Advances in Internet of Things, 2015, 5, 21-25
Published Online July 2015 in SciRes. http://www.scirp.org/journal/ait
http://dx.doi.org/10.4236/ait.2015.53004

Scientific Research Publishing

Hybrid Security Techniques for Internet of Things Healthcare Applications

Lobna Yehia[1], Ayman Khedr[2], Ashraf Darwish[1]

[1]Computer Science Department, Faculty of Science, Helwan University, Cairo, Egypt
[2]Information Systems Department, Faculty of Computers & Information, Helwan University, Cairo, Egypt
Email: lobna.yehia2015@hotmail.com

Received 17 June 2015; accepted 27 July 2015; published 30 July 2015

Abstract

The Internet of Things (IoT) describes the future where every day physical objects will be connected to the internet and be able to identify themselves to other devices. IoT is a new revolution of the Internet and It will effect in a large number of applications such as smart living, smart home, healthcare systems, smart manufacturing, environment monitoring, and smart logistics. This paper provides integration, summarizes and surveys some of the security techniques especially hybrid techniques that can be applied with healthcare applications in IoT environment.

Keywords

IoT, Healthcare Applications, Hybrid Security Techniques, Body Area Networks

1. Introduction

IoT aims to enable things to be connected anyplace, anything and anytime using any service/network. IoT will create technological revolution in a large number of applications [1]. Internet technology has become ubiquitous within our society which is infiltrating all aspects of our lives, and it is better to call it as necessity rather than convenience [2]. The term IoT was first used by Kevin Ashton [3], where the physical world is becoming one big information system. Because of the continuing decline in the cost of hardware and network connections used in the IoT, it would be easy to see everything and everyone in our physical world connected to the Internet through wireless network 24 hours per day. In 2020, it is expected that the number of Internet-connected devices ranges from 26 billion to 50 billion as in [1]. There are many IoT applications, and within those healthcare systems, it is considered one of the most important challenges that our society faces today and will be surveyed with security hybrid techniques in this paper. IoT could fetch many advantages in the field of healthcare, through the use of smart sensors, equipment, detectors, etc. These allow the identification and patient tracking

How to cite this paper: Yehia, L., Khedr, A. and Darwish, A. (2015) Hybrid Security Techniques for Internet of Things Healthcare Applications. *Advances in Internet of Things*, **5**, 21-25. http://dx.doi.org/10.4236/ait.2015.53004

online, the locations of the doctor, and keep track of the medical report of the patient. IoT will revolutionize healthcare in terms of security, privacy and Investment, if actually it has been trusted by the medical institutions and the community [4].

Healthcare systems create an IoT network by using a set of interconnected devices for healthcare assessment, including monitoring, tracking patients and automatically detecting situations where medical interventions are required [5]. One of the most important challenges of the IoT is security; the need to provide adequate security for the IoT infrastructure becomes ever more important [6]. Data security is one of the most critical challenges in the digital world and the transfer of data. It is a fundamental requirement for all transactions and operations that take place on the Internet related to data, like web services, transfer sensitive information and many numbers of other operations which need data security. It is also very important in databases.

In this paper the IoT and healthcare systems are summarized, reviewed and surveyed through the security hybrid techniques. This paper is organized as follows. Section 2 introduces IoT with some of the used security techniques. Section 3 discusses the secure healthcare application. Section 4 concludes this paper.

2. Internet of Things and Security Techniques: Overview

In the future, everything will be connected to the web; mobile phones will serve as the remote control, or the hub, for all the things in our physical world which is broadly termed as IoT [2]. IoT is an integrated part of future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network [7]. In this network, the mobile phone will help you coordinate the interactions of the things around you and provide real-time access to all types of information, including the people you meet, the places you go and the content that's available there. Some research estimates that the number of connected objects will reach 50 billion by 2020 [8]. The IoT promises humans to provide a smart life, highly networked world, which allows for a wide range of interactions with this environment. Techniques for interacting with wireless sensors such as IoT and sensor cloud aim to overcome restricted resources and efficiency. The data captured by a set of sensors can be collected, processed according to an application-provided aggregation function, and then perceived as the reading of a single virtual sensor [9]. This data should be protected and secured.

