Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Security Architecture of IoT

Bobby.S,
Assistant Professor, Department of Computer Science, St. Joseph's College of Arts and Science for Women, Hosur

Abstract-- IoT can be defined as things belonging to the Internet to supply and access all of real-world information. IoT is the biggest promise of the technology today, but still lacking a novel mechanism which can be perceived. In this scenario, the satisfaction of security and privacy requirements plays a fundamental role. Such requirements include data confidentially and authentication access control within the IoT network, privacy and trust among users and things and the enforcement of security and privacy policies. Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. In this survey we present the main for the IoT security architecture and suggesting some hints for future research.

Keywords-- *Internet of Things, Security Architecture, Privacy.*

I. INTRODUCTION

Internet Of Things(IoT) was first proposed in 1999 by Auto – ID Center and has become a spotlight after U.S President made a positive statement to encourage the development of IoT, praising it as a future strategic newly-emerged industry. IoT involves many technologies including architecture, sensor/identification, coding, transmission, data processing , network, discovery, etc. IoT development depends not only on the progress and standardization of technologies, but also on the improvement of our social perception, knowledge, rules and laws. For example in the future IoT era the way we live like components or nodes of the network and the exposition of our activities to the public may bring for the many serious security and privacy problems.

IoT Definitions: The term internet of things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is however no single universal definition.

A. What is the internet of things?

The term "Internet of Things"(IoT) was first used by pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the internet by sensors. Ashton coined the term to the power of connecting Radio-Frequency Identification (RFID) tags; used in corporate supply chains to the internet in order to count and track goods without the need for human intervention. Today, the Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors and everyday items.

While the term Internet of Things is relatively new the concept of combing computers and networks to monitor and control devices has been around for decades. In the 1990s advances in wireless technology allowed machine-to-machine(M2M)enterprise and industrial solutions for equipment monitoring and operation to become widespread. Many of these early M2M solution, however were based on closed purpose built networks and proprietary or industry-specific standards rather than on internet protocol(IP) based networks and internet standards.

B. IoT Applications:

According to the characteristics of own internet of things, following categories of services should be provided.

1. Networking Service: goods identification, communication and positioning.
2. Informational Service: information collection, storage and query.
3. Operation Service: Remote configuration, monitoring, operations and control.
4. Security Service: User management, access control, event alarm, intrusion detection, attack prevention.
5. Management Service: Fault diagnosis, performance optimization, system upgrades, billing management services.

General types of service of IoT listed above which could extend on the basis of application requirements of IoT in diverse areas.

C. Relationship between IoT and Other Exiting Networks:

The explosive growth of the requirements communication for information between machines raised concerns, such as, the optimization of the human environment the management

Of the management of urban security the improvement living

Quality and effective management of production the "Internet Of Things"(IoT) is in great demand. Our government has a high regard to the research and development of IoT, as we are moving towards the "Internet Of Things"(IoT) as depicted by [1] millions of devices will be interconnected providing and consuming information available on the network and cooperate.

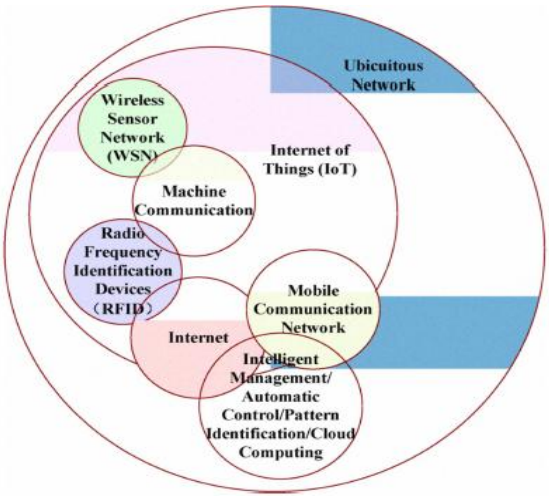

Figure 1: The Relation between IoT and Other existing networks

International Telecommunication Union (ITU) put forward "Internet Of Things" in the report in 2005 there is still not a generally accepted concept. The basic concept of IoT is: together with web services, such as Radio Frequency Identification Devices (RFID), Infrared sensor, Global

positioning System, laser scanner, a network of Internet-enabled objects connected with the Internet based on the conventional protocol, to exchange information and communicate, in order to achieve intelligent identify, locate, track, monitor and manage a network[2]. IoT evolves from the Internet and short-range communication network. The following shows the relationship between IoT and other existing networks.

