Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Assessment of Security Challenges and Remedies in IoT Applications

[1]Upasana Hebbar, [2]Saniya Sultana, [3] Mrs. Annie Sujith

Abstract

Internet of Things (IoT) is a new trend in technology that allows the people to associate or relate to anyone at any time and in any place. The various medical services of IoT such as Community Healthcare, Indirect Emergency Healthcare, Ambient Assisted Living(AAL), Embedded Gateway Configuration and Internet of m-health are surveyed in this paper. In addition to that, the applications of IoT in medication management, rehabilitation system, sensing blood pressure monitoring and ECG monitoring are analysed. The outcome of these applications shows that the usability of IoT in the medical field helps in improving the condition of lifetime, user understanding, real-time disease management and patient outcomes. The security threats such as confidentiality, authentication, privacy, access control, trust, and policy enforcement are analyzed. The existence of these security threats changes the IoT performance, therefore it uses Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES) and Data Encryption Standard (DES) which are cryptographic algorithms. It proves that RSA gives good security than AES and DES algorithms by investigating these techniques.

Keywords: Internet of Things (IoT), medical applications and services, security threats, Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Data Encryption Standard (DES).

INTRODUCTION

In recent days, Internet of Things (IoT) has achieved popularity for linking things such as software, equipment, sensors, instruments and information services [1]. With the help of internet, it also allows to exchange the information between these things. The key elements which are involved in the IoT are as follows: sensing, identification, service, semantics and communication. Within the network, the sensing element gains the data from different objects and then it sends back the sensed data to the cloud or to the database. The services are matched with the demand by the identification element. There are four classes such as ubiquitous services, identity related services, information aggregation service and collaborative services which are classified under service element. The semantic element is utilized for gaining the information from many devices.

And finally, for providing the specific smart services the communication element is used which links the heterogeneous objects. The commonly used computation elements are Microprocessor and microcontroller and the computation elements are the processing units of IoT.

According to [2], there are various applications of IoT. The medical applications are considered in this paper. The various services and applications of IoT are mainly concerned for analysis purpose.

This paper is arranged as follows; section II describes the existing IoT applications and services. Section III gives a detailed overview of the security challenges of the IoT. Section IV shows the anonymization techniques used for addressing the security challenges and cryptographic algorithms. Section V describes the descriptions and results. Section VI illustrates the proposed work and the paper is concluded in section VII.

MEDICAL APPLICATIONS AND SERVICES OF IOT

The use of IoT in medical sector is for improving and changing the condition of lifetime, to manage real time diseases, to improve user understanding and also in patient outcomes. As showed in fig. a, the IoT based on medical applications is classified into two categories such as services and applications [5].

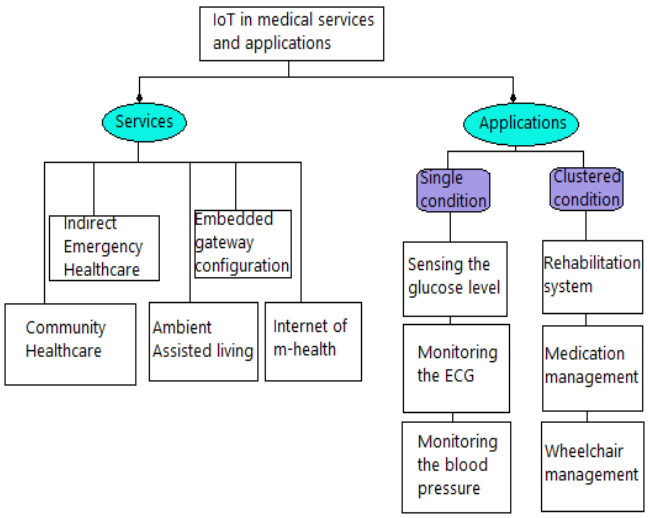

Fig. a. Medical applications of IoT

Services

The IoT services are represented in the above figure

a. Community healthcare

An IoT network is created around a local community such as rural community, hospital and residential area by monitoring the community healthcare in [10], to monitor the health and medical systems the Community Medical Network(CMN) is suggested. The cost and time requirements are reduced for diagnosing and treating the diseases by the suggested Community Medical Network(CMN). The electronic health records of the residents are monitored in [11] with respect to the health and medical information technology. The cooperative network structure is created by integrating the multiple smaller IoT network.

