Securing Combined Fog-to-Cloud Systems: Challenges and Directions

Sarang Kahvazadeh, Xavi Masip-Bruin, Eva Marín-Tordera, Alejandro Gómez Cárdenas

Advanced Network Architectures Lab (CRAAX) Universitat Politècnica de Catalunya(UPC), Barcelona, Spain
{skahvaza, xmasip, eva, alejandg }@ac.upc.edu

Abstract. Nowadays, fog computing is emerged for providing computational power closer to the users. Fog computing brings real-time processing, low-latency, geo-distributed and etc. Although, fog computing do not come to compete cloud computing, it comes to collaborate. Recently, Fog-To-Cloud (F2C) continuum system is introduced to provide hierarchical computing system and facilitates fog-cloud collaboration. This F2C continuum system might encounter security issues and challenges due to their hierarchical and distributed nature. In this paper, we analyze attacks in different layer of F2C system and identify most potential security requirements and challenges for the F2C continuum system. Finally, we introduce the most remarkable efforts and trends for bringing secure F2C system.

Keywords: Security, Fog-to-cloud computing

1 Introduction : Combining Fog and Cloud

Nowadays, the wide and continuous deployment of smart devices at the edge, such as sensors, actuators, smartphones, tablets, etc., setting the roots for the emerging Internet of Things (IoT) [1] paradigm, along with the recent developments in network technologies, from the network core (e.g., elastic or flexible optical networks) up to the user edge (e.g., LoRa), with an eye on the promising 5G, all enabling fast users and (even more important) Machine-to-Machine (M2M) communication [2] are, all in all, paving the way towards an innovative but also unforeseen scenario where devices, users, services and also data will interact in a, more than probably disruptive way. Aligned to this evolution, cloud computing [3] has been widely adopted to address some of the key concerns related to data, including aggregation, processing and storage leveraging the large capacity massive data centers located at cloud are endowed with.
Unfortunately, the far distance from the datacenters at cloud to the users and/or devices requiring the cloud services, brings undesired concerns –in terms of for example

scalability, security or quality of service (QoS), just to name a few–, that may become critical challenges for some applications, for instance applications demanding real-time processing. Recognized this weakness, a new computing paradigm, fog computing [4], recently came up, and intended to sort this weakness out by moving cloud capacities closer to the edge. To that end, nodes with some computing capacities are distributed close to users and devices at the edge, referred to as fog nodes [5], thus facilitating real-time processing and low-latency guarantees. Interestingly, fog computing does not compete with cloud computing, rather they both complement each other to guarantee a service to be allocated to those resources best suiting its demands. Thus, a new scenario comes up, built upon considering the whole set of resources from the edge up to the cloud, coined as IoT continuum [6], [7].

A key challenge in this combined scenario refers to resources management assuming the specific requirements coming when considering the heterogeneous set of potential resources at the edge. Some ongoing efforts are already addressing this challenge, such as the OpenFog Consortium [8] or the EU mF2C project [9], the latter aimed at designing and developing the Fog-to-Cloud (F2C) concept proposed in [10], and both aimed at optimizing services execution and resource utilization. Recognized the potential benefits brought in by such optimization, a key and highly critical component refers to security provisioning. Indeed, there is no doubt that the edge context, putting together low control, low power, and generally speaking, considering a vast set of heterogeneous devices on-the-move, is highly vulnerable to attacks and security breaches that may put the whole system at risk. Therefore, it seems reasonable to devote some efforts to analyze and characterize what security provisioning means, what the challenges are and how could be addressed.

To that end, this paper illustrates the particular scenario built by the F2C approach, as a potential candidate to the final optimization objective, although certainly the analysis performed in the paper might be adopted for any solution aligned to a decentralized architecture for combined fog and cloud systems. Indeed, F2C is proposed as a hierarchical multi-layered control architecture designed to manage the whole stack of resources from the very edge up to the cloud in a coordinated way, putting together the advantages of both computing paradigms, i.e., proximity at the fog and high performance at the cloud.

From an organizational perspective, the combined F2C ecosystem is organized into areas, each including its whole set of resources (fog nodes and IoT devices) see Figure 1 –the exact scope of an area and the individual allocation of resources into each area are ongoing research topics, certainly affecting the scalability of the system, but out of the scope of this paper. One node at each area is selected to serve as the fog leader (policies yet to be defined), thus responsible for managing the devices inside the area as well as coordinating with higher hierarchical layers. The set of fog leaders are also connected through a higher layer, thus setting the envisioned multi-layered hierarchical control architecture (see Figure 1 as a topological example, where fog leaders are connected through cloud).

However, as briefly introduced above, this highly distributed and heterogeneous scenario fuels many security gaps and weaknesses that must be properly addressed. Certainly, it is worth emphasizing that most of the IoT devices included in the different

areas will have low computational power and consequently, will not be able to handle their own security, nor support any highly demanding external security solution either. In fact, the scenario is not promising, since neither cloud computing (as a centralized strategy located far from the devices to secure) nor fog computing (using fog node resources to support security functionalities may have a non-negligible impact on the individual fog node QoS performance) seem to be the proper solution to provide the expected security guarantees. Moreover, beyond specific security provisioning limitations in IoT devices, any combined F2C-like system might impose additional security requirements due to its distributed, decentralized and layered nature, thus making security provisioning even more challenging.

