Allowing Privacy-Preserving Fog Computing with Digital Identity Assurance in Remote Clinical Services

Francesco Buccafurri

DIIES Department,
University of Reggio Calabria,
Reggio Calabria, Italy
E-mail: bucca@unirc.it

Gianluca Lax

DIIES Department,
University of Reggio Calabria,
Reggio Calabria, Italy
E-mail: lax@unirc.it

Antonia Russo

DIIES Department,
University of Reggio Calabria,
Reggio Calabria, Italy
E-mail: antonia.russo@unirc.it

Abstract: Nowadays, there is an increasing demand for cloud-based remote clinical services, both for diagnosis and monitoring. The COVID-19 pandemic has dramatically amplified this need. E-government programs should quickly go towards the expansion of this type of services, also to avoid that people (especially elderly) renounce treatment or adequate health care. However, to be effective, latency between IoT medical devices and the cloud should be reduced as much as possible. For this reason, fog computing appears the best approach, as part of the elaboration is moved closer to the user. However, some privacy threats arise. Indeed, these services can be delivered only based on secure digital identity and authentication systems, but the intermediate fog layer should learn nothing about the identity of users and the link among different service requests. In this paper, we propose a concrete solution to the above issue by leveraging eIDAS-compliant digital identity and by including a cryptographic protocol to provide anonymity and unlinkability of user's access to fog servers.

Keywords: e-health; eIDAS; remote patient monitoring; unlinkability.

Reference to this paper should be made as follows: XXX, *International Journal of Metadata, Semantics and Ontologies*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes:
Francesco Buccafurri is a full professor of computer science at the University Mediterranea of Reggio Calabria, Italy. In 1995, he received the PhD degree in computer science from the University of Calabria. His research interests include cybersecurity and privacy, social networks, deductive-databases, knowledge-

representation and non-monotonic reasoning, model checking, data compression, data streams, agents, P2P systems. He has published more than 160 papers in top-level international journals and conference proceedings. He is Associate Editor of Information Sciences (Elsevier) and IEEE Transaction on Industrial Informatics.
Gianluca Lax is an associate professor of computer science at the University Mediterranea of Reggio Calabria, Italy. In 2005, he received the PhD in computer science from the University of Calabria. In 2018, he got the habilitation as full professor of computer science by the Italian National Scientific Qualification Procedure. His research interests include information security and social network analysis. He is an author of more than 130 papers published in leading international journals and conference proceedings.
Antonia Russo is PhD student in computer science at the University Mediterranea of Reggio Calabria. In 2018, she received the MsC Degree in Telecommunication Engineering from the University Mediterranea of Reggio Calabria. Her research interests include security, privacy, and social network analysis.

1 Introduction

The use of information technology and communication to improve the delivery of information and services to citizens is one of the main goals of e-government. *Remote clinical services*, which consist in the digital transmission of medical information for remote medical diagnosis and monitoring, are assuming a very important role, also due to the increasing need determined by the COVID-19 pandemic (Durgadevi & Kalpana, 2020; Koti et al., 2020). This claim is widely recognized, even just by referring to *remote patient monitoring*, which allows continuous, real-time, non-invasive monitoring through wearable devices that wirelessly transmit patient information to a healthcare entity.

Therefore, e-government programs should devote a lot of resources to the development of these services, which give considerable benefits to public health, also beyond the emergency we are living.

Large-scale services, especially those requiring a certain server-side computational load, must be thought of as services provided under the cloud paradigm. For massive and ubiquitous remote clinical services, it would be anachronistic not to use this approach, because a traditional client-server solution does not scale (Abraham et al., 2020).

Moreover, cloud-based solutions give many other advantages: the reduction of the size of data centers, the dynamic adaptation of power computation for peak times and low-use times, the improvement of worker collaboration by allowing dispersed groups of people to meet virtually and share information in real-time, the availability of data and applications independently of the part of the world where a worker is.

However, in the case of remote clinical services, there is a specific issue to consider. Indeed, the latency between IoT medical devices and providers is critical. Therefore, standard cloud-based architectures are not the best solutions.

To overcome this issue, fog computing has been proposed (Bonomi et al., 2012): it extends the cloud close to the device that produces or generates the data, exploiting its network connection, storage, and computing features. In this case, the device is known as a *fog server*, and examples include switches, routers, cameras. The literature has shown that fog computing is the most promising solution to reduce latency without renouncing to the cloud paradigm (Gharami et al., 2019; Yousefpour et al., 2019; Naeem et al., 2019; Mahmud et al., 2018): indeed, this approach allows a user to communicate only with the closest

fog server, which queries the cloud only when this is necessary. Moreover, by designing a suitable scheme for moving user's requests from a fog server to another fog server when a user moves, we can enhance the user's mobility (Luan et al., 2015). In fact, mobility is another important feature to take into account in our application setting.

Besides the numerous advantages such as efficiency, low-latency, resource-load optimization among others, some security issues should be considered in the context of e-health, especially remote clinical services (Khan et al., 2017). For this reason, the provision of services should be done by adopting strict security measures, among which the user's identification with a high level of assurance. Therefore, strong mechanisms to manage digital identities and authentication should be used by the cloud provider. However, in a solution adhering to the fog computing paradigm, there is an intermediate layer to consider, also from the security and privacy point of view. Indeed, the layer between the cloud and user introduced by fog computing belongs to third parties that should be not aware of the real-life identity of users as well as the content of their interactions with the provider, even though users have to be authenticated by fog server to allow service delivery (Braeken, 2018; Ibrahim, 2016; Buccafurri et al., 2019). Also, the possibility for a fog server to link different (even anonymous) interactions would be an intolerable privacy leakage.