D. Characteristics of IoT:

Internet of things has three important characteristics:

1. Comprehensive sense: Using RFID, Sensor, two-dimension code to collect information of objects anytime, anywhere.
2. Reliable transmission: Accurate real-time delivering information of objects through meshing a variety of telecommunications network and internet.
3. Intelligent Processing: Using intelligent computing such as cloud computing and fuzzy identification to analyze and process vast amounts of implementation of intelligent control to objects.

II. SECURITY IN IoT

The protection of data and web ought to be outfitted alongside these properties such as identification, confidentially, integrality and undeniability. Disparate from internet, the IoT will be requested to the critical spans of nationwide economy, e.g., health ability and condition care, and intelligent transportation, therefore protection needs in the IoT will be higher in potential and dependability [5].

A. Secure Architecture

In general, the IoT can be divided into four key levels. Figure. 2 shows that the level architecture of the IoT.

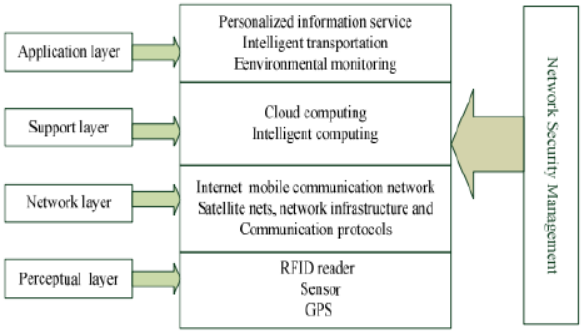

Figure 2: Security architecture of Internet of Things

The most frank level is the perceptual layer (also recognized as credit layer), that accumulates all kinds of data across physical supplies and identifies the physical globe, the data includes object properties, environment condition etc; and physical equipments contain RFID reader, all kinds of sensors, GPS and supplementary equipments. The key constituent in this layer is sensors for seizing and representing the physical globe in the digital world.

The subsequent level is web layer. web layer is accountable for the reliable transmission of data from perceptual layer, Early processing of data, association and polymerization. In this layer the data transmission is relied on countless frank webs, that are the internet, mobile contact web, satellite nets, wireless web, web groundwork and contact protocol are additionally vital to the data transaction amid devices.

The third level is prop layer. Prop layer will set up a reliable prop period for the request layer, on this prop period all kind of intelligent computing. It plays the act of joining request layer upwards and web layer downward.

The request layer is the topmost and terminal level. Request layer provides the personalized services according to the needs of the user, user can admission to the internet of thing across the request layer interface employing of television, confidential computer or mobile supplies and so on.

Network protection and association frolic an vital act in above every single level. Next we will scrutiny the protection features.

B. Security Features

Perceptual Layer: Usually perceptual nodes are short of computer manipulation and storage capacity because they are easy and alongside less power. Consequently it is incapable to apply frequency hopping contact and area key encryption algorithm to protection protection. And it is extremely tough to set up protection system[6]. temporarily aggressions from the external web such as repudiate of ability additionally hold new protection problems. In the supplementary hand sensor data yet demand the protection for integrity, authenticity and confidentiality.

Network Layer: Although the core web has moderately finished protection skill, but man-in-the Middle attack and counterfeit attack yet continue, temporarily junk mail and computer virus cannot be flouted, a colossal number of data dispatching cause congestion. Consequently protection mechanism in this level is extremely vital to the IoT.

Support Layer: Do the mass data processing and intelligent decision of network behaviour in this layer, intelligent processing is limited for malicious information, so it is a challenge to improve the ability to recognize the malicious information.

Application Layer: In this level protection needs for disparate request nature are disparate and data allocating is that one of the characteristics of request layer, that crafting setbacks of data privacy, admission manipulation and disclosure of data.

C. Security Requirements

According to the above analysis, we can summarize the security requirements for each level in the following, as shown in Figure.3

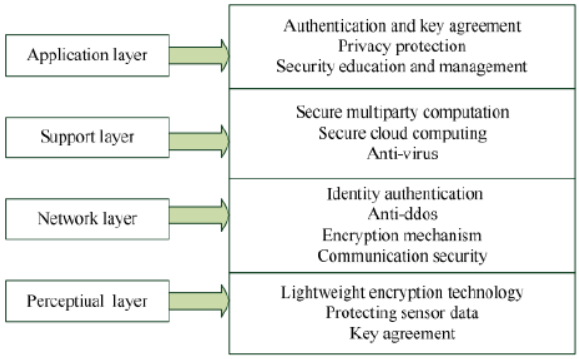

Figure 3: Security requirements in each level

Perceptual Layer: At early node authentication is vital to stop unlawful node access; secondly to protect the confidentiality of data transmission amid the nodes, data encryption is definite necessity; and beforehand the data encryption key accord is a vital procedure in advance; the stronger are the protection

measures, the extra is consumption of resources, to resolve this setback, handy encryption knowledge becomes vital, that includes handy cryptographic algorithm and handy cryptographic protocol[7]. At the alike period the integrity and authenticity of sensor data is becoming scrutiny focus, we will debate this question extra in-depth in the subsequent serving.

