Analysis Of Security Requirements In The Context Of Edge Computing

Fatma Hendaoui

Abstract— Billions of objects are being connected to the internet which makes the internet of things reality. Connected devices exchange a huge amount of data that should be processed with low latency. Cloud computing processes data on a centralized way which involves several issues such as technical issues and a single point of failure. Fog and edge computing may be considered as complementary to cloud computing. However, considering the heterogeneity of IoT objects and the large number of connected devices, data security is a must. This paper investigates the security challenges of edge computing and unveils a security model that presents the security requirements with respect to the IoT challenges.

Index Terms— Cloud Computing, Edge computing, Fog computing, Iot, Security

1 Introduction

The number of embedded devices communicating together and connected to the internet is increasing exponentially which makes the Internet of Things (IoT) a reality. IoT uses a variety of devices that deliver several services such as home automation, healthcare, smart cities, pollution control…With the developpement of connected devices, a huge amount of data is being exchanged. For instance, data processing is an open issue. Several research efforts investigated on the field of data processing. Cloud computing serves to store and to process data on a centralized way. Fog computing is located between cloud servers and the devices and it serves to manage data near to the devices. Edge computing brings processing close to the data source and it does not need to be sent to a remote cloud or other centralized systems for processing [1]. By this way, response time between the device and the service provider is being low. Indeed, in stead of sending data for centralized servers, edges near to the devices can accelerate the response time. For this purpose, data exchanged between edges and he devices is becoming more and more sensitive and diverse. It is possible to announce that decentralized edge and fog computing resolve the single point of failure and the availability issues. However, data exchanged between the devices and the edges remains sensitive and it needs to be secured in order to grant a robust computing service. Many research efforts ([2]-5]) have shown that edge computing security constitutes a challenge. This paper unveils new security requirements introduced by edge computing and presents a security model that can be extended for any IoT device.

This paper is organized as follow:

Section 2 details the difference between cloud, fog and edge computing and proposes a figure that models edge computing concept. Section 3 outlines different characteristics of the edges and devices that compose the edge computing. Section 4 presents the security requirements that edge computing introduces and presents a unified security model. Section 5 concludes the paper and outlines the perspectives.

- ***Fatma Hendaoui,***
  Assistant professor, University of Ha'il, Community College
  Email: fatma.hendaoui@yahoo.fr

2 Architecture of Edge Computing

Near field Communication (NFC) and Wireless Sensor and Actuator Networks (WSAN) together with RFID are recognized as the atomic components that will link the real world with the digital world [6]. For instance, the interconnection of physical objects with sensing and communication components such as sensors or actuators is not new. The novelty remains on the integration of Internet protocol (IP) connections that guarantee the interconnection of the devices via the Internet. For example, the 6LowPAN standard, defined by IETF [7], allows the transmission of IPv6 packets through computationally restricted networks [8]. Subsequently, it is possible to announce that the internet of *Things is almost composed of billions of tiny devices interconnected together in order to deliver the required services. Figure 1 shows the general architecture of the IoT.