In this paper, we provide a solution to the above trade-off by proposing a fog-computing-based approach for remote clinical services, which guarantees the security level and the technological features introduced by the eIDAS Regulation (Mocanu et al., 2019) for the identification and authentication of users. Indeed, this approach can solve the security issues related to the access to a service relying on fog computing (Salis et al., 2019). The privacy threats introduced from the fog middleware are contrasted by using a cryptographic protocol that supports anonymity and unlinkability while ensuring strong authentication.

The solution presented in this paper takes origin from the proposal given by Buccafurri et al. (2019), which basically focuses on the security of the device authentication by allowing a device to be authenticated by a fog server without sharing any secret and using the same credential for any fog server. However, the solution given by Buccafurri et al. (2019) is not secure in the adversarial model of honest-but-curious fog servers considered in this paper because the authentication with the fog server is based on the user identity. In fact, this paper overcomes the above drawbacks.

This paper is structured as follows. Fog computing and the state of the art are discussed in Section 2. In Section 3, we introduce some concepts that are the basis of our solution. In Section 4, we present the considered scenario and define the individuated security problems. The previous solution proposed by Buccafurri et al. (2019) is presented in 5. Its improvement, which represents the core of our contribution, is presented in Section 6. Section 7 is devoted to the security analysis of our proposal. Section 8 provides a specific use case to show the potentialities of our proposal. Finally, we draw our conclusion in Section 9.

2 The concept of Fog Computing and State of the Art

Cloud is migrating to the edge of the network, and the components of the network are aligning towards a virtualization infrastructure, called *fog computing*. Fog computing extends the cloud computing paradigm to the edge of the network and facilitates innovative applications and services for IoT devices (Bonomi et al., 2012). This emerging model provides the end-users with some advantages such as mobility, low latency, and location

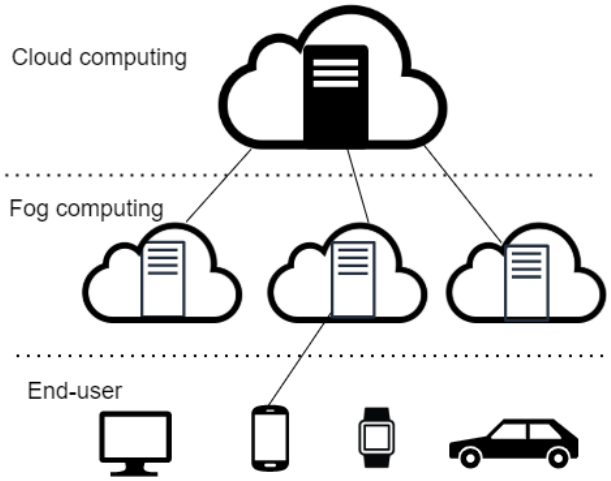

Figure 1 An example of Fog computing architecture.

awareness related to a widespread geographical distribution of nodes. These advantages are suitable for a wide number of applications in the fields of Smart Cities, Grid or Wireless Sensors, and Actuators Networks.

As mentioned above, fog computing cooperates with cloud computing. In Figure 1, it is represented a scheme of the three-layers infrastructure made of the cloud and fog computing, and the end-user.

Fog computing faces new security and privacy challenges besides those derived from cloud computing. Mukherjee et al. (2017) observe that the existing security and privacy measurements for cloud computing cannot be directly applied to fog computing due to its features. Indeed, the surveys (Khan et al., 2017; Yi et al., 2015b) individuate the security challenges and give the corresponding solutions about trust and authentication, network security, secure data storage in the fog computing technology. These papers face up different security areas and highlight the recommendation to take among main applications such as healthcare systems, vehicular networks and road safety, video stream processing.

In a fog computing application, the users' privacy has to be preserved: particularly, location privacy and usage pattern privacy are two very relevant issues. Although these two problems have been studied and addressed for various applications, the study (He et al., 2017) provides a solution to maintain the best possible delay and energy consumption performance, still considering the privacy protection of users.

Zhang et al. (2018) identify the access controls problems related to fog computing technology: users must be authorized by the cloud or the fog servers to access a resource or a service, and at the same time, fog servers and cloud need to be authenticated reciprocally. Access control models are presented to highlight their application and their aim of protecting user's privacy and ensure system security in an environment of fog computing.

Yi et al. (2015a) underline that the access of fog computing services and resources needs to be authenticated and authorized. The solution they provide is a prototype fog computing platform, evaluating users' privacy awareness in order to preserve them from some known attacks. Account hijacking is an attack based on social engineering, in which, after having stolen credentials, an attacker simulates the victim's behavior in the network. On the other

hand, considering the access to a fog server, the insider threat is a malicious threat (Stolfo et al., 2012) that involves an internal actor of an organization who could gain the network access with no fair intentions.

