International Journal of Multidisciplinary Research and Modern Education (IJMRME)
ISSN (Online): 2454 - 6119
(www.rdmodernresearch.org) Volume I, Issue II, 2015

INTERNET OF THINGS ARCHITECTURE BASED ON SECURE LAYERS

Priya Thomas
Krupanidhi Group of Institutions,
Bangalore, Karnataka

Abstract:

The Internet of Things (IoT) is a smart machine/object/thing network-based system where each machine is capable of self-configuration and communicates with physical objects based on common and interoperable protocols of communication. Identities are the fundamental characteristics of physical objects. Autonomous individuals using smart interfaces and embedded in the new and emerging data networks seamlessly is provided. In fact, with this intense open contact between objects, stable and protected objects for IoT services come to light. The paper, therefore, proposes a novel computational cross-layer design that ensures proper use with a 5- 5-layer protection function of the Adaptive Interface Translation Table (AITT). Each layer has a particular responsibility to process the assigned job and to transmit data for further processing and inferences to the next layers.Finally, for the safety of IoT apps and services, we present a conceptual solution.

Key Words: Future Internet Services, 6LoWPAN, IoTarchitecture, WSN, IoT security

Introduction:

All links, which share information and interact seamlessly in the Internet of Things, are part of the world. IoT refers to as linked objects in some literature. The Internet of Objects was also referred to[1]. IoT is defined as a point in time, by Cisco Internet Business Solutions Group (IBSG)[2], when "the number of internet-connected objects will be greater than that of people who have Internet connectivity". IoT is necessary because all data unprocessed must be converted into data and subsequently into meaningful information. There is a knowledge discovery from this information. Knowledge gives results by sharing this among IoT modules.The impact on security, military, medical science, education, and business of the Internet today is huge[3]. This shows that the Internet is quite important in human history. NTT GROUP[4] reveals that anti-virus technologies fail to detect 54% of malware planned to take over the networks that are infected and 71% of all modern malware are intended to make money or steal information. We currently do not have a successful IoT identity fraud protection approach (IITP).

The Semantic Fusion Model (SFM) for future services was addressed in our previous work [5]. Here the semantic model of information in the IoT domain sensors and gates are incorporated. The semantic model also takes into account the complexities of using bandwidth and approaching the millions of IoT sensors especially. The Internet is undergoing an evolution, and the next big step is to create IoT objects and interact on IoT models and platforms. Based on the ZigBee network, new implementations are explored at IoT. According to [3] and [5], a trust center, which handles security demands, determines the security of sensor networks through architecture. The IoT is a massive phenomenon, in which many 6lowpan networks and sensor nodes (IPv6 via low-power wireless networks) are linked to data gateways which is extremely challenging as the transfer to them is not fast. The implementation of IPv6 across the world and electricity grids in millions of nodes would otherwise be cost-effective for the whole IoT purpose. Therefore a general set of specifications must be standardized for communication protocols over IoT objects. In the area of defense, there

are unique problems. The understanding of the environmental challenge is one of the increases as we cross the IoT with the IPv6 and Potential Internet domains. There is a rising need for consumers to access any device they want and have an interest in the site itself. This broad access to infrastructure and expertise requires new IoT security solutions.In this article, we discuss the security problems of the Internet of Things and the way to implement the stable application in a protected IoT architecture. The challenges and the strategic plan of our strategy have been discussed.

Observation and Challenges:

With the expanded availability of distributed networks, intelligent devices are growing every day. The built-in devices have the IoT set of devices attached. From passive RFID tags to powerful embedded sensors, we experience a broad spectrum[6]. Similarly, a variety of apps now have a certain amount of connectivity to the Internet, enabling connectivity and information access, and difficulties related to enterprise infrastructure to gain market benefits.

A. Problem and resolution in Mobility:

In particular, when talking about mobility conformity of IoT artifacts, IoT protection is a big area of concern. Management of mobility can have a veiled identity that may misrepresent the node's true identity. The present format will recognize a variety of challenges.

- Integration in a single network with all heterogeneous IoT platforms. IPv6 is also a major consideration for solving IoT artifacts' scalability and mobility problems.
- Privacy and integrity of IoT allowed objects and existing internet users
- Mobility: the device allowed by IoT must work all while the mobility of the IoT devices is met. In today's environment, there is a rise in mobile phones, tablets that are omnipresent in device management. Real-life is packed with Smart phone apps and therefore mobility in its implementation context is important for IoT devices.
- Data management: Big data must be managed by the volume of data that is supposed to be produced by thousands of IoT devices.