With the aim of illustrating the security concerns in combined F2C-like systems, this paper analyzes main security requirements and challenges for such scenario, with particular focus, for the sake of illustration, on the F2C approach.

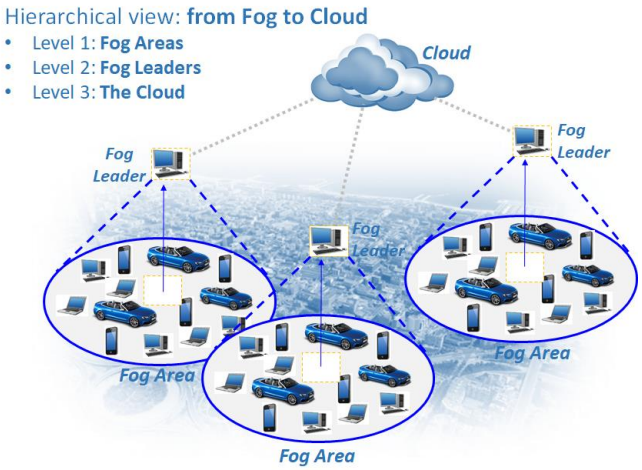


Figure. 1. Combined F2C system

This paper is organized as follows. In section 2, we identify security requirements in combined F2C systems. Then, section 3 discusses and analyzes security challenges and provides some directions to move forward and section 4 illustrates some existing efforts and trend to provide F2C security. Finally, section 5 concludes the paper.

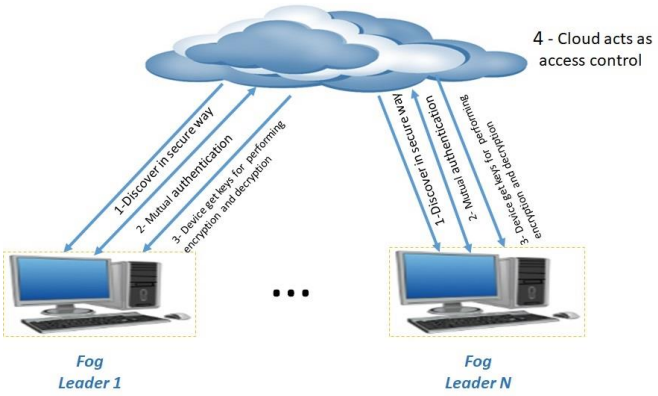
2 Security Requirements for F2C-like Systems

A mandatory step previous to a potentially successful design of a security solution for combined fog and cloud systems boils down to identifying the particular set of security requirements demanded by such scenario. Contributions led by the OpenFog Consortium and the mF2C project, are currently trying to set the roots for such a definition. This section, focuses on the latter, considering the F2C architecture as an illustrative and sound approach for combined fog and cloud systems –although the

security characteristics described in this paper should accommodate needs for any other F2C-like system. Moreover, it is worth highlighting that, from the design perspective, whatever the solution to be proposed is, it should benefit from recent technology innovations to improve or facilitate security provisioning. In this direction, just as an example, [11] briefly introduces potential benefits from adopting blockchain to security provisioning in fog systems.
Before digging into the set of security requirements, we first summarize the whole distributed security procedure as proposed for the F2C layered architecture, describing specific steps for each one of the two envisioned domains and then we introduce potential attacks a F2C-like system may deal with.

2.1 Security process in F2C

As shown in Figure 1, F2C proposes a distributed and layered architecture where devices closer to the edge are clustered into different Fog Areas, each managed by a Fog Leader, logically located at an upper layer. Certainly, Fog Leaders enable both area-to-area and area-to-cloud connectivity, hence consequently a secure communication on two domains, fog-cloud and device-fog, is a must to avoid any passive or active attack.
On the first domain, i.e., fog-cloud, some steps are needed to bring security in, as illustrated in Figure 2. More specifically, we may consider that first, each fog leader must be securely discovered and then perform mutual authentication with cloud through some credentials and identities, in order to provide system and data integrity and confidentiality. Once authenticated, fog leaders either generate keys, or get keys from cloud if key generation is not enabled at fog leaders. Fog leaders can then use these keys to encrypt and decrypt the information flow with cloud, aimed at preventing attackers to eavesdropping, modifying, or deleting information between cloud and fogs. From a technology view, the network technologies supporting cloud and fog leader communications (e.g., wired, wireless, etc.) must be secured to avoid passive and active attacks, turning into secure channels (blue lines in Figure 2.a).
Once the fog leaders are properly installed and authenticated to the F2C cloud, they are authorized to provide computation, network, storage, and shareable computational environment to fog nodes and IoT devices at the edge of the network in a distributed way. Thus, the second domain, i.e., device-fog, as illustrated in Figure 2.b, starts when a device reaches out to a fog area, demanding the device to be discovered by a fog leader in a secure way. Then, as done for the first domain, fog leaders and devices must be mutually authenticated through some credentials in order to guarantee data and system integrity and confidentiality at the edge of the network. Once authenticated, devices either generate keys or get keys from the fog leaders, in case they cannot generate keys, to be used for encryption and decryption. The information flow between devices (IoT devices and fog nodes) and fog leaders must be properly encrypted to prevent attackers from eavesdropping, modify, or delete the information. Similarly, all information must be conveyed through secure channels regardless the deployed technology (blue lines in Figure 2.b).