Fog computing applications are growing, and the requirements of fog platforms have to be diversified for the specific needs. The study (Ahmed et al., 2019) presents a representative collection of actual or proposed solutions based on the fog computing paradigm. By dividing the proposals into categories, the authors highlight the specific features that fog platform designers can follow during the development of the application.

Nowadays, the number of connected IoT devices is rising challenges into various sectors, such as healthcare, energy, smart cities, education. The presence of these different types of devices and technologies connected simultaneously raises some problems. A relevant aspect to be addressed is the security related to safe and reliable operations of IoT-connected devices. As Ramesh et al. (2017) suggest, identity-based cryptography (IBC) plays a promising role in IoT: a feasibility study of the applicability of IBC in IoT is proposed.

Yousefpour et al. (2019) propose some solutions to improve current security systems and protocols and aim at addressing security and privacy challenges in fog computing.

The authors of Salis et al. (2019) propose a smart hub to provide real-time information in a public environment, such as an airport, and based on fog computing. They analyze the security and privacy issues to provide users with good service. The eIDAS Regulation is taken into account as a possible option to carry out the registration at the system.

A lightweight privacy-preserving data aggregation scheme is proposed in (Lu et al., 2017). The authors demonstrate that this scheme is privacy-preserving and resistant to false data injection from external attacks. An approach against stolen-device attacks is proposed by Braeken (2018). A Physically Unclonable Function enables secure authentication and message exchange among the IoT devices, and the proposed scheme provides identity-based authentication and repudiation and achieves an efficient key agreement between two IoT devices connected to the same authentication server.

Fog computing presents many advantages (Stojmenovic & Wen, 2014) for different scenarios, such as smart traffic lights and connected vehicles or software-defined networks. The authors focus on a man-in-the-middle attack, in which gateways used as fog servers may be compromised or replaced by malicious ones. Indeed, the attacker takes control of gateways and even of victims' communications, and, then, exploits cascading vulnerabilities related to users and fog infrastructure.

Inside a platform that provides a carpooling service, users' sensitive information could be disclosed at the expense of their privacy. In order to address this issue, a solution based on fog computing is proposed by Li et al. (2018). Specifically, the authors highlight the privacy and security aspect of the solution: a private blockchain is used to store carpooling records. Platform users, such as passengers and drivers, perform anonymous authentication and encrypt data before transmission.

It is evident that fog computing and its security issues are relevant topics in the literature. To the best of our knowledge, the solution we propose is the first one (1) exploiting eIDAS-compliant digital identity for the identification and authentication, and (2) preserving privacy and unlikability of users among different fog servers.

3 Background

In this section, we recall some concepts related to our proposal, which are digital identity, eIDAS Regulation, and Public System for management of digital identity (Buccafurri et al., 2019).

A digital identity is the core information about an individual, organization, application, or device that exists online. This term also denotes aspects of civil and personal identity. Furthermore, the entire collection of the information generated by a person's online activity is linked to her/his digital identity.

The eIDAS Regulation (Electronic Identification Authentication and Signature) (Marina Kirova, 2019) aims to ensure full interoperability in Member States for electronic signatures, identification, and authentication services. Each Member State maintains its electronic identification systems, which have to be accepted by all other member states. The eIDAS Regulation gives European citizens the possibility to access online services of other EU countries (university services, banking, public administration services, other online services) using the same credential. All Member States have to notify one eID scheme to the European Commission, which is published in the Official Journal of the European Union. Estonia, for example, has already notified its eID scheme to the European Commission. Estonia has long-term experience in using electronic authentication, and in the technical document about the Estonian eID scheme (Estonian eID scheme: Digi-ID, 2018), the digital certificate of identity concept is highlighted and treated deeply.

In Italy, the Public System for management of digital identity, named SPID (SPID Sistema Pubblico di Identità Digitale, 2019), has been designed in compliance with eIDAS Regulation, and it allows access to online services of the Public Sector with a single credential set. A user can use SPID credentials for education, public administration services, health systems, and many other services. There is a high number of services enabled by SPID, and nowadays, they are growing in different online areas. In general, an eIDAS-compliant eID offers various advantages related to the secure cross-border authentication through different current eID schemes in Europe. The eIDAS key benefits are interoperability, also on the legal side, and security and trust, because of the validity of transactions made across borders.

4 Scenario and problem formulation

In this section, we present a general scenario and define the security problems our proposal solves.

Generally, fog servers can acquire and process data sent from authorized users: for example, if a user is near a fog server, she/he can decide to communicate with this server instead of the cloud. When a user moves from a fog server to another fog server, the service used by the user can be provided by the latter fog server after verifying the authorization of the user.

In the considered scenario, we can identify the following actors:

- Users, who are the owners of processed data.
- Users' devices, which are health devices, typically wearable, generating user data.
- Cloud servers, a group of computers connected over the Internet, providing storage and computing power available on-demand by users.

- Fog servers, a middle layer between the cloud and the users, enabling efficient data process. Fog servers do not know each other and could be untrusted.

- The Identity Provider, an entity that creates, maintains, and manages the user's identity information and provides an authentication service. Note that users can have different digital identities, for example, issued by different Identity Providers: this is encouraged to increase system resilience. Clearly, in the case of multiple identities, a user chooses the Identity Provider to use for authentication.

