Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/106489, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Survey of Security in Internet of Things – Importance and Solutions

Javeria Ambareen[1*], Pritam Gajkumar Shah[2] and M. Prabhakar[3]

[1]Reva University, Bangalore - 560064, Karnataka, India; javeriaster@gmail.com
[2]Department of ECE, Jyothy Institute of Technology, Bangalore - 560082, Karnataka, India; wsnpgs@gmail.com
[3]School of Computing and Information Technology, Reva University, Bangalore - 560064, Karnataka, India; prabhakar.m@reva.edu.in

Abstract

Background: Internet of Things (IoT) has the potential for societal, environmental as well as economic impact. This comes with a huge responsibility, that of securing all the communications, data and participating things. **Method:** Surveys and comparative studies are used for understanding the security in IoT. **Findings:** This paper surveys the IoT at the architectural and protocol stack level. We outline an effective architectural and stack level restructuring. The integration issues at the IPv6 enabled Low Power Wireless Personal Area Network (6LoWPAN) layer along with the security challenges and existing solutions are discussed and summarized under the chosen parameters. These parameters are Privacy, Authentication, Confidentiality, Denial of Service (DOS) Protect, Replay Protect, Impersonate Protect, End-to-End(E2E) Security.

Keywords: Internet of Things, 6LoWPAN, Security

1. Introduction

Radio Frequency Identification (RFID) technology powered with sensor and a top up of internet has the potential to invade into every sphere of our lives and every ecosystem. This ubiquitous technology is establishing its insidious presence in an expanding range of applications from stack and supply chain management, health care, farming, commerce, surveillance, entertainment to sports.

If IoT has to reach every corner of our lives and be a part of everything, then it must support low cost, low power and low computation devices. Associating a microcontroller with every sensing device or with every "thing" connected to the IoT is not practical. A low cost architecture must be designed that supports these devices giving them the power of IoT. Since every device is connected, since every device taps, stores and communicates information, it becomes mandatory to protect this information from being leaked into the hands of the intruders or from being manipulated.

Security plays an important and vital role in the successful deployment of IoT at the grass root level. It is also necessary that security solutions must be lightweight, in the sense that the security solutions must be capable of operating in low computation power, low memory and mow cost devices.

There are several security solutions available, even so for the constrained devices, but many of these were designed for individual constrained devices and not for the integration into the IoT. The heterogeneity of devices, their varied computational specifications and complexity of the network points to the need for security solutions that are lightweight and operated with global standards.

The remainder of this paper is organized as follows. In Section II, background, definitions, devices and applications of IoT are summarized, in Section III IoT architecture and protocol stack are discussed. Section IV includes issues and attempts for integration of constrained devices into IoT mainly focusing on the 6LoWPAN layer. Finally Section V provides briefs on the

*Author for correspondence

surveys of security challenges and prevailing solutions in IoT, followed by the conclusion in Section VI

2. Background

The Internet of Things (IoT) definition proposed in[1] is "A world where physical objects are seamlessly integrated into the information network and where the physical objects can become active participants in business processes".

The Internet of Things(IoT) is also envisioned in[2] as "enhancing connectivity from any-time, any-place for any-one into any-time, any-place for any-thing".

The "thing" in IoT can be described as objects that are common and special, like the smart phones, laptops, Internet TVs, sensors, RFID systems, thermostats, actuators etc. The most important elements in the IoTs paradigm are Wireless Sensor Networks (WSNs)[3] and RFID technology[4].

Wireless Sensor Networks consist of Sensor nodes with low computational power, low battery power and less memory[5]. These sensor nodes are deployed generally in an unattended area that is spread across larger area to monitor the environmental or physical conditions such as humidity, temperature, noise or even the motion sensing for intrusion detection etc. most of these sensors are not in close contact with humans, and are mostly left to die when drained out of battery power. However the current situation today demands the deployment of sensors more close to the humans and is prone to human intervention. The sensors part of WSNs today also requires them to be charged and maintain a long life time.