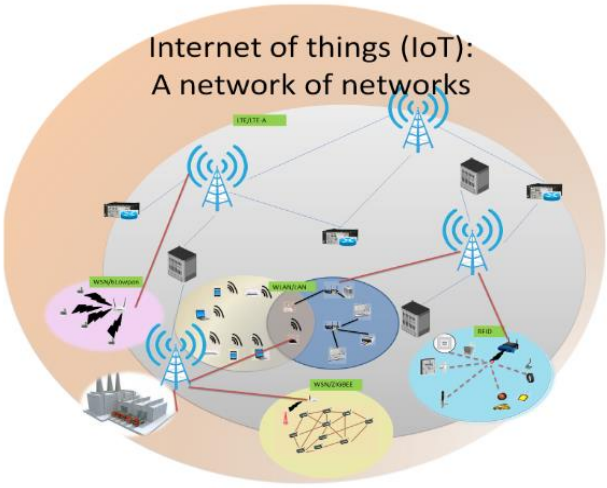

Figure1: Architecture of the IoT

As depicted in Figure 1, the IoT incorporates heterogeneous devices where RFID tags can be considered as the most restricted devices. As an example, a RFID tag carries no more than 2 kilobytes of memory. Same, sensor networks are among the basic components of the IoT. Sensor devices are also restricted in terms of hardware resources. Sensor node with Atmega128L processor possesses 4 kilobyte of EEPROM memory. In this context, data computing is becoming a challenge in the IoT. To compute a huge amount of data delivered by IoT smart devices, cloud computing was first introduced. In this concept, a 'vertical' communication between

the end devices and the central servers is produced. Central servers process data and deliver services to the end users. A number of issues regarding cloud computing were introduced. Those issues incorporate compatibility compliance of the cloud, standardizing cloud technology, monitoring while in the cloud security ([9], [10]). Even cloud servers are protected with various security strategies, centralizing the traffic around some designated servers introduces several security issues such as traffic analysis, the single point of failure and the high latency.
Coming back to the deficiency criterion of the tiny devices, it is almost not possible to directly communicate with the central cloud servers. In this context, fog computing comes as an intermediate between cloud servers and physical devices. Fog computing provides distributed computing, storage, control and networking closer to the user ([11], [12]). Fog computing bridges the gap between the cloud and the devices (IoT nodes) by enabling computing, storage networking and management on network nodes within the close vicinity of IoT devices [13]. Subsequently, using fog computing, data aggregation of GPS data may be accomplished by the edges near devices before sending them to the cloud servers. Intelligent transpiration systems [14] are involved to aggregate data before being sent to the cloud server. When talking about fog computing, unlike cloud computing, "horizontal" system level architecture between end devices is introduced. While fog nodes are closer to the end devices than cloud servers, fog computing outcomes the low latency issue by delivering the service with satisfactory latency. However, fog computing stills introducing several issues such as the heterogeneity of the end devices and the cloud providers. This means that the fog needs control interfaces as well as appropriate data interfaces to enable interoperability at the level of service providers and fog platform modules [15]. Same the single point of failure issue remains. Fog devices are susceptible to faults and errors which make it 1 fail stop processor. This means that the fault of the fog may lead to the non deliverance of the service. Edge computing is relatively junior paradigm in which the computing happens at the edges near to the end devices. Edge computing allows data to be processed at the network edge without being sent to the cloud or to the fog servers. This paradigm is going to reduce the latency delay and the communication cost. Unlike cloud computing, edge paradigm introduces several advantages such as the low latency delay, the availability of the edges. Edge computing is k-fail stop processor where k refers to billions of connected devices. Same, in modern IoT, embedded chips have became cheaper and more widely adopted [16]. For instance, it is possible to localize computing at nodes level which ensures less resources utilization such as communication and storage resources. However, several issues remain unresolved with edge computing. First, due to the heterogeneity of the end devices and the systems, edges face the interoperability issue. Second, IoT devices are resources deficient which means that edge computing introduces resource optimization issue. Third, due to the resource deficiency challenge, edges are vulnerable to the big variety of attacks. In this context, security and privacy constitute a challenge for the edge computing. Figure 2 models the architecture of cloud, fog and edge computing.