b. Indirect emergency healthcare

To moniter the health and analyse the risks in the eastern sites, a model called an immune theory-based health monitoring and risk evaluation is proposed in [12]. It gives very good precised outcomes on the health risks of the single environmental factor of earthen sites. An Intelligent Community Security System (ICSS) is proposed in [13].

c. Ambient Assisted Living (AAL)

Ambient Assisted Living(AAL) tries to give a human-servant like assistant for any problem and it also provides medical assistance for the independent living of the disabled people, elderly people and also to their their families. Blood glucose level and insulin therapy are managed by introducing an IoT-based AAL architecture in [6]. The patients are supervised at their home and they are also provided with a personal health card based on web diabetes management portal and RFID by the suggested approach. To provide a secure communication between people and things, people and people and things and things, a combination of closed loop healthcare services and KIT technologies are suggested in [7].

d. Embedded Gateway Configuration (EGC)

The EGC is an architectural service that connects the network to the internet and other medical devices. In [14], the embedded services are exploited for the healthcare systems. An open, secure, and flexible IoT-based platform is suggested in [15] for the medical applications.

e. Internet of m-health

The m-health gives the healthcare services by exploiting the communication technologies and medical sensors. For sensing the non-invasive blood glucose level, m-IoT is utilized and it is also used to

manage them in the heterogeneous environment. To address the challenges in m-health, the concept of 4G health is proposed in [9].

Applications

There are various applications of IoT in medical field and are mainly categorized into two types such as single condition and clustered condition. The following sections gives a short note on each of the applications.

Single condition

The single condition applications are used for a particular disease.

a. Sensing the Glucose level

The medical condition called Diabetes or diabetes mellitus is such a condition where the person will have higher glucose levels for a longer period of time. For providing a two-way interaction between IoT technology and diabetic patients a context-aware Interactive mobile-Health System (ImHS) is suggested in [16].

b. Monitoring the ECG

To analyse the electrical activity of the heart, the Electrocardiography (ECG) is used and in IoT based ECG monitoring, the constant information about the heart rate and the rhythm is resulted by placing the sensors in the position depicted in Fig.5. And to improve the interchangeability and connectivity, an intelligent home-based platform is proposed in [17]. The inkjet printing technology is connected with the wearable bio-medical sensor device.

c. Monitoring the blood pressure

Blood pressure indicates the pressure of the blood in the circulatory system. In [19], for tracking and regulating the health parameters such as Blood Pressure (BP), Hemoglobin (HB), blood sugar and abnormal cellular growth, a complaisant IoT approach is proposed. An intelligent heath service is suggested in [20] for monitoring the blood pressure, diabetes, and obesity.

Clustered condition

The clustered condition applications are designed to handle multiple diseases together.

a. Rehabilitation system

As the rehabilitation system improves the quality of living, the goal of IoT is to solve the issues concerning the aging population and the absence of the health experts. In [21], for increasing the rehabilitation exercise, the Body Sensor Network (BSN) is suggested. An ontology-based Automating Design Methodology (ADM) is suggested in [22] for providing a smart rehabilitation systems.

b. Medication management

The issues related to the inefficient medication process are addressed by IoT. A pervasive and preventive medication management system is suggested in [23] for addressing the issues related to the medication management.

a. Wheelchair management

A smart wheelchair is an automated wheelchair specially designed for the disabled persons. A computerized system observes the motions of the wheelchair hence sensing heart rate and other parameters. In [24], a Wireless Body Sensor Network (WBSN) is suggested for monitoring the various health parameters.

SECURITY CHALLENGES OF IOT

According to [26], the challenges faced by the IoT are as follows,

- Confidentiality
- Authentication
- Access control
- Privacy
- Trust
- Policy enforcement

Confidentiality

Confidentiality is the protection of personal information. Confidentiality of data in IoT can be ensured by using protocols and mechanisms. In [27], for the IoT, the Datagram Transport Layer Security (DTLS) protocol is proposed for supporting a two-way authentication.

Authentication

The authentication makes sure that the user is genuine. [29] Proposes an inter-device authentication and symmetric-key dispersal scheme for generating the symmetric keys.

Access control

When a new connection needs to be established, the communication quality is ensured using access control algorithm. It protects the IoT from different intruder attacks such as a man in middle, denial of service and replay attacks. In [30], the Identity Establishment and Capability-based Access Control (IECAC) protocol with Elliptical Curve Cryptography (ECC) algorithm suggested for providing the access control.