The problem we face is to strengthen classical solutions of fog computing by achieving the following objectives:

1. the solution should be resistant against stolen-device attacks, which occur when an adversary has the physical possession of the device of the victim so that device-based authentication can be performed successfully. For example, in the literature, there exist several solutions that exploit *Physical Unclonable Functions* (PUFs), which are low-cost primitive exploiting the unique random patterns in a device and are applied for secure key generation and key agreement (Braeken, 2018).

2. for privacy reasons, a fog server should not know the identity of the user exploiting the service;

3. again for privacy reasons, the unlinkability of the accesses of the user to the same fog server in different moments should be guaranteed.

5 Previous Solution and Improvements

In this section, we briefly describe the solution presented in (Buccafurri et al., 2019) on which our proposal is based. Figure 2 depicts the solution in the considered scenario. First, the user contacts fog server B (Step 1), and an Identity Provider is used for authentication: the user exploits her/his digital identity for authentication with fog server B. In particular, fog server B authenticates the user by an eIDAS-compliant scheme (Steps 2-4). If the user completed authentication, the Identity Provider ensures the user log-in and prepares a response that includes the assertion containing the user's authentication statement intended for the fog server. This response is returned to the user by the Identity Provider and forwarded to fog server B (Step 5), which verifies that the authentication succeeded. In the positive case, the user's data are moved from fog server A to fog server B. This operation consists of different phases: initially, the fog server B makes a data request to the cloud server (Step 6) which forwards this request to the fog server A (Step 7); then, fog server A transfers the user's data to the fog server B (Step 8), which communicates with fog users.

With regards to the three objectives defined in Section 4, we note that the proposal presented in (Buccafurri et al., 2019) reaches only the first objective (i.e., it is resistant against stolen-device attacks), but fails with respect to objectives 2 and 3. In this paper, we provide an improvement of (Buccafurri et al., 2019) by defining a technique that is able to guarantee users privacy by preventing fog server from knowing user's identity (objective 2) and from linking different accesses of the same user to the fog server (objective 3).

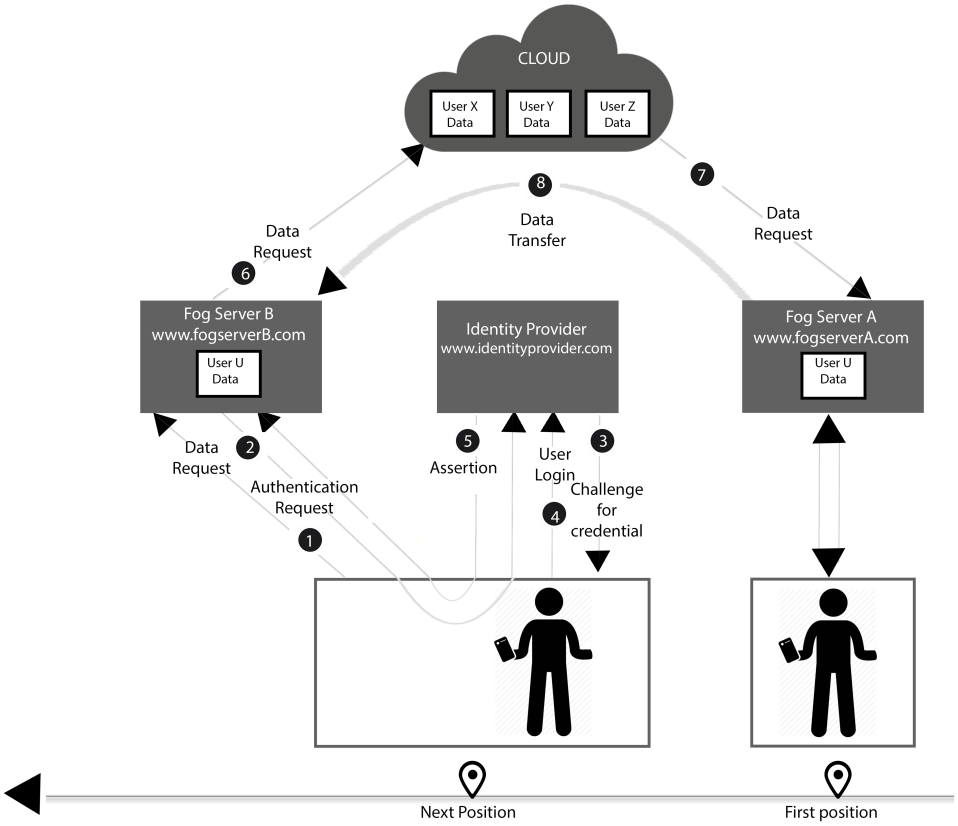

Figure 2 The solution presented in (Buccafurri et al., 2019).

6 Our Solution

In this section, we describe our proposal to improve the security of fog computing in a scenario of mobility and in which the users' privacy is considered a relevant issue. Although the chosen application setting is that of remote clinical services, in principle the solution can be considered from a more general point of view. As a matter of fact, no different real-life application setting mixes all the features that motivate our research.

The solution we present exploits *anonymous credentials*, which allow an entity to prove statements about itself and its relationships with other entities anonymously.

We suppose that users are provided with their public digital identity to perform the authentication by the cloud and fog servers in an eIDAS compliant scheme. Indeed, the user is provided with a pair of ⟨username, password⟩, and these credentials are used to access a service or a resource granted by service providers (cloud or fog server).

