Security Means in Multilayered Architecture of Internet of Things for Secure Communication and Data Transmission

Raimundas Savukynas
Supervisor: Dalė Dzemydienė

Vilnius University, Institute of Data Science and Digital Technologies,
Akademijos str. 4, LT-04812, Vilnius, Lithuania
raimundas.savukynas@mii.vu.lt

Abstract. The Internet of Things (IoT) is a global network of objects with sensors, controllers, software and capable of gathering, processing, exchanging information, which functioning is based on interactions between existing or completely newly developed information and communication technologies. This allows to link a many various types of objects over the internet, so it is necessary to develop a multilayered architecture of IoT with security means, which would allow identifying physical objects, establish their operation rules, protect outgoing confidential information, ensure the integrity of data received and lower consumption of energy resources. The agents in the smart environment of objects of the IoT interact with each other with application layer protocols, which must ensure accessibility of information for authorized users, reliability of the messages between a sender and a receiver, security of the data at any time. The communication of objects of the IoT an application layer is often attempted to interfere with during malicious scripts, social engineering, software vulnerabilities, phishing and sniffing attacks. This paper presents a systematic literature review of conference and journal articles on the topic of IoT security. The review has been undertaken to define IoT security at the application layer, identify the security requirements and analyze proposed security means solutions for their integration in multilayered architecture of IoT.

Keywords: Internet of Things, Data transmission, Multilayered architecture, Secure communication, Security means

1 Introduction

The surroundings of the smart devices and the internet have become a common daily phenomenon in our lives. In most areas of life and economy, the management and monitoring take place through the using of the internet as well as various digital devices interacting across the network. The data transmitted over the network not just through „human to human" or „human to computer" interactions but also through the sensors interacting with devices, which otherwise called of the internet objects [20]. This has formed the IoT, which is a new network configuration that includes the communication of physical objects and interaction of various objects with the internet.

Lupeikiene A., Matulevičius R., Vasilecas O. (eds.):
Baltic DB&IS 2018 Joint Proceedings of the Conference Forum and Doctoral Consortium.

The IoT is often referred to as the next stage of the evolution of the internet, where things become active participants of business, information, and social processes, who can communicate and interact with each other, as well as a smart environment surrounding them by exchanging data, reacting autonomously to the events of the physical world and influencing the environment by carrying out various activities and providing the smart services [28]. The benefits of smart environments and the IoT include comfort, security, optimal use of energy resources and many other services that greatly improve the quality of life. The possibilities of using the IoT are not limited just to providing services to people but allows to adopt technologies in the industry, trade, education, transport and even in the digital reality, where smart software agents communicate and make decisions [14].

The IoT understood as the global infrastructure, which is committed for the information society, providing modern services, connecting objects with the basis of already existing and developing information and communication technologies [24]. By identifying, collecting data, processing and using communication capabilities, the IoT allows the full use of objects for various services, ensuring high security and privacy requirements. The security is one of the core components of the smart environments of the IoT, as these environments interact with people and objects in the environment [10]. Smart environments designed for manufacturing, military, health and other very critical applications from a security point of view and it is necessary to protect these environments from dangers and external malicious effects. An important aspect of safety is privacy, which is defined as an indicator of the protection of human rights, establishing rules and limits, that prevent interference with a personal life, because smart environments and IoT technology become a part of the everyday and everywhere life of the future are directly threatened by the fact that these systems will be used for tracking and interfere in the private life [16].

The number of things connected to the internet is steadily increasing and it is predicted that by 2020, there will be about 16 billion interacting physical objects [27]. Such a scale of objects of the IoT closely connects the real-world with the digital information technology world, which is based on automatic identification, real-time location, sensors and controllers technologies [12]. The IoT resources and provided services are distributed across the information network, so it is necessary to develop a multilayered architecture with flexible interfaces, which would ensure the interoperability of resources, security, and reliability [4].

The aim of this paper is to overview and analyze security means at the application layer in the multilayered architecture of the IoT, which would allow secure communication of objects of the IoT in a smart environment, reliable data transmission and ensure lower consumption of energy resources.