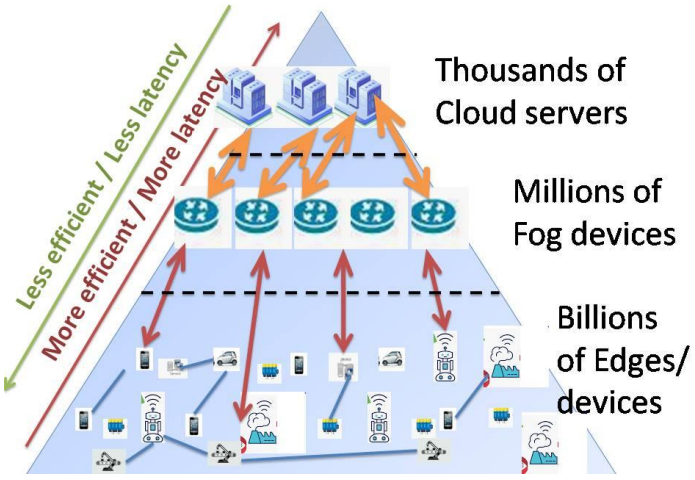

Figure2: Cloud, fog and edge computing structure

3 EDGE COMPUTI NG CHALLENGES AND REQUIREMENTS

Edges devices are almost resource deficient. Data processing in the edges is different than which of fog and cloud servers. For instance, in the cloud and fog servers, data is produced by more resourceful devices. This is not the case of the edges where things are the main data producers and consumers. Summarizing the most challenge of edge computing is the deficiency of the devices.

Table 1 *presents the resources capabilities of some smart IoT devices including sensors, tags and other home automation devices.*

Device	Processor	Memory	Radio range	Voltage
Telosb (Sensor)	8Mhz TiMsp 430	10KB RAM	125 m	3v/1.8 mA
Micaz (Sensor)	2.4Ghz MPR2400 Atmega128L	4KB EEPROM	75 to 100 m	3v/8 mA
IT70 (RFID/NFC tag)	860 Mhz to 928 Mhz	1280 bits to 1792 bits	10m	
A9 (smart home gateway)	1Ghz	1Gbyte	Wire connection	12v/ 2.5A

TABLE1: CHARACTERISTICS OF SOME IOT DEVICES

For Telosb motes, the time of 1 clock cycle is presented by (1).

$$\boldsymbol{C = \frac{1}{F} = \frac{1}{8Mhz} = 0.125\mu S} \quad (1)$$

'C' refers to the clock cycle while F refers to the frequency of the microprocessor.
This means that each clock cycle the sensor looses around 0.7 nanojoules (2).

$$\text{Energy cost (1 clock cyle)} = 1.8\text{mA} * 0.125\mu\text{s} * 3\text{v} = 0.675 \text{ nano joules} \quad (2)$$

While AA batteries have around 12.6 joules, Telosb has 2AA batteries (around 25.92 joules). This means that Telosb batteries support around 38.4 10^9 clock cycle.

Summarizing, processing cost is a major concern for low powered devices.

Table 2 outlines the issues of Edge computing based on restricted IoT devices.

Issue	Description
Deficiency	Most of the edges are restricted in terms of: • Processing • Energy • Storage • Communication
Distributed environment	The devices collaborate in a distributed way. For this purpose, nodes synchronization is an issue for the edges
Expansion	The network devices increase in an exponential way which makes data control hard.
Heterogeneity	The operating systems of the devices and their characteristics are heterogeneous
Vulnerability	As most of the devices are deficient, edges are vulnerable to several kinds of attacks
Lossy environment	Edges communicate via radio channel which makes packet loss probability frequent
Nodes mobility	Edges change their positions frequently which makes human surveillance impossible

TABLE2: ISSUES OF EDGE COMPUTATION

4 Security model for edge computing

Considering the edges characteristics investigated in Section 3, proposing a security model for edge computation should respect the issues of edge computing. Same, the proposed model has to provide tradeoff between the edges characteristics and the robustness criteria. Md.Hossain et al. [17] have classified the security requirements into three categories based on the information security requirements, the access level security requirements and the functional security requirements. Identification requirement: the aim of this requirement is to ensure the identity of the external actors that are not included to the designated network.

