficulties of security answers for IoT to structure describes for connections with IoT that disheartens such movement. Immense test lies as per interests of organizations for profiling and knowledge investigation with client's protection prerequisites.

(3) Secure Data Transmission: Security is to ensure that information is transmitted in safer way through the open medium without knowing data to anybody and during this manner forestall unapproved assortment of information about things and individuals.

(4) IoT Security Framework: Many security frameworks are develops various types of integration systems to overcome the issues and security threats in the network or for data transmission these better frameworks are required. An IoT framework is a set of regulations, protocols, and standards which simplify the vulnerabilities of IoT applications. These applications mainly depends on the ecosystem characteristics of the IoT framework, with the emphasis on the security methods employed in it, where issues related to security and privacy are pivotal

(5) Authentication and secret key:

Authentication is used to provide the security for the registered users. Many of the users should be authenticated to become authorized users. This system can be implemented in IoT devices or any network. To access the data or to communicate the various users secret key generator should be used. Secret key can be accessed by the authorized users or nodes only. Current policy mechanisms to manage and control access to customer and enterprise networks map deeply to the IoT/M2M needs. The big challenge is to design an network that can scale to handle billions of IoT/M2M gadgets with varying trust relationships. Traffic policies and adequate controls will be applied throughout the network to segment data traffic and provide end-to-end communication.

The authors in [8] have defined a security design that addresses the safety objectives examined within the paper. Proposed arrangement works as indicated by the lifespan shrewd article in IoT. The keying material is overseen by TTP framework. The proposed structure is employed to provide the important items in an ensured way.

The authors in [9] have proposed an asset well disposed, quick and dispersed security instrument for key understanding and recognizable proof parameters in WSN. The proposed framework depends on alpha secure polynomials that are

proposed for key conveyance and foundation. The authors in [10] have proposed components to build the computation of polynomials progressively lightweight for IoT.

Lightweight key development techniques are explained in [11]. Such plans are proposed for improvement in asset proficiency of such calculations is proposed in [12]. More endeavors on enhancement of the cryptographic activities in IoT security provisioning are proposed in [13] where the authors have demonstrated the equality of the MMO issue to discovering close relations during the cross section. In [14], the approach described another productive ID-based key foundation plot. The personality based plan comprises of a hub with an identifier and a trusted third party (TTP) which furnishes the hub within the system with mystery keying material connected to the devices identifier during a safe manner. Hidden key data and therefore the character of the opposite hub are utilized by different hubs to make a typical pair wise key for secure correspondence. Plan set forward by the creators is proficient as far as key calculation time. In [15], the authors have developed a key administration for BSNs (body sensor systems). The key administration considers the asset wastefulness of IoT and low-power devices.

Table: I VARIOUS ISSUES IN IOT

AUTHOR NAME	TITLE	PROPOSED SYSTEM	ADVANTAGES	DISADVANTAGES
Rijo Jackson Tom et.al	IoT based SCADA Integrated with Fog for Power Distribution Automation	Supervisory Control and Data Acquisition (SCADA) with Fog	This will reduce the internet bandwidth	This is limited for some components in IoT
Shan Zhong et.al	Energy Allocation and Utilization for Wirelessly Powered IoT Networks	low-complexity algorithm	This will solves the sub problems efficiently	Hidden energy issues in IoT
Tai-Yeon Ku et.al	IoT Energy Management Platform for MicroGrid	IoT energy management platform with energy big data system	These are various self-sufficient in small areas	Limited Energy in IoT
Arun M et.al	Smart Grid Robot Exclusively Designed for High Power Transmission Lines	Smart sensing System	This will improve efficiency and to be as much user friendly.	Power line loss detection smart grid robots

IV.OBSERVATIONS

Various issues of IoT as cited above from the table-I are discussed here in detail with some observations.

IoT Based SCADA: IoT industrial SCADA system contains of Sensors, Arduino UNO, display, Wi-Fi and controlling modules. This system is used to monitor and control the various parameters of the industrial operational

Process such as temperature, pressure, speed etc. Arduino UNO is the heart of the system.

Powered IoT Networks: To minimise vulnerable attacks and to keep up the confidentiality and integrity of the transmitted information against the adversaries, it should be protected before transmission. However, issues such as power efficiency, low computational complexity need to be considered when designing security algorithms for CPS/IoT networks.

Energy Management: The most flexible way to save energy is to cut down on wasting it. Smart lighting, learning thermostats and sensor-based HVAC systems of the new generation are designed to maintain the deserve conditions in spaces and keep energy use at the optimum level.