Many broker agents are responsible for the initialization of several essential features such as technologies, frameworks, and item cost problems.

B. Problem and resolution in Security:

The benefit of the 6lowpan network is that it can be connected to all sorts of IoT devices including smart home automation, smart city, intelligent security management, intelligent energy management, logistics management, etc. However, 6lowpan networks are primarily concerned with stability. We must also concentrate on mobile and static data protection strategies.

- Confidentiality of Message: End-to-end messages shared between IoT devices need to be secure. To secure data pass across the internet, some type of encryption and decryption algorithm must be given.
- Message Data integrity: Data from source and destination must never be altered.
- Message Source Authentication: The various sources should be able to be established through authentication protocols as given in [7].
- Message availability: Device intrusions and malicious activity. Different forms of intrusion device monitoring may be used to fix the system's protection problems.
- Message replay protection: Safety must also be taken care of at all intermediate nodes. Both repeat messages and replaying saved messages must be closely

identified by strict mechanisms. Configurations such as sequence numbers or network layer time stamping can be an immense help to the security of IoT.

C. Problem and Resolution in 6LoWPAN Node Space:

In the 6LoWPAN stack, IPv6 was compressed. The actual IoT is the current IPv6 network connected with intelligent devices. In nature, the IoT world is extremely diverse. IoT device composition can vary in different fields. It can be a sensor node, a ventilator, a bulb, a fridge, a TV with LED, a Smartphone, an embedded device, and even a cloud. Thus the number of devices on an IoT platform can go up to thousands of thousands of devices. The IP-based infrastructures and WSNs are integrated with 6LoWPAN. To achieve this goal, the standard 6LoWPAN proposes context-conscious mechanisms of header compression[8]. For the IPv5 header and the User Datagram (UDP) header, the IPv6 header compression (IPHC) for the IPv6 headers exists. Generic Header Compression (GHC) has also been introduced in [9]. The 6LoWPAN networks are connected via the Internet 6BR or gateway LoWPAN's border router.

Cross-Layer Architecture:

On the IoT network, there are many innovations. They turn from stateless to stately, from very restricted to unrestricted, from difficult in real-time to soft-real time systems. The physical object of the IoT universe consists of virtual modules which can create and use resources across the Internet. The number of interacting objects will grow by billions and thus maintain the IoT universe and demand new protection and technical approaches to IoT objects. We are visualizing a future in which all living entities will be part of the groundbreaking IoT universe as good as non-living objects. The location, address, and user-friendly description of each such object on the Internet will be part of IoT.

For starters, a user's machine knows about itself.The machine knows the identity and purpose of the physical counterparts can interact with them and can make its own decisions. IoT stretches from everywhere, anyway, anywhere, to anything, anybody, any service. With the arrival of IoT-based artifacts and solutions around the world, the modern Internet is evolving many times. Ipv6 protocols are being used to interconnect the latest series of computers in the same way as clever artifacts in the wireless network region (WSNs).

This integration of IoT-based devices with the Internet would revolutionize the world as we feel it. Take into account the entire universe of IoT-based artifacts and smooth connectivity on Ipv6 platforms. The most important thing is the protection of the objects and the safety of the transmitted data.The internet we know has devised its approach of protecting and stopping disruptive assaults. The future we envision is filled with the internet and intelligent, resource-constrained networks. It is also imperative that we obey the security line which is the basis of communication with the IoT objects. Security, secrecy, honesty, and authentication services are the fundamental foundation of all contact related to security. The network must therefore be protected from malicious attack. It is of utmost importance that data reside in the sensor nodes. The node sensor must be physically secured as well as the data must be encrypted. We have seen IoT protection as a layered architecture, in which data on multiple layers can be protected.

For more rigid security measures, the layers may be modified at the application's discretion. Normally protection in various layers exists on the IEEE 802.15.4 security adapter, on the IP Security Network Layer (IPSec), and Datagram Transport Layer Security (DTLS) transport layer [10]. After the architecture and encryption of the senor node have taken all security precautions the data from inside the WSN networks can

still be damaged as an Internet host. The need for firewalls is also justified in the context of an intrusion detection system (IDS). This paper has considerable feedback from the latest architecture of cross-layer stack creation that provides the data packets residing in the data format with adequate protection and independence.

