Journal of Engineering and Applied Sciences 12 (16): 4132-4137, 2017
ISSN: 1816-949X

An Overview on Security Features for Internet of Things (IoT) in Perception Layer

Nur Syazarin Natasha Abd Aziz, Salwani Mohd Daud, Sya Azmeela Syarif,
Hafiza Abas and Azizul Azizan
Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

Abstract: The evolution of Internet of Things (IoT) becomes more prominent and obtrusive in human life. More gadgets are being connected to other gadgets and networks in gathering, collecting and sharing data and information with each other in real time or virtual existence. Nevertheless, security is experiencing more advanced challenges and issues regarding user privacy and confidentiality as well as integrity and authenticity of the data collected. The purpose of this study is to review, analyze and discuss the existence of the security system in inhibiting those issues. As IoT consists of three distinct layers including application layer, transportation layer and perception layer, this study will delve deeper on the security features, issues and further solution in the perception layer. Furthermore, this discussion will highlight more clearly about the security issues faced.

Key words: Security feature, IoT, perception layer, wireless sensors network, clearly, Malaysia

INTRODUCTION

Internet of Things (IoT) refers to a network of gadgets which connect to each other to collect, capture and share the information through the Secure Service Layer (SSL) in the area of wireless communication (David, 2013; Sanots *et al*., 2014; Oh *et al*., 2014). This paradigm enables people realizing smart environments such as; smart cities (e.g., smart transport system) smart health care and smart energy (e.g., smart grid and smart lighting (David, 2013; Moosavi *et al*., 2015). IoT plays an important role in broad range of applications (David, 2013). There are some examples how IoT potential is playing out in clinical care the hospitalized patient who needs close attention can be constantly monitored by non-invasive monitoring (David, 2013) as it will regularly check on patient's vital sign and update into the system. Next, the elderly who lives alone can remotely monitoring their health by connecting through IoT devices which comprises of variety of sensors with complex algorithms to analyze and share the data through wireless connectivity with the medical professionals (David, 2013; Sanots *et al*., 2014). The advanced IoT technology along with the security concern may establish the ubiquitous ambient assisted living for healthcare applications (Sanots *et al*., 2014).

Yet, there are still number of challenges and issues are debating now (Jing *et al*., 2014). In this context, security aspect must be evaluated in terms of functional benefits for protecting the patient's privacy and data security to service providers and healthcare professionals that are highly sensitive nature (Aramudhan and Mohan, 2010; Marti *et al*., 2004). Security protection is a must to ensure the privacy, authenticity, confidentiality and integrity of the information is securely protected from any threats and malicious malware.

Marti *et al*. (2004) has categorized the four types of security services: confidentiality, integrity, authenticity and system performance including availability, reliability and accountability. Confidentiality acts as a data protector from any unauthorized access during communication or in storage. Meanwhile, integrity is a data protector against any modification, substitution, addition, deletion or insertion of the data from non-authorized user. Authentication is an approach to correlate between identity and entities.

In this study, first we will review various security threats involved in IoT infrastructure and present the security architecture of IoT. Next, we will classify the security features available in the perception layer. Then, we will analyze and discuss deeply the issues and corresponding technology solutions for each of the listed features. Finally, the comparative analysis is done for future direction.

MATERIALS AND METHODS

Security architecture of IOT: Security is one of the significant features needed in designing IoT because of the sensitivity and privacy of the data (Oh *et al*., 2014).

Corresponding Author: Nur Syazarin Natasha Abd Aziz, Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

