Adaptive Security in Cloud and Edge Networks

New IoT Security Approach

Tewfiq El-Maliki, Nabil Abdennadher and Mohamed Nizar Bouchedakh
Information Technology department-hepia
University of Applied Sciences Western Switzerland
1202 Geneva - Switzerland
Email: {tewfiq.elmaliki, nabil.abdennadher, mohamed-nizar.bouchedakh}@hesge.ch

Abstract—Edge and cloud networks have emerged during the rapid evolution of networking in the last years, mainly as part of Internet of Things network. Security has become a key issue for any huge deployment in this network. Moreover, data reliability combined with performance is really a challenging task, particularly to maintain survivability of the network. This paper addresses this task using an Adaptation Security Framework, which is an efficient edge-cloud security deployment capable of trading-off between security and performance. It is based on an autonomic computing security looped system, which fine-tunes security means based on the monitoring of the context. An evaluation of the approach is undergoing in the context of smart city through a simulation tool and real-world large deployment.

Keywords **– Edge; Cloud; Framework; Autonomic; Security adaptation; Internet of Things (IoT).**

I. INTRODUCTION

Data Protection and trust are no longer just a compliance or security issue. They have become strategic topics since significant changes are introduced into the new European legislation. Indeed, it is highly challenging to maintain the overall security at the highest level due to the configuration complexity and the runtime changing context. The incoming edge computing as an adjacent network to the cloud creates many challenges, particularly in security field.

Accordingly, any concept that needs to cope with this new security challenge has to be based on overall performance aspects such as power consumption, this being a key issue in wireless networks, especially in sensor networks or the Internet of Things (IoT) [1]. It is imperative to address these problems from the earliest point of the system's design. All software development projects need a well-balanced amount of security awareness, right from the beginning [2].

In addition to the security challenge, data transfer in IoT is more susceptible to attack due to the nature of the edge nodes and the high error rate of wireless links. Therefore, the most crucial constraint in this network is reliability of any piece of information.

Trust mechanisms can solve these challenges. Indeed, they give a trust value about the behavior of an IoT device compared to standard behavior or similar IoT devices. By trust, we mean a particular level of a subjective opinion (Probability of a value - temperature, humidity, image etc. - to be accurate) with which an edge device will perform a particular action for many applications.

There is a rapidly growing literature on the theory and applications of trust systems. General surveys could be found easily and we suggest the survey of Josang [3], which is a reference in this field.

Moreover, IoT data sensing may be affected by deterioration of the hardware and environmental perturbations. However, we deploy multiple space located homogeneous sensors to provide redundant information to fix the uncertainty of sensing. This approach gives flexibility and cost-effectiveness to the deployment of IoT devices and deals with fault tolerance, random errors as well as the drift of the sensitivity or accuracy of the measurements of the IoT devices overtime [4]. Thereby, we do not need any heavy full security process to trust a single value obtained from an IoT device, as long as we have a lot of similar value extracted from cheap IoT devices spread over the entire environment. A spatio-temporal correlation could be used to rate the relevance of any value of a device to his neighbors' values.

Thanks to trust, we could build a solid general trust system to rate the accuracy, sensitivity and quality of wireless connection of any IoT device related to the provided data over time. Many trust models for wireless environment have been proposed, such one is described in [5] and the trust model for data described in [6].

In general, many applications can not operate under significant packet loss. Thus, reliability is one of the important criteria to evaluate the quality of wireless IoT networks. Thereof, the concept that must cope with this new security challenge has to be based on dynamic adaptation security system to satisfy an overall performance such as network reliability, being a key issue especially in sensor networks. We have already proposed a generic security adaptation framework as a compelling solution for such problems [7]. In this article, we will apply it to the IoT network by dividing our Security Adaptation Framework (ASF) into edge security part and cloud security part. The two parts will collaborate to optimize global security.

In this paper, we use security in a general sense including availability, reliability and survivability.

