Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 7; October, 2014 pp. 71-75
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Internet of Things (IoT) Reliability in Transport Encryption System with Cryptographic Solution

Shailendra Singh Tanwar[1], Gamini Sharma[2], Dixit Soni[3]

[1]*Computer Engineering, Poornima College of Engineering, Jaipur*
[2,3]*Student, B Tech V Sem, Computer Engineering, Poornima College of Engineering, Jaipur*

Abstract: **The Internet of Things is a new paradigm that is revolutionizing computing. It is intended that all objects around us are connected to the network, providing "anytime, anywhere" access to information. This concept is gaining ground, thanks to advances in nanotechnology which allows the creation of devices capable of connecting to the Internet efficiently.**

Today, a large number of devices are connected to the web, ranging from mobile devices to appliances. In this paper, we focus on the problem of lack of encryption transport which results in the information leakage in the system and usage of cryptographic algorithms in order to make effective transfer of data in the network.

Keywords: **Computing, Encryption, Cipher text, Decryption.**

1. INTRODUCTION

The creation of the Internet has marked a foremost milestone towards achieving ubiquitous computer's vision which enables individual devices to communicate with any other device in the world. The inter-networking reveals the potential of a seemingly endless amount of distributed computing resources and storage owned by various owners.

Internet of things (IOT) is a network which combines all kinds of information sensors with the Internet. Realizing the vision of sustainable IoT applications requires the enhancement of IoT technologies with new ways that will enable things and objects to become more reliable, more resilient, more autonomous and smarter. As highlighted in [1]: "Data is the raw material that is processed into information. Individual data by itself is not very useful, but volumes of it, which will come from the Internet of Things, can identify trends and patterns. These sources of information then come together to form knowledge. Wisdom is then born from knowledge plus experience." The quotation is based on the fact that humans evolve because they communicate, creating knowledge out of data and wisdom based on experience. Applying this metaphor to the IoT domain means enhancing objects with technologies that would enable them to evolve based on the knowledge derived from the data streams and the experience of their exploitation and of other objects exploitation by IoT applications.

According to CISCO [2], during 2008, the number of things connected to the Internet exceeded the number of people on earth and by 2020 there will be 50 billion, shaping a rich digital environment. Sensors, intelligent fixed and mobile platforms (e.g. smart phones, tablets and home gateways), massive scale cloud infrastructures and other network-enabled devices will all need to cooperate and interact to create value across many sectors in smart cities. This digital environment creates a treasure trove of information, which is the key enabler for embedding wisdom into objects. The added value in a city context is that by making objects smarter cost savings and increased efficiencies will be created, thus allowing for long-term economic growth [3]. Furthermore, emphasis is currently put upon sustainable and green smart city applications [4].

While the technology already exists, the challenge is to put it all together into a unified, easily-managed environment [5]. Sustainability requires the management of millions of objects in an efficient way, optimizing energy and resource usage [6], while also considering that space is bound to get tight raising the need for new techniques that will coordinate and manage all available objects under different contexts, applications, environments, administrative domains and locations. Besides, making things more resilient and smarter in a smart city environment [7] implies services and ICT systems adaptability to IoT applications requests as well as to real-world events that need to be monitored and assessed since they may influence the lifecycle of these applications.

Things have identities, physical attributes and virtual personalities (as highlighted in the corresponding definition by ITU and IERC [4]) and according to a report by Economist [8], future smart cities will base IoT service provision on the digital reflection of things and citizens, which will bring much greater efficiency. Tussles of personal privacy [9] and freedom of expression [10] are expected to be a consequence. Even more, in spite of increased use of mobile devices for specific and well-defined uses, many remain skeptical about the broader deployment of Internet of Things [11], fearing Big Brother intrusion rather than seeing the opportunity of accessing and exploiting the content feeds in new and creative ways that benefit those same skeptical users. Consequently, developing sustainable IoT applications calls for mechanisms to ensure security and trust and preserve privacy [12].

Such approaches should address both the low levels of IoT environments (i.e. hardware-coded techniques) as well as the data management and application levels. Tamper-resistant smart devices, dynamic and evolutionary trust models, secure data stores, applications with build-in security and privacy are critical for sustainable IoT applications [13].