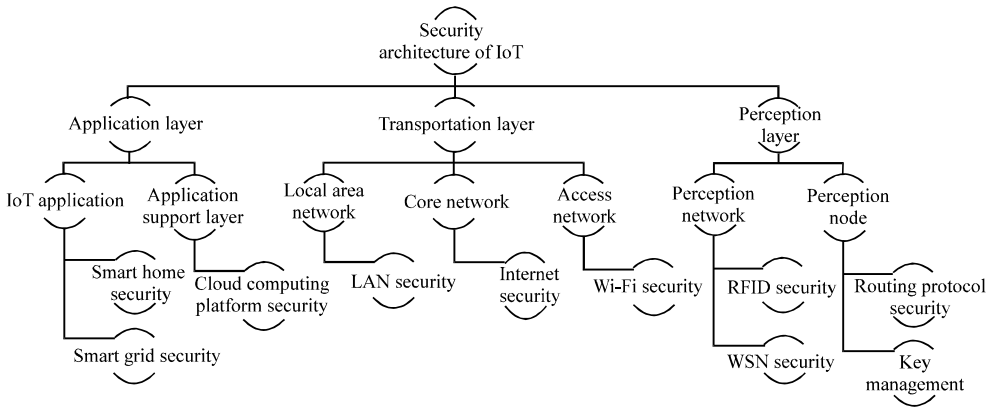

Fig. 1: Security architecture of IoT (Jin *et al*., 2014; Yang *et al*., 2012; Sharma and Jhawala, 2015)

Table 1: Summary of multi-layer security infrastructure or architecture of IoT (Oh *et al*., 2014; Jin *et al*., 2014; Yang *et al*., 2012; Sharma and Jhawala, 2015)

Criteria	Perception/Physical layer	Network/transportation layer	Application layer
Criteria and function	Comprises of various types of data collecting and controlling modules Perceiving and gathering information	Transmits data through internet and mobile telecommunication network	Process data intelligently
Examples	Sensor nodes RFID readers Cameras Gateways	Internet Mobile communication network Heterogeneous network fusion	Smart city Smart home Pollution monitor Intelligent transportation Logistics supervise
Risks	Eavesdropping attack	Authentication security problem Denial of Service (DoS) attack Heterogeneous network attacks Application risk of ipv6 WLAN application conflicts	Application layer attack
Security	RFID security WSN security RSN security	3G Access network security Ad-Hoc network security Wi-Fi security	Remote medical security Smart home security Encryption/decryption mechanism

Even though IoT network allows only authorized users to access it is necessary for IoT to prevent from any unauthorized connection as well as attacks mounted against network (Santos *et al*., 2014; Oh *et al*., 2014). There are abundant studies have been proposed to improve security in IoT system (Sharma and Jhawala, 2015).

According to Fig. 1, the infrastructure or architecture of IoT is divided into three layers which are application layer, network or transportation layer and perception or physical layer (Jing *et al*., 2014; Yang *et al*., 2012; Sharma and Jhawala, 2015). Application layer is further divided into IoT application and application support layer. Mean while, transportation layer is categorized into three divisions; local area network, core network and access network. Besides, perception layer is classified into Perception network and Perception node. IoT must take security into account for all layers. Hence, security must be implemented in the whole IoT system crossing all the three layers.

Table 1 presents the simplified requirements including criteria and function, examples, risks as well as security in all the three layers based on (Oh *et al*., 2014; Jing *et al*., 2014; Yang *et al*., 2012; Sharma and Jhawala, 2015). According to Oh *et al*. (2014), Denial of Service (DoS) attacks occur rapidly disrupt the communication in the network or transportation layer. This attack repeatedly send the packets to the targeted objects, therefore it will harm the computational resources. Furthermore, eavesdropping attack which occur in perception or physical layer actively steal information between the nodes. In addition, the application layer attack will cause operating system errors thus this allows for unauthorized access controls.

Classification of security features in perception layer: There are several security features that have been extracted out from the existing researches including.

Variety and heterogeneity of sensor devices: There are various kinds of sensor nodes and high heterogeneity. Thus, they will have whether simple or complex structures and processors. These could make them facing a security protection capability (Zhao and Ge, 2013).

Resources (storage capacity and space, computational capabilities, power limitation): Resource is a part of system performance where it relates to availability, reliability and accountability (Marit *et al*., 2004), etc. This feature need to be paid close attention as with the limitation of the resources it will directly affected the other features.

Data security: This feature plays a significant role as many previous researches have been done to improve the issues of this feature. The information integrity, confidentiality and authenticity need to be concerned during the data acquisition, data transmission as well as in the data storage (Kumar *et al*., 2016).

Secure routing mechanism: This feature is to ensure the correct and secure route discovery while maintaining the target from any threats and attacks (Gou *et al*., 2013).