a)

b)

Figure. 2. (a) Fog-cloud domain security; (b) Device-fog layer security

It is worth highlighting that in the first domain, cloud acts as access control providing the access to cloud data centers for the distributed fog leaders, according to their attributes and thus preventing any unauthorized access, while in the second domain, fog nodes are responsible for such task, preventing any unauthorized access to the F2C system at the edge of the network.

The F2C scenario described so far may be more complex if mobility is also considered. More specifically, whatever the security strategy proposed is, the effects of the handover process triggered by a device on the move leaving one area (i.e. a fog leader) and getting into another one must be considered. This shift may drive the need for both areas to communicate each other to facilitate the handover process. Two options come up, one through cloud and the other one enabling horizontal communication among fog leaders. For the sake of processing time we may assume the latter to be the optimal one, hence demanding direct secure inter-communication between fog leaders.

2.2 Attacking a F2C system

Unfortunately, there are many potential security vulnerabilities in F2C-like systems, paving the way for attackers to launch attacks in different layers in the system. In this section, we identify most potential attacks to be faced by F2C-like systems as illustrated in Figure 3, all grouped into three categories, as follows.

Man-in-the-middle attack: Attackers can take the network control between devices at different levels (IoT devices, fog nodes, fog leaders and cloud) to either eavesdrop communication, modify information or even to inject malicious information and code into the system. For example, attackers can obtain the identity of a F2C component and then impersonate it to be an eligible component. Due to the obtained identity, the attacker can impersonate a fog leader (malicious fog leader) thus getting devices and users information and locations. Also, an attacker can impersonate users and devices to take information or gain access to services it is not authorized to. In upper layers, i.e. fog-cloud communication, an attacker can impersonate fog leader or even cloud to launch a man-in-the-middle attack. In all these cases, attackers can launch the attack in passive (eavesdropping without changing information) and active (information modification, manipulation and malicious injection) ways. This type of attack effects the integrity and confidentiality of any F2C-like system (see Figure 3.A).

Denial of service and Distributed denial of service (DoS and DDoS): In this case, attackers either launch multiple service requests to the fog leader or perform a jamming wireless communication between fog leader-devices to deplete the fog leader resources and consequently making it down. An attacker can use legitimate devices, such as IoT devices, fog devices or fog leaders to launch DoS and DDoS using their identities. DoS and DDoS attacks can also occur in upper layers such as fog leader-cloud. As a consequence, attackers successfully prevent legitimate users and devices from accessing services provided by a fog leader or even by cloud (see Figure 3.B). In short, this attack severely affects the availability of the F2C system.

Database attacks: In a F2C system, databases may meet a hierarchical architecture, keeping for example one centralized at cloud and some other locally distributed at fog layers. If an attacker can access to these databases, it can modify, manipulate and even leak the data, what may have a high impact on the total system performance. Database attacks may be internal –coming from F2C service providers–, or external –legible and illegible users. This attack intensely effects the F2C integrity and confidentiality (see Figure. 3C).

