Fog Computing: Modeling the future of smart cities

Costel CIUCHI
Assoc. Prof., Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania,

costel.ciuchi@upb.ro

Gabriel PIRLOGEANU
Student, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania,

gabriel.pirlogeanu@stud.etti.upb.ro

Gabi CROSMAN
Student, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania,

gabriel.crosman@stud.acs.upb.ro

Abstract

IoT is one of the most impactful technologies in recent years and is the cornerstone of Smart Cities. IoT solutions benefit from Cloud Computing services through scalability, performance and through data sent from millions of interconnected devices and sensors in a city. To mitigate risks, secure architectures have been developed in recent years, but a major issue identified using Cloud technology is the concentration of large amounts of sensitive data and the large number of security solutions that need to be managed. Regarding this, a new emerging technology, Fog Computing, is presenting many solutions to solve some of the limitations of the Cloud by bringing the processing of data closer to the edge.

A Fog Computing model not only offers low latency transmission, power efficiency and great bandwith, but also makes vulnerable edge devices and sensors more secure. The aim and objective of the article is to present a Fog Computing model with 2 main directions in developing this concept: data-as-a-service (DaaS) and security-as-a-service (SaaS) and an analysis of the security improvements that Fog Computing can bring to an IoT network (Fog

Computing over Cloud Computing). Fog Computing and its impact on IoT technologies is a new research topic regarding the performance and resilience of a smart city. But there are also cyber security concerns, such as the threat of cyber attacks (DDoS, hijacking, APTs, etc) and risks related to the safety of sensitive data transiting IoT networks. The paper was constructed on secondary research published by companies, researchers and public institutions.

Smart Security is a crucial concern for a Smart City's infrastructure and to the privacy of its citizens. Fog Computing can solve some of Cloud Computing's security limitations and can make major improvements in the reliability and resilience of security systems, but also in the efficiency of data processing and secure assets capabilities.

Keywords: *smart security, edge computing, IoT, smart data, cyber security.*

1. Introduction

IoT is the technology that allowed the concept of Smart Cities to take shape and develop more and more throughout the years, taking new and diverse challenges, on different layers. It isn't surprising that the revolutionary invention of Internet would lead someday to a world of interconnected devices that communicate data in real time with each other. Becoming popular around the year 2011, IoT implementation in the development strategies of cities opened a door to a world of infinite possibilities, imagination being probably the biggest challenge facing IoT engineers, but also governments and businesses. The advantages that IoT offers, such as managing and monitoring many activities in the same time made people realize the huge financial benefits of implementing such technologies in a city, being able to save time and human resources, but also gain new insights from the data gathered for future planning on tasks such as: traffic management, pollution reduction, improving infrastructure and keeping citizens safe.

Even if the technology started being widely implemented recently, the technology and concept aren't new to us. The term *Internet of Things* was coined by Kevin Ashton in 1999 and the idea of devices connected and controlled over the Internet has already took shape in the 1980s [1]. The IoT industry keeps growing and the industry's global worth is considered to be more than 200 Billion U.S. dollars and there are more than 50 billion IoT devices in the world [2]. The idea that any physical object can be transformed into an IoT device, the continuous fall in the price of adding sensors and an internet connection to devices and the need for an interconnected world will keep the IoT industry's exponential growth.

IoT networks are comprised of millions of interconnected devices with sensors and actuators, that constantly send vast amounts of data. The „cloud" is responsible with processing, analyzing and storing data sent by IoT devices and is an inalienable piece in the architecture of an IoT network due to several advantages such as interoperability, scalability, processing and storage power. Yet, in recent years, people realized that cloud computing has several limitations when it comes to cyber attacks, speed, reliability on internet, downtime issues, etc. The term "fog computing" was coined by Cisco and is in reference to an extension of cloud computing to the edge of the network. By bringing the functionalities of the cloud closer to the edge, fog computing redefines the architecture of the IoT network, creating opportunities for new technologies to be effectively implemented and improving the overall sustainability and security of the network through low latency, high response time, decentralization or location awareness.