We introduce the notation used in the following. We define the set $F = \{f_0, \ldots, f_n\}$, where f_0 is the cloud and $f_1, \ldots, f_n$ are fog servers. Moreover, ID(f) denotes the identifier of the fog/cloud f.

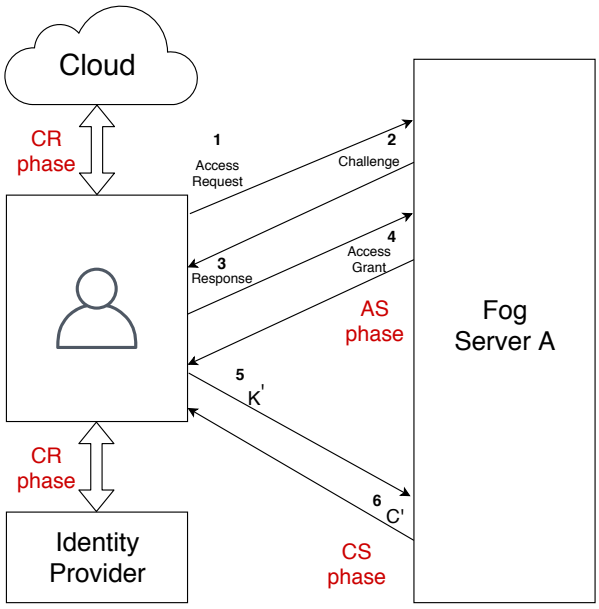

Figure 3 Data flow in our solution.

We define the element *(anonymous) credential* as $C = \langle ID$, exp_time, ID(f_o), ID(f_d), $C(f_o)$, K, $s\rangle$, where:

- ID is the identifier of the credential, which is usually derived from the timestamp of the issuing.
- exp_time (expiration time) is a determined date or time after which the credential should no longer be used. The validity of a credential is set on the basis of the specific application (so that it is not a core aspect in this paper).
- f_o and f_d are two distinct elements of the set F, which are said *(credential) origin fog* and *destination fog*, respectively.
- $C(f_o)$ is the certificate of the origin fog f_o. This field is optional and can be set to *null*.
- K is a public key.
- s is the signature of the credential.

Now, we are ready to present our proposal, whose phases are schematized in Figure 3 and described in the following:

Setup. This phase is carried out at the beginning. Here, the cloud generates a certificate, based on the standard X.509 (Cooper et al., 2008), for each fog server. A certificate is signed by the cloud and contains information about the fog server (such as its identifier) and the fog server's public key. Each fog server secretly stores the corresponding private

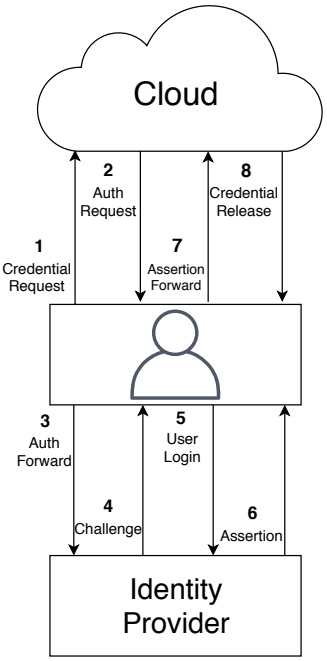

Figure 4 Credential release phase.

key. Observe that the cloud has a certificate too, which is self-signed and is known by all fog servers.

Moreover, users generate a digital identity by an Identity Provider. After verifying the user's data, the Identity Provider issues the digital identity and access information. The digital identity is a set of (personal) data containing at least the following attributes (according to the eIDAS scheme (eIDAS eID Profile, 2016)):

- a string PersonIdentifier, which is an identifier of the digital identity;
- a string FamilyName, the surname of the user;
- a string FirstName, the name(s) of the user;
- a date DateOfBirth, the date and year the user was born.

The user's access information is a pair ⟨username, password⟩ that the user will exploit to authenticate. In general, since there can be more Identity Providers, a user can be associated with one or more digital identities (for example, for redundancy reasons, in case one Identity Provider is not available).

CR. In this phase, said *Credential Release*, the user is authenticated by the cloud and receives an *(anonymous) credential* that will be used next. Specifically, the user exploits her/his digital identity for authentication with the cloud by an eIDAS-compliant identification scheme.

The operations carried out in this phase are detailed in Figure 4. First, the user contacts the cloud to request the credential (Step 1 of Figure 4); then, the cloud sends the user a request for authentication (Step 2), which is forwarded to the Identity Provider by the user's browser (Step 3). The Identity Provider verifies that the received request is valid (i.e., it is in the expected format and is signed by the sender), and starts a challenge authentication with the user. The user authenticates by the access information issued in phase Setup (Steps 4 and 5). If the user completed authentication, the Identity Provider prepares a response including an assertion, which is returned to the user by the Identity Provider (Step 6) and forwarded to the cloud (Step 7). In case of valid assertion, the user authentication successes (Step 8).