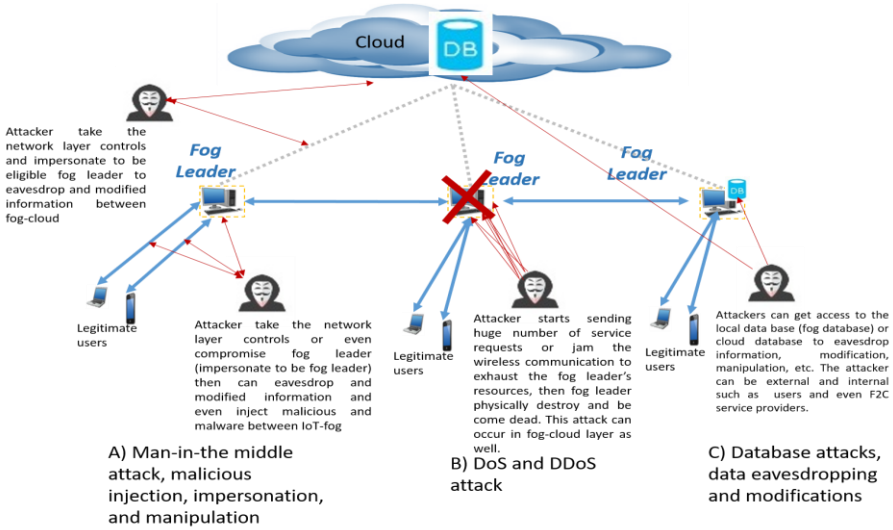


Figure 3. Attacks in F2C systems

2.3 Security Requirements in F2C

After describing the main scenario characteristics for combined fog-cloud systems, the security strategy for F2C and the set of potential attacks a F2C system may suffer from, next, potential security requirements for combined fog-cloud systems are introduced in Table 1 (see also [12-13] for more information), summarized into 9 main concepts, all in all driving a set of challenges, as introduced in next section, fueling novel research avenues. It is worth mentioning that despite the fact that the identified security requirements are not novel in their conception, what makes them specially challenging is the specific scenario security is to be designed for, i.e., F2C-like systems, where heterogeneity, volatility and dynamics are basic and undeniable characteristics.

Table 1. Combined F2C system security requirements

Security requirements in combined F2C system	Description
Authentication and authorization at the whole set of layers	Authentication must be done for all participant components in F2C systems to provide integrity and secure communication. A hierarchical authentication may be considered, in short, cloud authenticates fog leaders, and fog leaders authenticate edge devices (fog nodes and IoT devices).
Appropriate key management strategy	F2C systems must include a well-defined key management strategy for keys distribution and update as well as for key revocation.
Access control policies to reduce intrusions	Access control must be supported at cloud level and distributed access controls at fog layers

Providing confidentiality, integrity, and availability (the CIA triad) as a widely adopted criteria for security assessment	In a F2C system, user's information must stay private not to be disclosed to unauthorized users (confidentiality), information must be complete, trustworthy and authentic (integrity), and finally the whole system must work properly, reacting to any disruption, failure or attack (availability).
All network infrastructure must be secure	All components in a F2C system (users, devices, fog leaders, fog nodes, and cloud) must communicate through secure channels regardless the specific network technology used to connect (wired, Bluetooth, wireless, ZigBee, etc.).
All components must be trustable	In the proposed hierarchical approach, the set of distributed fog leaders act as a key architectural pillar enabling data aggregation, filtering, and storing closer to the users, hence making trustness mandatory for fog leaders.
Data privacy is a must	Data processing, aggregation, communication and storage must be deployed not to disclose any private information, or produce data leakage, data eavesdropping, data modifications, etc. To that end, data must be encrypted, and data access must not be allowed to unauthorized users. Moreover, assuming mobility a key bastion in F2C systems other particular privacy related issues come up, such as for example geo-location.
Preventing fake services and resources	Fake scenarios are highly malicious in F2C systems, hence some actions must be taken to prevent that to happen, such as services and resources must be discovered and identified correctly and services and resources allocation must be done securely.
Removing any potential mobility impact on security	Fog nodes and IoT devices might be on the move, thus demanding the design of secure procedures to handle mobility related issues, such as devices handover.

3 Open Challenges

This section, driven by the set of security attacks and requirements identified in section 2, is intended to go deep into the open challenges coming from the requirements above and necessary to provide security guarantees in a scenario combining fog and cloud computing. For the sake of understanding, the F2C approach is used to illustrate the specific details brought in when combining fog and cloud that make security provisioning even more challenging. In fact, the objective is not only to identify the challenges but also to highlight the open issues making them so challenging. To that end, challenges are split into 5 security concepts as shown in Table 2, aligned to and extending previous works in the area of fog computing.

3.1 Trust and authentication:

Trust: Traditional strategies applied to static or well defined scenarios do not match the particularities rolled in by the potential stack of heterogeneous and largely distributed resources considered in F2C systems. Working on that direction, the Open fog consortium [8] proposes to embed the hardware root of trust into the fog nodes to

provide security at the IoT layer. Certainly, this is still an ongoing effort where many challenges remain yet unsolved, such a potentially unaffordable cost or to what extent an attack on a fog node may compromise the security for its IoT devices. In the same direction, a joint effort within the mF2C project is analyzing a blockchain-based solution to provide a novel distributed trust strategy particularly tailored to face the specific trust needs and conditions of combined fog and cloud systems.

Authentication: Authentication is a key security component in any ICT system, but it is particularly important in scenarios where mobility and heterogeneity are undeniable characteristics. It is widely accepted that the use of the conceptually centralized cloud for handling device's and user's authentication cannot be sufficient for a F2C system. The reason for that is twofold. First, the huge number of messages forwarded between a large set of unstoppable increasing devices at the edge and cloud. Second, if cloud is down, compromised or attacked, the whole F2C system will be compromised. Fortunately, a solution based on the proposed hierachical layered architecture may be proposed. The main rationale for this proposal is that cloud can be used to authenticate fog leaders, and then, the authenticated fog leaders can handle IoT devices', fog nodes', and users' authentication in their area in a distributed fashion. This solution would reduce cloud dependencies, would facilitate redundancy at fog layers to deal with potential fog node breaches and promises to be scalable (per layer). However, the work is not completely done and there are some questions yet to be solved. Indeed, a key question refers to "how can these hierarchical authentication processes be done and which type of authentication for each layer can be used".