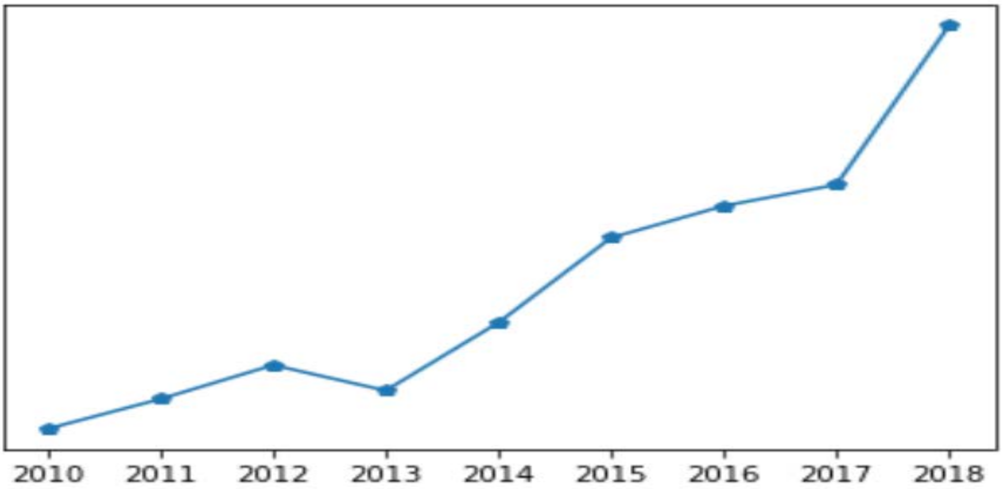

Fig. 1. Trend of vulnerabilities affecting manufacturing-related equipment reported to the industrial Control System Computer Emergency Response Team (ICS-CERT)
Source: [3]

Fundamentally, every new device added to an IoT ecosystem adds a new attack surface or opportunity for malicious attacks. Taking in consideration that an IoT network can be targeted by many attackers in different layers of its architecture and the fact that IoT is the backbone of a Smart City, it is important to consider Smart Security a crucial part in the development plan. Vast amounts of sensitive data are transmitted non-stop in the network, the privacy of the users and security of the data should be the main concerns of a Smart City. The IoT network must be trustworthy in face of different attacks, such as: APTs (advanced persistent threats), data and identity theft, device hijacking, DDoS attacks, Credential theft, etc. If we consider that a cyber attack can disrupt a whole industry and threaten the safety and privacy of citizens, we realize that Smart Security is one of the most important aspects when it comes to the reliability and survival of the Smart Cities' concept in the future.

2. Cloud computing

The "heart" of the IoT network is composed of all the sensors, actuators and identification technologies, such as RFID and Wireless Sensor Networks, used in IoT devices to gather and transmit data through the network. The network is similar to the blood vessels in the human body and it's responsible for the fast, efficient and secure transmission of data [4]. The “brain” of the IoT architecture is the place where we can store, process and analyze all the data sent by the end devices effectively, at the moment Cloud Computing being the most popular technology. The computing is the most important aspect of an IoT network, the cloud being able to identify the useful information contained in the data sent by the millions of sensors interconnected in the network, store the information and share it over the cloud platform between a number of interconnected servers. Cloud Computing has many advantages that go hand in hand with the nature of IoT networks being centralized, easily scalable, cheap and offering a vast amount of services.

Cloud computing architecture can be broken down in three cloud computing layers/models: Infrastructure-as-a-Service that “provides infrastructure like unlimited storage and computing power for developers without requiring any physical hardware on site”, Platform-as-a-Service that “includes resources like operating system, programming language, database, web server that automatically scales to meet the application demands” and lastly Software-as-a-Service which is the “top layer and most basic form of cloud computing, where the software and associated data are deployed and hosted on the internet which is accessed by the user via a web browser” [5]. This makes Cloud Computing very flexible, being able to be used in more or less complex applications by users.