RESULTS AND DISCUSSION

Security issues and solutions analysis in perception layer: As discussed by Bendovschi (2015), the most common attacks discovered are Denial of Services (DoS), malicious codes, viruses, worms and Trojans, malware, malicious insiders, stolen devices, phishing and social engineering as well as web-based attack. Nevertheless, this attacks can be split into four categories due to their objectives, cyber-crime, cyber espionage, cyber war and hacktivism. These attacks counter disastrous effects such as loss of information, disruption, revenue loss and equipment damage.

Externally, legal aspect is an essential context relevance to security as it developed to prevent or limit the cyber-crime yet, this subject is geographically limited to a certain region (Sicari *et al*., 2015). The following texts will further discussed about the issues and technological solutions based on previous researches.

Key management protocols: A lightweight end-to-end key management protocol has been presented (Abdmeziem and Tandjaoui, 2015). There are five phases involved in processing and exchanging messages with hash function implemented. They are Phase 1 (initial exchange), Phase 2 (securing connection between parties) Phase 3 (proving representatives of third parties from constrained nodes to remote server), Phase 4 (secret generation and delivery) and Phase 5 (termination phase).

Cryptographic algorithm: Security Gateway Application (SGA) is introduced by Chen *et al*. (2016) that provide security including light weight symmetry key cryptographic negotiation functions for Machine 2 Machine (M2M) message delivery function. SGA is designed in three phases in IoT system which are symmetric key encryption graphic function negotiation phase, key exchange generation phase as well as messages delivery phase. In symmetric key encryption graphic function negotiation phase, the two smart devices will generate their temporary key via SGA server.

Pattern detection: Two pattern detection techniques are being introduced by Oh *et al*. (2014) which are auxiliary shifting and early decision. These two techniques are proven to improve the performance of pattern matching system that operates in smart objects.

In addition, a refinement of the traditional authentication scheme is introduced by Hou and Yeh (2015). In this scheme, there are three entities involve which are user, authentication server and trusted Third-Party Authority (TPPA). All entities will come across two phases including registration phase and user identification and verification phase. In registration phase, each user will register an identity from TPPA and then obtained a secret token through a secret channel. Next, if user requests an authentication service from authentication server then the identification and verification phase is invoked.

Secure routing models: An extended secure Software-Defined Networking (SDN) architecture for IoT is designed and proposed by Oliver *et al*. (2015). The proposed architecture succeeds in swapping away security limitations of traditional architecture by enabling dynamic network configuration and security policies deployment.

Figure 2 shows the proposed architecture. The controller is being implemented to manage the security of one domain. Hence, each domain has their controller. Thus, all the domains will be extended as they are interconnecting between each other via the border controller in leading towards the secure IoT paradigm.

In addition, a Secure and Efficient Authentication and Authorization (SEA) architecture using smart e-Health gateway is being proposed by Moosavi *et al*. (2015) to securely and efficiently perform authentication and authorization activities. Smart e-Health has a local database which allows it to temporarily store information and provide local processing of the data. Therefore, the authentication and authorization activities can be handled by smart e-Health gateways. Mossavi *et al*. (2015) also implement the security protocol by firstly just re-use the existing security protocols. Then, they provide

security features to the constrained devices that have limited resource to securely communicate with the remote healthcare center and smart e-Health gateway is introduced to build an IP-based security protocol.

Trust management: Secure resource sharing proposed by Bulck *et al.* (2015) introduced a secure access control mechanism for embedded microcontrollers. A protected file system is encapsulated to ensure the integrity of the file system. Based on Fig. 2, this file system is illustrated in a layered design consist of front-end access control layer. The front-end offers the public interface to the user, meanwhile the back-end consists of private functions. There are two implementations of back-end structure which through shared memory and flash storage.

As an overall view of the security features allocated in the perception layer of IoT as being described in this study, Table 2 summarized the comparisons. From this, we can observe that each of the security features faced an issue. Hence, various technological aspects are being exposed as a solution to diminish and reduce those issues. However, the existing technologies are still not able to completely eliminate those issues as they are always lacking in their solutions. Hence, more researches need to be done in enhancing the security features of the perception layer.

