IOT Perception Layer Security and Privacy

Azza A. A.
Imam Abdulrahman Bin Faisal University, Faculty of Science and Humanities, Jubail
Computer Science Department

Hanaa F. M.
Imam Abdulrahman Bin Faisal University, Faculty of Science and Humanities, Jubail
Computer Science Department

Maissa A. Elmageed
Imam Abdulrahman Bin Faisal University, Faculty of Science and Humanities, Jubail
Mathematics Department

ABSTRACT

One of the current challenges in Internet of Things (IOT) security is the choice cryptography algorithms and key management mechanism to be used in the perception (hardware) layer. The purpose of this paper is to study the various security algorithms to achieve security standards (confidentiality, integrity, privacy) on the perception layer of IOT. The study is based on comparing the different characteristics of these algorithms, such as the degree of security of the algorithm, its speed, its achievement of various security standards, and determination of which algorithms are easy to apply to physical devices such as sensors.

Keywords

IOT, Perception Layer, Security.

1. INTRODUCTION

Technology interconnection is defined as a system of interconnected computers, mechanical and digital machines, objects or persons. It is also defined as internet of things (IOT). The interconnection of this technology provides a transition of sensitive information which must be as confidential as possible. So, the security is very critical concern in IOT.

Due to IOT devices are closely associated, any hackers can exploit a security gap to handle all data and making them unusable. However, hackers are not the only threat to the IOT. Privacy is another major consideration for users. For example, companies that manufacture and distribute IOT devices can use these personal digital devices to access personal data of users beside the diversion of this personal data. So, IOT may pose a threat to the vital infrastructure including electricity, transport and financial services.

IOT contributes in our daily life through numerous applications, for example healthcare [1], smart cities [2], smart buildings [3], transportation [4], and industrial manufacturing [5]. Smart healthcare services assume a huge part in social insurance applications through implanting sensors and actuators in patients' bodies for observing and following purposes. IOT is utilized as a part of medicinal services so as to screen physiological statuses of patients. The implanted sensors can gather data straightforwardly from the body territory of the patient and transmit it to the doctor. This innovation can possibly totally separate the patient from the unified framework which is the healing facility while keeping up ceaseless contact with the doctor. Also, smart cities consist of the most critical applications of IOT. In this specific circumstance, sensors are conveyed all over streets, buildings, smart healthcare, and so on to better oversee activity, adjust the climate, lighting takes after the situation [6].

The primary goals of security in any network are: Confidentiality, Integrity and Availability (CIA) of information. Confidentiality means concealment of the secret information, so that information is available or disclosed only to the parties concerned. The integrity means that the information is trustworthy so that no one other than the person concerned is able to create, modify or delete the information, including protection against the injection of fraudulent, duplicate or old information. The availability means access to information or resources at the time Appropriate and reliable manner [7].

IOT security levels are ranked up on the rank of IOT layers, i.e. each IOT layer concerned with different security goals up on the main characteristic of this layer. IOT layers are divided into three layers; a perception (hardware) layer, a network (communication) layer, and application layer [8] [9] [10]. Figure.1 illustrates the three layers of IOT. Perception (hardware) layer is the first layer in the IOT architecture that gives security features to physical structure. IOT Perception Layer security system is intended to gather and exchange information from the physical world. This layer needs to be served with three main security objectives: authentication, data privacy of sensitive information, and risk assessment.

In this research, the properties of some security algorithms were studied which can be applied into the physical layers (Perception). Comparison between certain criteria of these algorithms will be discussed. These criteria are speed, key size and safety, and the most important criterion is the ease of applying sensors where some algorithms are difficult to be applied in physical devices. Finally, determining which of these algorithms meets the security standards (integrity, privacy and confidentiality) together reach to a high-security system.

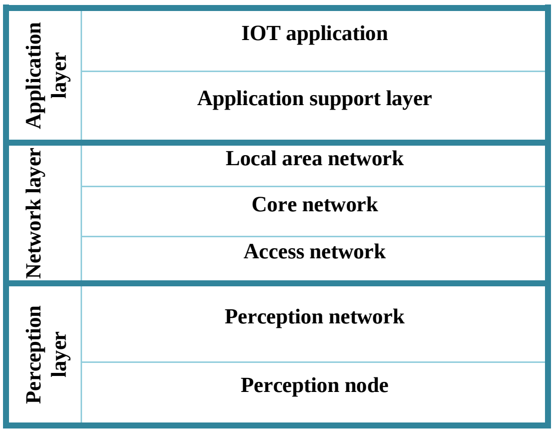

Figure.1 IOT three layers

2. IOT LAYERS SECURITY

IOT Perception Layer is designed to collect data from the main world. Hence, the perception layer contains various types of collecting and controlling modules, such as the temperature sensors, sound sensors, vibration sensors, pressure sensors, etc. [11]. The perception layer can be further divided into two parts: perception node (sensors or controllers, etc.), and perception network [11]. Perception node is utilized for acquisition and data control and perception network sends collected data to the gateway or sends control instruction to the controller.