RFID systems consist of a tag or transponder, a reader and a server at the backend. The tag and the receiver have an Integrated Circuit for computing and storing. It uses the Industrial Scientific and Medical (ISM) band for communication[6]. The RFID systems help to uniquely identify and locate an object or humans.

The tags in a RFID system consist of an Integrated circuit with memory for computing and an antenna for transmitting and receiving signals. Tags can be passive (no battery, draws power from the reader, inductive coupling), active (has battery to run IC and broadcast signals to reader) or Semi Passive (has battery to run IC but communicate by drawing from the reader). Each tag contains an Electronic Product Code (EPC) number that uniquely identifies the item to which it is attached. This EPC number is transmitted without requiring line-of-sight scanning, unlike the barcode reader. The RFID reader has a radio transmitter, a radio receiver, a memory unit and a control unit[7].

The RFID tags are highly resource constrained and so are the RFID readers. They are vulnerable to many attacks, making security a key concern. The current trends today are also moving towards the integration of WSN and the RFID technology[8]. This new trend opens up new avenue and opportunities for varied applications. The monitoring of environment along with identifying and locating the entity responsible for monitoring also becomes important. This has a special place in the IoT as it has the ability to elevate the power of IoT.

Hence WSNs and RFID systems cannot be directly integrated into the IoTs[6,9]. Also IoT is making a fast penetration into our lives and its benefits extending from remote access, surveillance, health, environmental study to intelligent cities and a smarter planet[10].

IoT finds its applications in variety of domains like logistics, transport, assert tracking, smart environment, smart homes and information, energy, defense, agriculture, smart cities etc[10]. According to[2,11], IoT can be applied in every value chain. The main value drivers identified "Automatic Proximity Trigger, Automatic Sensor Triggering, Automatic Product Security, Simple and Direct User Feedback, Extensive User Feedback and Mind Changing Feedback". IoT applications can also be based on the criticality of the information gathered and the kind of analysis to be performed or on the fact that the data is directed towards and output and relies on control.

3. Iot Architecture and Protocol Stack

[12]Puts forth IoT as a network that subsumes the Internet of People, Energy, Media and Services. The common architectural perception of IoT includes three layers, the Application layer, Network layer and Perception layer. We propose a restructuring of the IoT architecture as shown in Figure.1. This shows four layers the Application layer that has various application and user interactive modules, the Network Layer that enables interconnectivity of things through Zigbee, Wifi etc, the Security Layer that is responsible for the security solutions and a Perception Layer that includes the WSN and RFID as an integral part[13]. The Security layer ensures the embedding of security solutions at either the hardware level or the software level during the manufacturing of the things.

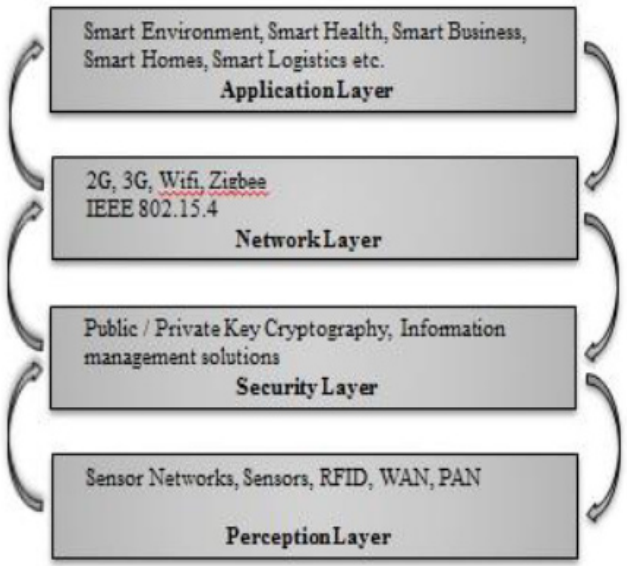

Figure 1. IoT Architecture.