Privacy

Privacy in one of the major apprehensions of the users as IoT is used in various applications. The users expect their information to be protected from intruders. As in [32], the privacy apprehensions in IoT are classified into following:

- Privacy in device
- Privacy throughout communication
- Privacy in storage
- Privacy at processing

In [33], a Continuously Anonymizing Streaming data via adaptive cLustEring (CASTLE) scheme that anonymizes the data streams and ensures the delay constraints on the data streams is suggested.

Trust

The foundation of IoT is based on trust. In [35] a trust management system is proposed which can be used to focus on the requirement of IoT. Based on the prior behavior, the trust system calculates the dynamic trust scores for all the cooperating nodes. These scores can be used for detecting the misbehaving nodes. In [36], a dynamic trust management protocol is suggested for handling the misbehaving nodes.

Policy enforcement

In [37], an effective implementation of security policy is proposed for tackling the security and privacy challenges.

COUNTERMEASURES FOR IOT CHALLENGES

This section elucidates existing measures which are used to tackle the IoT security challenges. There exists mainly two approaches for addressing the IoT security challenges, the cryptographic algorithms and anonymization technique, as shown in Fig. b.

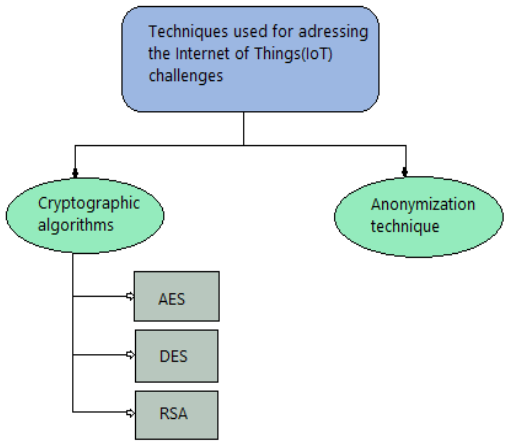

Fig. b: Categories of cryptographic algorithms

Cryptographic algorithms

Cryptographic algorithms perform encryption ad decryption using a key. In encryption, plain text is converted into unintelligible text called cipher text and in decryption, being the reverse of encryption, cipher text is decoded back to plain text. Some cryptographic algorithms are represented in Fig. b.

a. Advanced Encryption Standard (AES)

The AES algorithm is a symmetric encryption algorithm. It uses the same key for both encryption and decryption. The data is divided into 128-bit blocks and these data blocks are encrypted in 10, 12 and 14 rounds.

Data Encryption Standard (DES)

The DES algorithm is largely used for protecting the unclassified data from being attacked, The DES algorithm also uses the same key for the encryption and decryption processes, same as the AES algorithm. The data is separated into 64-bit blocks and these data blocks are encrypted in 16 rounds.

Rivest-Shamir-Adleman (RSA)

The RSA algorithm is an asymmetric encryption algorithm.it is a public key cryptosystem that uses one public key and one private key. It is called public key cryptosystem because one of the key is public and can be given to everyone whereas the other key must be kept private. It includes three main processes as follows,

- Key generation
- Encryption
- Decryption

Key generation

This step creates both the private key and public key. The overall steps involved in the key generation process are illustrated as follows [39],

Step 1: Assume two prime numbers say, a and r.

Step 2: Calculate s=ar and φ = (a-1)(r-1)

Step 3: Choose c such that 1 < c < φ

Step 4: Estimate the integer i such that 1 < i < φ where ci = φ

Step 5: Return public key (s, c) and private key i.

Encryption

In the encryption process, the plain text is converted into cipher text using the key generated. The encryption is done using the following equation,

$$\mathbf{Cj = m^c \bmod s} \quad (1)$$

iii. Decryption

In the decryption process, the cipher text is converted back to the plain text. It is based on the following equation,

$$\mathbf{m = C_j^{\,i} \bmod s} \quad (2)$$

When compared to AES and DES algorithms, the RSA algorithm is more efficient as it prevents multiple attacks and maintains data with more security.

A. Anonymization technique

To maintain the privacy of data, the anonymization techniques are used. Various hospitals disclose the details about the patients for statistical reasons. But the data being in the quasi-identifying attribute offers chances for the attackers to include the external information [40]. The personal data are anonymized in order to increase the privacy. In [41], to maintain the privacy of the individual users and avert the access of sensitive information by intruders, a privacy-preserving data publishing approach is proposed.