The rest of the paper is structured as follows. In Section 2, we give the motivation of our work. Section 3 introduces ASF for IoT and explains its components and functionalities.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-626-2

Section 4 concludes our paper and sketches the future work for validation and consolidation.

II. MOTIVATION FOR OUR FRAMEWORK

Edge or fog network aims to develop a new concept in networking, which stands on new context-aware sensors capabilities [8]. Sending and processing huge amounts of data to the cloud will not be "reasonable" due to latency and bandwidth limitation.

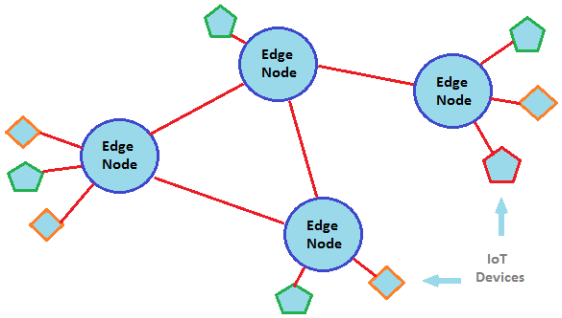

Figure 1. Edge node in IoT network

Edge computing could be the alternative. It will involve IoT connected devices capabilities in order to proceed locally rather than sending data to the cloud. Smart devices might be able to provide users' services and alleviate some latency issues. In figure 1, we see a typical edge network. The tendency is to use edge network as a distributed network. Edge computing covers a wide range of technologies including wireless sensor networks, mobile data acquisition, mobile signature analysis, cooperative distributed peer-to-peer ad-hoc networking and processing known as local cloud/fog computing and grid/mesh computing. It uses distributed data storage and retrieval system, autonomic self-healing networks, virtual cloudlets, remote cloud services, augmented reality, and more.

The approach is based on the principle of divide and conquer and it will guarantee the scalability by dividing the IoT universe into interconnected domains where a domain is associated to an edge node. This creates a sort of hierarchy that helps with the addressing and localization problems especially in dynamic networks with mobile devices.

The increasing complexity of communication in IoT applications makes the conventional static security almost obsolete, such as public key infrastructure. New mechanisms need to be set up in order to address this problem. One of the alternatives consists in using autonomic system techniques [9] to design adaptive security policy tailored to IoT applications.

Security in sensor networks [10] is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment. Individual sensor nodes in our case have inherent limitations in resources, which makes the design of security procedures more complicated. Each of these limitations is due in part to the two greatest constraints: limited energy and physical size.

Other security issues include security-energy assessment, data assurance, survivability, trust, end to end security, security support for data centric sensor networks and node compromise distribution. Due to a sensor network's special characteristics, it is very important to study areas such as: battery limitation, high failure probability nodes, easily compromised nodes, unreliable transmission media, etc. Mobility greatly exacerbates the problem. A lack of synergy between the cloud and edge security mechanisms is also noticed. Nowadays, there have been only a few approaches available, and more studies are needed in these areas [11]. On the other hand, trust is a good path to explore because it could give better results for some specific cases.

The best way to overcome these constraints is to implement a framework capable of adapting security to the "context" based on the ideas similar to those described in [12] and consequently having an overall security control. This idea is inspired by the concept of autonomic computing and an efficient Security Adaptation framework called SARM [7]. In this project, our new framework is called ASF (Figure 2).

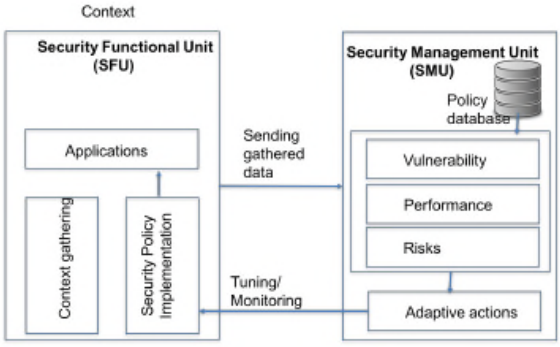

Figure 2. High level ASF approach.