Taking in consideration the immense size of the IoT architecture and the vast amounts of data that must pe processed, Cloud computing is a service that allows companies and users to avoid the cost and complexity of owning and maintaining their own IT infrastructure, by having access to storage, networking or processing power offered by the cloud service provider. The concept of cloud refers to the idea that the location of the service and other details such as hardware or software behind it are mostly irrelevant to the user, the cloud being able to manage the storage, networking and processing tasks demanded by the IoT network.

Cloud Computing provides huge cost savings for small and large companies when it comes to certain IT infrastructure requirements. The Cloud offers storage capabilities and computing capabilities to all the information sent by the different connected machines that are communicating, with easy implementation and no hardware required. The cloud can process data fast and assist decision support functions for the networking architecture, in this way time wasted on redundant data and other unexpected events can be reduced[6]. The stored data can be easily accessed, through cloud services, and has built in recovery capabilities. This makes an IoT architecture using Cloud Computing a centralized architecture, sending the data and processing of data away from the user and abandoning most of the front-end heavy processing.

Another big advantage of the Cloud is the pay-as-you-go nature. In the context of IoT networks where more and more data are sent to the cloud as number of devices increases, this payment method for cloud charges based on the data usage, offering more control over the costs of a certain project and scalability.

With all the above in mind, some of the biggest advantages of Cloud Computing present great risks and limitation. With different companies providing different services and devices for an IoT network, there is a need for standardized interfaces and standardized APIs for cloud services. SaaS applications suffer the most from this challenge of switching between applications, sometimes involving a change in the interface [7].

Another problem for Cloud Computing represents its dependency on internet connection, need high bandwidth to be performant, the risk of technical outages, limited control over business assets because of remote servers and vendor relationship management. Besides all of these technical disadvantages, cloud computing is vulnerable to cyber attacks too. The cloud handles big amounts of sensitive information about people, companies or government, so it becomes a target for hackers. From concerns such as the risk of data confidentiality (other people may have access to the data) to APTs, device hijacking, credential theft, etc.

Even if developers have come with many solutions such as encrypting the data, a strong security platform and a multi-environment support, the technology of the cloud is not enough unfortunately to efficiently fight all the attacks because the distance from the end device and centralized nature of the cloud makes the network vulnerable to attacks on different layers and connection devices, the difficult mitigation of SaaS and IaaS application, the fact that data from millions of devices is processed in a single area of the network makes it easier to target a wider area of network attack.

3. Fog computing

In response to the challenges faced by the Cloud Computing technology, a new concept named Edge Computing emerged, trying to solve some of the performance and security limitations of the cloud architecture. Edge computing is a concept that refers to moving the computation power of an IoT network to the edge of the architecture, directly on the device. The key difference between cloud and edge computing is the location in the network where data is processed, analyzed and stored. Fog computing is the standard that defines how edge computing should work. It uses the edge computing activities to the processors that are connected to the LAN making it a little farther from the sensors and actuators.

“Fog computing is generally considered as a non-trivial extension of cloud computing from the core network to the edge network” [8] and can also be considered the real implementation of the Edge computing technology. Following the trend of bringing computation closer to the edge of the network and making it decentralized, fog computing can definitely solve and improve on some of the limitation of cloud computing while giving up on some other functionalities such as access on spot to big datasets, interconnectivity between servers and user authorization. Fog computing can be found in the IoT architecture between the end device and cloud, bringing the services closer to the device than the cloud.

