MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System

This is the post-print of the following article: C. Suraci, S. Pizzi, A. Molinaro, and G. Araniti, "MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3130666.
Article has been published in final form at: https://ieeexplore.ieee.org/document/9631948.

MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System

Chiara Suraci, Sara Pizzi, Antonella Molinaro, and Giuseppe Araniti

***Abstract*—The COVID-19 pandemic has changed the world. Today, the use of Information and Communications Technology (ICT) in support of education, medicine, business and administration has become a reality practically everywhere. In particular, the eHealth (digital Health) sector is on the cusp of a revolution, fueled by the worldwide health emergency due to the spread of the new coronavirus. With a view to developing new sixth generation (6G)-oriented architectures, advanced eHealth services like telemonitoring would benefit from the support of technologies that guarantee secure data access, ultra-low latency and very-high reliability targets, which are hardly achievable by the fifth generation (5G). This is the reason why this work proposes an eHealth system architecture, in which low-latency enabling technologies like Device-to-Device (D2D) communications and Multi-access Edge Computing (MEC) are integrated and supported by security mechanisms for an optimal management of sensitive health data collected by Internet of Medical Things (IoMT) devices. A preliminary evaluation of the proposed framework is provided that shows promising results in terms of data security and latency reduction.**

***Index Terms*—MEC, D2D, Security, 6G, eHealth.**

I. Introduction

We are in the midst of a global pandemic which is bringing forth the importance of Information and Communications Technology (ICT) in support of several fields. The worldwide emergency caused by the spread of COVID-19 has paved the way for the remote management of numerous services, including education, business and administration, and health, and caught the eye of the researchers working for the development of pioneering solutions useful, for example, to the detection of Coronavirus disease [1]. Health is identified as one of the key addressed verticals of the upcoming sixth generation (6G) networks, especially due to the booming average age of the population and to the sharply increasing number of chronic patients that especially challenge the healthcare system. The design of new architectures and the careful management of security and privacy issues are mandatory for the provisioning of advanced healthcare services in future 6G systems [2]. Similarly, eHealth (digital Health) is listed as one of the key 6G use cases [3] that may benefit in terms of Quality of Service (QoS), reliability, latency, and mobility robustness from the 6G enabling technologies. They include some paradigms already emerged with the fifth generation (5G) but not yet commercially available, which then fall into the category of *evolutionary technologies* and differ from *revolutionary technologies*. Among the evolutionary ones are the Multi-access Edge Computing (MEC) and the Device-to-Device (D2D) communications.

Authors are with University Mediterranea of Reggio Calabria, and CNIT, Italy, e-mail: [chiara.suraci,sara.pizzi,antonella.molinaro,araniti]@unirc.it.

A. Related work

The provision of cloud services represents an increasingly decisive factor in the evolution of mobile networks towards 6G systems. Authors of [4] discuss that 6G will be pivotal in fostering a push towards edge computing paradigms able to significantly reduce latency and increase capacity, which are key performance indicators (KPIs) also for 6G like they were for 5G. MEC is a distributed cloud paradigm that came into the 5G picture for its capability to bring closer to users the storage, computation, and network resources to be provided. It can offer a wide range of beneficial properties, especially useful to the eHealth sector, notably *(i)* providing additional storage space to devices that need it, especially critical for memory-constrained Internet of Medical Things (IoMT) devices; *(ii)* reducing latency in data processing by leveraging proximity to the consumers to satisfy the stringent requirements of applications like patient telemonitoring; *(iii)* offloading the workload on resources-constrained devices (such as wearables) by performing computationally complex operations; *(iv)* offering context-awareness information (e.g., patients-related information) in order to foster the elaboration of personalized treatments based on the actual needs of the patients.

In order to reduce communication latency, the D2D paradigm represents a further interesting solution since it allows devices in mutual proximity to communicate directly without going through the base station. This direct D2D link is also known as sidelink. Communicating without the control of the base station requires special care in the protection with security mechanisms designed to deal with attacks to which it is vulnerable; for example, an architecture including secure sidelinks for the transmission of protected data in direct communications between Internet of Things (IoT) devices is presented in [5]. The security issue is crucial for D2D paradigm as highlighted, for example, in [6].

Wireless networks will be increasingly probed in everyday life, therefore privacy issues related to the pervasiveness of the technology in different aspects of society will be much more cumbersome in the 6G era. The security requirement falls within the KPIs of 6G services [7], therefore it is of prominent importance for the 6G design process, as also demonstrated by the massive presence in the literature of works that describe innovative and secure 6G systems (e.g., [8]). Especially with

a view to providing 6G healthcare services, the protection of data transmitted by IoMT devices is essential, given the sensitivity of the data and the vulnerability of the wireless medium [9].