- Information security requirement: this requirement includes five different requirements:
  - Integrity: Even if the confidentiality of the data is assured, the attacker can modify the content of the messages without knowing their contents. The integrity of the data ensures that the packets have not been altered during their exchange in the network. In other words, data integrity ensures data protection against destruction, duplication, insertion, modification, rejection and replay.
  - Information protection: In this requirement a node of the network should not forward information to its neighbors unless it is configured to do so.
  - Anonymity: This requirement is needed to guarantee data confidentiality and privacy. It aims to hide the identity of the data source.
  - Non-repudiation: This requirement ensures that the device is not able to deny the emission or the modification of the data.
  - Freshness: Data freshness avoids the opponent replaying old data. This requirement may be achieved via nonces or sequence numbers.
- Data Confidentiality: It keeps the data protected (secret). Confidentiality concerns ordinary data (sensitive information that must not be disclosed) and security information (cryptographic keys, nodes identities). Data confidentiality is accomplished by applying an encryption task. Encryption is a mathematical operation applied to a message M, via a cryptographic key k, to have an encrypted message C. Encryption can be symmetric or asymmetric in function of the encryption keys.
- Access level security requirement: this requirement is basically composed of :
  - Authentication: It ensures that all communicating entities are those claimed to be. This requirement aims at verifying the validity of both the data origin and the entity.
  - Authorization: It aims at guaranteeing that only authorized devices access to the network data and services.
  - Access control: Even a node of the network is authentic, it won't be able to access to things it is not authorized to.
- Functional security requirement: It is composed of four different requirements:
  - Exception handling (Fault Tolerance): This requirement ensures the robustness of the IoT network even in hazardous situations such as the infection of some designated nodes, hardware problems...
  - Availability: The IoT network should be able to serve nodes with the required service even in the presence of a denial of service attack or a failure due to hardware problems. It means that it is possible to access and to modify data by authorized entities whenever it is wanted.
  - Resiliency (Immunity Requirement): Even one or several attacks are present in the network, other non compromised nodes should still protected.
  - Self organization (Self-Healing):Each node is enough flexible and independent so that it may guarantee the continuation of the secured service even some nodes are altered.
- Intrusion Detection: The presence of attacks should be detected and altered nodes should be removed.
- Key Management [18]: Aims at managing the generation, the distribution, the storage and the update of the keys so that it is not possible for unauthorized nodes to participate on the key management task.
- Secure localization: Securely gather information about the node location in the network. Unauthorized nodes are not granted to access to the localization information of the network devices.
- Time synchronization: Time synchronization aims at providing a common time scale for local nodes' clocks.

The above requirements are all based on cryptographic keys. For instance, to ensure data confidentiality the sender should encrypt data with a symmetric or an asymmetric key. The receiver deciphers the encrypted data to obtain the clear text. Data authentication, integrity and non repudiation are achieved via keys and digital signatures.

Also, Access control, Audit and Availability are supporting services for cryptography and key management [19].

For this purpose, it is important to take into consideration the deficiency and other issues of edge computing while designing the security model.

Table 3 *provides an exhaustive detail of the security requirements and their relation with the edge computing issues.*

Edge computing issue	Security requirement	Security solution	Description
Single point of failure	Availability	Distributed security proposal	Each of the security requirements illustrated above should be based on a distributed solution and it should avoid centralization of the traffic around some designated nodes
Nodes deficiency	• Reliabiliy • Availability • Safety • Security	Efficiency	The propsed solution has to provide tradeoff between the efficiency and the robustness criteria
Distributed environment	Synchronization independence	Clocks synchroniza tion	The security proposal should use synchronization tools such as nonces and timestamps in order to avoid replay attacks
Nodes expansion	Scalability	Low costs	The proposal should not introduce high processing, storage and communication costs. Same, the costs should be independent from the number of devices
Heterogeneit y	Interoperability	A unified security platform	The proposal should be applicable for the different systems and characteristic of the edges
Lossy environments	Robustness to packet losses	Independen ce to packet losses	The proposed security model should send independent security packets.
			As an example, it should not use signature amortization solutions
Nodes mobility	Mobility support	Anonimity	The proposal security solution has to be independent from any human intervention. Same, it should be available even edges change their positions
Vulnerability	Resilience	Attacks resistance and intrusion detection systems	The proposed solution should respect the big possibility of attacks injection and it should use some intrusion detection systems to detect any attacks.

