ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Security in Internet of Things (IOT): Review

[1]Deepika Sherawat

[1]Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1]deepika.sherawat@Galgotiasuniversity.edu.in

Abstract: The internet of things (IOT) has been a research subject for the last decade. Security and privacy are the key issues facing IOT applications, and are still facing some huge challenges. To promote this emerging area, authors briefly review the progress of IOT research, and pay attention to security. Nevertheless, from a security and privacy viewpoint, this new reality (IOT) built on the Internet contains new kinds of challenges. Because of the various standards and communication stacks involved, conventional security primitives cannot be used directly on IOT technologies. In addition to issues of scalability and heterogeneity, the major part of the IOT infrastructure consists of resource-constrained devices such as RFIDs and wireless nodes. Hence, in such a dynamic environment, a versatile architecture is required capable of addressing security and privacy issues. The security requirements are given by means of a thorough analysis of the safety architecture and features. Based on these, authors address the research status of key technologies, including encryption mechanisms, communication security, sensor data protection and cryptographic algorithms, and outline the challenges concisely.

Keywords: Challenges, Confidentiality, Internet of Things, Privacy, Security.

INTRODUCTION

IOT concept has begun to shape our modern world, including the everyday life of a common man in society, a world where devices of all shapes and sizes are produced with "smart" abilities that enable them to connect and interact not only with other systems but also with people, exchange their information, make independent decisions and conduct useful tasks based on preset conditions. With its various implementations, IOT is becoming well-known across many horizontal and vertical markets. Just to give an example of how IOT can impact our everyday lives: you enter the supermarket and receive a text message from your fridge. “You are out of milk.” The early years of the Internet of Things (IOT) began with contact between Machine to Machine (M2M)[1]. M2M communication refers to two devices that interact with one another, usually without human involvement. The communication medium is not specified, and can be wireless communication as well as wired communication. The term M2M is derived from systems of telephony. In such systems, different endpoints, such as caller identification, were required to exchange information between each other. This information was sent without a human being needed to initiate the transmission between the endpoints. The term M2M is still very much in use, especially in the industrial market, and is widely considered to be a subset of IOT[2].

The IOT will be faced with more serious challenges as regards security. There are the following reasons: 1) the IOT expands the' Web' through the conventional Internet, mobile network and sensor network, and so on, 2) every' thing' connects to this' internet,' and 3) these' things' communicate with each other. Therefore there will be new security and privacy issues. They should pay more attention to the confidentiality, authenticity and integrity of data in the IOT research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

questions. The ambient intelligence and autonomous control at this stage are not part of the original IOT concept. With the development of advanced network techniques, distributed multi-agent control and cloud computing, there is a shift in M2 M research that integrates IOT concepts and autonomous control to produce an evolution of M2 M in the form of CPSs. CPS focuses primarily on interaction intelligence, digital applications, distributed real-time control, cross-layer optimization, cross-domain optimization, etc. For this purpose, all new technologies and methodologies should be established to meet the higher reliability, security and privacy requirements[3].

ATTENTION TO SECURITY IN IOT

Information and network security should be equipped with such properties as identification, confidentiality, integrality, and undesirability. Unlike the internet, the IOT will be applied to the crucial domains of the national economy, e.g., medical and health care, and smart transportation, hence the security needs in the IOT will be higher in availability and reliability[4].
Secure Architecture:
The IOT can generally be subdivided into four key levels (Fig. 1).