The rest of the paper is organized as follows. Section 2 presents related works on the security issues and challenges in the IoT. Section 3 discusses the multilayered architecture of the IoT that indicating the basic security aspects, which must be implemented. Section 4 describes the most common security problems at the application layer of the architecture of the IoT and provides an overview of the security means and their applicability to the IoT multilayered architecture. Section 5 concludes the paper and provides a discussion on the further research.

2 A Multilayered Architecture of the IoT

The IoT should be capable of interconnecting millions or billions of the heterogeneous objects through the internet, so there is a critical need for a flexible, reliable and secure multilayered architecture [5]. The increasing number of the proposed IoT architectures has not yet converged to a reference model, but some global projects are constantly developing try to create a common architecture based on the analysis of the needs of the researchers and the industry [2]. The security strategies should be very carefully designed for managing the tradeoffs among the security, privacy, and utility to provide the security in a multilayered architecture of the IoT [3]. Fig. 1 illustrates a multilayered architecture of the IoT, which consist of objects, objects communication, service management, application and business layers.

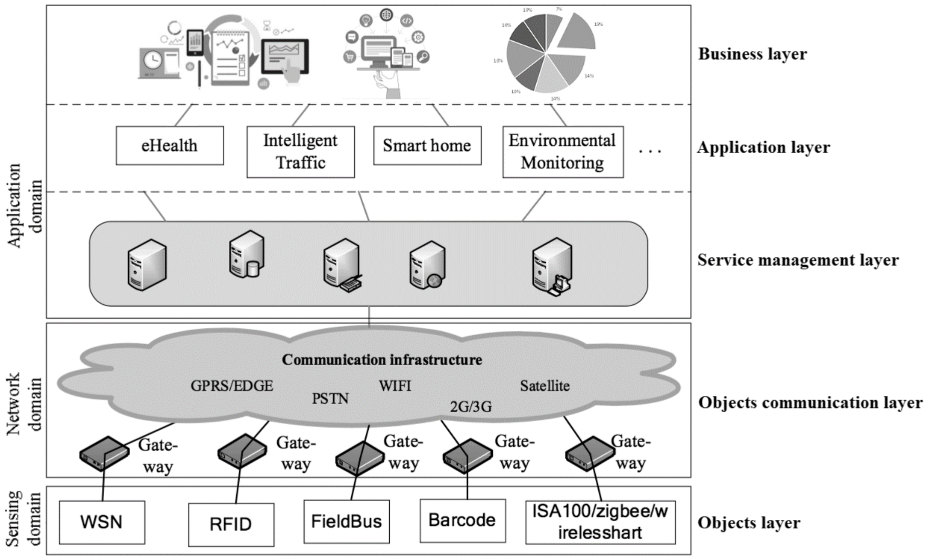

Fig. 1. A multilayered architecture of the IoT [18]

The objects layer is known as the perception layer, which collects all kinds of information through the physical equipment and identifies the physical world. This layer includes the sensors and actuators in order to perform different functionalities such as acceleration, humidity, location, proximity, temperature, vibration, etc. The miniaturization of hardware has enabled the powerful sensors due to producing in much smaller forms, which are integrated into the objects in the physical world. The sensors can be a barcode, embedded or infrared sensor depends upon the identification method of the objects. The collected and digitized information from sensors is passed to the object abstraction layer for its secure transmission to the processing system of information. Some common security problems in this layer are node capture, fake node, malicious data, timing, and reply attacks [7].

The objects communication layer is known as the network layer, which transmits the information produced by the objects layer to the service management layer through the secure channels. This layer is responsible for aggregating the information from existing sources and transmitting it to correct destinations. The transmission of information is based on networks like local area network (LAN), radio access network (RAN), wireless sensors network (WSN), etc. These networks can be in the form of a private, public or hybrid models and are built to support the objects communication requirements for latency, bandwidth or security. Some security problems in this layer are acknowledgment flooding, malicious code injection, unauthorized network access, denial of service, and man in the middle attacks [13].

