ECHAHID HAMMA LAKHDAR UNIVERSITY - EL-OUED
Under the Supervision of the DGRSDT and in collaboration with the CRTI
International Pluridisciplinary PhD Meeting (IPPM'20)
23-26, 2020 1st Edition, February
Theme: Modern Technology and Fineness Life

Adaptation of Data and Comminication Security Techniques in the Context of Internet of Things

Student: Melle. Kebache Romaissa
Thesis Director: Dr. Laouid Abdelkader MCA Univ Eloued
Co-director: Dr. ElMoatez Billah Nagoudi MCB Univ Eloued

Exact Sciences Faculty, Computer Sciences Department
Operator theory laboratory and its applications (LABTHOP)
El-Oued University, Algeria

Email: romaissa-kebache@univ-eloued.dz

Abstract

The Internet of Things (IoT) is one of the most discussed and tackled topics in the field of computer science research. Some of the researchers are also looking to the future of the world with this technology. Due to significant research and development that has taken place on the Internet of Things, various vulnerabilities have been observed that IoT should be kept as a technology subject. As a result, many attacks against the IoT were invented before its commercial implementation.

In this thesis project, we seek to study in-depth the existing security techniques. Indeed, traditional security mechanisms such as firewalls, intrusion detection, and prevention systems are deployed at the Internet level are used to protect the network from external attacks. Such mechanisms must be adapted to secure the Internet of the new generation. Many security techniques have been proposed in the literature, where an in-depth analysis must be initiated to adapt some of them in the context of the IoT. As soon as the objects can include simple sensors, medical devices, cars, planes, and even nuclear reactors and other objects which can pose risks to human life, the solutions proposed must respond in particular to the restrictions and constraints posed by this type of network.

Keywords: Internet of things, Protocols Adaptation, Data Protection, Secure communication.

Approach

Till nowadays, manufacturers are implementing and marketing IoT devices successfully without taking into consideration any kind of security precautions as a priority (e.g. fewer updates, default passwords, etc.). Besides, the enlargement of consumers' surface has created concerns about data privacy within society which is transferred through the IoT ecosystem (sensing layer, Network Layer, Data processing Layer, and Application layer).

IoT security is the technology area that is concerned with safeguarding connected devices and networks on the internet of things. While dealing with IoT devices, researchers mostly encounter challenges such as the Objects propagation, interoperability and limitations of IoT devices, and the development of cyber-attacks. Although few existing approaches (like Gurucul with machine learning techniques, PubNub Global Data Stream Network using publish/subscribe paradigm, Multi-Pronged Data Analysis, etc.) support security function integration, they are not fully adapted to the development of IoT data managers and communication protocols (Authentication, Integrity, availability problems).

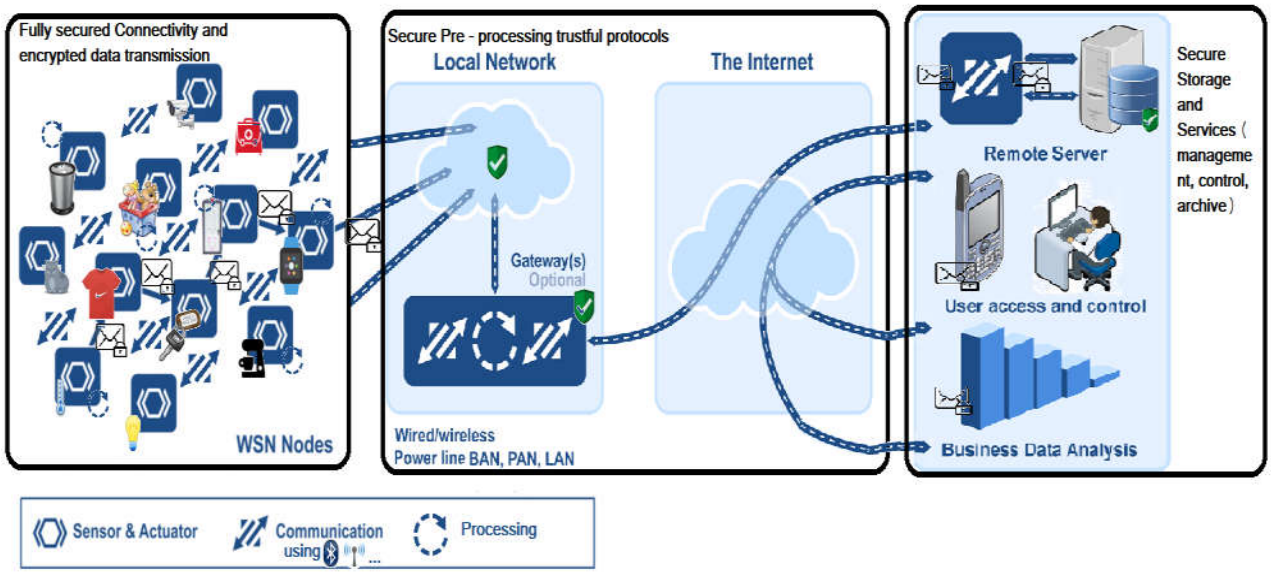
For that, this work aims at developing another approach that serves at securing the collected data and its transmission starting from the sensing phase that is more trustful and adaptive.

Obstacles encountered

The Adaption of existing data and communication security techniques in the IoT ecosystem reveals several obstacles such as:

- Objects are small, variant, heterogeneous, and connected in different environments.
- IoT devices are exposed to environmental influences (availability problems).
- Objects have poor calculation and memory and seen as constrained resources (microcontrollers) limited for crypto and authentication solutions.
- IoT devices are Autonomous and hard to be controlled.
- The surface of Cyber-attacks, hardware or software, has real-world consequences (e.g. a connected object controls a car, an alarm, connected system, etc.).
- The complexity of the security protocols and the software loaded in the IoT ecosystem.
- Development of a new generation of data storage and analysis (e.g. blockchain).
- Few special open source security tools for IoT are available.

General graphical Abstract



Preliminary Illustration for Secure IoT ecosystem

References

Benabdessalem, Raja, Mohamed Hamdi, and Tai-Hoon Kim. "A survey on security models, techniques, and tools for the internet of things." 2014 7th International Conference on Advanced Software Engineering and Its Applications. IEEE, 2014.

Chen, Dong, et al. "A novel secure architecture for the internet of things." 2011 Fifth International Conference on Genetic and Evolutionary Computing. IEEE, 2011.

Flauzac, Olivier, Carlos Javier Gonzalez Santamaría, and Florent Nolot. "New security architecture for IoT network." (2015).

Said, Omar. "Development of an innovative internet of things security system." International Journal of Computer Science Issues (IJCSI) 10.6 (2013): 155.

Yashiro, Takeshi, et al. "An Internet of Things (IoT) architecture for embedded appliances." 2013 IEEE Region 10 Humanitarian Technology Conference. IEEE, 2013.

Zhang, Congyingzi, and Robert Green. "Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network." Proceedings of the 18th Symposium on Communications & Networking. Society for Computer Simulation International, 2015.