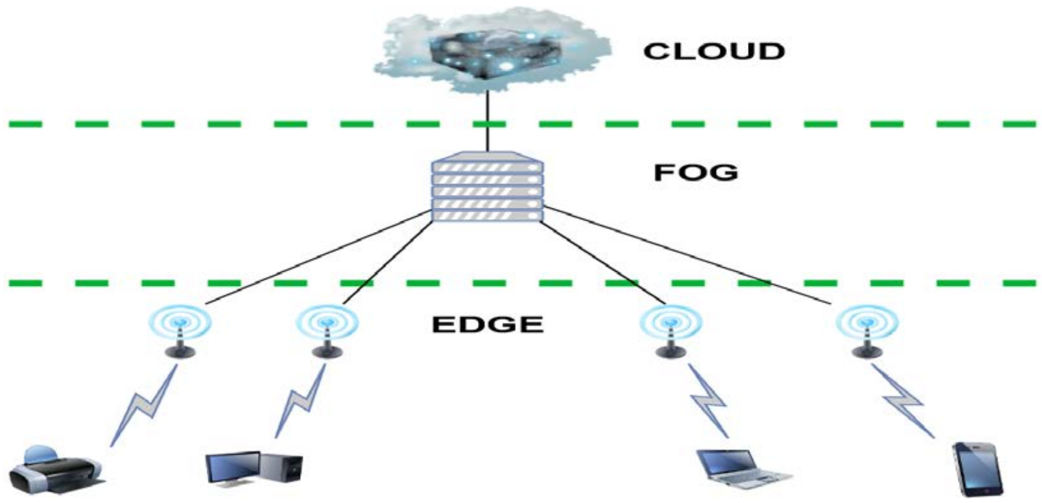

Fig. 2. Relationship between cloud and fog computing

Fog computing has a big range of applications and comes with a very large contribution in the development of smart cities. Most important examples are Smart Vehicles (with light scheduling, congestion mitigation, parking facility management), Health Data Management (patients can take possession of their own health data locally, reducing the risks of GDPR violation), Smart Grid. The smart grid is an electricity distribution network based on smart meters that measures the real-time status information. That information is centralized by a server called SCADA which sends commands to respond to any demand change or emergency to stabilize the power grid. Fog computing can make from SCADA a “decentralized model with micro-grids with a better cost, scalability, security, which can also integrate power generators with main power grid.”[8]

In terms of performance, fog computing is superior to cloud computing when it comes to low latency and high response times, thanks to the wide spread topology of the network. Also, the decentralized nature of the fog lowers the bandwidth requirements, as some of the requests are solved close to the edge, while the more demanding ones are sent to the cloud. The decentralization and distribution also make it better in terms of mobility, taking in consideration the inexpensive, flexible and portable deployment in terms of both hardware and software and are able to process data from a diverse set of devices.

Fog computing provides location awareness in comparison with cloud computing where everything is based on Internet and the location of the servers is unknown, this resulting in better supporting capabilities for the large number of servers in the network.

The fact that data is analyzed and stored in the local network makes fog computing incredibly stable in stressful situations compared to the cloud and a lot more reliable in real time applications such as autonomous vehicles because of the need of fast responses from the network.

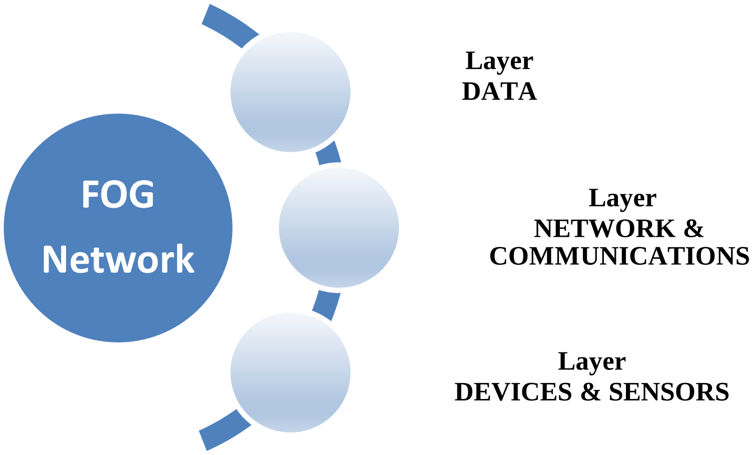

Fig. 3. Fog computing layers

Fog computing implementation can greatly improve IoT networks when it comes to security of data, as less sensitive data is sent to the cloud to be stored or analyzed. “Edge computing is the least vulnerable form of decentralized storage. On the cloud, data is distributed to dozens of servers, whereas edge computing uses hundreds, possibly thousands of local nodes. Each device can act as a server in the edge network.