Key management: Scalability is also a non-negligible drawback when considering a centralized key generator center (KGC) in combined fog and cloud systems. Indeed, beyond the effects of compromising the KGC, a large number of messages would be expected. Although a distributed key management strategy for generating, assigning, updating and revoking keys seems to be the proper approach, many open questions come up, mainly referring to:

- How can IoT devices (in a large number and with low computational power) get keys to encrypt data?
- Would it be possible fog layers to handle distributed key management for both IoT devices and users?
- Would it be reasonable to assume cloud to act as key manager for fog layers and so the latter as distributed key managers for their areas? And if so, what should be the proper key management algorithm (symmetric or asymmetric) for each F2C layer?

Identity management: The main aim is to assign an ID to all devices, what is pretty challenging for devices with low computational power, since ID storage might be not affordable. Indeed, some questions come up:

- How can distributed IDs manager in fog layer be secured?
- Would ID fragmentation be a candidate solution to minimize scalability issues? (i.e., using different fragment's size for each layer [14])
- If so, what would the right fragmentation policy to support an optimal fragment storage?

- And what is the max/min fragment size allowed per layer?

3.2 Access control and detection:

Access control: Considering the large set of devices at the edge as well as the different characteristics shown by the whole set of resources in the continuum from the edge up to the cloud, the key question may be stated as "how to design a global access control, supporting the different systems characteristics and constraints". The hierarchical model envisioned by the F2C model addresses this challenge proposing a hierarchical access control, deploying distributed access controls located at fog layers responsible for controlling devices and users at the edge of the network, and a centralized access control located at cloud layer responsible for controlling the distinct fog leaders. This may be a tentative solution that is currently being developed within the mF2C project.

Intrusion detection mechanism: Deploying a centralized intrusion detection solution managing the envisioned huge number of participant devices in F2C systems brings many weaknesses, for example malicious activities or nodes might not be detected due to either the huge volume of traffic analysis, or the centralized approach it self. Indeed, whether a centralized intrusion detector collapse or it is compromised, the whole intrusion detection solution may fail, what would not be sane for the system.

Malicious IoT and fog device detection*:* Recognized the fact that the near to the edge a system is the more is its level of vulnerability as well, the massive deployment number of devices at the edge of the network facilitates attackers to successfully launch attacks or faking devices to eavesdrop the system. Obviously, if a device gets compromised or attacked, it must be properly detected and rapidly revoked from the system. Thus, the challenging question is "how can malicious devices in different layers be detected and what strategy or algorithm can be used to detect the malicious device on real-time processing and revoke them?".

3.3 Privacy & sharing:

Privacy: Data anonymization and data privacy are crucial components to protect user's private information. However, in scenarios where data is a must, notably leveraging data collection and processing to offer innovative services, a key challenge may be stated as "which data anonymization can be applied to the the combined F2C scenario to keep the suitable trade-off between privacy and data utilization?" A tentative solution suggested for F2C systems may rely on keeping data as close to the edge as possible. To that end, fog leaders closer to users will take over the data processing, analysis and storage thus removing the need to go to higher lavers in the hierarchy, consequently reducing the privacy gap. Another recently relevant concern refers to mobility aspects. Indeed, there are many services and apps demanding user's location to be executed, but the system should include strategies for users not willing to disclose their location. Indeed, some negotiation may be deployed between security and privacy, normally the more the security levels the lower the privacy guarantees and vice-versa. In fact, when an attack is detected, the system must be able to react and consequently should be able to find out attacker's location. In short, privacy must be analyzed at different layers, privacy concerns must be identified, and finally, data and location privacy must be applied appropriately without impacting the whole security.

Secure sharing computation and environment: In the envisioned combined model, resource sharing is an instrumental concept to move research but also market opportunities forward. In this sharing scenario fog nodes may complement IoT devices with low computational power, with additional resources. Although conceptually, this looks to be a promising model, attackers may benefit from it and may fake themselves as legible devices (as IoT devices, as fog nodes, and as fog leaders) to launch passive and active attacks. Three main relevant challenges come up: first, "how can a fog node or fog leader share their resources in a secure way with low computational power devices?"; second "how can IoT devices trust fog nodes?"; and third "how can IoT devices outsource their service execution to fog nodes they share resources with?". Trust establishment and the ability to distinguish between legible and illegible devices is paramount here. Therefore, threat models and security analysis for the hierarchical shareable F2C environment must be done in each layer at an early stage, and all needed security requirements such as authentication, privacy, etc. must be provided before any device share their computational power with the system.

3.4 End-to-end security solution:

Network security: Interestingly, when moving close to the edge many different network technologies may be deployed, such as wireless, wired, zigbee, bluetooth, etc., that along with the candidate technologies to connect the edge to the cloud build a highly diverse technological scenario. Then, the main aim is to develop a network security strategy ensuring end-to-end security guarantees regardless the network technologies in place. It must be also considered that network technologies are not working in an isolated paradigm, rather different security protocols for different technologies might impact each other. Certainly, network technologies diversity is not a new problem and as said above, connectivity to cloud is agnostic of the technology used to connect. However, the single point failure concern and the long distance between the edge to cloud do not make cloud approach sound for the envisioned scenario. Therefore, network security must be re-designed to handle all type of network technologies, to provide end-to-end security, and to avoid the negative impact of handling different technologies and protocols.