Integration of sensor nodes into IoT can be achieved by Front-end solution, Gateway solution or TCP/IP solution. In Front-end solution the WSN is totally independent of the internet and free to implement its own set of protocols. All interactions between the sensor nodes and the internet host are managed by a centralized device like the base station. The IoT protocol stack[14] is shown in Figure.2, the application layer is guarded by Constrained Application Protocol (CoAP), which is standardized as a web protocol for IoT. Datagram Transport Layer Security (DTLS) in Constrained Environment (DICE).

[13]in transport layer runs over User datagram Protocol(UDP). Routing over Low Power Lossy Networks (ROLL) is achieved through the Routing Protocol for Low-power and Lossy Networks(RPL) is a protocol that is implemented over the basic IPv6 enabled over Low Power Wireless Personal Area Networks(6LoWPAN) or IPv6 over Time Slotted Channel Hopping(6TiSCH). These protocols are guided by Authentication and Authorization in Constrained Environment (ACE) and Lightweight Implementation Guidance (LWIG). Link layer security is provided by IEEE 802.15.4 MAC and IEEE 802.15.4e MAC. The physical layer implements the IEEE 802.15.4 PHY[15].

The authors have proposed use of IPsec and DTLS for secure communication in the IoT, they have proposed and developed lightweight IDS for 6LoWPAN networks that use RPL as routing protocol in the IoT.

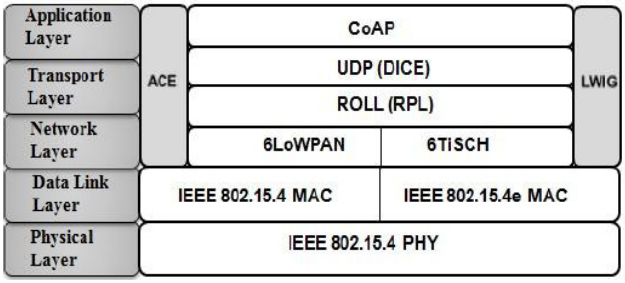

Figure 2. IoT Protocol Stack.

4. Integration of Constrained Devices into IoT

6LoWPAN aids the integration of constrained devices into the IoT over an IPv6 based communication and using the IEEE 802.15.4 links[16]. IPv4 has only 32 bits for addressing were as IPv6 has 128 bits for addressing. IPv6 supports 2128 unique addresses, sufficient enough to connect the future heterogeneous devices to the Internet. 6LoWPAN is an adaptation layer, intermediate to the MAC and the Network layer. It supports and coordinates with the IEEE 802.15.4 standards[17]. It also deals with address management, fragmentation and reassembly. The authors of[16] suggest that the AES security that is part of the IEEE 802.15.4 link layer is not full proof and needs to be strengthened.

As the number of "things" getting connected to the internet increases, the need to provide IP connectivity to these devices also increases. Figure.3. shows the different scenarios in which IP connectivity can be achieved in the IoT. A thing could be a part of the small interconnecting domain that connects to the internet through the edge router, or it could be an Ip enabled device that directly connects to the internet.

[18]Presents and demonstrates an efficient implementation of 6LoWPAN stack on the AWSAM-1 wireless sensor node. The authors of[18]conclude that it if feasible to implement 6LoWPAN on constrained devices, however memory management and logical timer management needs enhancement.

The heterogeneity of devices connected over the IoT makes it very important for the establishment of a common language between the devices that will enable them to communicate with each other. 6LoWPAN is one such enabler, but as evaluated by[19] the performance of 6LoWPAN and present the numerical results in terms of packet loss rate, payloads, throughput, hops required

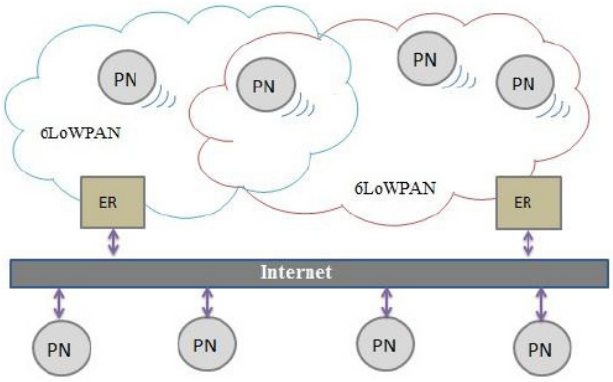

Figure 3. Connectivity Scenarios in IoT.

and the round trip time. [17]also presents a survey on the state-of-art implementation techniques available for the 6LoWPAN stack.