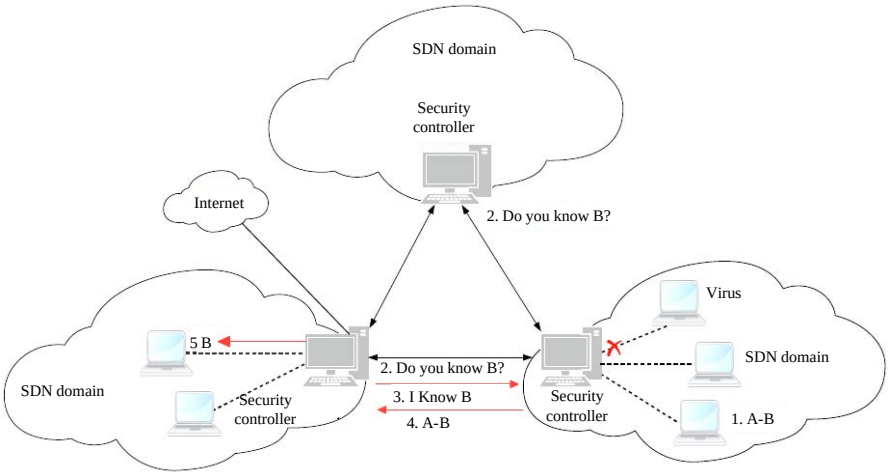

Fig. 2: Security implemented in SDN domain (Olivier *et al.*, 2015)

Table 2: Comparative analysis of security features in perception layer

Features	Issue	Technology	Pros	Cons
Various kind and high heterogeneity of sensor nodes and devices	Lack of node authentication and access control mechanism	RFID system protocol	Provides mutual and key authentication of tags and readers as well as secure data exchange between tags and readers	-
Resources (storage capacity and space, computational capabilities, power limitation)	Limited resources, limited computing power, storage space, differences of storage formats and data processing methods	Secure resource sharing	Offers strong authentication,ensures confidentiality and integrity of logical files	Unprotected test setup back-end runs and concerning the protected flash driver which the access control module only allows single private data section per module
-	-	Pattern detection scheme:	Reduces the limitation of memory usage by skipping unnecessary matching operations	Additional memory reading operation is required auxiliary shift value for corresponding index as well as save the auxiliary shift values
	to access	Auxiliary shift		
-	-	Early decision	Inhibit the complexity of the character matching	Require more processing time due to pattern sorting when the pattern number is increased
Data security	Weak key management system and eavesdropping attack	Symmetry and public key encryption	Keeping the exchanged data confidential	Energy consumption increases due to communication overhead
-	-	Digital signatures	The keys can be periodically established to strengthen the confidentiality	
-	-	Authentication scheme	The keys can be preventing alteration of data and sending from legitimate nodes	-

Table 2: Continue

Feature	Issue	Technology	Pros	Cons
-	-	SGA	Robustness of entity authentication and data communication security provide the mutual authentication mechanism and at the same time,prevent from keyguessing attack, data privacy attack as well as relay attack	-
Secure routing mechanism	Attacks on routing protocols	SDN architecture	SDN controller behaves like a security guard as begin with authenticating the network devices to secure network access and resources. Then, it will push the appropriate software and hardware access switch	-
-	-	SEA architecture	Can lower down a risk of broken domain when attacked by DoS threats only the associated sub-domain can be disrupted	-

CONCLUSION

In this study, the security issues and challenges as well as the existing security features and system in inhibiting those issues have been reviewed, analyzed and discussed. The security architecture are being focused and exposed as there are three main layers occupied. Application layer, transportation layer as well as perception layer. Next, the security features are being divided into four main divisions: variety and heterogeneity of sensor devices; resources (storage capacity and space, computational capabilities, power limitation); data security; as well as secure routing mechanism. Furthermore, the security issues and technological solutions are being discussed according to the listed features. As IoT goes advanced in future, the security services also need to be further developed in order to prevent from the advanced of any attacks, threats and malicious malware exists.

ACKNOWLEDGEMENTS

We would like to express our gratitude to Ministry of Higher Education (MOHE Malaysia) for providing financial support (research grant Q.K130000.2538.11H85) in conducting our study. Our special thanks to Universiti Teknologi Malaysia (UTM) and specifically Advanced Informatics School (AIS) for realizing and supporting this research work.