The service management layer is known as the middleware layer, which pairs different types of services with its requester based on addresses and names. This layer is responsible for processing systems of information that take automated events based on the results of processed data and links system with a database, which provides storage capabilities to the collected data. The core set of services in this layer might include components, like an event processing service, integration services, analytics services, user interface services, security, and management services. This layer provides the secure connectivity between the sensors and application layer, processes the received data, makes the decisions and delivers the required services over the network wire protocols. Some security problems in this layer are identity masquerade, privacy threats, services abuse, replay, and routing attacks [8].

The application layer is known as the abstraction layer, which specifies the shared communications protocols and interface methods used by hosts in a communications network. This layer is responsible for interfacing the user’s applications with the network services or the operating system and allows applications to communicate with the protocol stack. The application layer uses different protocols such as advanced message queuing protocol (AMQP), simple object access protocol (SOAP) and extensible messaging and presence protocol (XMPP) [25]. This layer has the ability to recognize the malicious data, spam data, valid data and filters them at the right time. Some security problems in this layer are social engineering, software vulnerabilities, malicious scripts, phishing, and sniffing attacks [19].

The business layer is known as the management layer, which manages the system activities and services of the overall IoT. This layer is responsible for creating models, graphs, flowcharts based on the accurate and received data from the application level, as well as analyze, create, develop, evaluate and monitor elements related to the IoT. The real success of the IoT technology depends on the good business models and analysis results, so the business layer helps functional managers or executives to make accurate decisions for future roadmaps, actions, and strategies. This layer compares the output of each layer with the expected output to enhance services, maintain the user's privacy and support the decision making processes based on the analysis of the big data. Some security problems in this layer are data confidentiality, information security, privacy protection, flooding, and integrity attacks [11].

The IoT has the most significant architecture elements of the future internet, but applications and services are unsecured the most in the abstraction layer, so in order to protect against these issues, a security means, is needed at the application layer [30].

3 Related Work

Several researches have been led to deal with the security issues in the IoT. Most of these researches focus on the security attacks and threats of the IoT. A summary of the mentioned researches on the security issues in the IoT is provided in Table 1.

Table 1. Researches on the security issues in the IoT

References	Year	Security issues
[6]	2015	Evasion attack, insertion attack, side channel attack, spoofing attack
[17]	2014	Congestion attack, cloning attack, flooding attack, integrity attack
[22]	2013	Distributed denial of service attack, network attack, radio signal attack
[26]	2012	Counterfeit attack, malicious attack, meanwhile attack, phishing attack
[29]	2013	Exploit attack, node capture attack, replay attack, side channel attack

Glenn A. Fink et al. [6] discussed various kinds of vulnerabilities in the IoT and also societal effects such as standards, privacy, and security. The discussion on the security system, which is related to crime, cyber welfare, emergent behavior, scientific and technology challenges, social and regulatory challenges, was made. Various kinds of techniques were provided to mitigate these threats.

Gurpreet Singh Matharu et al. [17] described the general architecture and briefed several challenges in the IoT such as robustness in connectivity, interoperability, and standardization, naming and identity management, safety and security of objects, data confidentiality, and encryption. Security issues related to all the four layers of the IoT general architecture were discussed, analyzed and determined. Finally, the appropriate strategies for solving security issues were suggested.

Chen Qiang et al. [22] discussed the privacy protection, wireless communication, and information security. The existing researches on the network security technology were investigated. Based on that, a new IoT security method was provided. The difficulty in processing of the massive amount, the ensuring security and reliability of the IoT data were highlighted. The need to solve security issues and avoid a big security risk of the application of the IoT was stressed.

Hui Suo et al. [26] reviewed the researches of the IoT and discussed the security issues. The discussion on the security architecture, features, and requirements in each level of the IoT was made. The issues, which are related to the key agreement, identity authentication, cloud computing, authentication in the IoT layers namely perceptual layer, network layer, support layer, and application layer were discussed. Eventually, several key challenges in the IoT were summarized.

Kai Zhao et al. [29] discussed the security issues of the IoT three-layer system structure and offered some different solutions in each layer. The common attacks such as node capture, fake node, malicious data, replay attack and routing threats in object layer were elaborated. The cryptographic algorithms and key management techniques were deployed in order to solve these attacks. The compatibility and cluster security problems were resolved key agreement mechanism.