2. IOT IN COMPUTING

Ubiquitous computing in the next decade the effort by researchers to create a human-to-human interface through technology in the late 1980s resulted in the creation of the ubiquitous computing discipline, whose objective is to embed technology into the background of everyday life. Currently, we are in the post-PC era where smart phones and other handheld devices are changing our environment by making it more interactive as well as informative. Mark Weiser, the forefather of Ubiquitous Computing (ubi comp), defined a smart environment [14] as ‘‘the physical world that is richly and invisibly interwoven with sensors, actuators, displays and computational elements, embedded seamlessly in the everyday objects of ourlives and connected through a continuous network’’.

The phrase “Internet of *Things*” was coined by Kevin Ashton [15] in 1999. Although the concept of interconnecting devices and people for various reasons has existed for much longer **-** i.e. via the *traditional* Internet and social networks **-** this model of interconnecting devices, people and *everything else* is relatively new and still in its introductory stages [16]. Control over these devices will be spread over a spectrum of stakeholders: owners, manufacturers, law enforcement, and participatory governments. This control can be expected to take various forms; from “direct-touch” (physical) control to remote control or control via web browsers and the Internet.

2.2 Ubiquitous computing

For the realization of a complete IoT vision, efficient, secure, scalable and market oriented computing and storage resourcing is essential. Cloud computing [17] is the most recent paradigm to emerge which promises reliable services delivered through next generation data centers that are based on virtualized storage technologies.

This platform acts as a receiver of data from the ubiquitous sensors; as a computer to analyze and interpret the data; as well as providing the user with easy to understand web based visualization.

Ubiquitous computing is characterized by small computers that communicate spontaneously, which are integrated in almost everyday objects thanks to their small size. The Internet of things still has challenges that are inherent in its three layers (hardware, infrastructure and applications and services) -

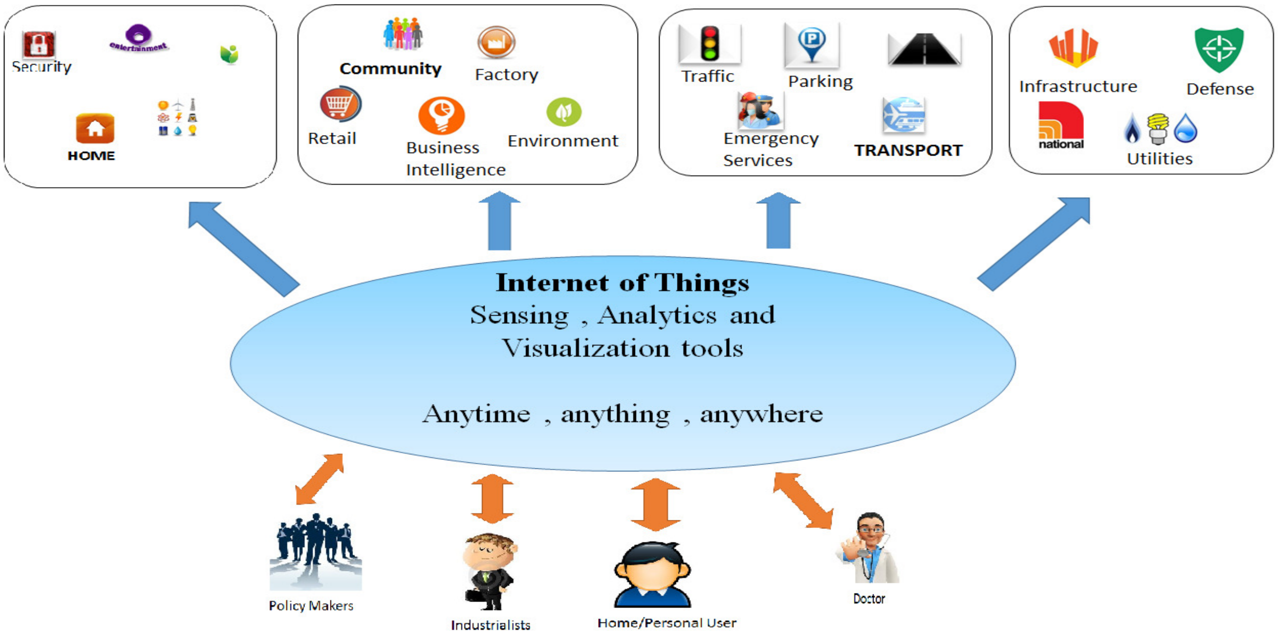

Fig. 1: Internet of Things (IoT) diagram with end users and application areas

- **First level:** Hardware, that allows the interconnection of physical objects through sensors and related technologies. The challenges associated to this layer are related to miniaturization. Internal components should be smaller and more efficient although today they are equipped with devices with processing, storage and connectivity capability.
- **Second level:** The infrastructure level corresponds to the connectivity capacity for internet access, which is currently with 3G and 4G networks. The great challenge is to connect billions of devices on a wireless network, being necessary the expansion of bandwidth and the electromagnetic spectrum.
- **Third level:** Applications and services level, which is plenty of opportunities to over solutions to supply and provide information, from the physical to the virtual objects, as well as the interaction with people, making life easier and more efficient all the time.