Normal TCP/IP blocks are transmitted to the stack above. The security and AITT features can allow us to compact security bytes and thereby provide more space for interacting with real applications. With an example of basic home automation methods, we illustrate our architecture. We might be speaking about home control in which we attempt to remotely obtain the rights of each appliance. We can operate remotely and turn off our home appliances at least with the slightest hesitation or in the event of a warning. Thus, our proposed new cross-layer architecture will accomplish a great case of home automation.

The IoT view is usually that it cannot be extracted from one scheme. Many minor contributions and specifications will help us develop the IoT and security architectures using the IPv4-IPv6 crossover and the use of IoT web services.There are several benefits that the IoT device would explore. It will make for a homogenous framework for application integration with the Internet host gateways as well as common frameworks for streamlined cross-platform development.

IoT is a dynamic combination of homogenous as well as heterogeneous structures that is supported by a variety of third-party implementations on all manner of cross-layer platforms. With scarce capital, there is a significant justification for pursuing and being a standard for security technologies and protocols in the IoT world. Normally any architecture is a structure that is used to coordinate and customize the physical components of the network. It further addresses the operating standards and procedures of data formats and packets used for information communication and sharing.

Security Concern Architecture:

In the final correspondence, separate solutions can be sought at the respective layers of the stack. In the respective layers of the IoT stack, we addressed several typical protection solutions.

A. Link Layer: IEEE 802.15.4 Security

According to [11] 6LoWPAN networks are connected to IEEE 802.15.4. The latest IoT security approach is 802.15.4 link-layer security[12]. The node involved in the coordination mechanism must be trusted in the connection layer. Different node numbers, as well as multiple hops, may be used for connectivity. Until communication, a key is established. This key is used to encrypt any contact occurring during the communication period. If the key is affected, the protection of the entire layer is affected. In each hop unauthorized change can be identified by the protection arrangement per hop.In hop-based protection arrangements for the 6LoWPAN networks, data protection must be established. The protection of the connection layer is restricted to maintaining contact between two nearby nodes. This is one of the versatile choices that can be found in the layers above ties with several protocols.

B. IP Security: Network Layer

The IP Protection (IPSec) protocols provide security on the network layer as specified under [13], [14]. This protocol guarantees end-to-end safety with the above-described authentication, honesty, playback security, and confidentiality. In a network layer, the protocol IPsec can be used by different protocols for transport layers, such as TCP, UDP, HTTP, and CoAP [14]. It encourages IPSec, thus using the Authentication

Header (AH) protocol with the assistance of [13]. IPSec is a network layer solution that is thus shared with all software on a single computer in terms of confidentiality.

C. CoAP Security for Transport Layer:

On this layer, protocols like Transport Layer Security (TLS) or Secure Sockets Layer (SSL) are widely used. Only street-oriented TCP can be used with TLS protocol, which may not be a perfect way to connect wirelessly. The Datagram of TLS [15] is another protocol, which is a UDP TLS adaptation. DTLS ensures end-to-end protection in numerous applications. Also, with cookies on the network protocol domain, DTLS allows for security against Denial-of-service (DoS) attacks. Just the UDP protocols can be used for DTLS. This means that DTLS help for IoT becomes imperative.

D. Network Security:

The network is also vulnerable to network attacks that could jeopardize stability, taking the above precautions. Many Intrusion Detection Systems (IDS) may be implemented to identify impostors and malicious network operations. Unauthorized network connections must be blocked by firewalls. There are thousands of computers in the IoT universe and any component we consider to be part of the big bang virtual world can now be identified with. 6IoT LoWPAN networks are vulnerable to a variety of Internet threats and network attacks. The wireless domain resource limits of the IoT universe are more quickly violated than a standard Internet. We need specific IDS, which will make IoT-activated systems more holistic.

E. Data Security in the IoT World:

It can be argued confidently that network and connectivity can be protected by the implementation of different methods of communication and network security.

The next problem is to store the data kept by IoT computers. Stored data can be private, sensitive and should be secured in the IoT products. The IoT universe would consist of small nodes that are limited in the capital. The physical or use of Trustworthy Platform Modules (TPM) [15] is quite challenging to keep any billion devices secure.

The latest variation of IoT system management protocolsis the ZigBee standard [16]. IoT's protection infrastructure continues to evolve. A reference model is better defined and therefore the system cannot be described with a single architecture. Too many unknown technologies and applications are being developed. A layered protection architecture model is therefore ideally suited to this purpose. The layers can be tailored to the emerging security tradition as defined in our architecture [17].