Now we explain how this credential is used. Suppose that the user needs to connect to the fog server f (because it is the closest one). A pair of asymmetric cryptographic keys (K_p, K_s) is generated: the private key K_s is known by the user, the public key K_p is also known by the cloud. Moreover, the cloud generates and releases to the user an anonymous credential in which $f_o = f_0$ (i.e., the origin fog f_o is the cloud f_0), $f_d = f$, $C(f_o)$ is null, $K = K_p$, and s is the signature of this credential done by the cloud.

AS. *Access to the Service*. Once the user has acquired a credential C, she/he can use it for authentication with a fog server, said f (e.g., the fog server A in Figure 3). First, the user sends a request to f that includes the credential C described above (Step 1 of Figure 3). Observe that the fog server cannot know the identity of the user from C, because no identifying information is included in C. The fog server f verifies the validity of C carrying out the next checks:

1. f extracts the public key of the credential signer f_o from the certificate $C(f_o)$. Observe that if $f_o = f_0$ (i.e., the certificate has been released by the cloud), the public key needed for the verification is extracted from the cloud certificate, which is publicly available. Then, f extracts the signature s and this signature is verified to guarantee the integrity and authenticity of the credential. In the positive case, the fog server keeps on the other checks.
2. The credential has a validity time, which, if expired, enforces the deny of the user request.
3. The fog server checks that the value of ID(f_d) in the credential is correct.
4. Each fog server maintains a list of already received credentials so that f checks that the value of the filed ID of C is not included in this list. Moreover, this ID is now added to this list.

After the validity of the credential is checked, f randomly generates a value x as a challenge, encrypts x by the public key K included in C, and transmits this information to the user (Step 2), who must return the initial value x, thus proving that she/he was able to decrypt the challenge (Step 3).

If all the above checks succeed, then the fog server accepts the user's request and grants the service (Step 4).

CS. *Credential Switch*. In a scenario of mobility, it may occur that while a fog server f_a is elaborating the user's data, the user moves from a point close to another fog server f_b. The user could exploit the current credential to request access to f_b. However, in

this case, the third issue described in Section 4 arises (i.e., we cannot guarantee the unlinkability of the accesses of the user). The phase credential switch is carried out by the user to solve this problem. Specifically, a new pair of asymmetric cryptographic keys (K'_p, K'_s) is generated, in which the private one K'_s is known only by the user (Step 5 in Figure 3). Then, f_a generates a new anonymous credential C' in which $f_o = f_a$, $f_d = f_b$, and $K = K'_p$ (Step 6). Now, the user has a new (different) credential and can exploit this credential to access f_b. Clearly, this credential is verified by the procedure described in phase AS. This way, the fog server f_a can authorize the user to access a service provided by another fog server f_b, without relying on the cloud.

By comparing our solution with the one described in Section 5, we observe that the number of eIDAS-based authentications is reduced since anonymous credentials are used instead of that authentication. Moreover, the use of anonymous credentials is more efficient (and less invasive) than eIDAS authentication, because no interaction with the user is needed.

7 Security analysis

In this section, we discuss the security of our solution. We start from our threat model: we assume that any fog server can be an honest-but-curious adversary (i.e., a legitimate participant in the system that not deviates from the defined protocol but attempts to learn all possible information from legitimately received messages (Liu, 2016; Yang et al., 2018)). We assume no collusion attack occurs (Gu et al., 2019): thus, we do not consider the possibility that two or more fog servers collude each other to break the security properties.

We observe that all messages and credentials exchanged by the parties are signed by the sender, which ensures their integrity and authenticity.

Concerning the Requirement 1 listed in Section 4 (i.e., robustness against stolen-device attack), we observe that the use of digital identity allows us to contrast stolen-device attacks because we implemented a two-factor authentication (Manzoor et al., 2019): indeed, users authenticate by something they know (eIDAS password) and something they have (the device).

The second security property requires that any fog server does not know the identity of the user using the service: this is guaranteed because the (anonymous) credential defined in Section 6 does not contain any personal information about the user. Only the cloud knows this information, and without the collusion with the cloud (as assumed in our threat model), no fog server can guess the user identity.

The third security property requires the unlinkability of the accesses of the user to the same fog server in different moments. Concerning this aspect, consider that the credential-switch phase is carried out to generate a sort of *authentication token*, which is used to access another fog server without the need to contact the cloud or to provide any identifying information. Moreover, since this token changes each time, users accesses are unlinkable, and no tracking of users is possible.

Observe that, after a phase Credential Switch having f_a as origin fog and f_b as destination fog, when the user accesses f_b, the latter might guess that the user comes from f_a. To avoid this, we allow other switches involving further fog servers. This way, the user introduces *obfuscation* in such a way that the above information (i.e., the fog server previously used by the user) cannot be guessed with certainty. An example is provided in Figure 5, where the user contacts the fog server f_c before accessing f_b in such a way to simulate to come from f_c instead of the actual fog server f_a.

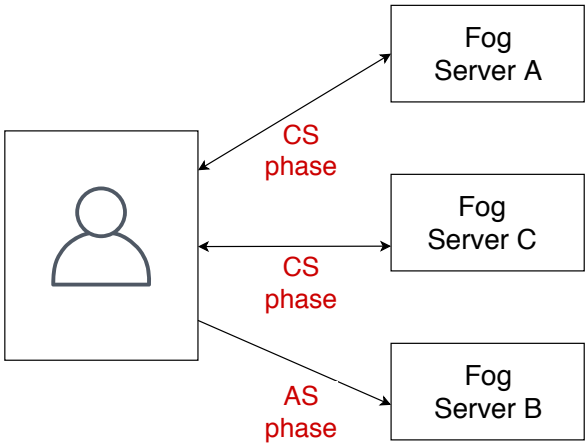

Figure 5 Credential switch phase.