RESULTS AND DISCUSSIONS

This section addresses the existing medical applications, the security issues faces by the applications and measures to tackle these issues. The analysis results show that the IoT is suitable for the medical field. Using IoT reduced cost, improved health care in [45]. The security threats were tackled using DTLS, IEAC-ECC and CASTLE. The countermeasures to address the security attacks cryptographic algorithms are used such as AES, DES and RSA. AES is fast in encryption and decryption. DES has moderate speed of encryption and decryption process. RSA has a low speed of encryption and decryption. Other than the cryptographic algorithm, Anonymization technique is also used to protect data from attacks.

PROPOSED WORK

The proposed system first extracts health data of the patients from the electronic devices associated and transfers the data into the cloud database by following these steps,

- Pre-processing
- Key generation
- Data encryption
- Data transmission
- Data decryption

The obtained health data has to be transferred to the cloud database. This process is vulnerable to many security attacks. Hence, this issue is addressed using asymmetric cryptography based algorithm is used for data transmission. The proposed algorithm takes advantage of the

Modified Rivest-Shamir-Adleman (MRSA) algorithm for encryption and decryption.

CONCLUSION

This paper provides a detailed analysis of the different medical applications and services of IoT. The major services of IoT in the medical field are Ambient Assisted Living, Internet of m-health, community healthcare, indirect emergency healthcare, and embedded gateway configuration. The medical applications of IoT are categorized into two types, single condition, applications meant for a particular disease such as glucose level monitoring, ECG monitoring, and clustered condition, applications that handle multiple diseases together such as rehabilitation system, medication management, and wheelchair management. The various security challenges faced by the medical IoT are privacy, trust, confidentiality, authentication, access control, and policy enforcement. To tackle these challenges, two types of countermeasures are used, the cryptographic algorithms and Anonymization technique. In the cryptographic algorithms, based on the survey results, RSA algorithm provides better protection against multiple attacks and is not vulnerable to brute-force attacks as AES and DES. Anonymization technique is also used to protect data from attacks. Based on the survey results, an asymmetric key cryptography based anonymous health data storage system is proposed. The proposed system extracts the health data of the patient and transfers them to the IoT devices. In the conventional systems, the extracted health data are transferred from the electronic gadget to the cloud database. This process is vulnerable to multiple security attacks and challenges, such as man-in-the-middle attack and data modification attack. Hence, this issue is addressed using asymmetric cryptography based algorithm. MRSA algorithm is used for encryption and decryption of data. The anonymous data storage helps prevent intrusion.

References

[1] H. H. G. Afshan Samani , Abdulmutalib Wahaishi "Privacy in Internet of Things: A Model and Protection Framework," 6th International Conference on Ambient Systems, Networks and Technologies vol. 52, pp. 606-613, 2015.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.

[3] B. R. Ltd. (2014). Towards Smart Farming Agriculture Embracing the IoT vision Available: https://www.beechamresearch.com/files/BRL%20Smart%20Farmi ng%20Executive%20Summary.pdf

[9] R. S. H. Istepanaian and Y. T. Zhang, "Guest Editorial Introduction to the Special Section: 4G Health—The Long-Term Evolution of m-Health," IEEE Transactions on Information Technology in Biomedicine, vol. 16, pp. 1-5, 2012.

[10] Y. Lei, L. Chungui, and T. Sen, "Community Medical Network (CMN): Architecture and implementation," in 2011 Global Mobile Congress (GMC), 2011, pp. 1-6.

[11] W. Wang, J. Li, L. Wang, and W. Zhao, "The internet of things for resident health information service platform research," in IET International Conference on Communication Technology and Application (ICCTA 2011), 2011, pp. 631-635.

[12] Y. Xiao, X. Chen, L. wang, W. Li, B. Liu, and D. Fang, "An Immune Theory Based Health Monitoring and Risk Evaluation of Earthen Sites with Internet of Things," in IEEE International Conference on and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom), 2013.

[13] J. Liu and L. Yang, "Application of Internet of Things in the Community Security Management," in Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), 2011, pp. 314-318.

[14] M. F. A. Rasid, W. M. W. Musa, N. A. A. Kadir, A. M. Noor, F. Touati, W. Mehmood, et al., "Embedded gateway services for Internet of Things applications in ubiquitous healthcare," in 2nd International Conference on Information and Communication Technology (ICoICT), 2014, pp. 145-148.