To break into, hackers would need access to thousands of distributed devices, which is practically impossible”[9]. The fact that fog computing are placed to the edge, means they’ll have rich and heterogeneous end-user support, being another layer of security in the IoT network. Also the fact that there should be a single hop between end devices and the fog, means there is less space for attacks in the network. “Fog computing has all applicable security controls and processes in place which solves the problems of security risks and mitigate the threads” [10].

Cloud can store much more data than a fog system and can aim for long-term deep analysis, while fog performs short-term edge analysis due to almost instant responsiveness. „A report by Verizon discovered that instances with little data losses (around 100 lost or compromised record) costs an average of 18,120 to 35,740 $, while large-scale data loss costs an average of 5 to 15.6 million $”. When taking in consideration the real cost of data loss, fog computing’s implementation costs start looking more and more appealing.

Table 1. Cloud and Fog Computing: a Comparison Chart

	CLOUD	**FOG**
Architecture	Centralized	Distributed
Communication with devices	From a distance	Directly from edge
Data processing	Far from the source of information	Close to the source of information
Computing capabilities	Higher	Lower
Number of nodes	Few	Very large
Analysis	Long-term	Short-term
Latency	Higher	Lower
Connectivity	Internet	Various protocols and standards
Security	Lower	Higher

Source: *sam-solutions.com - Fog Computing vs. Cloud Computing for IoT Projects*

Disadvantages of fog computing are the higher cost of implementation because devices like hubs, routers, gateways are necessary, they have less computational resources than cloud servers and there is the challenge of maintaining so many local servers in the network. Fog computing isn't meant to replace cloud computing, but work together with it, creating a more stable and resilient IoT infrastructure.

4. Security model for IoT networks with fog computing

Our research is focus on implementation of a security validation model that revolves around the 3 main attributes of any secure system: integrity, confidentiality and availability. STRIDE[11] is a model of threats implemented to help consider and identify potential threats to a system.

Table 2. Impact on CIA Triade by the main threats(STRIDE methodology)

Fog Layer	**THREAT**	**Impact on CIA Triade**		
		Confidentiality	**Integrity**	**Availability**
Devices & sensors	Spoofing	major	minor	none
	Tampering	none	major	none
	Repudiation	none	major	none
	Information disclosure	major	none	none
	Denial of service	none	none	major
	Elevation of Privilege	major	major	none
Data layer	Spoofing	major	minor	none
	Tampering	none	major	none
	Repudiation	none	major	none
	Information disclosure	major	none	none
	Denial of service	none	none	major
	Elevation of Privilege	major	major	none
Network & communications	Spoofing	major	minor	none
	Tampering	none	major	none
	Repudiation	none	major	none
	Information disclosure	major	major	none
	Denial of service	none	none	major
	Elevation of Privilege	major	major	major

A bidirectional communication between the fog - end devices and the fog - cloud that enables real time analysis of the network's state, so the fog network can change between different levels of security in each node.

If a fog node is compromised/affected, neighbouring fog nodes can increase the level of security in order to detect attacks. This can be realized with the cloud that analyze the state of the fog network and send reports back to each node, after that the fog node analyzes the cloud report and takes the needed measure.

By creating a fog framework where each node adapts to realtime necesities such as security over computing or vice versa, we create a dynamic system that is cost effective and more reliable. We consider it hard to attack the whole Fog layer due to the big number of heterogenous nodes, so it is easier to locate and solve attacks earlier through the reports.