4 Security Means of the IoT at the Application Layer

At IoT application layer, there are not many security solutions, and most of them rely on the security means. The application level has to ensure the privacy, the confidentiality, and the secure storage of information in order to cover the individual privacy protection. A summary of the security means of the IoT at the application layer is provided in Table 2.

Table 2. Security means of the IoT at the application layer

References	Security issues	Security effects	Security means
[1]	Malicious script	System hijacking	Authentication
[9]	Phishing attack	User data leakage	Risk assessment
[15]	Sniffing attack	Data interception	Data security
[21]	Social Engineering	Illegal intervention	Access permissions
[23]	Software vulnerabilities	Buffer over flow	Awareness of security

The malicious script [1] is the kind of harmful computer code designed to create the system vulnerabilities, security breaches, the information and data theft. The application layer can be secured by authentication, which prevents the access to any miscreant users by integrated identity identifications.

The phishing attack [9] is an attempt to obtain the sensitive information such as usernames, passwords, money for malicious reasons. The application layer can be secured by a risk assessment that gives justification for the security strategies and provides improvements in the security of structure.

The sniffing attack [15] is theft or interception of data by capturing and analyzing traffic transmitted over the network using a sniffer application. The application layer can be secured by a data security that gives privacy of the overall system, protects any unauthorized access and prevent malicious activities.

The social engineering [21] refers to psychological manipulation of people into performing actions or divulging confidential information. The application layer can be secured by access permissions, which prevents and controls the ability of the attackers to view, change and execute contents of the file system.

The software vulnerabilities [23] are a weakness, which can be exploited by a threat actor to perform unauthorized actions within a computer system. The application layer can be secured by the awareness of security including maintenance system, best practices in deployment and development auditing.

5 Conclusion

This paper respectively expounds the IoT multilayered architecture problems and the security means at the application layer. The analysis of the security problems in different architecture layers demonstrate that there is no reliable protection in many IoT areas and resolve these existing issues research should be done. In future research is planned to make a detailed security analysis in multilayered architecture of the IoT.

References

1. Alaba, F. A., Othman, M., Hashem, I. A. T., Alotaibi, F.: Internet of Things security: A survey. International Journal of Network and Computer Applications 88, 2017, 10-28.
2. Baghli, R. B., Najm, E., Traverson, B.: Towards a multi-leveled architecture for the Internet of Things. In: Proceedings of the 20th IEEE International Enterprise Distributed Object Computing Workshop (EDOCW), Vienna, Austria, September 5-9, 2016, 182-187.
3. Basu, S. S., Tripathy, S., Chowdhury, A. R.: Design challenges and security issues in the Internet of Things. In: Proceedings of the IEEE Region 10 Symposium (TENSYMP), Ahmedabad, India, May 13-15, 2015, 90-93.
4. Benabdessalem, R., Hamdi, M., Kim, T. H.: A survey on security models, techniques, and tools for the Internet of Things. In: Proceedings of the 7th International Conference on Advanced Software Engineering and Its Applications (ASEA), Haikou, China, December 20-23, 2014, 44-48.
5. Fersi, G.: A distributed and Flexible Architecture for Internet of Things. In: Proceedings of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT), Tunisia, North Africa, October 5-7, 2015, 130-137.
6. Fink, G. A., Zarhitsky, D. V., Carroll, T. E., Farquhar, E. D.: Security and privacy grand challenges for the Internet of Things. In: Proceedings of the International Conference on Collaboration Technologies and Systems (CTS), Atlanta, GA, USA, June 1-5, 2015, 27-34.
7. Gomba, M., Nlwya, B.: Architecture and security considerations for Internet of Things. In: Proceedings of the 7th IEEE International Conference on Global Wireless Summit (GWS), Cape Town, South Africa, October 15-18, 2017, 252-256.
8. Hinai, S. A., Singh, A, V.: Internet of Things: Architecture, security challenges and solutions. In: Proceedings of the International Conference on Infocom Technologies and Unmanned Systems (ICTUS), Dubai, UAE, December 18-20, 2017, 197-201.
9. Hossain, M. M., Fotouhi, M., Hasan, R.: Towards an analysis of security issues, challenges, and open problems in the Internet of Things. In: Proceedings of the 11th IEEE World Congress on Services, New York, NY, USA, June 27-July 2, 2015, 21-28.
10. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., Qiu, D.: Security of the Internet of Things: Perspectives and Challenges, International Journal of Wireless Networks 20(8) (2014), 1-30.
11. Khan, R., Khan, S. U., Zaheer, R., Khan, S.: Future Internet: The Internet of Things architecture, possible applications and key challenges. In: Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, December 17-18, 2012, 257-260.
12. Kim, H., Wasicek, A., Mehne, B., Lee, E. A.: A secure network architecture for the Internet of Things based on local authorization entities. In: Proceedings of the 4th IEEE International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, August 22-24, 2016, 114-122.
13. Kraijak, S., Tuwanut, P.: A survey on Internet of Things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In: Proceedings of the 16th IEEE International Conference on Communication Technology (ICCT), Hangzhou, China, October 18-20, 2015, 26-31.
14. Leo, M., Battisti, F., Carli, M., Neri, A.: A federated architecture approach for Internet of Things security. In: Proceedings of the 53rd International Conference on Euro Med Telco (EMTC), Naples, Italy, November 12-14, 2014, 1-5.
15. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A Survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. International Journal of IEEE Internet of Things 4(5) (2017), 1125-1142.

16. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of Things (IoT) security: current status, challenges and prospective measures. In: Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, December 14-16, 2015, 336-341.
17. Matharu, G. S., Upadhyay, P., Chaudhary, L.: The Internet of Things: Challenges and security issues. In: Proceedings of the International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, December 8-9, 2014, 54-59.
18. Mynzhasova, A., Radojicic, C., Heinz, C., Kölsch, J., Grimm, C., Rico, J., Keith, D., Castro, R. G., Oravec, V.: Drivers, standards and platforms for the IoT: Towards a digital VICINITY. In: Proceedings of the International Conference on Intelligent Systems (IntelliSys), London, United Kingdom, September 7-8, 2017, 1-7.
19. Nastase, L.: Security in the Internet of Things: A survey on application layer protocols. In: Proceedings of the 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, May 29-31, 2017, 659-666.
20. Pal, S., Hitchens, M., Varadharajan, V.: Towards a secure access control architecture for the Internet of Things. In: Proceedings of the 42nd IEEE International Conference on Local Computer Networks (LCN), Singapore, October 9-12, 2017, 219-222.
21. Patra, L., Rao, U. P.: Internet of Things – architecture, applications, security and other major challenges. In: Proceedings of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), India, March 16-18, 2016, 1201-1206.
22. Qiang, C., Quan, G., Yu, B., Yang, L.: Research on security issues of the Internet of Things. International Journal of Future Communication and Networking 6(6) (2013), 1-10.
23. Ren, Z., Liu, X., Ye, R., Zhang, T.: Security and privacy on Internet of Things. In: Proceedings of the 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), Macau, China, July 21-23, 2017, 140-144.
24. Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., Coen-Porisini, A.: A secure and quality-aware prototypical architecture for the Internet of Things. International Journal of Information Systems 58 (2016), 43-55.
25. Solapure, S. S., Kenchannavar, H.: Internet of Things: A survey related to various recent architectures and platforms available. In: Proceedings of the 5th IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, September 21-24, 2016, 2296-2301.
26. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the Internet of Things: A review. In: Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, March 23-25, 2012, 648-651.
27. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikiras, P.: On the security and privacy of Internet of Things architectures and systems. In: Proceedings of the International Workshop on Secure Internet of Things (SIoT), Vienna, Austria, September 21-25, 2015, 49-57.
28. Xingmei, X., Jing, Z., He, W.: Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of Things. In: Proceedings of the 3rd International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, October 12-13, 2013, 825-828.
29. Zhao, K., Ge, L.: A survey on the Internet of Things Security. In: Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS), Leshan, China, December 14-15, 2013, 663-667.
30. Zhu, T., Dhelim, S., Zhou, Z., Yang, S., Ning, H.: An architecture for aggregating information from distributed data nodes for industrial Internet of Things. International Journal of Computers and Electrical Engineering 58 (2017), 337-349.