[15] X. M. Zhang and N. Zhang, "An Open, Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine," in International Conference on Computer and Management (CAMAN), 2011.

[16] S. H. Chang, R. D. Chiang, S. J. Wu, and W. T. Chang, "A Context-Aware, Interactive M-Health System for Diabetics," IT Professional, vol. 18, pp. 14-22, 2016.

[17] G. Yang, L. Xie, M. Mantysalo, X. Zhou, Z. Pang, L. Da Xu, et al., "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and

intelligent medicine box,"IEEE Transactions on Industrial Informatics, vol. 10

[19] V. M. Rohokale, N. R. Prasad, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," in 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE) 2011, pp. 1-6.

[20]B. M. L. a. J. Ouyang, "Intelligent Healthcare Service by using Collaborations between IoT Personal Health Devices,"International Journal of Bio - Science and Bio - Technology, vol. 6.

[21] B. Tan and O. Tian, "Short paper: Using BSN for tele-health application in upper limb rehabilitation," in IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 169-170.

[22] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, "IoT-Based Smart Rehabilitation System," IEEE Transactions on Industrial Informatics, vol. 10, pp. 1568-1577, 2014.

[23] Z. Pang, J. Tian, and Q. Chen, "Intelligent packaging and intelligent medicine box for medication management towards the Internet-of-Things," in 16th International Conference on Advanced Communication Technology (ICACT), 2014, pp. 352-360.

[24] L. Yang, Y. Ge, W. Li, W. Rao, and W. Shen, "A home mobile healthcare system for wheelchair users," in IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2014, pp. 609-614.

[26] A. K. Ashvini Balte, Balaji Patil "Security Issues in Internet of Things (IoT): A Survey," International Journal of Advanced Research in Computer Science and Software Engineering vol. 5, pp. 450-455, 2015.

[27] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, pp. 2710-2723, 2013.

[28]G. C. a. P. L. Ismail Mansour, "Key Management in Wireless Sensor Networks," Journal of Sensor and Actuator Networks, vol. 4, pp. 251-273, 2015.

[29]N. P. a. N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle," Sensors, pp. 1-16, 2016.

[30]P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity establishment and capability based access control (IECAC) scheme for Internet of Things," in 15th International Symposium on Wireless Personal Multimedia Communications (WPMC), 2012, pp. 187-191.

[32]D. R. P. J. Sathish Kumar, "A Survey on Internet of Things: Security and Privacy Issues " International Journal of Computer Applications, vol. 90, pp. 20-26, 2014.

[33]J. Cao, B. Carminati, E. Ferrari, and K. L. Tan, "CASTLE: Continuously Anonymizing Data Streams," IEEE Transactions on Dependable and Secure Computing, vol. 8, pp. 337-352, 2011.

[35]Y. B. Saied, "Trust management system design for the internet of things: a context-aware and multi-service approach," Computers & Security, vol. 39, pp. 351-365, 2013.

[36]F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," presented at the Proceedings of the 2012 international workshop on Self-aware internet of things, San Jose, California, USA, 2012.

[37]R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the Internet of Things," in 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2014, pp. 165-172.

[39]P. Mahajan and A. Sachdeva, "A study of Encryption algorithms AES, DES and RSA for security," Global Journal of Computer Science and Technology, vol. 13, 2013.

[40]G. Ghinita, Y. Tao, and P. Kalnis, "On the anonymization of sparse high-dimensional data," in IEEE 24th International Conference on Data Engineering, 2008, pp. 715-724.

[41]W. K. Fung BCM, Chen R, Yu PS. , "Privacy-preserving data publishing: A survey of recent developments.," ACM Comput. Surv., vol. 42(4), 2010.

[45] A. P. Moeen Hassanalieragh, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, Silvana Andreescu, , "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges," IEEE International Conference on Services Computing, pp. 285-292, 2015.

[49]X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," in 2014 IEEE International Conference on Communications (ICC), 2014, pp. 725-730.

Author's details

1. Student, Department of Computer Science and Engineering, T. John Institute of Technology, Karnataka, India, upasna.hebbar@gmail.com

2. Student, Department of Computer Science and Engineering, T. John Institute of Technology, Karnataka, India, Saniyasultana0000@gmail.com

3. Asst. Professor, Department of Computer Science and Engineering, T. John Institute of Technology, Karnataka, India, annies@tjohngroup.com