The idea behind ASF is to adapt the security policy according to the context of the application. A security functional unit implements and executes the security policy, it gathers data related to the context and sends them to a security management unit. The security management unit can decide to update the security means in order to react to the new context.

III. ASF DESCRIPTION

A. ASF

We would like with ASF to fine-tune security means as best as possible taking into account the risk of the current application environment and the performance of the system especially regarding the optimization of its energy consumption. Thereby, our system differs from others by its [7]:

a) Autonomic computing security looped system

b) Dynamic and evolving security mechanisms related to context-monitoring

c) Explicit energy consumption management

The concept of isolating various functions and restricting their access to specific systems can also be applied to security in wireless environment integrated in the mobile

operating system itself. The best way to overcome the nonrealistic constraint of implementing the framework in each communication program is to integrate it in the kernel and consequently having an overall security control. Thus, all communication programs go through ASF at some stage in order to gain access to communication resources.

Information about ASF high-level components can be found in [5].

B. ASF for IoT

Having a centrally distributed (respectively cloud-edge) system helps deploy distributed IoT applications with central components deployed on cloud level and distributed components deployed on edge nodes.

For these reasons, we propose an autonomous and adaptive security system with two levels/scopes:

The first level consists of a “Local ASF" that manages security means locally on the edge node by using inputs coming from the local IoT environment (local IoT devices, gateways, etc). The role of the local ASF is to adapt the security means on the edge node to the local context changes with respect to a local security policy that implements general rules (e.g., energy saving, performance) and users’ preferences.

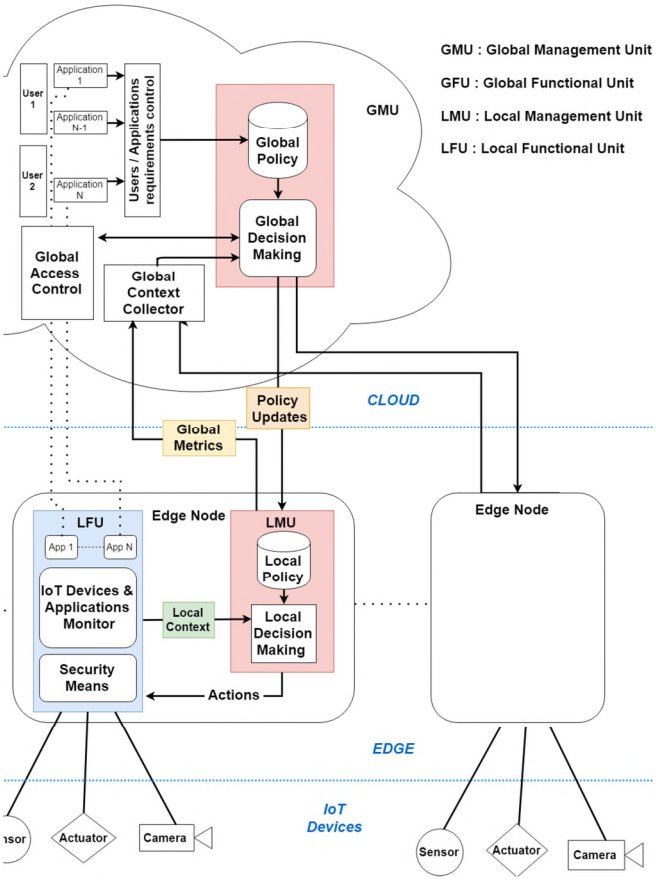

Figure 3. ASF for IoT network

The second level is a “Global ASF” on the cloud level that has a global view of the overall system (edge nodes, IoT devices and gateways). The global ASF’s role is (1) to control deployments of distributed application components on the edge nodes, (2) to update the local ASF policy with security updates or with new user’s preferences, (3) to adapt security means on the edge network level based on the global context gathered from different edge nodes and based on the global security policy.