In light of the above, cloud (meant as MEC), D2D, and security can be seen as well-suited solutions to be exploited for the management of eHealth services that require low latency and high reliability in 6G. The most relevant works in the literature providing security solutions for cloud-based healthcare systems are outlined in Table I; for each paper, the presence or absence of a proposal that includes MEC and/or D2D and/or security mechanisms is highlighted. To the best of our knowledge, the ability of D2D to improve the transmission of health data from the collecting sensors to relay nodes, specially deployed also for forwarding the gathered information to the base station, is not exploited enough in the literature as well as the secure management of health data transmitted and stored on MEC servers.

B. Contribution of this work

In line with the related work, we introduce a hierarchical architecture for the delivery of eHealth services in 6G-oriented networks, which is characterized by the integration of *D2D* communications, *MEC* technology, and customized *security* mechanisms. Specifically, a pragmatic approach has been followed in this work that has been oriented to the realization of an architecture adaptable to the management of different eHealth services. The novelty of our work can be outlined in the following main contributions:

- A 6G-oriented eHealth system is proposed that includes a novel hierarchical architecture featuring data sensing, processing and storage capabilities, and groundbreaking security-by-design mechanisms for the protection of sensitive health information and of the privacy of involved people, devices, and data.
- The Sensing functionality is executed by IoT devices deployed for the collection of medical data, therefore classifiable as IoMT, which are organized in clusters. The data collected by each sensor is sent to the controller of the belonging cluster via D2D communications.
- The Processing role is played by the cluster controller (CC) nodes that receive data from the sensors via D2D communications and either forward them directly to the MEC server or send the obtained information after a simple data processing.
- The Storage of information sent by the controllers is delegated to MEC servers located in the base stations of the 6G networks. One of the 6G-oriented features of the introduced architecture consists in the lightening of the workload on MEC servers which in 6G could be increasingly congested [17]. To this aim, the CC nodes can perform simple processing on the data received from the sensing devices, sending only the necessary data and delegating the complex operations to the MEC servers.
- D2D is leveraged in the data delivery from IoMT devices to controllers in order to reduce latency.
- As regards the security assurance, a primary requirement is faced that is the authentication of devices involved in the D2D communications. In order to obtain mutual authentication between the resource-constrained IoMT nodes and the controllers in charge of receiving data from them, an innovative lightweight protocol is proposed in this work, which generates a fake identity for each device running it in order to hide its real identity, thus also protecting its privacy. Furthermore, possible security measures are proposed for the management of the multi-tenancy of the target scenarios.
- A simulation campaign is carried out to demonstrate the ability of our proposal to provide a secure and lightweight solution for the support of eHealth services, specifically addressing message authentication, identity privacy protection, mutual authentication, resistance to replay and man-in-the-middle attacks. Our proposal shows good performance thanks to a prompt detection of any attacks against the CC node.

The paper is organized as follows. The presented architecture is thoroughly discussed in Section II. The steps of the presented authentication procedure are deeply described in Section III, where security measures for multi-tenancy are also proposed. Results are discussed in Section IV. Conclusions are drawn in the last Section.

II. The proposed architecture to support 6G eHealth Systems

A secure MEC-based architecture for the D2D-aided collection of health data coming from low-end IoMT devices is proposed in this work. The security and privacy issues, which arise from the transmission and storage of highly sensitive health data, are addressed by design and an innovative solution for the fulfilment of the mutual authentication requirement between D2D communicating devices is proposed.

Two examples of aimed use cases are caring-at-home and caring-at-hospital for which the IoMT devices can be deployed in the collection of health data useful for the telemonitoring of patients who are at home or of those hospitalized in intensive care, in order to minimize contacts between patients and medical staff. These applications consist in the adoption of advanced sensors both inside and on the body of the patient, for the real-time control of his medical condition, therefore they require a low-latency, ubiquitous, tailored, and secure system which can be realized by means of the 6G technology [2]. The inconvenience caused by the spread of the COVID-19 to the worldwide health systems has highlighted the insufficient adequacy of current technologies to guarantee the requirements demanded by eHealth services. Therefore, the improvement in terms of QoS expected with the 6G deployment could enable an effective and wide management of eHealth services around the world. Regarding the 6G technologies applied in our proposal, a significant latency reduction can be obtained thanks to the establishment of D2D communications for the health data transmission, which can be really useful to ensure greater promptness in accessing the necessary care; the context-awareness provided by the MEC servers can improve the completeness of the patients-related information and can foster the elaboration of a personalized

TABLE I
RELATED WORK ON CLOUD-BASED SOLUTIONS FOR E-HEALTH.