Network Layer: In this layer continuing contact protection mechanisms are tough to be applied. Individuality authentication is a kind of mechanism to stop the unlawful nodes, and it is the premise of the protection mechanism, confidentiality and integrity mechanism. As well distributed denial of ability attack (DDoS) is a public attack method in the web and is chiefly harsh in the internet of thing, so to stop the DDoS attack for the vulnerable node is one more setback to be resolved in this layer.

Support Layer: Support layer needs a lot of the request protection design such as cloud computing and safeguard multiparty computation, nearly all of the forceful encryption algorithm and encryption protocol, stronger arrangement protection knowledge and anti-virus.

Application Layer: To resolve the protection setback of request layer, we demand two aspects. On is authentication and key accord across the heterogeneous web, the supplementary is user's privacy protection. In supplement, education and association are extremely vital to data protection, exceptionally password management[8].

III. SECURITY ARCHITECTURE ELEMENTS

Based on a threat analysis for three reference scenarios the IoT work project is developing security architecture elements encountering security threats on multiple layers starting from the network layer over the device layer towards the application and service layer. This paper is focused on the architecture elements from a network and devices perspective[9] only which are:

Secure device identifier: Devices shall provide a cryptographic secure identifier that is bound to the device in such a manner that it is hard to manipulate or clone the identity.

Secure credential management: The automation environment shall provide components and mechanisms to manage credentials.

Secure network access of devices: A devices shall be authenticated before access to the operational network is granted.

Policy enforcement for devices: The compliance of a device to given polices shall be assessed during network access and regularly during normal operation.

Device and system integrity assurance: The integrity of devices of an automation environment shall be devices of an automation environment shall be verified regularly.

A. Secure Device identifier

Devices that compose future flexible and more open automation networks are designed for unattended autonomous operation and usually don't provide user interaction and authentication. Malicious devices could interfere communication and could use credentials of authenticated devices and users [10]. Secure identifier are a enable secure communication and secure plug & work and are an enable for various security services like:

1. Secure Authentication
2. Access control and policy checks
3. Auto-configuration
4. Authorization
5. Secure inventory
6. Localization
7. Anti-counterfeiting

We analysed different approaches regarding the support for these requirements:

1. Secure ID based on symmetric mechanisms.
2. IDs using Group Signature Scheme and Variations.
3. IDs using Physical Unclonable Function.

B. Bootstrapping of security credentials

A security architecture based on cryptographic mechanisms demands for appropriate mechanisms to provide and bootstrap the necessary security credentials.

Security credentials are, like other type of data or equipment, part of a cycle. They are created, applied, and destroyed and need to satisfy a certain security policy. The typical life cycle of security credentials are[11],

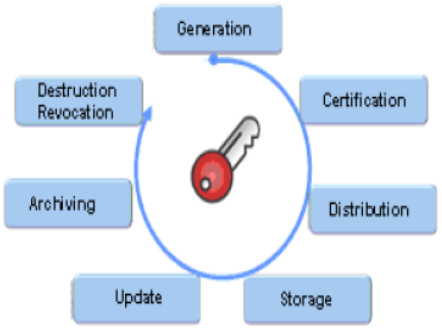

Figure 4: Security parameter life cycle

1. Generation: Devices keys can be created on the device itself or they may be created externally and installed on the target device.
2. Certification: Typically done for asymmetric keys through a certificate authority. Depending on the key generation this can be part of the key generation in a trust center or may be done on information sent in a certificate signing request.
3. Distribution: In case of off-device key generation the device key has to be installed on the target device.
4. Storage: The private/secret device key can be stored in secured memory or in a separate hardware module.

Generally, security credentials can be initially bootstrapped by offline means by out-of-band or by in band distribution.

C. Network Access Control

One of the security challenges in Internet of Things scenarios concerns the increasing need for devices –to device identification, authentication and network access authorization in addition to the usual user authentication. Network Access Control (NAC) is one important element of a defence in depth strategy in depth strategy providing secure plug & work and secure communication.