Quality of service (QoS): Service execution in combined fog and cloud scenarios must be supported by an optimal resource allocation, regardless where the resource is, as long as it perfectly meets service requirements, all in all to provide the expected QoS. However, whatever component is added for security provisioning some resources will be consumed, thus affecting the delivered QoS. The main rational behind this assessment seats in the huge volume of computational crypto requirements needed when implementing security. The services to be delivered through a combined fog and cloud deployment must positively benefit from such a resources combination in terms of a much better QoS while keeping solid levels of security on the whole stack of resources. Thus, to make it happen some open issues must be solved first, such as "if the distributed fog leaders take over security provisioning at the edge devices would they still have room to meet the expected QoS?, or in other words, "how do both security and QoS meet expected performance in combined F2C systems?"

Heterogeneity: An F2C system is expected to manage heterogeneity at distinct levels, from network technologies, hardware or infrastructure providers, the latter being

particularly interesting in terms of interoperability and also on a business oriented perspective. In fact, the envisioned F2C scenario should deal with distinct cloud providers (as already managed by the cloud sector) and also with fog providers. Certainly, what a fog provider may be is yet requiring sometime in the market, but it reasonable to consider cities, communities, malls, that is, "groups" of users that may become a "fog" provider for other users. In this scenario when providers become volatile (beyond the resources), setting agreements and "reliable" connections become a very challenging task. Consequently, a strategy should be sought to analyze how the different security strategies can be applied by the different providers, how they all can be compatible with each other and how the agreements may be set among them.

Secure visualization: Interestingly, in a combined F2C system, fog nodes and fog leaders provide virtualization closer to the end users. The fog nodes and leaders might host the virtualization environment in their hypervisor. It means that, should the hypervisor gets attacked, then the whole fog's virtualization environment might be compromised. Recognized the high vulnerability inherent to virtualization environments, in terms of virtualization attacks, such as virtual machine scape, hypervisor attacks, etc. Therefore, virtualization must implement in a secure way in the hierarchical F2C system.

Monitoring: The vast amount of devices distributed at the edge of the network, makes a centralized monitoring at cloud not adequate enough for F2C systems. The challenging questions are "which monitoring strategy/ies must be deployed to correctly monitor the huge amount of distributed devices located at different stack layers?", and "how the huge traffic analysis should be managed to detect malicious activities?" To that end, the solution pushed for by the mF2C project considers a distributed monitoring strategy implemented at fog layers to detect any malicious or abnormal behavior at the edge of the network, combined with a centralized monitoring strategy located at cloud for fog layers.

Security management: The main challenges and questions here are, "can cloud as a centralized concept be sufficient to act as a security manager for the whole hierarchical F2C system?" The answer to this question is no, cloud as a centralized point failed to provide security and prevent several appeared attacks in past decades, although another challenge is, "What security management strategy must be taken into account for the distributed fogs and IoT devices?" To tackle with all these challenges, a new security management strategy, such as distributed security manager at fog layers and centralized at cloud, can be a suitable for the current security management for the F2C system.

Centralized vs distributed security management: The key question refers to the capacity cloud as a centralized approach may have to serve as the security provider for the whole hierarchical F2C system. In fact, the correct answer is not positive since many reported attacks already exploited the cloud security vulnerabilities. Beyond that, the distributed nature of the F2C scenario, enriched with aspects related to mobility, volatility and heterogeneity make a centralized approach not to be the proper solution. Then, a distributed solution should be designed to handle the hierarchical nature of the F2C system, simultaneously handling the required security for distributed devices at the edge.

Secure devices bootstrapping*:* All components in the combined F2C system must bootstrap in a secure way by getting public and private parameters. In this scenario, the traditional centralized cloud or centralized trusted authority usually used for bootstrapping cannot be affordable due to the huge number of devices in the F2C system. Then, main questions are: "which distributed component must take cloud responsibility for bootstrapping devices at the edge of the network?", "can we apply a strategy where the cloud bootstraps fog leaders and fog leaders bootstrap devices in their area in a distributed fashion?"

3.5 Mobility support:

Secure mobility: Recognized the inherent mobility shown by devices at the edge, the main challenge arises when trying to handle secure handover and secure mobility. As discussed before, the centralized and remote cloud cannot handle secure mobility for distributed devices at the edge of the network, fog leaders closer to the users might do so instead. To that end, distributed fog leaders must have secure intercommunication among them to provide secure handover for devices on the move. Open challenges are, "how does a fog leader hand secure mobility and secure handover for devices on the move?", and "should a fog leader is also on the move, who is providing its secure mobility and secure handover".