Some of the common security techniques that are used in the protection and immunization databases [6] and in IoT:

1) Access Control: Access control is a security technique which restricts the access to the data on database and its information except for the authorized users.

There are two main types of access control:

a) Physical access control limits access to rooms, buildings and physical IT assets.

b) Logical access control limits connections to data, system files and computer networks.

2) Hashing: Hashing is used to index and retrieve items in a database by using hash functions and can be defined as the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.

3) Steganography: Steganography is process of hiding/encrypt sensitive information in any type of media.

4) Cryptography: Cryptography is the practice and study of techniques for secure communication in which the ordinary text is converted to cipher text by encryption.

5) Hybrid Cryptography: Hybrid cryptography is a technique using multiple ciphers of different types together (symmetric and asymmetric ciphers), to take benefit of the strengths of each type of cryptography [10] [11]. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message. Most security systems use cryptography because it offers various algorithms and techniques practically impossible to break because of their complexity. There are three main types of cryptographic algorithms: symmetric (or secret key) cryptography, asymmetric (or public-key) cryptography, and hash functions (**Figure 1**).

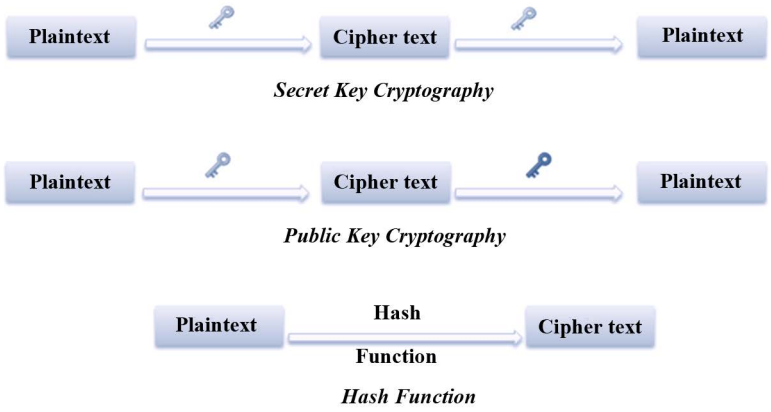

Figure 1. Three types of cryptography [12].

2.1. Secret Key (Symmetric) Cryptography (SKC)

This type of cryptography uses the same (only one) key for both encryption and decryption, and it is called also secret cryptography (SKC) and it works as the following:

- The plaintext is encrypted with the key and the cipher text is sent to the receiver who uses the same key to decrypt the cipher text and recover the plaintext.
- Both the sender and receiver must know the key to use this technique.

Stream chipper and block chipper are the most popular secret key cryptography schemes. The stream ciphers generate a sequence of bits used as a key called a key stream and by combining the key stream with the plaintext, the encryption is achieved. A block cipher transforms a fixed-length block of plaintext into a block of cipher text of the same length. By applying the reverse transformation of the cipher text block, the same secret key is used for the decryption [12] [13].

2.2. Public-Key (Asymmetric) Cryptography (PKC)

This type of cryptography requires two kinds of keys. One to encrypt the plaintext and other one to decrypt the cipher text. It is called asymmetric cryptography because it is used a pair of keys: one is the public key that can be advertised by the owner to anyone who wants, and the other one is the private key and it is known only by the owner. Public key cryptography algorithms that are in use today for key exchange, digital signatures, or encryption of small blocks of data is RSA algorithm. It uses a variable size encryption block and a variable size key. The reason for the RSA algorithm's security is that the factorization of very large numbers. Two prime numbers are generated by a special set of rules, and the product of these numbers is a very large number, from which it derives the key-set [12].

2.3. Hash Functions

A hash function creates a fixed size blocks of data by using entry data with variable length. It is called also message digest or one-way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. The smallest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages. The most common hash algorithms use today is Message Digest (MD) and Secure Hash Algorithm (SHA) for computing a finger print of a data file. SHA-1 produces a 160-bit (20 byte) message digest. Although it is slower than MD5, it stronger against brute force attack, it has a larger digest size. The advantage of MD5 is that it can be implemented faster, due to its 128 bit (16 byte) message digest [12].