Smart connectivity with existing networks and context aware computation using network resources is an indispensable part of IoT. For the Internet of Things vision to successfully emerge, the computing criterion will need to go beyond traditional mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment. For technology to *disappear* from the consciousness of the user, the Internet of Things demands:

(i) A shared understanding of the situation of its users and their appliances

(ii) Software architectures and pervasive communication networks to process and convey the contextual information to where it is relevant

(iii) The analytics tools in the Internet of Things that aims for autonomous and smart behavior. With these three fundamental grounds in place, smart connectivity and context-aware computation can be accomplished.

According to Forrester [18], a smart environment –

- Uses information and communications technologies to make the critical infrastructure components and services of a city's administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive and efficient.

In our definition, we make the definition more users centric and do not restrict it to any standard communication protocol. This will allow long-lasting applications to be developed and deployed using the available state-of-the-art protocols at any given point in time.

3. ARCHITECTURE OF IOT

According to data flow and process mode in the network, IOT can be divided into three layers: the apperception layer, the transport layer, the application layer [20].

3.1 Apperception layer

Apperception layer, also known as the information identification layer, bases on the two dimensional code, RFID and sensor to achieve object recognition and perception monitoring. The RFID [19] system identifies and collects the information of marker stored on the labels via radio frequency signal, sends the information to computer information management system, and communicates between the marker and computer. Among all objects labeled with markers, the objects have their own mutual perception ability and make information communication among different objects in their own local space.

3.2 Transport layer

Transport layer, also known as the network communication layer, accesses to IoT via the existing Internet, mobile communication network and satellite, which realizes the further processing and transmission of data. Data security is a core problem in the network communication of IoT.

During transmission, data are vulnerable and could be changed. Also conflict, congestion and retransfer of data would happen. Therefore during data transmission, data fusion and safety control technology should be involved to improve fault-tolerance of the network and ensure the reliability of data. In the transport layer, a global and open identification standard using the Electronic Product Code assigns a unique code for each object.

3.3 Application layer

The application layer, also known as the terminal transact layer, is control terminal of inputting and outputting, which includes computer, mobile phone and server terminal and realizes storage, mining, processing and application of information sent by the transport layer.

IoT terminal has three parts: sensor interface, the central processing module and external communication interface. And the IoT terminal is the intermediate equipment of the apperception layer and the transport layer which is in charge of data receiving, processing and integration. It can identify the information of the marked objects which are monitored through information process, analysis and statistics and achieve 'communication among things'. In the treating process, problems arise from the essential elements will prevent network terminal from collecting accurate and reliable information, which would further induce failure in 'communication among things'.

4. PROBLEM - LACK OF TRANSPORT ENCRYPTION

Lack of transport encryption allows data to be viewed as it travels over local networks or the internet. It has following problems:

- **Threat Agents**

Consider anyone who has access to the network the device is connected to, including external and internal users.

- **Attack Vectors**

Attacker uses the lack of transport encryption to view data being passed over the network. Attack could come from external or internal users. Attackers may be unknown users and it also violates several files in a system.

- **Security Weakness**

Lack of transport encryption is prevalent on local networks as it is easy to assume that local network traffic will not be widely visible, however in the case of a local wireless network, misconfiguration of that wireless network can make traffic visible to anyone within range of that wireless network. Automated tools can also look for proper implementation of common transport encryption such as SSL and TLS

- **Technical Impacts**

Lack of transport encryption can result in data loss and depending on the data exposed, could lead to complete compromise of the device or user accounts.

5. PROPOSED SOLUTION

To determine the device which use transport system we configure that if the device uses transport encryption is fairly straight forward by reviewing network traffic of the device, its mobile application and any cloud connections to determine if any data is passed in the clear. The use or lack of use of Secure Socket Layer (SSL) or TLS can also be reviewed to ensure it is in use and properly implemented.

Sufficient transport encryption requires:

1. Ensuring data is encrypted using protocols such as SSL and TLS while transiting networks.

2. Ensuring other industry standard encryption techniques are utilized to protect data during transport if SSL or TLS are not available.