Fog computing allows for malware and infected files to be found at an early stage in their cycles at the device level long before they even have the opportunity to infect the whole network because a fog node can allow operations managers to remotely isolate and shutter the zone that is infected keeping disruption to a minimum. During an attack, fog nodes are operating using only their local intelligence and locally stored data to manage permissions and data accessibility of the system.

Model that creates a platform for the fortification of security in IoT networks and that can be applied in different economics sectors such as healthcare, transport, banking, energy or surveillance. We take in consideration the impact that fog computing implementation has on the IoT network and cloud in both functioning state and also compromised state, having the goal to minimize data loss and to make even more resilient systems to attack. The fog nodes in the model act as gates that moderate the ratio of resources allocation to security and computing through several reports from the cloud and other nodes in the fog, taking in consideration different applications and their necessities.

We imagine a strongly communicative network that has constant knowledge about the other nodes in the fog so it can effectively take measures in case of emergencies. Each node in the fog sends key information about the state they are in and after processing all the data from the nodes, a global report is sent back to each fog node so it can take security measures in response to the report (increase the level of security if the close nodes of an attacked node for example). This report and respond system enforces the need of a fog computing platform that can support different applications implemented by multiple independent data providers.

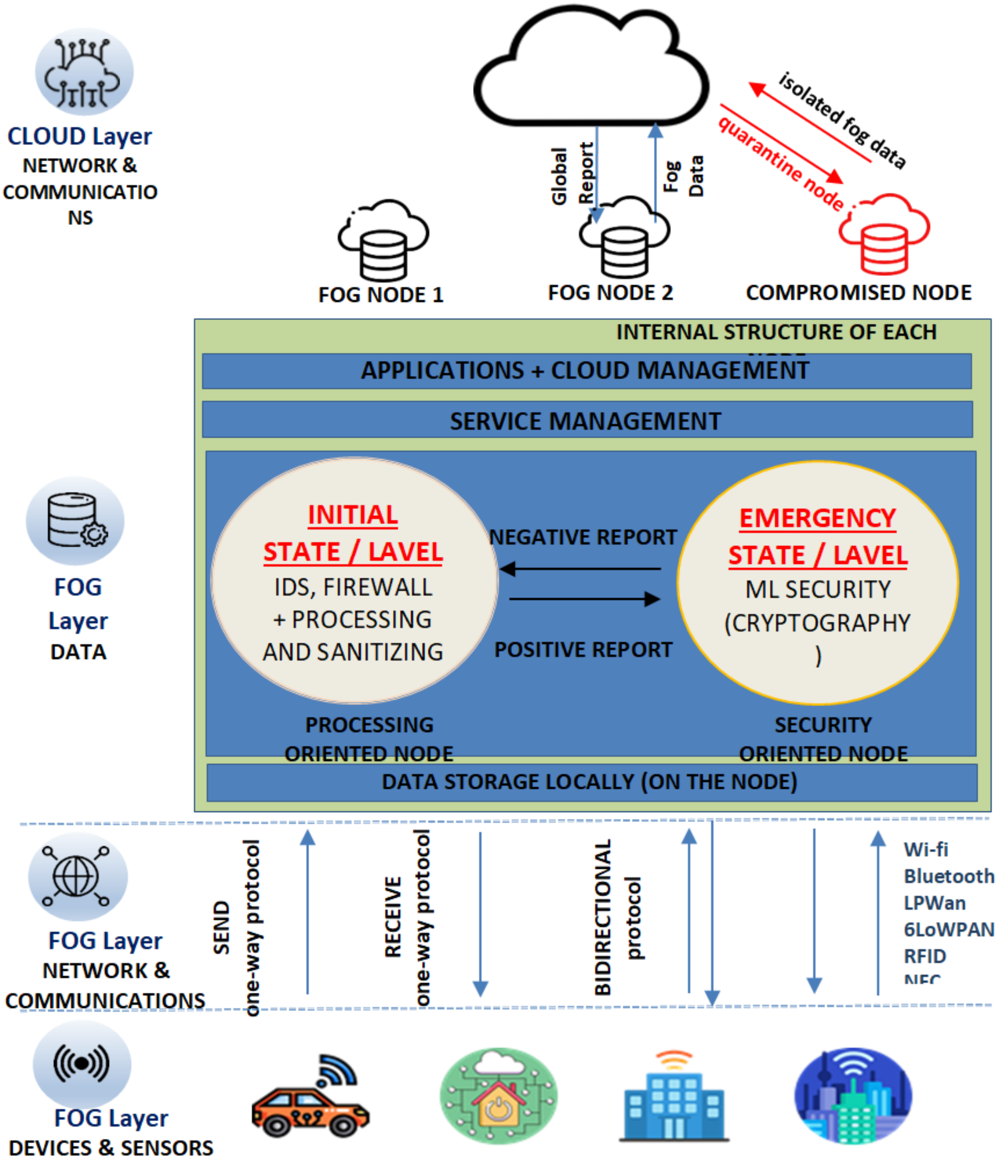

Fig. 4. Security Model for IoT Networks with Fog Computing

Taking in consideration good practice implementations present in any security system we can apply fog computing in:

- ***Real Time Alerts***: With fog computing, we can concentrate on key access points in a network where most sensitive data is(through risk assessment) and fortify the security on those points mananging real time alerts.
- ***Data Minimization and storage in multiple locations***: spread small amounts of data in several fog nods, so it’s harder to target and attack big datasets. Less demanding tasks processed by the fog, while the others go to

the cloud. The less time data spends traveling in the network, the smaller the chance for it to be lost.