Note that each fog server stores the credential received by a user to access the service. This is done to avoid that someone re-uses a credential before the expiration. Moreover, replay attacks are avoided because an adversary who eavesdrops or intercepts a credential cannot fraudulently use it to impersonate the user. Indeed, the adversary cannot respond to the challenge because she/he does not know the private key to be used to decrypt the challenge.

8 Use case

This section aims to help the reader to understand how our solution works through the description of a use case that is relevant from the application point of view.

Consider an e-health ecosystem: therein, patients are increasingly becoming central in healthcare, and the IoT technology can enable this process towards patient-centric healthcare. Fog computing is a strategic technology able to fulfill the requirements of computing, real-time interactions, data storage, and network connectivity for the IoT devices connected to the cloud. Furthermore, fog servers are closer than the cloud to the medical devices that produce data, thus reducing the latency and traffic towards the cloud (Kumari et al., 2018; Thota et al., 2018; Kraemer et al., 2017).

In this use case, fog servers process and filter personal e-health data. A user is provided with an IoT medical device used to monitor and analyze her/his heart rate. The device is wearable and has limited computation power and resources so that collected data should be sent directly to the cloud, which analyzes them and provides the user with the required results of the analysis. By adding the middle layer of fog computing, the elaboration of such data is carried out closer to the user. However, the adopted solution should offer the following features:

- for privacy reasons, a fog server should not know the identity of the user exploiting the service;

- again for privacy reasons, the unlinkability of the accesses of the user to the same fog server in different moments should be guaranteed.

The solution proposed in this paper guarantees these two characteristics. Indeed, users gain access to the fog server through anonymous credentials so that their identities are hidden to the fog server. The second feature to guarantee concerns unlinkability. We observe that in the protocol defined in our proposal, users who need to access a service contact various fog servers during the credential switch phase (see Figure 5). At the end of this phase, an anonymous credential is returned chosen among the credentials obtained by the fog servers. Moreover, users can collect as many anonymous credentials as they want; however, they use each credential only one time to avoid that reusing the same credential makes it possible to link their accesses and elaborated data.

9 Conclusion

Fog computing is an emerging topic and aims at extending the benefits of the cloud by improving its effectiveness and efficiency in providing mobile users with data and applications by exploiting the awareness of their location. However, moving data and applications from one fog server to another one raises several security and privacy problems. In this paper, we focused on two privacy issues: a fog server should not know the identity of the user, and it should be guaranteed the unlinkability of the accesses of the user to the same fog server in different moments.

We proposed a new approach to solve these problems, which exploits the authentication mechanism offered by the EU Regulation eIDAS, thus directly exploitable by all EU citizens. The use of digital identity allows us to contrast attacks of the type stolen-device as shown by Buccafurri et al. (2019), but in the new solution, the authentication is less expensive for the user thanks to the use of anonymous credentials. Moreover, anonymous credentials solve the problem that users do not want to be tracked by every fog server, which is an additional problem not solved by the state-of-the-art solutions.

The main implication of our study is related to the possibility of offering a solution for using fog computing in a way that is compliant with the GDPR principles, and, in particular, with the principle of data minimization, which limits data processing to only data that are necessary in relation to the purposes for which they are processed. Indeed, in many applications, knowing the identity of users or linking different accesses of the same user do not respect the data minimization principles. Thanks to the adoption of our proposal, a company can exploit the advantages of fog computing keeping the compliance with the GDPR.

Besides various advantages, a limitation of our proposal is that autonomous devices are not supported, because no user is present to carry out the eIDAS authentication.

As future work, we are studying how to design a similar and efficient fog server authentication mechanism in such a way that a user can authenticate the fog server that will receive her/his data: this is particularly important in the case of health data, which are sensitive information.

Acknowledgment

This paper has been partially supported by the project "Security Framework for IoT (SE.FR.IOT)" funded by POR Calabria FESR-FSE 2014-2020.

References

Abraham, A., Hörandner, F., Zefferer, T., & Zwattendorfer, B. (2020). E-government in the public cloud: Requirements and opportunities. *Electronic Government*, *16*.

Ahmed, A., Arkian, H., Battulga, D., Fahs, A. J., Farhadi, M., Giouroukis, D., Gougeon, A., Gutierrez, F. O., Pierre, G., Souza Jr, P. R. et al. (2019). Fog computing applications: Taxonomy and requirements. *arXiv preprint arXiv:1907.11621*, .

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13–16). ACM.

Braeken, A. (2018). Puf based authentication protocol for iot. *Symmetry*, *10*, 352.

Buccafurri, F., Lax, G., & Russo, A. (2019). Exploiting digital identity for mobility in fog computing. In *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 155–160). IEEE.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W. T. et al. (2008). Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile. *RFC*, *5280*, 1–151.