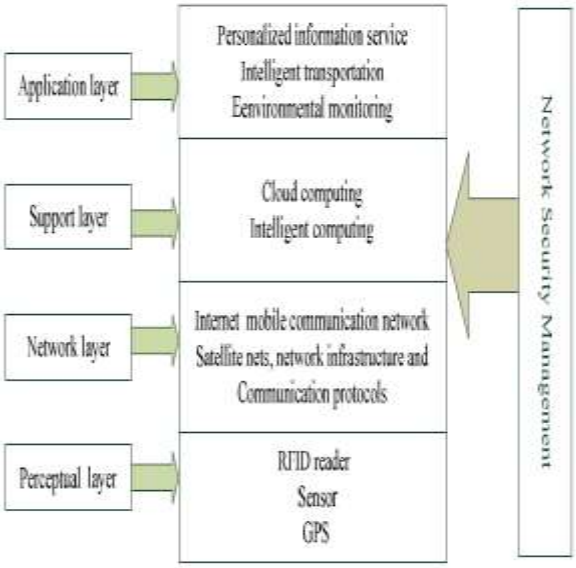

Figure 1: Security Architecture

The most general level is the perceptual layer, which gathers all kinds of information via physical equipment and defines the physical world, the data includes object properties, environmental conditions, etc., and the physical equipment includes RFID readers, sensors of all kinds, GPS and other devices. The key component in this layer is sensors that capture and reflect the world of physics in the digital world.
The second level is layer of network. Network layer is responsible for the efficient transmission of perceptual layer information, initial information processing, classification, and polymerization. In this layer, the transmission of information is based on several basic networks, including internet, mobile communication networks, satellite networks, wireless networks, network infrastructure and communication protocols, which are also essential for the exchange of information between devices.
Third one is support layer. Support layer would set up a stable support platform for the application layer, organizing all kinds of intelligent computing powers through network grid and cloud computing on this support platform. It plays the role of mixing up layer of application with down layer of network. The layer of application is at the top and the terminal level.
The application layer provides the customized services according to the users ' needs. Users can access the Internet of Things using television, personal computers or mobile equipment, and so on, through the application layer interface.

SECURITY FEATURES:

a) Perceptual Layer: Generally perceptual nodes lack the power and storage capacity of the computer because they are easy and with less energy. Thus it is unable to apply frequency hopping communication and the algorithm for public key encryption to the safety defense. And the setting up of a security protection system is very difficult. Although external network attacks such as denying service frequently bring with them new security issues. On the other hand, sensor data still need the honesty, authenticity and confidentiality protection[5].
b) Network Layer: Though the core network has relatively complete safety protection capability, there

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

is still a man-in - the-middle attack and counterfeit attack, while junk mail and computer virus cannot be ignored, congestion is caused by a large number of data sending. Therefore security mechanism is very important to the IOT at this level.

c) Support Layer: This layer is responsible for the mass data processing and smart network behavior decision; smart processing is limited for malicious information, so enhancing the ability to recognize malicious information is a challenge.

d) Application Layer: Security requirements for different application environments are different at this point, and data sharing is one of the features of the application layer that causes data privacy issues, access controls and information disclosure.

SECURITY REQUIREMENTS:

Security requirement on each level is shown in the Fig. 2.

a) Perceptual Layer: Firstly, authentication of nodes is necessary to prevent illegal access to nodes; secondly, to defend the confidentiality of information transmission between nodes, data encryption is absolutely necessary; and before the key agreement on data encryption is an important process in advance; the stronger the security measures, the more resources are consumed, Lightweight encryption technology, including Lightweight Cryptographic Algorithm and Lightweight Cryptographic Protocol, becomes important in solving this problem. At the same time as the validity and reliability of sensor data is becoming a subject of analysis[6].

b) Network Layer: Existing communication security mechanisms are hard to implement in this layer. Identity authentication is a kind of system for preventing unauthorized nodes, and it is the principle of the security mechanism, confidentiality and integrity are of equal importance, so user must also create the mechanism for data confidentiality and integrity. Meanwhile Distributed Denial of Service Attack (DDoS) is a common strategy in the network and is particularly severe on internet of thing, so preventing the vulnerable node DDOS attack is another problem to be solved in this layer.

c) Support Layer: Support layer requires a lot of application security infrastructure like cloud computing and secure multiparty computing, nearly all of the efficient encryption algorithm and encryption protocol, better system security technologies and anti-virus.

d) Application Layer: To solve the application layer security problem there are two aspects. The first is the authentication and key agreement throughout the heterogeneous network, the other is privacy protection for users. Additionally, education and management are very important for security of information, particularly password management.

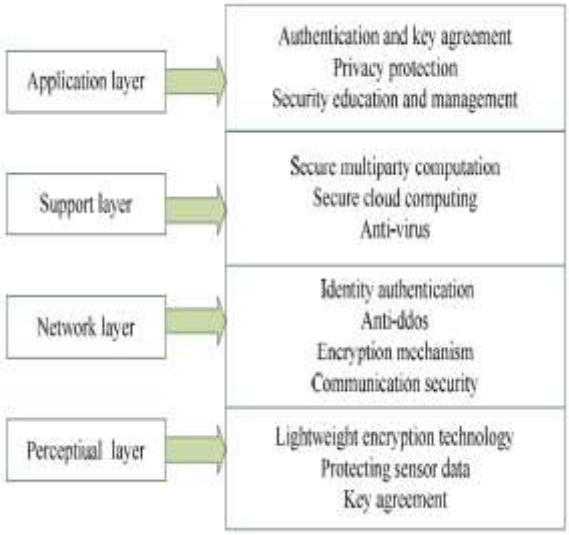

Figure 2: Security Requirements in Each Level

SECURITY SOLUTIONS APPROACHES:

Centralized Approaches: Centralized security solution solutions are considered to be effective and ideal for resource-restricted sensor networks, but the common problem is key management scalability; node must be pre-configured with shared keys from all stakeholders prior to deployment. Some of popular centralized solutions are SPINS (a centralized architecture for securing uniand multicast communication in restricted networks, composed of two security protocols; SNEP and μTESLA) and the polynomial-based scheme (Polynomial schemes seek to simplify the main agreement process in distributed sensor networks,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

main idea is to assign a polynomial share F (n:y) to each node n, derived from the secret symmetric bi-variate polynomial F (x:y). This allows establishing a common secret by any possible pair of nodes with a polynomial share)[7].