- ***Continuous monitoring***: fog nodes that continuously monitor and signal security problems using multiple levels of security based on the reported state of the network. Cryptography is a compute intensive process and it depends a lot on the cryptographic abilities of the IoT devices.

Different economic sectors such as transportation[12], healthcare[13] or banking demand high security by default because of the sensitive data used and the human safety implications of autonomous driving for example, while other domains such as energy or surveillance can be implemented with increasing levels of security depending on the state of the network(if it's attacked or not) so it can channel the computing power of the fog node to other tasks.

This way, we realize a model where we constantly monitor the state of the other close nodes in the fog or the state of the cloud and increase the level of security only in case of emergency. This way we efficiently concentrate the limited computing resources of each node in most of the cases so we can improve performance of the IoT network, making the fog a triage layer for data that should be sent to the cloud for the hardware and software demanding tasks.

In normal states, the IoT architecture is not unprotected because the fog layer automatically improves security of the network if we implement the fog as proxy server with Intrusion Detection Systems and/or firewall capabilities. With this, most of the attacks can be prevented by the firewall and harmful intrusion attempts can be detected by IDS and mitigated in the fog, not even reaching the cloud that has its own security services too.

In the case of services that require authentication, if several layered authentication methodology (one at FCG, one at the cloud, etc.) is used then this might be a very secure solution. Otherwise, if all authentication operation is left to the FCG devices, this might create problems when the FCG devices get compromised. Any failure in security would only affect a limited number of IoT devices connected to the respective fog node/nodes, while the cloud would remain mostly unaffected and functional so it can start solving the problem.

No system is invincible and perfectly secure and with so many heterogenous devices working together constantly, there will always be vulnerabilities that can be exploited, the main goal being the minimization of damage.

If we extend the topic to confidentiality which is crucial in healthcare, a suggestion would be the storage of private data on the edge while sending just the necessary data on the cloud. This way, data would be spread and it would be harder to affect the overall integrity of the system. In case of compromise, the other nodes would receive a report of the affected node's state and would implement a higher level of security, giving up on the processing power of data.