Cryptography is the practice and study of techniques for secure communication. Until modern times cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible text (called cipher text). Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption.

The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret usually a short string of characters, which is needed to decrypt the cipher text. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cipher texts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks. Effective transport encryption can be achieved by using RSA (Rivest, Shamir and Adleman) public key algorithm.

6. CONCLUSION

In this paper we have proposed a solution regarding the problem of lack of transport encryption by using RSA algorithm while transmitting data over the network. At present, IoT has already caused the great attention from the industry, education and other fields.70 percent of the IoT devices did not use encryption when transmitting sensitive data across the LAN and internet. Future IoT infrastructures will aim at supporting the on-going creation of IoT applications which will utilize data and services from many different (heterogeneous) device platforms, locations and environments.

This paper introduced challenges and enablers for smarter, more reliable and more autonomous IoT infrastructures along with a conceptual architecture encompassing various components as enabling technologies across four main pillars. The goal is to enable the provision of a scalable and privacy-aware IoT infrastructure that considers social relationships among objects, while being able to self-adapt itself according to environmental context changes in a decentralized and real-time way. Core to the architecture are the ability of things to learn and evolve by exploiting things social-behavior and use it as a basis to share and exchange experiences, as a means to make things smarter and more autonomous.

In order to increase the transparency of these systems, we are suggesting in this work solutions likely to permit a flexible discovery adaptable to the context of the internet of things At the time being, the implementation is in progress. As a next step, we aim to evaluate our process in order to determine the performance and the precision it offers.

REFERENCES

[1] D. Evans. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. CISCO white paper, 2011.

[2] CISCO. The Internet of Things, Info graphic. Available online at http://blogs.cisco.com/news/the-internet-of-thingsinfographic, 2011.

[3] IBM. Cities Outlook 2012. Available online at http://www.ibm.com/cloud-computing/us/en, 2012.

[4] European Research Cluster on the Internet of Things – IERC. The Internet of Things 2012 - New Horizons. Cluster Book 2012, 2012.

[5] Orange Labs - France Telecom. Smart Cities: True icons of the 21st century. Available online at http://www.orangebusiness.com/microsite/solutionsoperators/documentation/download/smart-cities/, 2011.

[6] Arup. The Smart Solutions for Cities. Arup Urban Life, 2011.

[7] Gonzalez J, Rossi A. New Trends for Smart Cities. Available online at http://www.opencities.net/sites/opencities.net/files/contentfiles/repository/D2.2.21%20New%20trends%20for%20Smart%20Cities.pdf, 2011.

[8] Economist Report. It's a smart world. Available online at http://www.managementthinking.eiu.com/sites/default/files/downloads/Special%20report%20on%20smart%20systems.pdf, 2010.

[9] Boniface M, Pickering B. Legislative Tensions in Participation and Privacy. Available online at http://www.scribd.com/doc/55260687/Legislative-Tensions-In-Participation-And-Privacy, 2011.

[10] La Rue F, Report of the Special Report on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council, 16, available online at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, 2011.

[11] Pickering B, Boniface M. Social Future Internet Activities. Available online at http://www.scribd.com/doc/68338983/D3-1-First-Report-on-Social-Future-Internet-Coordination-Activities, 2011.

[12] Moss Kanter R, Litow S, and Informed and interconnected: A manifesto for smarter cities, Harvard Business School General Management Unit Working Paper, 2009.

[13] Correia L, Wünstel K, Smart Cities Applications and Requirements, Net! Works European Technology Platform Expert Working Group White Paper, 2011.

[14] M. Weiser, R. Gold, The origins of ubiquitous computing research at PARC inthe late 1980s, IBM Systems Journal (1999).

[15] K. Ashton, "That ‘Internet of Things’ Thing, " RFiD Journal, vol. 22, pp. 97-114, 2009.

[16] R. H. Weber, "Accountability in the Internet of Things, " Computer Law & Security Review, vol. 27, pp. 133-138, 4, 2011.

[17] R. Caceres, A. Friday, Ubi comp systems at 20: progress, opportunities, and challenges, IEEE Pervasive Computing 11 (2012) 14–21.

[18] J. Belissent, Getting clever about smart cities: new opportunities require new business models, Forrester Research, 2010.

[19] Zhiyu Ren and Peiran Ren, “IOT and EPC/RFID technology, ”The forest engineering, vol. 22, pp.67-69, Jan 2006.

[20] Zhishuo Liu and Wei Feng, “Research of IOT architecture in our country, ” Logistics technology, pp.1-3, Apr 2010.