Secure devices joining and leaving: The centralized cloud providing secure joining and leaving for the the huge number of devices in different layers cannot be sufficient for F2C systems, due to scalability issues. A hierarchical strategy can be useful to be applied here, such as, cloud can manage secure joining and leaving of fog leaders, and in parallel, each fog leader can control secure joining and leaving of devices in its area. On the other hand, in the F2C system, fog leaders should have secure intercommunication among them to provide secure devices joining in another area in case of mobility.

Secure discovery and allocation: All resources, services, and devices must be discovered in a secure way. Services must be allocated to resources, previously authenticated. Hence, different challenges arise: "how can services and devices be discovered in an authenticated secured way in the hierarchical F2C system?", "how can services be allocated to the corresponding authenticated resources securely?", "are fog leaders getting responsibility for securely discovering devices and allocating services to authenticated resources in a distributed fashion?", considering the different technologies such as Wi-Fi, zigbee, bluetooth, etc. "which strategy can be applied in the F2C system to provide secure discovery for all mentioned technologies?" According to these challenges, "can a strategy for resource and service discovery, as well as allocation in a secure hierarchical authenticated fashion be re-designed for the combined F2C system?" With this idea, fog leaders can get authorization to provide distributed secure resources discovery.

To tackle all the questions and challenges mentioned above, proper security threats analysis must be done for the F2C system. Our proposal is then, to re-design a hierarchical distributed security architecture for the combined F2C sytem, able to provide all the precious identified security.

Table. 2. Main security challenges for F2C-like scenarios

Security Area	Challenge	Description
Trust & Authentication	Trust Authentication Key management Identity management	Authentication is mandatory to prevent unauthorized users to access the system. The authentication mechanism needs identity or certificate to be verified and give users authorization to be involved into the system. Trust can be established between components after their authentication. Trust is one of the key component for establishing security between distributed fog nodes. Then, keys for encryption and decryption process can be distributed for components. Both Keys and identities need to be generated as unique, updated, and revoked during attacks, therefore, in F2C system handling key and identity management are the bottleneck due to hierarchical nature and huge number of distributed low-computational IoT devices. For Authentication and establishing trust, the traditional cloud as centralize point cannot be sufficient in F2C system due to distrusted nature. Therefore, as the main challenge here, trust and authentication must be redesigned to be handled in F2C system in hierarchical and distrusted way.
Access Control & Detection	Access Control Intrusion detection mechanism Malicious IoT and fog device detection	Access control is used to put rules that who and what can access the resources. In the case, the unauthorized users access the resources, intrusion and malicious device detection is needed. In case of access control and intrusion detection, handling the huge number of distributed IoT devices and fog nodes is one the main challenge in F2C security. Therefore, a need rises to re-design access control and intrusion detection in distributed way to be handled in F2C system
Privacy & Sharing	Privacy Secure sharing computation and environment	Privacy means that all the user's private information should not be disclosed to the others. In F2C system, fog nodes in hierarchical way would share their resources to users and IoT devices with low-computational power to run services. In this case, one of critical issues is how to handle user's, IoT devices', and Fog device's privacy in hierarchical F2C system without disclosing any critical information about each one of them to each other or even others.

End-to-end Security	Network security Quality of Service Heterogeneity Secure visualization Monitoring Centralized vs distributed security management Secure devices bootstrapping	Providing secure end-to-end communication between all components in a F2C system is one the challengeable issue due to different network protocols, huge amount on distributed devices at the edge of the network, and hierarchical F2C architecture. To provide secure communications, initially each one of the participant devices in F2C system must bootstrap in secure way. Fog nodes can be host virtualization environment to run the services, therefore, secure virtualization is a must at fog layers. All the secure communications must be monitored to detect any abnormal or malicious activities. All fog and cloud providers must set agreement to provide secure communications between their components in F2C system. At the end, a most challengeable secure communication issue is to design a new distributed security architecture to handle end-to-end security with less impact on the Quality of service.
Mobility support	Secure mobility Secure devices joining and leaving Secure discovery and allocation	In the F2C system, devices such as IoT devices, mobiles, cars, etc. are dynamic. The devices are on the move. All devices arrive to the fog nodes must be securely discovered. A device joining in F2C system for the first time and even the existing device join the fog area must be done in secure way. Then, a securely leaving fog area to join another area must be considering as well. The most challengeable secure mobility issues are using cloud as single point of failure and even bring scalability issues. In hierarchical F2C system, a new distributed security must be design to handle device discovery, joining and leaving, mobility, and handover in secure way.

4 Remarkable Current Efforts and Trends

Certainly, there are many contributions dealing with security provisioning at cloud and recently many contributions came up focusing on the fog arena as well. Undoubtedly, the scenario brought in by combining cloud and fog (also including devices at the edge) poses several challenges not well covered by current solutions for either fog or cloud. However, any potential solution in the area of security must not start from scratch but

learnt for past efforts in similar fields, what obviously includes efforts in cloud and fog. It is not the aim of this paper to go deep into these efforts but rather to highlight initiatives working on such a combined scenario and also other notable efforts pretty close to the F2C scenario, as briefly illustrated next.