A deeper investigation into the management issues of resource constrained devices is provided by[20]. They make a deeper investigation of how the existing Simple Network Management Protocol (SNMP) and the Network Configuration Protocol (NETCONF) can be implemented in resource constrained devices such as the 8-bit Atmel AVR Raven device, using the Contiki operating system. The main challenges that emerged are the message fragmentation, session establishment and security issues.

The RFID systems face several issues when trying to find a place in the IoT. Some of these issues are low processing capabilities, low battery power and most of all the security issue. [21]propose a lightweight protocol called the LRMAPC – Lightweight RFID Mutual Authentication Protocol with Cache. This cache is placed at the reader. This protocol has been successful in achieving stronger security compared to schemes like the Hash Lock Protocol etc, mentioned in the paper but at the cost of larger space at the reader.

5. Security Challenges and Prevailing Solutions

The main challenges for IoT security are from the heterogeneity, the large scale of objects and Adhoc deployment of devices.

- Object Identification
- Standardisation
- Interoperability
- Privacy, Authentication and Authorization
- Lightweight Crypto Systems and Security Protocols
- Software Vulnerabilities and Backdoor Analysis
- Malware in IoT
- Self Healing

IPSec provides security for the IoT enabled devices, by assuring them authentication and privacy in terms of encryption. [22]Shows an implementation and evaluation of IPSec over 6LoWPAN and provide with critical conclusions that it is possible to secure the end-to end (E2E) communication between a sensor node in WSN and an IPv6 enabled node.

The Datagram Transport Layer Security (DTLS) is not a lightweight protocol, rather it is a heavyweight protocol and cannot be directly implemented at the 6LoWPAN layer of the IoT[23]. In[24] the DTLS is compressed and integrated into the 6LoWPAN. It is found that this has a direct impact on the security bits, as they have found to be reduced by 62%.

The Public Key Infrastructure (PKI) supported by conventional WSNs cannot be directly integrated into the IoT and the 6LoWPAN. The authors of [25] propose an edge router to take the responsibility of being higher in computation power, maintaining the Key database and communicating with the server for the Certificate Authority (CA) over the IPv6 network. But the implementation and performance evaluation showed that through this scheme security was achieved but at the cost of time and packet count.[26] Performs an analysis of the impact of fragmentation at the 6LoWPAN adaptation layer on the energy consumption and finds that there was an increase by 5% to 10% at the sensor nodes.

[27]Addresses the security issues that may arise at the 6LoWPAN layer and the available security schemes. The current security protocols and the security solutions such as the Carrier Sense Multiple Access – Collision Detection (CSMA-CA), Secure Firmware for the Physical layer, Advanced Encryption Standards (AES) for Link Layer, Hash Chains for Application layer are suggested.

[28]Proposes a Symmetric Key Cryptographic scheme, the EAKES6Lo that operates at the 6LoWPAN layer for a sensor node enabled IoT. This scheme was successful in preventing some of the main attacks such as the replay attack, impersonation attack, compromised key attack etc.

Since the sensors are usually small and inexpensive and have limited energy sources, any protocols to be deployed in sensor networks need to be aware of the

resource constraints. The limited memory (about 4KB) of a sensor node imposes challenges on management of a large key (such as a 1024 bit key), hence lightweight protocols need to be used ensuring the same level of security[29]. One such scheme for consideration is Elliptical Curve Cryptography[30].

The security across the different layers is addressed by[31]. The application layer messages are communicated over a secure channel between the application layer and transport layer in a lightweight manner.

A study of real world scenarios and deployments of IoT help in analyzing the security risks. One such scenario, the home automation is closely studied by[32] addressing the security issues and privacy preservation over a network with a compromised remote server. The two techniques used are cryptographic and information manipulation techniques.