Figure 3 represents with details the deployment of ASF for IoT network. It shows the separation cloud-edge and local-global units

This architecture guarantees a loose cooperation between local “edge” ASF and global “cloud” ASF. In fact, the global ASF is an enabler that helps the local ASF perform better but a local ASF could work just fine by itself. So, in case of a connection failure between the cloud and the edge node, as its name implies, a local ASF can run perfectly.

A promising approach is to use a trust and reputation based system to assess trustworthiness of IoT devices or edge devices. Our proposed solution uses trust estimation of IoT devices, on the edge nodes level, as one of the security means of the local ASF. We also use trust estimation of the edge nodes, on the cloud level, based on the trust and the reputation. This later concept (reputation) is an indicator that assesses a nodes trustworthiness based on the indirect trust a.k.a the recommendations of other nodes of the network. Reputation is usable on the global ASF’s level thanks to the interaction between edge nodes and the global view of the system.

C. Trust for IoT

When the IoT application is not critical and does not require individual authentication of the IoT devices, we can replace the “stringent” authentication/encryption method by a heuristic estimation of the “trust” we can assign to IoT devices. This method overcomes the limitation of the traditional security mechanism. In many cases, trust management is the key to building trustworthy and reliable IoT networks.

Trust evaluates the overall behavior of IoT devices. It is often calculated as follows:

a) receive data from the IoT device,

b) use a reference model (previously set-up) to “extract” information modeling the consistency of the received data,

c) use this information to calculate the trust of the IoT device.

The trust value assigned to a peace of data (received from a given IoT device) is used to make necessary “arrangements”: isolate the IoT device, fix the problem, etc.

Trust of an IoT device (or the data coming from a given IoT device) can be represented by a function of several parameters, which are related to:

a) the connection with the edge device: Example: in a wireless connection, one of the parameters is the Packet Error Rate (PER),

b) the correlations of the IoT device with “temporal” factors: Example: temperature is lower during the night and

higher during the day, the correlations of IoT devices with "spatial" factors: two neighbor sensors should provide similar measures.

Each of these parameters is weighted by a coefficient, which reflects its relevance. Thereby, the trust of a given device is represented by a function:

$$\text{TrustFunct(IoT-device)} = \alpha_0 * \pi_0 + ... + \alpha i * \pi i \quad (1)$$

where α_i are the coefficients and π_i are the parameters.

The coefficients may vary from one IoT application to another. This means that an IoT device has different values of trust for different IoT applications. Indeed, trust is a subjective value and each application has its own rating value depending on the end user security policy. Hence, TrustFunct should be written as follow:

$$\text{TrustFunct(IoT-device,IoT-App)} = \alpha_0 * \pi_0 + ... + \alpha i * \pi i \quad (2)$$

In equation (2), coefficients αi are related to the IoT application.

IoT devices having the same "features" (for example, measuring the same thing: temperature, humidity, pressure, etc.) must use the same Trust function for the same IoT application.

The objective of the "trust for data" mechanism is to develop a trust management system and deploy it on the cloud/edge device. This trust management system must set up the coefficients of the trust function (TrustFunct) for each IoT device. These coefficients are calculated according to a simplified version of the method presented in [6].

For each data value received from an IoT device, deduce the estimated values of the different parameters composing the Trust function (πi). These estimations are often based on machine learning methods and then calculate the trust value of the IoT device using (2).

This subsection introduces trust for data in a simplified way. In several research and industrial projects, trust computing is more complicated than presented here: it is done between edge devices and the cloud: machine learning (ML) models are generated by the cloud and sent to the edge devices. The edge devices receive data from the IoT devices, calculate the parameters of the trust function by using the ML models and send feedback to the cloud, which corrects the ML models and sends them back to the edge devices. As an illustration of this approach, the reader can view the Microsoft Azure solution [13].

D. Validation Application Domain: Smart City

To validate the model, we will apply an adapted version of ASF to the application domain of IoT – Smart City. In this domain, the trust value of IoT devices will be based on the solution described in the last subsection. The trust function (2) will be mainly based on four common parameters, accuracy, sensitivity, response time and packet error rate. According to the type of the IoT device, other specific parameters could be considered.