There are two main ongoing efforts very aligned to the combined fog and cloud concept. The OpenFog Consortium (OFC) [8] aims to provide security by embedding hardware Root of Trust (HWRT) on the fog nodes. The HWRT can be programmed either when configuring (at the factory) or when booting. According to OFC expectations this module guarantees security against data breaches, spoofing, and hacking by providing secure identification, secure key store, protected operations, secure boot, etc. Another ongoing initiative is the mF2C project [9], yet in an early stage, theta proposes the use of distributed smart gateways (following a software approach) to ease the distribution of credentials and certificates. Thus, when a device enters an mF2C area for the first time, the device uses the smart gateway to connect to the certificate authority (CA) and gets credentials and certificate. Then, the device can establish secure and authenticated communication with the fog leader in that area, hence protecting users against man-in-the-middle attack, spoofing, etc.

Among other references found in the literature not linked to wide ongoing projects or initiatives, we may emphasize the work in [15] proposing end-to-end security mobility-aware for IoT-cloud systems using fog computing. In this work, smart gateways (Fog layer) provide device-users-cloud authentication and authorization remotely by using certificate-based data transport layer security (DTLS) handshakes. The end-to-end security between end users and devices is provided based on session resumption, and finally a robust secure mobility is implemented by secure inter-connection between smart gateways (Fogs). The solution proposal provides confidentiality, integrity, mutual authentication, forward security, scalability and reliability.

Similarly, authors in [16] propose a new security architecture for combined F2C systems, leveraging the use of a centralized F2C controller deployed at cloud and several distributed security control-area-units (CAUs) deployed at the edge of the network (fog layers) in different areas. Authentication and authorization procedures are defined to improve security guarantees.

5 Conclusion

This paper aims at highlighting the need to devote more efforts to sort out the large set of security concerns inherent to scenarios combining IoT, fog and cloud paradigms. In fact, this combined scenario brings together the different security challenges inherent to any of each paradigm, setting a complex setting demanding a comprehensive solution for security provisioning to guarantee the expected benefits brought in to run apps and services.

The paper introduces security requirements tailored to combined F2C-like systems, also analyzing what most sensitive attacks may be and ends up listing the. Main security challenges a F2C-like system must deal with to become a reality.

Acknowledgements

This work is supported by the H2020 projects mF2C (730929). It is also supported by the Spanish Ministry of Economy and Competitiveness and the European Regional Development Fund both under contract RTI2018-094532-B-100.

References

1. Ala Al-Fuqaha, et al., Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEEE Communications Surveys & Tutorials.
2. Kwang-Cheng Chen, Shao-Yu Lien, Machine-to-machine communications: Technologies and challenges, Ad Hoc Networks, Elsevier 2014.
3. J.Gonzalez-Martinez, et al., Cloud computing and education: A state-ofthe-art survey, Computers & Education 80 (2015) 132-151, 2014.
4. F. Bonomi, et al., Fog Computing: A Platform for Internet of Things and Analytics, Big Data and Internet of Things: A Roadmap for Smart Environments Vol. 546 of Studies in Computational Intelligence 2014.
5. E.Marín-Tordera, et al., "Do we all really know what a Fog Node is? Current trends towards an open definition", Computer Communications (2017).
6. H.Gupta, et al. "SDFog: A Software Defined Computing Architecture for QoS Aware Service Orchestration over Edge Devices", https://arxiv.org/pdf/1609.01190.pdf , [Accessed: September 2018]
7. T. Coughlin, "Convergence Through the Cloud-to-Thing Consortium," IEEE Consumer Electronics Magazine, vol.6, no.3, pp. 14-17, 2017.
8. The OpenFog Consortium at https://www.openfogconsortium.org, [Accessed: April 2018]
9. mF2C project at http://www.mf2c-project.eu [Accessed: April 2018]
10. X. Masip-Bruin, et al., Foggy Clouds and Cloudy Fogs: A Real Need for Coordinated Management of Fog-to-Cloud Computing Systems. In IEEE Wireless Communications, 23(5), 120-128, October 2016.
11. S.Irwan, Redesigning security for fog computing with blockchain", https://www.openfogconsortium.org/redesigning-security-for-fog-computing-with-blockchain/ [accessed November 2018]
12. J.Ni, et al., Securing Fog Computing for Internet of Things Applications: Challenges and Solutions, IEEE Communications Surveys & Tutorials (2017).
13. B.A.Martin, et al., OpenFog security Requirements and Approaches, Fog world congress 2017.
14. Alejandro Gomez, et al., A Resource Identity Management Strategy for Combined Fog-to-Cloud Systems, IoT-SoS (2018).
15. SR Moosavi, et. al, "End-to-end security scheme for mobility enabled healthcare Internet of Things," Future Generation Computer Systems, 2016.
16. S.Kahvazadeh, et, al., Securing combined Fog-to-Cloud system Through SDN Approach, Crosscloud (2017).