TABLE 3: SECURITY MODEL FOR EDGE COMPUTING

5 CONCLUSION

Edge computing introduces several issues when focusing on the special characteristics of the edges devices. The deficiency is the main issue of edge devices which make them an easy target for the attacks. For this purpose, security is a major concern in the context of edge computing. Designing a security solution for edge computing should respect the special requirements of the edges. This paper investigated the issues and requirements of edge computing and it unveils a security model that respects the different issues of edge computing. In the sequel, when designing a proposal, it is important to provide a solution that respects the tradeoff between the robustness and the efficiency criteria.

REFERENCES

[1] D. Linthicum , Edge computing vs. fog computing: Definitions and enterprise uses, Cisco Digital Network Architecture (Cisco DNA)

[2] S.Khan, S.Parkinson, Y. Qin,, Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing, 6(1), 2017 doi:10.1186/s13677-017-0090-3

[3] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016. doi: 10.1109/JIOT.2016.2579198

[4] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick and D. S. Nikolopoulos, "Challenges and Opportunities in Edge Computing," 2016 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, 2016, pp. 20-26.doi: 10.1109/SmartCloud.2016.18

[5] S. N. Shirazi, A. Gouglidis, A. Farshad and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586-2595,Nov.2017.doi: 10.1109/JSAC.2017.2760478

[6] International Organization for standardization,

information technology - security techniques - entity authentication mechanisms; part 1: General model, tech. report, ISO/IEC 9798-1, Second Edition, 1991.

[7] G.Montenegro, N.Kushalnagar, J.Hui, and D~Culler, Transmission of ipv6 packets over ieee 802.15.4 networks, network working group request for comments: 4944, tech. report, 2007.

[8] An enterprise guide to understanding key management}, tech.report,https://www.ciosummits.com/Gemalto$_$AnEnterpriseGuidetoKeyManagment$_$White$_$Paper.pdf.

[9] J.R.Ghayatreenee, Dr.S.Vijayalakshmi, A Study on Cloud Computing and Hybrid Cloud, Our Heritage, Vol 68, Issue 19, January 2020

[10] R. Khurana, G.Himanshu, A Hybrid Model on Cloud Security 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO),Volume.16,pp:347-352,,2016

[11] M. De Donno, K.Tange, N.Dragoni, Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog, IEEE Access, 1–12019, doi:10.1109/access.2019.2947652

[12] M. Chiang, S. Ha, C.-L. I, F. Risso, and T. Zhang, "Clarifying fog computing and networking: 10 questions and answers," IEEE Commun. Mag., vol. 55, no. 4, pp. 18–20, Apr. 2017.

[13] A.Yousefpour, C.Fung, T. Nguyen, K. Kadiyala, F.Jalali, A. Niakanlahiji, J.P.Jue, All One Needs to Know about Fog Computing and Related Edge Computing Paradigms, Journal of Systems Architecture, Volume 98, September 2019, Pages 289-330,

[14] J. Acharya, S. Gaur**Edge compression of gps data for mobile iot,** 2017 IEEE Fog World Congress (FWC), IEEE (2017), pp. 1-6,

[15] L. Chenlei, F. Xiang, P. Wang, Z. Sun, A review of issues and challenges in fog computing environment, 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress, 2019, pp.232-237

[16] W. Yu et al., "A Survey on the Edge Computing for the Internet of Things," in IEEE Access, vol. 6, pp. 6900-6919, 2018.doi: 10.1109/ACCESS.2017.2778504

[17] M. Hossain, M. Fotouhi, and R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in 2015 IEEE World Congress on Services, New York, NY, USA, 2015, IEEE, pp. 21–28.

[18] European telecommunications standards institute technical report, security techniques advisory group (stag) baseline security standards; features and mechanisms,tech.report,http://www.etsi.org/deliver/etsi$_$etr/200$_$299/237/01$_$60/etr$_$237e01p.pdf, 1996.

[19] An enterprise guide to understanding key management, tech.report,https://www.ciosummits.com/Gemalto$_$AnEnterpriseGuidetoKeyManagment$_$White$_$Paper.pdf.