According to [18] the world of IoT is widely dispersed and the use of embedded technology in a public space will leave ample holes for the harsh hackers to exploit. On-street IoT-enabled items are vulnerable to physical damage. Adding threats to access to sensitive and private data of the device or social elements is the user profiling of certain IoT objects [18]. Generally, when an IoT-based system interacts with other IoT objects, a safe connection is required from end to end. The channel demands that the two participating partners jointly create a shared hidden key. Under the [19] basic key exchange protocols such as Transportation Layer Security Handshake (TLS) or Internet Key Exchange can provide this key control (IKE). This calls for costly cryptographic solutions that leave an object based on IoT for additional resources.

Conclusion:

A radically new understanding of AITT has been implemented in a stable cross-layer architecture for IoT. In the future, real deployment in a home automation system will be included. IoT is a dynamic heterogeneous and uniform sensor system. Protection and secrecy are the main concerns for IoT implementations and also face immense difficulties and have addressed the safety design and functionality review. The key

aspects of layered design and safety problems were discussed. The philosophical perspective of our protection work will change the framework. Applications can be created and the framework can be updated according to its security specifications. The IoT-enabled artifacts have been attempted to overview the safe.

References:

1. The Internet of Things-How the Next Evolution of the InternetIs Changing Everything – Cisco white paper – April 2011, www.cisco.com/web/about/ac79 /docs/innov/iot_ibsg_0411final.pdf Accessed by July 14, 2015.
2. Cisco defines the Internet of Everything in http://www.cisco.com/web/about/ ac79/index.html, Accessed by July 13, 2015
3. Alberti A. M., Singh D., "Internet of Things: Perspectives, Challenges and Opportunities", International Workshop on Tele communications (IWT2013), June 2013.
4. Global Threat Intelligence Report, 2014 NTT Innovation Institute 1 LLC, Accessed by July 14, 2015
5. Singh, D., Tripathi, G., and Jara, A. J., "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in Proc. of the IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, IEEE, 2014.
6. Singh D. "Developing an Architecture: Scalability, Mobility, Control, and Isolation on Future Internet Services", Second International Conference on Advances in Computing,Communications and Informatics (ICACCI-2013), Mysore, India, 2013, pp.1873-1877.
7. Cisco disused RFID Tag technology, accessed on Oct. 30, 2015, http://www.cisco. com/c/en/us/td/docs/solutions/enterprise/mobility/wifilbs-dg/wifich6.pdf,
8. Singh D. (2015), Secure 6LoWPAN Networks For E-Healthcare Monitoring Applications. Journal of Theoretical and Applied Information Technology, E-ISSN: 1817-3195
9. Raza, Shahid, et al. "Securing communication in 6LoWPAN with compressed IPsec." Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference, IEEE, 2011.
10. Soro, A.; Lacan, J.; Chaput, E.; Donny, C.; Baudoin, C.,"Evaluation of a Generic Unidirectional Header Compression Protocol," Satellite and Space Communica., 2007. IWSSC'07. International Workshop on, vol., no., pp.126, 130, 13-14 Sept. 2007
11. Datagram Transport Layer Security: https://tools.ietf.org/html/rfc4347, Accessed by July 22, 2015.
12. Culler, David E., and Jonathan Hui. "6LoWPAN Tutorial: IP on IEEE 802.15. 4 Low Power Wireless Networks." Arch Rock Corporation (2007).
13. Kothmayr, Thomas, et al. "DTLS based security and two-way authentication for the Internet of Things." Ad Hoc Networks 11.8 (2013): 2710-2723.
14. S. Kent. IP Encapsulating Security Payload. RFC 4303, 2005. http://tools.ietf. org/html/rfc4303.
15. Singh Dhananjay, "Secure 6LoWPAN Computing Stack forGlobal Health care Monitoring Services", Journal of Theoreticaland Applied Information Technology, Vol. 76, No.2, pp. 143 ~151, 2015.
16. ZigBee. http://www.zigbee.org/
17. Trusted Platform Module (TPM) Work Group. TCG specification architecture over view (TPM 2007), 2007. http://www.trustedcomputinggroup.org/.

18. Suo, Hui, et al. "Security in the internet of things: a review."Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference. Vol. 3. IEEE, 2012.