REFERENCES

Abdmeziem, M.R. and D. Tandjaoui, 2015. An end-to-end secure key management protocol for e-health applications. Comput. Electr. Eng., 44: 184-197.

Aramudhan, M. and K. Mohan, 2010. New secure communication protocols for e-mobile health system. Proceedings of the 2nd International Conference on Networked Digital Technologies, July 7-9, 2010, Springer, Prague, Czech Republic, pp: 639-647.

Bendovschi, A., 2015. Cyber-attacks–trends, patterns and security countermeasures. Procedia Econ. Finance, 28: 24-31.

Bulck, V.J., J. Noorman, J.T. Mühlberg and F. Piessens, 2015. Secure resource sharing for embedded protected module architectures. Proceedings of the IFIP International Conference on Information Security Theory and Practice, August 24-25, 2015, Springer, Heraklion, Crete, pp: 71-87.

Chen, H.C., I. You, C.E. Weng, C.H. Cheng and Y.F. Huang, 2016. A security gateway application for End-to-End M2M communications. Comput. Stand. Interfaces, 44: 85-93.

David, N., 2013. How the Internet of Things is Revolutionizing Healthcare. Freescale Semiconductor, Austin, Texas, USA.,.

Gou, Q., L. Yan, Y. Liu and Y. Li, 2013. Construction and strategies in iot security system. Proceedings of the IEEE International Conference on Internet of Things Cyber, Physical and Social Computing Green Computing and Communications, August 20-23, 2013, IEEE, Beijing, China, ISBN:978-0-7695-5046-6, pp: 1129-1132.

Hou, J.L. and K.H. Yeh, 2015. Novel authentication schemes for IoT based healthcare systems. Intl. J. Distrib. Sens. Networks, 2015: 1-9.

Jing, Q., A.V. Vasilakos, J. Wan, J. Lu and D. Qiu, 2014. Security of the internet of things: Perspectives and challenges. Wireless Networks, 20: 2481-2501.

Kumar, S.A., T. Vealey and H. Srivastava, 2016. Security in internet of things: Challenges, solutions and future directions. Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), January 5-8, 2016, IEEE, Koloa, Hawaii, USA., ISBN:978-0-7695-5670-3, pp: 5772-5781.

Marti, R., J. Delgado and X. Perramon, 2004. Network and application security in mobile e-health applications. Proceedings of the International Conference on 2004 ICOIN Information Networking, February 18-20, 2004, Springer, Busan, Korea, pp: 995-1004.

Moosavi, S.R., T.N. Gia, A.M. Rahmani, E. Nigussie and S. Virtanen *et al*., 2015. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Comput. Sci., 52: 452-459.

Oh, D., D. Kim and W.W. Ro, 2014. A malicious pattern detection engine for embedded security systems in the internet of things. Sens., 14: 24188-24211.

Olivier, F., G. Carlos and N. Florent, 2015. New security architecture for IoT network. Procedia Comput. Sci., 52: 1028-1033.

Santos, A., J. Macedo, A. Costa and M.J. Nicolau, 2014. Internet of things and smart objects for m-health monitoring and control. Procedia Technol., 16: 1351-1360.

Sharma, D. and D. Jinwala, 2015. Functional encryption in IoT e-health care system. Proceedings of the International Conference on Information Systems Security, December 16-20, 2015, Springer, Kolkata, India, pp: 345-363.

Sicari, S., A. Rizzardi, L.A. Grieco and P.A. Coen, 2015. Security, privacy and trust in internet of things: The road ahead. Comput. Networks, 76: 146-164.

Yang, X., Z. Li, Z. Geng and H. Zhang, 2012. A multi-layer security model for internet of things. Proceedings of the International Conference on Internet of things, Communications in Computer and Information Science, August 17-19, 2012, Springer, Changsha, China, pp: 388-393.

Zhao, K. and L. Ge, 2013. A survey on the intenet of things security. Proceedings of the 9th International Conference on Computational Intelligence and Security, December 14-15, 2013, IEEE, Leshan, China, ISBN:978-1-4799-2549-0, pp: 663-667.