Durgadevi, M., & Kalpana, R. (2020). A cooperative ga-sm-based prediction model for healthcare services. *Electronic Government, an International Journal*, *16*, 7–24.

eIDAS eID Profile (2016). URL: `https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20Message%20Format_v1.1-2.pdf` online; accessed 17 August 2020.

Estonian eID scheme: Digi-ID (2018). URL: `https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Estonia`.

Gharami, S., Prabadevi, B., & Bhimnath, A. (2019). Semantic analysis-internet of things, study of past, present and future of iot. *Electronic Government, an International Journal*, *15*, 144–165.

Gu, K., Wu, N., Yin, B., & Jia, W. (2019). Secure data query framework for cloud and fog computing. *IEEE Transactions on Network and Service Management*, *17*, 332–345.

He, X., Liu, J., Jin, R., & Dai, H. (2017). Privacy-aware offloading in mobile-edge computing. In *GLOBECOM 2017-2017 IEEE Global Communications Conference* (pp. 1–6). IEEE.

Ibrahim, M. H. (2016). Octopus: An edge-fog mutual authentication scheme. *IJ Network Security*, *18*, 1089–1101.

Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*, *6*, 19.

Koti, P., Dhavachelvan, P., Kalaipriyan, T., Arjunan, S., Uthayakumar, J., & Sujatha, P. (2020). An efficient healthcare framework for kidney disease using hybrid harmony search algorithm. *Electronic Government, an International Journal*, *16*, 56–68.

Kraemer, F. A., Braten, A. E., Tamkittikhun, N., & Palma, D. (2017). Fog computing in healthcare–a review and discussion. *IEEE Access*, *5*, 9206–9222.

Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for healthcare 4.0 environment: Opportunities and challenges. *Computers & Electrical Engineering*, *72*, 1–13.

Li, M., Zhu, L., & Lin, X. (2018). Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet of Things Journal*, .

Liu, D. (2016). Efficient processing of encrypted data in honest-but-curious clouds. In *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)* (pp. 970–974). IEEE.

Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot. *IEEE Access*, *5*, 3302–3312.

Luan, T. H., Gao, L., Li, Z., Xiang, Y., Wei, G., & Sun, L. (2015). Fog computing: Focusing on mobile users at the edge. *arXiv preprint arXiv:1502.01815*, .

Mahmud, R., Kotagiri, R., & Buyya, R. (2018). Fog computing: A taxonomy, survey and future directions. In *Internet of everything* (pp. 103–130). Springer.

Manzoor, A., Shah, M. A., Khattak, H. A., Din, I. U., & Khan, M. K. (2019). Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges. *International Journal of Communication Systems*, (p. e4033).

Marina Kirova (2019). eIDAS Regulation (Regulation (EU) N°910/2014). `https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014`. Online; accessed 17-August-2020.

Mocanu, S., Chiriac, A. M., Popa, C., Dobrescu, R., & Saru, D. (2019). Identification and trust techniques compatible with eidas regulation. In *International Conference on Security and Privacy in New Computing Environments* (pp. 656–665). Springer.

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges. *IEEE Access*, *5*, 19293–19304.

Naeem, R. Z., Bashir, S., Amjad, M. F., Abbas, H., & Afzal, H. (2019). Fog computing in internet of things: Practical applications and future directions. *Peer-to-Peer Networking and Applications*, *12*, 1236–1262.

Ramesh, C., Rao, K. V. G., & Vasumathi, D. (2017). Comparative analysis of applications of identity-based cryptosystem in iot. *Electronic Government, an International Journal*, *13*, 314–323.

Salis, A., Jensen, J., Bulla, R., Mancini, G., & Cocco, P. (2019). Security and privacy management in a fog-to-cloud environment. In *European Conference on Parallel Processing* (pp. 99–111). Springer.

SPID Sistema Pubblico di Identità Digitale (2019). `https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014`. URL: `https://www.spid.gov.it/` online; accessed 17 August 2020.

Stojmenovic, I., & Wen, S. (2014). The fog computing paradigm: Scenarios and security issues. In *2014 Federated Conference on Computer Science and Information Systems* (pp. 1–8). IEEE.

Stolfo, S. J., Salem, M. B., & Keromytis, A. D. (2012). Fog computing: Mitigating insider data theft attacks in the cloud. In *2012 IEEE symposium on security and privacy workshops* (pp. 125–128). IEEE.

Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., & Priyan, M. (2018). Centralized fog computing security platform for iot and cloud in healthcare system. In *Fog computing: Breakthroughs in research and practice* (pp. 365–378). IGI global.

Yang, R., Xu, Q., Au, M. H., Yu, Z., Wang, H., & Zhou, L. (2018). Position based cryptography with location privacy: A step for fog computing. *Future Generation Computer Systems*, *78*, 799–806.

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015a). Fog computing: Platform and applications. In *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)* (pp. 73–78). IEEE.

Yi, S., Qin, Z., & Li, Q. (2015b). Security and privacy issues of fog computing: A survey. In *International conference on wireless algorithms, systems, and applications* (pp. 685–695). Springer.

Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., Kong, J., & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture*, *98*, 289–330.

Zhang, P., Liu, J. K., Yu, F. R., Sookhak, M., Au, M. H., & Luo, X. (2018). A survey on access control in fog computing. *IEEE Communications Magazine*, *56*, 144–149.