Also, when a node is compromised, the system should "quarantine" that node until the problem is solved. Yet this thing would render the devices connected to the node non functional, raising the question: what's the impact of a compromised fog node? In most cases, the IoT end devices suffer the most while the cloud can be unaffected by breaking the connection with that node when danger is detected.

Having just as few nodes compromised as possible is absolutely necessary and can be realized with a multiple levels of security system that increases cryptography and the “defenses” in the other nodes of the network when a fog node was compromised.

In the case of compromising a few nodes of the fog in comparison with the huge servers of the cloud, we reduce the losses by a lot. On the other hand, compromising a fog node can mean the hijacking of an autonomous car which can lead to devastating consequences so that’s why we need to have a high level of security implemented for the get-go on this type of applications.

This way we divide fog nodes in two categories: security dominant nodes and processing dominant nodes. In security dominant nodes, applications that include the use of private/confidential data or that could lead to the endangerment of people should allocate most of their resources on security services while the processing dominant nodes would concentrate on the sanitizing of the network – preprocessing of data and getting rid of unnecessary data that would uselessly flood the cloud, with a changeable level of security depending on the state of the nodes in the fog/cloud network.

In cases where both the processing and security are highly needed like in the case of autonomous vehicles that need very fast response times and good security, servers with greater computing capabilities need to be implemented in the fog in combination with the already powerful machines in the cloud.

5. Conclusion

Taking in consideration that an IoT network can be targeted by many attackers in different layers of its architecture and the fact that IoT is the backbone of a Smart City, it is important to consider Smart Security a crucial part in the development plan. Vast amounts of sensitive data are transmitted non-stop in the network, the privacy of the users and security of the data should be the main concerns of a Smart City.

Using unidirectional data transmition protocols (dioda), separating devices and sensors into dedicated nodes according to the described security model can ensure much higher security for IoT networks. The usefulness of such a conceptual model can reduce the attack surface, reduce the vectors and possible attack scenarios by adding a cybersecurity component to the local nodes in fog computing

The IoT network must be trustworthy in face of different attacks, such as: APTs (advanced persistent threats), data and identity theft, device hijacking, DDoS attacks, Credential theft, etc. If we think that a cyber attack can disrupt, in a moment, a whole industry and threaten the safety of citizens and their privacy, Smart Security becomes one of the most important aspects when it comes to the reliability and survival in the future of the concept of Smart Cities.

References

[1] https://www.researchgate.net/publication/273693976_A_Review_on_Internet_of_Things_IoT, 2015, International Journal of Computer Applications 113.

[2] https://www.researchgate.net/publication/327272757_IoT_Elements_Layered_Architectures_and_Security_Issues_A_Comprehensive_Survey, 2018

[3] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments

[4] https://www.researchgate.net/publication/273693976_A_Review_on_Internet_of_Things_IoT

[5] https://www.researchgate.net/publication/264458816_Layers_of_Cloud_IaaS_PaaS_and_SaaS_A_Survey, 2014

[6] https://www.researchgate.net/publication/308600978_Internet_of_Things_IoT_with_Cloud_Computing_and _Machine-to-Machine_M2M_Communication

[7] https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf

[8] https://www.researchgate.net/publication/301691282_Fog_Computing_Platform_and_Applications

[9] https://www.digiteum.com/cloud-fog-edge-computing-iot

[10] https://arxiv.org/ftp/arxiv/papers/1904/1904.04026.pdf#:~:text=Expensive%3A%20Fog%20computing%20is%20very,a%20very%20complicated%20computing%20process

[11] Threat Modeling, Microsoft Security Development Lifecycle (SDL), https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling#:~:text=The%20Microsoft%20Threat%20Modeling%20Tool, structure%20of%20their%20software%20design.

[12] https://www.researchgate.net/publication/317018257_On_Developing_Smart_Transportation_Applications_in_Fog_Computing_Paradigm

[13] https://www.researchgate.net/publication/281176022_Fog_Computing_in_Healthcare_Internet-of-Things_A_Case_Study_on_ECG_Feature_Extraction