By these cryptography techniques, we propose a hybrid approach which combines them for collecting benefits from all of their strengths and tries to reduce as much as possible the weakness of one with the advantages of the other, briefly as the following:

- The original message's message digest is digitally signed (the digital signature uses RSA algorithm).
- Symmetric cipher is used to code the original message. The secret key is obtained using a key generator and

it is changed periodic-time.

- The private key used for symmetric cipher is coded using also RSA algorithm, but with different keys.
- The coded private key is attached to the encrypted message together with the digital signature.

The combination of different cryptography algorithms provide a maximized efficiency, correcting or compensating each other's weaknesses. It can be applied to health care applications mentioned below and their own data.

3. Security for Healthcare Systems

Internet of Things (IoT) plays a significant role in a broad range of healthcare applications, from managing chronic diseases at one end of the spectrum to preventing diseases at the other. This requires sensors to gather physiological information and uses gateway devices and the cloud to analyze and store the information and then send the analyzed data wirelessly to healthcare providers for further analysis and review [1]. These applications will not only improve the access to care while increasing the quality of care but also reduce the cost of care. Publishing new technologies in healthcare applications without considering security makes patient privacy vulnerable; the physiological data of an individual are highly sensitive. Modern healthcare will need ubiquitous monitoring of health with least actual interaction of doctor and patients, which can be achieved by the concept of Internet of Things (IoT) using wireless medical sensor network (WMSN). Wireless medical sensors may be wearable, implantable or portable, and integrated on various kinds of wireless communication motes (such as, Mica2, MicaZ, Telos, etc.) [14]. These wireless medical sensor collected/generated large amounts of data which must be secured from security attacks. By applying security algorithms/techniques, we can prevent many malicious attacks of data when transmitting to the remote locations [15]. Therefore, security is a main requirement of healthcare applications. The success of healthcare application depends mainly on patient security and privacy, for ethical and legal reasons [1] [15]. Some of the secure healthcare applications based on wireless medical sensor network (WMSN):

1) Remote Monitoring: Can be used to securely capture patient health data from sensors, apply complex algorithms to analyze the data and then send it through wireless connectivity with medical professionals who can make appropriate health recommendations.

2) Physical Activity Monitoring for Aging People: Body sensors network (BSN) [16] measures motion/acceleration, vital signs, temperature, blood pressure, heart rate and a mobile unit collect, visualizes and records activity data.

3) Patients' Self-Care: Body area network (BAN) [16] network on a diabetic patient could be helpful to auto inject insulin though a pump, as soon as their insulin level declines).

4) Chronic Disease Management: Patient-monitoring systems with comprehensive patient statistics could be available for remote residential monitoring of patients with chronic diseases such as pulmonary and heart diseases and diabetes.

The following **Figure 2** [17] shows the healthcare architecture using wireless medical sensor network (WMSN):

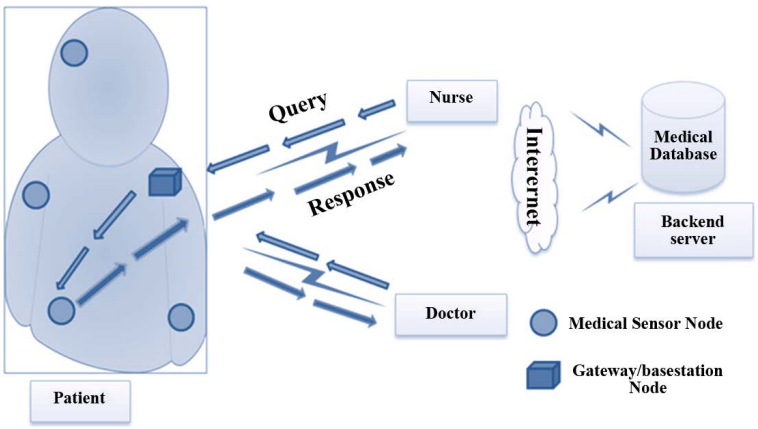

Figure 2. Healthcare architecture for patient monitoring [17].