Protocol-based Extensions and Optimizations: Approaches like compression aim to optimize the protocol without violating the security features. Many compression schemes are being suggested, such as IPV6 header compression, extension headers, and UDP (User Datagram Protocol) header now common in 6LoWPAN. Several of these approaches are DTLS Handshake abbreviated (enables a shorter handshake to reuse the previous session's state information to resume the session). TLS Session Resumption without Server-Side State where the server does not have any state needed to restart a session, rather the encrypted state of the server is offloaded to the client during the handshake and in caching; the TLS Cached Information extension allows cached information to be omitted, such as those broad handshake certificate chains. Compression of header information is an approach for reducing the overhead transmission of packets in restricted environments; 6LoWPAN describes header compression method for IP packets.

Hardware-based Approaches: A class of security solutions depends on extra security hardware modules, like TPMs. A Trusted Platform Module (TPM) is a tamper-proof hardware which offers support for cryptographic computations, particularly cryptographic primitives based on the public key. TPMs can hold keys in a secure memory area, such as private RSA keys. In addition, the TPMs cryptographic accelerator is capable of higher frequency processing of the cryptographic computations. In comparison, with significantly smaller key sizes, ECC offers the same level of security. Therefore ECC is preferred for restricted conditions and is recommended.

CHANLLENGES

Security Structure: IOT will remain stable as a whole over time, establishing the security mechanism of each logical layer cannot implement system defense-in-depth, so building a security structure with a combination of control and information is a challenge and an important research area.

Key Management: Since key management is the essential basis for more security mechanism, it's always the field of hot research It's still the cryptographic security aspect that is most challenging. The researchers actually aren't finding the right solutions. Lightweight cryptographic algorithm or greater sensor node efficiency is still not applied. The actual large-scale sensor network is still barely put into practice so far. In this network environment, the issues of network security will be given greater importance and become key points and study difficulties[8].

Security Law and Regulations: Today, security law and regulations are not yet the focus of attention, and there is no IOT application standard. The IOT has to do with knowledge about national security, corporate secrets and personal privacy. Our country therefore needs the legislative point of view in order to promote the growth of the IOT.

Requirements for Burgeoning Applications: CPS, an evolving type of IOT, is becoming a reality with the advancement of WSNs, radio frequency identification (RFID), ubiquitous computing technology, network communication technology and distributed real time control theory. The high protection is expected in this system to guarantee system performance.

The security issues for the IOT, as all said above are severe. Sound protection framework needs to be established. Key management in the actual large-scale sensor network is always a challenge, and IOT-related policies and regulations will be a challenge too.

CONCLUSION

This paper intends to provide the reader with a basic summary of the Internet of Things, the major security and privacy challenges due to its exponential growth and what kind of security primitives and solution approaches are used to make communication secure and to protect user data. This emerging domain for the IOT has attracted significant interest in the last couple of years, and will continue for years to come. Given the rapid evolution, researchers still face new problems and serious difficulties. They concisely reviewed security in the IOT in this literature, and

analyzed security characteristics and requirements from four layers including perceptual layer, network layer, support layer and application layer. Current solutions rely on pre-deployed, pre-shared keys on both ends, while certificate-based authentication is generally regarded as infeasible for resource sensors that are limited. For key establishment protocols that are lightweight for resource-constrained sensors and secure through strong encryption and authentication, a new security paradigm is needed.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2015.2444095.

[2] P. Rawat, K. D. Singh, and J. M. Bonnin, "Cognitive radio for M2M and Internet of Things: A survey," *Comput. Commun.*, 2016, doi: 10.1016/j.comcom.2016.07.012.

[3] A. Lele, "Internet of things (IoT)," in *Smart Innovation, Systems and Technologies*, 2019.

[4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," 2012, doi: 10.1109/ICCSEE.2012.373.

[5] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, 2015, doi: 10.1109/ACCESS.2015.2437951.

[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Computer Networks*. 2015, doi: 10.1016/j.comnet.2014.11.008.

[7] O. G. O. & M. A. B. Muhammad A. Iqbal, "A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches," *Glob. J. Comput. Sci. Technol. E Network, Web Secur.*, 2016, doi: 10.1111/j.1399-6576.1984.tb02071.x.

[8] A. R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," 2015, doi: 10.1145/2744769.2747942.