The common definitions of the four parameters listed in (2) will be:

Accuracy : accuracy of a sensor is the maximum difference existing between the actual value and the value received from the sensor,

Sensitivity: sensibility of a sensor is the minimum input of a physical parameter that creates a detectable output change,

Response time: the response time is the time required for a sensor output to change from its previous state to a final settled value,

PER: PER is the number of incorrectly received data packets divided by the total number of received packets. PER evaluates the quality of the transmission channel over time. It is used for evaluating the reliability of the transmission channel. This last parameter is extracted directly from the data link layer.

To calculate the three first parameters, we need two inputs:

a) data received from the IoT device and, "estimation" of the real value. This estimation is deduced from a predictive model based on machine learning,

b) machine Learning models runs on the edge devices. They are generated and updated in the cloud.

The trust (trust function) is calculated in the edge devices. It can be transferred to the cloud in order to have a global overview of the trust at the scale of the entire IoT platform.

Therefore, we would like to achieve global objectives:

a) keeping an appropriate level of security at edge level depending on the context ;

b) whilst maximizing the overall data reliability at the cloud level;

c) and controling the overall security .

IV. CONCLUSION AND FUTURE WORK

We have proposed a Security Adaptation Framework for IoT based on concomitant combination of edge and cloud ASF repartition. It uses an Autonomic Computing Security pattern to support both context monitor and behavior control. This paper explains the trust approach that will be used based on tempo-spatial correlation between sensors using machine learning. The validation will be in a context of smart city project.

Other strategies that could automatically optimize the trade-off between overall security and data trust will be explored.

REFERENCES

[1] F. Hamad, L. Smalov, and A. James, "Energy-aware Security in M-Commerce and the Internet of Things", IETE. 26: pp. 357-362, 2009.

[2] J. Chen, C. Hu, and H. Zeng, "A Novel Model for Evaluating Optimal Parameters of Security and Quality of Service" - Journal of Computers, VOL. 5, NO. 6, pp. 973-978, 2010.

[3] A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision", Decision Support Systems, 43(2), pp. 618-644, 2007.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-626-2

[4] E.Asmare and J. McCann, “Lightweight Sensing Uncertainty Metric – Incorporating Accuracy and Trust”, IEEE Sensors Journal, pp. 4264 – 4272, 2014.

[5] T. El-Maliki, “Security Adaptation in Highly Dynamic Wireless Networks”, Ph.D. thesis, 2014.

[6] R. Gwadera, M. Riahi, and K. Aberer “Pattern-wise trust assessment of sensor data”, 15th IEEE International Conference on Mobile Data Management IEEE MDM 2014.

[7] T. El Maliki and J-M Seigneur “Security Adaptation Based on Autonomic and Trust Systems for Ubiquitous mobile network and Green IT”, Ubicomm 2013.

[8] K. Bierzynski, A. Escobar and M. Eberl, “Cloud, fog and edge: Cooperation for the future?”, Second International Conference on Fog and Mobile Edge Computing (FMEC), 2017.

[9] M. Parashar and S. Hariri, “Autonomic Computing: An overview”, vol 3566, Springer, Berlin, Heidelberg 2005.

[10] T. El-Maliki and J.-M. Seigneur, “Security Adaptation Based on Autonomic and Trust Systems for Ubiquitous mobile network and Green”, The Seventh International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Portugal, UBICOMM, 2013.

[11] R. Roman, J. Lopez and M. Mambo, “Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges”, Future Generation Computer Systems, vol. 78, pp. 680-698, 2018.

[12] B. Badrinath, A. Fox, L Kleonrock, G. Popek, and M. Satyanarayanan, “A conceptual Framework for Network and Client Adaptation”, Mobile Networks and applications, v.5 n.4, Dec. 2000, pp. 221-231, 2000.

[13] https://azure.microsoft.com/en-us/services/machine-learning-studio/ [accessed April 2018]

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-626-2