NAC comprise the detection and assessment of the relevant parameters as well as functions to bring the devices to a policy compliant status. These parameters are collected prior to

access to the infrastructure in a so called pre-connect assessment.

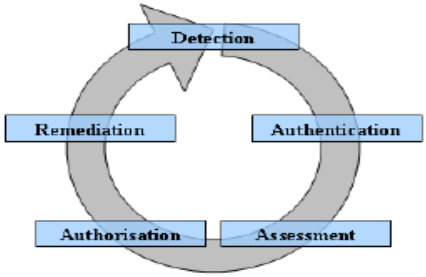

Figure 5: Network access control steps

We identified three important properties which should be verified during the NAC assessment phase of automation devices [12].

1. First, it should be assured that only allowed or engineered devices gain access to the operational automation network.
2. Second, it should be verified that the device firmware or important parts of it represent the expected firmware version. A mismatch may result unintentionally ,but a mismatch could also result by international actions or manipulation of an attacker to influence or disturb the production process.
3. Third, it should be verified that the device configuration represents the expected configuration and was not manipulated. A mismatch of the configuration data may happen unintentionally by error or intentionally by an attacker.

D. System Integrity Assurance

This assessment is only once when devices are trying to connect to the network. For a proper and continuous verification process the attributes need to be validated also in recurring time intervals [13].

The primary goal of the system integrity assurance component to observe the integrity of automation devices has failed. Therefore, it is necessary that some major security requirements are addressed by the system integrity assurance architecture:

1. Integrity of attributes: It needs to be assured that the integrity of the devices attributes cannot be modified by unauthorized devices.
2. Authenticity of attributes: It needs to be assured that the attributes originate form specific devices.
3. Confidentiality of attributes: It needs to be accessible by unauthorized devices.
4. Replay protection: it needs to be assured that attributes of past assessments are not re-used for or replayed in future assessments

The verification of device integrity, that means device attributes map to the expected attributes, is divided into two phases [14]:

1. Collection of device attributes.
2. Verification of device status, that is the comparison of the collected attributes to the expected ones [15].

IV. FUTURE WORK IN IOT SECURITY

The ongoing research areas will be briefly described for the aspects of IoT infrastructure, cryptography, software vulnerability, malware, and mobile devices [16].

A. Object Identification and Locating in IoT

To uniquely identify an object is the first important issue that came before other security issues. A proper identification method is the foundation of IoT. An ideal identification methodology not only identifies the objects uniquely, but also reflects the property of the object. Example, DNS (Domain Name System) is a good identification method which uniquely identifies a host on the Internet; it also reflects host's property through FQDN(Fully Qualified Domain Name) naming policy, and provides address mapping through DNS resolution.

B. Authentication and Authorization in IoT

Authentication is also an important area in research. Traditionally, authentication is achieved through many methods such as ID/Password, pre-shared secrets, and public-key cryptosystems. Authorization can be achieved by database-based crypto-based access control. Due to the heterogeneity authentication and authorization methods may not be applicable. For instance, authenticating and authorization through cryptographically pre-shared keys is not applicable.

C. Privacy in IoT

At the current stage, information about user behaviour whilst browsing the internet is collected to enrich the user experience on the internet. As for IoT[17], the amount of information collection is not limited to internet browsing behaviour; information about a user's daily routine is also collected so that the "Things" around the user can cooperate to provide better services that fulfil personal preference.

D. Lightweight Cryptosystems and Security Protocols

In IoT, there are various resource-constrained devices such as sensor nodes, smart devices, and wearable devices, which only have limited computing power and battery capacity. Although many proposed cryptosystems and security protocols are considered secure and robust, they may not be suitable for the resource-constrained devices.

E. Software Vulnerability and Backdoor Analysis in IoT

In additional to the authentication and authorization problems, software vulnerability plays an important role in current security research domain. During the development stage of a piece of software, programming bugs produced by developers are unavoidable. Bugs that result in security incidents are known as software vulnerabilities. In the traditional PC industry, system architectures are similar amongst the machines. At the current stage, a number of research works identified that IoT devices have vulnerabilities exposed to attackers. Program analysis can discover software vulnerabilities before the product is released. To verify a program, the dynamic analysis approach monitoring the targeting program in a controlled environment is an effective approach.