Smart Sensing: Smart sensor has three major components: a sensor that captures data from an space, microprocessor which computes on the output of the sensor via programming and communications capabilities that enable the sensor to transfer the microprocessor's output for action.

V.CONCLUSION

In this paper, we have validated and discussed the traditional work done in ensuring security issues in the IoT network. Efforts in privacy provisioning, cryptographic framework, authentication, Profiling, tracking, resilience management, denial of service, and insider attack detection are discussed comprehensively. Privacy is essential in IoT especially as the characteristics of such a network are different than the typical Internet. Such issues and requirements are identified and explained in this paper. Besides privacy for ensuring Security in the IoT network, cryptographic primitives are required which are well suited for IoT network. All the efforts in this direction are compiled and future actions are discussed

REFERENCES

[1] X. Xiaohui, “Study on security problems and key technologies of the internet of things,” in Proceedings of IEEE Fifth International Conference

Computational and Information Sciences (ICCIS), Hubei, China, June 2013.

[2] A. Kanuparthi, K. Ramesh, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, pp. 61–64, Berlin, Germany, November 2013.

[3] H. Lin and N. Bergmann, "IoT privacy and security challenges for smart home environments," Information, vol. 7, no. 3, p. 44, 2016.

[4] D. Evans and D. M. Eyers, "Efficient data tagging for managing privacy in the internet of things," in Proceedings of 2012 IEEE International Conference on Green Computing and Communications, pp. 244–248, Besancon, France, November 2012.

[5] H. Yang, H. Luo, Y. Fan, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38–47, 2004.

[6] N.Upendra Yadav, Prof Kamalakannan, "Smart Vehicle Monitoring System using IOT", International Journal for Development of Computer Science and Technology (IJDCST), March-April-2017,Issue-V-5,I-3,SW-31.

[7] T.Prasheesh, G. Sreenivasa Rao, Raspberry Pi based Interactive Home Automation System through IOT, International Journal for Development of Computer Science and Technology (IJDCST), July-Aug-2017, Issue- V-5, I-5, SW-19.

[8] B. Khoo, "RFID as an enabler of the internet of things: issues of security and privacy," in Proceedings of 4th International Conference on Cyber, Physical and Social Computing, pp. 709–712, Dalian, China, 2011.

[9] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, and S. L. Keoh, "HIP security architecture for the IP-based internet of things," in Proceedings of IEEE Advanced Information Networking and Applications Workshops (WAINA), Barcelona, Spain, March 2013.

[10] O. Garcia-morchon, R. Rietman, and I. E. Shparlinski, "Interpolation and approximation of polynomials in finite fields over a short interval from noisy values," Experimental Mathematics, vol. 23, no. 3, pp. 241–260, 2014.

[11] H.-C. Chen, "Secure multicast key protocol for electronic mail systems with providing perfect forward secrecy," Security and Communication Networks, vol. 6, no. 1, pp. 100–107, 2012.

[12] O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, and J. L. Torre-Arce, "DTLS-HIMMO: efficiently securing a post-quantum world with a fully collusion resistant KPS," IACR cryptology, 2014.

[13] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-End transport security in the IP-based internet of things," in Proceedings of 21st International Conference on Computer Communications and Networks (ICCCN), pp. 1–5, Munich, Germany, July–August 2012.

[14] O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez, R. Rietman, B. Schoenmakers, and L. Tolhuizen, "HIMMO-a lightweight collusion resistant key predistribution scheme," in Proceedings of IACR 2015, Mumbai, India, 2015.

[15] O. Garcia-Morchon, R. Rietman, L. Tolhuizen, D. Gomez, and J. Gutierrez, "The MMO problem," in Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, New York, NY, USA, July 2014.

[16] O. Garcia-Morchon, L. Tolhuizen, D. Gomez, and J. Gutierrez, "Towards fully collusion-resistant ID-based establishment of pairwise keys," in Proceedings of Extended Abstracts of the Third Workshop on Mathematical Cryptology (WMC 2012) and the Third International Conference on Symbolic Computation and Cryptography (SCC 2012), pp. 30–36, Castro Urdiales, Spain, July 2012.

[17] O. Morchon, H. Baldus, and D. Sanchez, "Resource-efficient security for medical body sensor networks," in Proceedings of Wearable and Implantable Body Sensor Networks, BSN 2006, pp. 80–83, Cambridge, MA, USA, April 2006.