The perception layer needs to be served with four main security objectives: authentication, data privacy of sensitive information, user anonymous and risk assessment.

- **Authentication:** The cryptographic Hash-based algorithms are used to provide digital signatures for all devices to resist all hacked attacks such as Collision attack, Side-channel attack, Brute force attack, etc.

- **Data privacy:** Data privacy is secured by some data Symmetric and asymmetric encryption algorithms such as BLOWFISH, RSA, DES, etc. These algorithms prevent unauthorized access to sensitive data during compilation or delivery to the next layer. It is recommended to apply these algorithms in this layer because it consumes a little energy.

- **User Anonymous:** The concept of non-privacy is used $K -$Anonymity $algorithm$ disclosure that ensures anonymity and identity of the user. This concept is useful in keeping the user away from multiple attacks [12].

- **Risk assessment:** It can't be abandoned in IOT security, this idea serves to expose the new risks to the system. Risk assessment is useful in analysis of security strategies and defense of security breaches. Example: Dynamic risk assessment method which express a continuous process of risk detection and risk analysis that can be used to monitor the system [13]. Even after employing these security measures, if a security hole is detected in the system, a built-in kill command is ordered by the RFID reader to RFID tagging tag to prevent unauthorized access to data[14].

The network layer is exposed as hacked. The security requirements at network layer are listed as following:

- **Authentication:** can prevent unauthorized access to sensor nodes by appropriate authentication and peer to peer encryptions algorithms. DoS attack is the famous attack on networks, where the network is flooded miscellaneous.

- **Routing Security:** using routing after authentication ensuring data access to their destination. Many studies of routing have been done such as Bop-hop routing, Source Routing.

- **Data Privacy:** Data privacy tests the security methods of safety control mechanisms of the system against hacking and also depend on the methods of testing integrity of the data.

Also, there are some security applications must be set between the middle layer (network layer) and the application layer. The following security requirements should be achieved between network layer and the application layer:

- **Authentication:** to prevent any malicious user from logging in automatically. Authentication depends on user identity.

- **Intrusion Detection**: It generates intrusion detection techniques and alerts when there is any suspicious activity in the system.

- **Risk Assessment**: Risk assessment ensures rationalization. It is adopting security strategies and helps to improve pre-existing security tools.

- **Data security:** Many security technologies and algorithms provide data encryption and prevent data theft. Many software has been introduced to reduce these attacks such as AntiDos Firewalls.

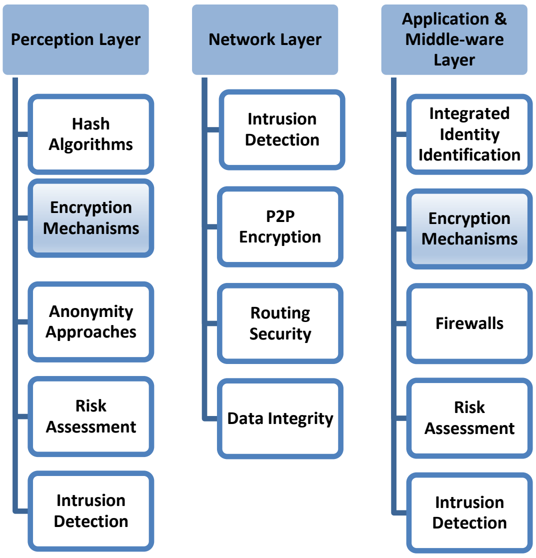

Figure.2 Security requirements for each layer.

In order to achieve the privacy of data at perception layer, the privacy, integrity and confidentiality criteria of the data, sent by the sensors must be met. Therefore, a set of algorithms characteristics is studied that meet some of the above criteria. The characteristics of these algorithms are speed of work, safety level and size of the secret key used**.** They are easy to be applied on the physical sensors device which is one of the most important criteria for the selection of these algorithms. The selected algorithms are AES, DES, 3-DES, RSA, RC4, and SHA.

3. RESULTS AND DISCUSSION

Table.1 illustrates that each algorithm can be applied on sensors as a physical device, and that AES, SHA algorithms are easy to apply to sensors compared with other algorithms.

The algorithms were also compared in terms of speed. The fastest ones were found to be the AES and SHA algorithms. Figure.2 shows that the slowest are DES and RSA algorithms.

Also, comparison between the algorithms were done, whence more key length increases the safety of the algorithm. Table.1 shows that the AES and RC4 algorithms have a key length begins from 128 to 256 bits, which is long enough to achieve high security for the secret key. Compared to the DES with key length equal to 56-bit for 16 round, and 3DES algorithms with 168 to 112 bit for 3 × 16 round, which increases the time of encryption and makes 3DES very slow compared with AES and RC4 which are so fast. It is also shown from Table.1 that RSA algorithm does not have a fixed length of the key and depends on number of bits in the modulus n where $n = p \times q$ [3]. Also, AES, DES, RC4 and 3DES used for encryption only and that achieves the confidentiality goal only.