4. Conclusion

IoT as a new technology has been more widely used. There are many related applications: healthcare application which depends on one of the most important technologies, and wireless sensor networks that can be used for connecting the physical world with the logic information world. The open nature of the information/data media has brought risks to the security of the wireless sensor networks and their collected data. In this paper, authors surveyed and discussed some of the security techniques for healthcare application that can be applied in IoT environment issue, and introduced some of security techniques that are used in data security and immunization.

References

[1] Vermesan, O. and Friess, P. (2014) Internet of Things Applications—From Research and Innovation to Market Deployment (River Publishers Series in Communications).

[2] Tyagi, S., Darwish, A. and Khan, M.Y. (2014) Managing Computing Infrastructure for IoT Data. *Advances in Internet of Things*, **4**, 29-35. http://dx.doi.org/10.4236/ait.2014.43005

[3] Ashton, K. (2009) That "Internet of Things" Thing. *RFiD Journal*, **22**, 97-114.

[4] Darwish, A., Tyagi, S. and Agarwal, A. (2015) A New Model for IoT Based Healthcare Systems Using Cloud Computing. (Under Publication)

[5] Tarouco, L.M.R., Bertholdo, L.M., Granville, L.Z. and Arbiza, L.M.R. (2012) Internet of Things in Healthcare: Interoperatibility and Security Issues. 2012 *IEEE International Conference on Communications* (*ICC*), Ottawa, 10-15 June 2012, 621-6125. http://dx.doi.org/10.1109/ICC.2012.6364830

[6] Kayarkar, H. (2012) Classification of Various Security Techniques in Databases and Their Comparative Analysis. *ACTA Technica Corviniensis*, **5**, 135-138.

[7] Yu, S. (2013) IEEE Standards Association to Exhibit at 2013, International Consumer Electronics Show and Highlight Enabling Consumer Connectivity through Consensus Building. http://standards.ieee.org/news/2013/ces2013.html#sthash.7rFlFzwB.dpuf

[8] Schonfeld, E. (2010) Costolo: Twitter Now Has 190 Million Users Tweeting 65 Million Times a Day. http://techcrunch.com/2010/06/08/twitter-190-million-users/

[9] Li, W.C., Yi, P., Wu, Y., Pan, L. and Li, J.H. (2014) A New Intrusion Detection Application Based on KNN Classification Algorithm in Wireless Sensor Network. *Journal of Electrical and Computer Engineering*, **2014**, Article ID: 240217. http://dx.doi.org/10.1155/2014/240217

[10] Gupta, R.K. and Singh, P. (2013) A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network. *International Journal of Emerging Technology and Advanced Engineering*, **3**, 2250-2459.

[11] Yu, L.L., Wang, Z.J. and Wang, W.F. (2012) The Application of Hybrid Encryption Algorithm in Software Security. 2012 4*th International Conference on Computational Intelligence and Communication Networks* (*CICN*), Mathura, 3-5 November 2012, 762-765. http://dx.doi.org/10.1109/cicn.2012.195

[12] Kessler, G.C. (2013) An Overview of Cryptography. http://www.garykessler.net/library/crypto.html

[13] RSA Laboratories—Chryptographic Tools. Section 2.1.5. (Unpublished) http://www.rsa.com/rsalabs/node.asp?id=2174

[14] Malan, D., Jones, T.F., Welsh, M. and Moulton, S. (2004) CodeBlue: An *Ad-Hoc* Sensor Network Infrastructure for Emergency Medical Care. *Proceedings of the MobiSys* 2004 *Workshop on Applications of Mobile Embedded Systems*, Boston, 6-9 June 2004.

[15] Kumar, P. and Lee, H.-J. (2012) Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *Sensors*, **12**, 55-91. http://dx.doi.org/10.3390/s120100055

[16] Karulf, E. (2008) Body Area Networks (BAN). A Survey Paper Written under Guidance of Prof. Raj Jain. http://www.cse.wustl.edu/~jain/cse574-08/ftp/ban.pdf

[17] Kumar, P., Lee, S.-G. and Lee, H.-J. (2012) E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks. *Sensors*, **12**, 1625-1647. http://dx.doi.org/10.3390/s120201625