Software vulnerabilities can lead to a number of backdoor problems. First, with software vulnerabilities, attackers exercise malicious intents without any artefact in a victim's system. Consequently, a backdoor can be planted in a vulnerable device by attackers to control the device. Another type of backdoor is deliberately inserted in a software product by vendors for management or testing purposes. These

backdoors may be discovered and used by adversaries to steal user data.

F. Malware in IoT

The IoT services embrace the great connectivity among various devices while attracting adversaries as a hotbed to widely spread out their crafted malware[18]. Upon connection to a victim user, any of the infected IoT devices could contaminate a device held by the victim and thus get one step further to the targeted critical device with the massive data of interest it stored.

G. Android Platform

Android platform, the most popular mobile operating system, has overwhelmingly taken the mobile market share. Based on Android, more and more smart devices have been developed as personal assistants that surely headlined the IoT. With its open and embedded-system oriented design, the Android platform attracted IoT developers attention in many aspects, Many Android features have been adopted in IoT devices, such as power saving, near-field communication, multi-sensors, voice control.

CONCLUSION

The architecture and key technology of Internet of Things, moreover the application of IoT are interpreted. Physical items are no longer disconnected from the adjacent globe but can be manipulated remotely and can deed as physical admission points to Internet services. One of the toughest trials of this knowledge is its security.

In Internet of Things enabled industrial automation network. Additional security architecture elements are required to support open automation environments. The security architecture elements are not considered as single standalone solution but rather to interwork providing a common solution.

Acknowledgment

First of all, I am glad to thank THE LORD ALMIGHTY for giving me the spirit in completing this paper. I would thank my family for the constant support they provided throughout my preparation.

References

[1] W.K. Edwards, "Discovery systems in ubiquitous computing", IEEE Pervasive Computing, 2006, pp. 7077.
[2] E. Fleisch, and F. Mattem, Das Internet der Dinge, Springer, 1 edition, July 2005.
[3] Gubbi, Jayavardhana, RajkumarBuyya, SlavenMarusic, and MarimuthuPalaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29, no. 7 (2013): 1645- 1660.
[4] Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. "Security in the internet of things: a review." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, pp. 648-651. IEEE, 2012.
[5] Altolini, Diego, VishwasLakkundi, Nicola Bui, Cristiano Tapparello, and Mattia Rossi. "Low power link layer security for IoT: Implementation and performance analysis." In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, pp. 919-925. IEEE, 2013.
[6] Roman, Rodrigo, Cristina Alcaraz, Javier Lopez, and Nicolas Sklavos. "Key management systems for sensor networks in the context of the Internet of Things." Computers & Electrical Engineering 37, no. 2 (2011): 147-159.
[7] Batina, Lejla, Jorge Guajardo, Tim Kerins, NeleMentens, PimTuyls, and Ingrid Verbauwhede. "An Elliptic Curve Processor Suitable For RFID-Tags."IACR Cryptology ePrint Archive 2006 (2006): 227.
[8] Saied, Yosra Ben, and Alexis Olivereau. "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things." In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a, pp. 1-7. IEEE, 2012.
[9] IEC/TR 62443-3-1, "Industrial communication networks-Network and system security - Part 3-1: Securitytechnologies for industrial automation and control systems", 2009
[10] NIST SP800-82, "Guide to Industrial Control Systems (ICS) Security", June 2011
[11] ISO/IEC 27002, "Information technology — Security techniques — Code of practice for information security management", June 2005
[12] D. Chaum and E. van Heyst, Group signatures, Advances in Cryptology — EUROCRYPT 1991, volume 547 of Lecture Notes in Computer Science. pages 257–265
[13] Pappu Srinivasa Ravikanth, Physical One-Way Functions, PhD Massachusetts Institute of Technology,March 2001
[14] IEEE 802.1AR, „Secure device identity", 2009
[15] K. Fischer, J. Geßner, S. Fries, "Secure identifiers and initial credential bootstrapping for IoT@Work", In SixthInternational Conference on Innovative Mobile andInternet Services in Ubiquitous Computing (IMIS), pages 781-786, July 2012
[16] GS1, Object Name Service (ONS) Standard [Online].http://www.gs1.org/gsmp/kc/epcglobal/ons/, accessed on October 8, 2014.
[17] L. Zhang, A. Afanasyev, J. Burke, claffy, L. Wang, V. Jacobson, P. Crowley, C. Papadopoulos, B. Zhang, "Named Data Networking," in ACM SIGCOMM Computer Communication Review, July 2014
[18] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang,"Securing building management systems using named data networking," IEEE Network Special Issue on Information-Centric Networking, April 2014.