It is concluded that the AES and SHA algorithms together achieve the highest safety standards and ease of application on sensors.

After studying the different characteristics of the AES, DES, 3-DES, RSA, RC4, and SHA [15] algorithms in terms of achieving sensor data security standards and studying their applicability with physical devices, the study concludes that the AES or RC4 and SHA algorithms are integrated to achieve safety standards and can be applied to sensors. Also, SHA can be applied at message authentication code (MAC) [16] to achieve authentication requirement also. Therefore, recommendation of this study is using AES and SHA with MAC to achieve as much data security as possible in sensors in IOT sensors object. The study also recommends that all security standards be applied to all layers of Internet objects so that can feel comfortable and safe using such smart devices.

4. CONCLUSIONS

By the study of encryption algorithms characteristics such as AES, DES, 3-DES, RSA, RC4, and SHA, it has been concluded that the three main basic data security criteria (confidentiality, integrity, privacy) are not all available in one algorithm. For example, it was found AES, RC4, and DES achieve data confidentially standards only while the RSA algorithm achieves the standard of data confidentiality in addition to data privacy but does not achieve data integrity. Only the SHA algorithm achieves integrity and privacy as combined with Mac algorithms. Therefore, recommendation of study is using AES or RC4 combined with SHA with MAC to achieve as much data security as possible in sensors in IOT sensors object

Table.1. Comparison of algorithms in terms of safety, safety and applicability of sensors.

Factors	AES	SHA	RC4	DES	3DES	RSA
Key Length	128, 192, or 256 bits	128 to 512 bit	128-bits	56 bits	168 bits (k_1, k_2, k_3) 112 bits (k_1, k_2)	Depends on number of bits in the modulus n where $n = p \times q$
Block size	128-bit	128 to 512 bit size of the output	128 bits	64 bits	64 bits	Variable
Speed	Fast	Fast	Fast	Slow	Slowest	Slowest
Security	Excellent Security	Excellent Security	Excellent Security	Not Secure Enough	Adequate Security	Least Secure
CIA security goals	Confidentiality	Integrity	Confidentiality	Confidentiality	Confidentiality	Confidentiality And Authentication
Applied on the physical sensors	Can be applied	Can be applied	Can be applied	Cost to be applied	Cost to be applied	Cost to be applied

5. REFERENCES

[1] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[2] Deakin, Mark; Al Waer, Husam (2011). "From Intelligent to Smart Cities". Journal of Intelligent Buildings International: From Intelligent Cities to Smart Cities. 3 (3): 140–152. doi:10.1080/17508975.2011.586671.

[3] Deakin, Mark (22 August 2013). "From intelligent to smart cities". In Deakin, Mark. Smart

[4] Cities: Governing, Modelling and Analysing the Transition. Taylor and Francis. p. 15. ISBN 978-1135124144.

[5] Y. Leng and L. Zhao. Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things. In Proceedings of 2011 International Conference on Electronic Mechanical Engineering and Information Technology, volume 6, pages 3190– 3193. IEEE, Aug 2011.

[6] Davis, Jim; Edgar, Thomas; Porter, James; Bernaden, John; Sarli, Michael (2012-12-20). "Smart manufacturing, manufacturing intelligence and demand-

dynamic performance". Computers & Chemical Engineering. FOCAPO 2012. 47: 145–156.

[7] Hanaa F. M., Entesar H. I., Azza A. A." Internet of Things Applications and its Security", International Journal of Computer Applications, V.182. No. 41, 2019.

[8] H. Noura. Adaptation of Cryptographic Algorithms According to the Applications Requirements and Limitations: Design, Analyze and Lessons Learned. HDR dissertation, UNIVERSITY of PIERRE MARIE CURIE -Paris VI, 2016.

[9] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[10] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[11] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (sIOT)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[12] M.M.Noor, Wan H.H.," Current research on Internet of Things (IOT) security: A survey ", Computer Networks 148 (2019) 283–294

[13] K.E. Emam, F.K. Dankar, "Protecting Privacy Using Anonymity", Journal of the American Medical Informatics ، Volume.15, No. 5, 2008.

[14] C. Liu, Y. Zhang, J. Zeng, L. Peng, R. Chen" ،Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology "، Eighth International Conference on Natural Computation (ICNC), 2012.

[15] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips" Guidelinesfor Securing Radio Frequency Identification (RFID) Systems ", National Institute of Standards and Technology.

[16] Henri Gilbert, Helena Handschuh: Security Analysis of SHA-256 and Sisters. Selected Areas in Cryptography 2003: pp175–193.

[17] Goodrich, Oded (2001), Foundations of cryptography I: Basic Tools, Cambridge: Cambridge University Press, ISBN 978-0-511-54689-1