[33]Surveys a wide literature and performs an effective implementation to achieve E2E security through connectionless, caching and multicast support. A novel authentication scheme based on packet analysis that yields in low energy consumption is shown in[34].

[35]Also address the authentication issue and introduces a key management protocol that handles multicast improving the network overhead. Privacy at the customer level using a "Ring Communication Architecture" that results in low E2E delay is achieved in[36].

The smart city scenario is analyzed by[37], focusing on the participating things and their life cycle. The security scheme proposed based on "HIMMO" is lightweight, efficient and can be integrated into the existing communication protocols.

The following table shows the comparison of the existing security solutions over the chosen parameters.

Table 1. Comparison of Security Solutions

Parameters	Paper Contributions									
	22	25	28	32	34	35	36	37	33	31
Privacy				✓			✓	✓		
Authentication					✓	✓		✓	✓	
Confidentiality						✓	✓		✓	
DOS protect			✓			✓			✓	✓
Replay protect			✓						✓	✓
Impersonate protect			✓							
E2E security	✓	✓					✓		✓	

6. Conclusion

In this survey of the Internet of Things, we have considered the different things and their integration issues into IoT. The IoT architecture and protocol stack have also been surveyed. The security layer at the architectural level can further be enhanced by both software and hardware integration. The existing security solutions are compared and analysed over the chosen parameters. It is found that most the analyzed solutions do not provide a standardized solution capable of addressing the key security parameters. A standard compliant solution on the 6LoWPAN layer is yet to be achieved. These are the findings of our initial research. This paves way for the development of further firm security aware architecture and security solutions.

7. References

1. Haller S, Karnouskos S, Schroth C. The internet of things in an enterprise context: Springer, 2009.
2. Coetzee L, Eksteen J. The Internet of Things-promise for the future? An introduction. IST-Africa Conference Proceedings, 2011, 2011. p. 1–9.
3. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013; 29:1645–60.
4. Sun C. Application of RFID technology for logistics on internet of things. AASRI Procedia. 2012; 1:106–11.
5. Akyildiz IF, Vuran MC. Wireless sensor networks. John Wiley & Sons, 2010; 4.
6. Juels A. RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications. 2006; 24:381–94.
7. Thompson DR, Di J, Daugherty MK. Teaching RFID Information Systems Security. IEEE Transactions on Education. 2014; 57:42–7.
8. Mitrokotsa A, Douligeris C. Integrated RFID and sensor networks: architectures and applications. RFID and sensor networks: Architectures, protocols, security and integrations. 2009; 511–35.
9. Hyuk Park J, Gritzalis S, Hsu C-H, Roman R, Lopez J. Integrating wireless sensor networks and the internet: a security analysis. Internet Research. 2009; 19:246–59.
10. Liu J, Yang L. Application of Internet of Things in the community security management. 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN). 2011. p. 314–8.

11. Fleisch E. What is the internet of things? An economic perspective. Economics, Management, and Financial Markets. 2010; 125–57.
12. Vermesan O, Friess P, Guillemin P, Gusmeroli S, Sundmaeker H, Bassi A et al. Internet of things strategic research roadmap. Internet of Things: Global Technological and Societal Trends. 2011; 1:9–52.
13. Wu M, Lu T-l, Ling F-Y, Sun L, Du H-Y. Research on the architecture of Internet of things. 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). 2010. p. V5-484–V5-487.
14. Sajjad SM, Yousaf M. Security analysis of IEEE 802.15.4 MAC in the context of Internet of Things (IoT). 2014 Conference on Information Assurance and Cyber Security (CIACS). 2014. p. 9–14.
15. Bagci IE, Raza S, Chung T, Roedig U, Voigt T. Combined secure storage and communication for the internet of things. 2013 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON). 2013. p. 523–31.
16. Xin M, Wei L. The Analysis of 6LowPAN Technology. Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. PACIIA '08. 2008; 963–6.
17. Chen Y, Kun-Mean H, Haiying Z, Hong-Ling S, Xing L, Xunxing D et al. 6LoWPAN Stacks: A Survey. 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM). 2011. p. 1–4.
18. Pediredla B, Kevin IKW, Salcic Z, Ivoghlian A. A 6LoWPAN implementation for memory constrained and power efficient wireless sensor nodes. IECON 2013 - 39th Annual Conference of the IEEE in Industrial Electronics Society. 2013. p. 4432–7.
19. Gardasevic G, Mijovic S, Stajkic A, Buratti C. On the performance of 6LoWPAN through experimentation. 2015 International in Wireless Communications and Mobile Computing Conference (IWCMC). 2015. p. 696–701.
20. Sehgal A, Perelman V, Kuryla S, Schonwalder J. Management of resource constrained devices in the internet of things. Communications Magazine, IEEE. 2012; 50:144–9.
21. Kai F, Chen L, Hui L, Yintang Y. LRMAPC: A Lightweight RFID Mutual Authentication Protocol with Cache in the Reader for IoT. 2014 IEEE International Conference on Computer and Information Technology (CIT). 2014. p. 276–80.
22. Raza S, Duquennoy S, Chung T, Yazar D, Voigt T, Roedig U. Securing communication in 6LoWPAN with compressed IPsec. 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS). 2011. p. 1–8.
23. Capossele A, Cervo V, De Cicco G, Petrioli C. Security as a CoAP resource: An optimized DTLS implementation for the IoT. 2015 IEEE International Conference on Communications (ICC). 2015. p. 549–54.
24. Raza S, Trabalza D, Voigt T. 6LoWPAN Compressed DTLS for CoAP. 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS). 2012. p. 287–9.
25. Goswami S, Misra S, Taneja C, Mukherjee A. Securing intra-communication in 6LoWPAN: A PKI integrated scheme. 2014 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS). 2014. p. 1–5.
26. Mesrinejad F, Hashim F, Noordin NK, Rasid MFA, Raja Abdullah RSA. The effect of fragmentation and header compression on IP-based sensor networks (6LoWPAN). 2011 17th Asia-Pacific Conference on Communications (APCC). 2011. p. 845–9.
27. Hennebert C, Dos Santos J. Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis. Internet of Things Journal, IEEE. 2014; 1:384–98.
28. Yue Q, Maode M. An authentication and key establishment scheme to enhance security for M2M in 6LoWPANs. 2015 IEEE International Conference on Communication Workshop (ICCW). 2015. p. 2671–6.
29. Stankovic J. Research directions for the internet of things. Internet of Things Journal, IEEE. 2014; 1:3–9.
30. Shah PG, Xu H, Sharma D. Analytical Study of Implementation Issues of Elliptical Curve Cryptography for Wireless Sensor networks. 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA). 2010. p. 589–92.
31. Bhattacharyya A, Bose T, Bandyopadhyay S, Ukil A, Pal A. LESS: Lightweight Establishment of Secure Session: A Cross-Layer Approach Using CoAP and DTLS-PSK Channel Encryption. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA). 2015. p. 682–7.
32. Schurgot MR, Shinberg DA, Greenwald LG. Experiments with security and privacy in IoT networks. 2015 IEEE 16th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). 2015; 1–6.
33. Vucinic M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R. OSCAR: Object security architecture for the Internet of Things. 2014 IEEE 15th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). 2014; 1–10.
34. Bartoli A, Hernandez-Serrano J, Leon O, Kountouris A, Barthel D. Energy-efficient physical layer packet authen-

ticator for machine-to-machine networks. Transactions on Emerging Telecommunications Technologies. 2013; 24:401–12.
35. Nicanfar H, Jokar P, Leung V. Smart grid authentication and key management for unicast and multicast communications. 2011 IEEE PES in Innovative Smart Grid Technologies Asia (ISGT). 2011; 1–8.
36. Li S, Choi K, Chae K. An enhanced measurement transmission scheme for privacy protection in smart grid. 2013 International Conference on Information Networking (ICOIN). 2013. p. 18–23.
37. Garcia-Morchon O, Rietman R, Sharma S, Tolhuizen L, Torre-Arce JL. A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO. Algorithms for Sensor Systems, ed: Springer. 2015; 112–28.