Reference	Topic	MEC	D2D	Security
[10]	A fine-grained searchable encryption scheme is presented where a blockchain network is leveraged to execute computationally intensive tasks of a typical attribute-based searchable encryption (ABSE) scheme.	✗	✗	✓
[11]	A Cloud-centric IoMT solution is developed supported by security mechanisms and a D2D protocol for smart healthcare.	✗	✓	✓
[12]	The proposal of this work concerns an eHealth system improved by the implementation of D2D communications, to accelerate the transmission of health data, and the support of a mutual authentication protocol.	✗	✓	✓
[13]	A MEC-based hierarchical architecture is proposed for tracking the COVID-19 pandemic which includes the IoT end device, the edge, and the cloud levels and a user front-end.	✓	✗	✗
[14]	A system which combines 5G, MEC, and Artificial Intelligence is presented for remote health monitoring, data analysis, and high-quality data transmission.	✓	✗	✗
[15]	A Lightweight Privacy-preserving Medical diagnosis in Edge computing is introduced in order to offer timely and secure diagnosis to users who submit their requests to the edge.	✓	✗	✓
[16]	Authors face some issues related to clinical decision support systems by proposing a solution which integrates MEC and Software-Defined Networking (SDN) technologies. Furthermore they rely on homomorphic encryption mechanisms to protect the privacy of medical information.	✓	✗	✓

treatment based on the actual needs of the patient; the execution of the proposed security protocol can guarantee the protection of extremely sensitive health data thanks to the achievement of mutual authentication between the devices exchanging medical data through the implementation of light operations, easily performable by the resource-constrained IoMT devices deployed for data collection.

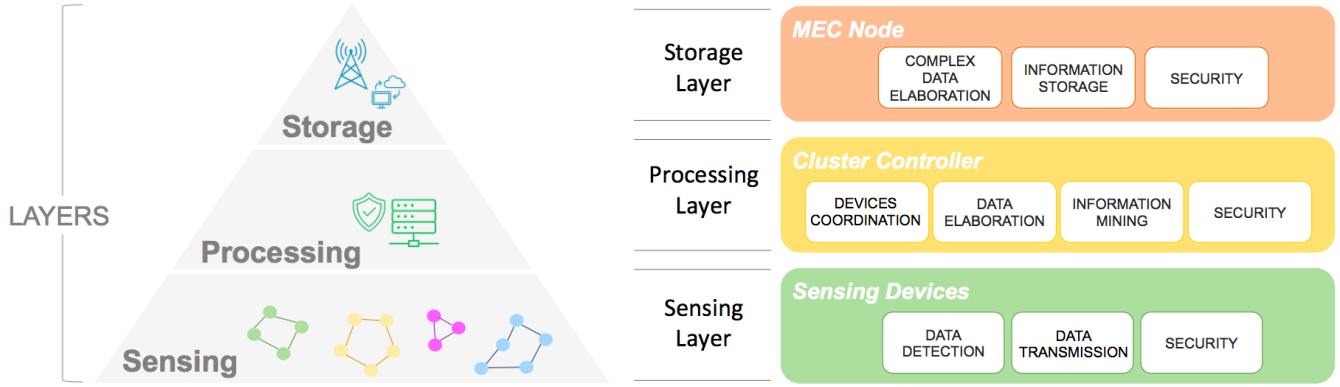
Fig. 1 shows the hierarchical eHealth system that represents the main novelty of our work. In Fig. 1a the three layers that compose the proposed architecture are depicted at a high level, only showing the major functionality of each one, i.e., Sensing, Processing, and Storage. In Fig. 1b the functional components of the three layers are illustrated, each with corresponding block of executable operations. In particular, the Sensing Devices are the functional component of the Sensing layer since they execute Data Detection, Data Transmission, and Security operations; the Cluster Controller (or CC node) performs Devices Coordination, Data Elaboration, Information Mining, and Security management in the Processing layer; finally, the MEC node is the functional component of the Storage layer, being it in charge of carrying out Complex Data Elaboration, Information Storage, and Security supervision.

Hereinafter, more details are provided on the three layers of the proposed architecture, on the related functional components, and on the operations executed by each.

1) Sensing: The lowest level is that of Sensing, consisting of the IoMT devices deployed for the health data (e.g., blood pressure, blood oxygen saturation, heartbeat) detection and organized in clusters, then divided into groups based on a specific criterion. In the case of the telemonitoring service identified as target application, all the sensors monitoring the same patient may be grouped in a cluster (*Data Detection*). The measured data are sent from the devices to the CC node via D2D communications, enabled by the proximity between the IoMT devices and the CC node (*Data Transmission*).

2) Processing: Each cluster is managed by a CC node, deployed with the aim of reducing the workload on low-end IoMT devices, but also of lightening the tasks executed by the MEC servers. The CC nodes are not mere IoT gateways as they may be either ad-hoc-created or existing devices in use by the patient, which must be equipped with a SIM card and a software capable of executing the main functions of controlling the activity of the IoMT devices and forwarding the information obtained from the Sensing layer. Therefore, the controller represents a *Broker* in the interaction between MEC server and IoMT devices, and a "smart leader" for the latter. In fact, similar to a SDN solution, the controller represents the software and smart component of the cluster, in charge of instructing sensing devices on the operations to carry out and the modalities to be engaged (e.g., it communicates the timing of data collection). In addition, it collects the data obtained within its own cluster and extracts information from it, then transmitting data or information to the MEC server by acting as a relay node. For example, let us consider using a smart-oximeter on a patient: the CC node instructs the oximeter on the time intervals that must elapse between one measurement and another (*Devices Coordination*); once the controller receives the data coming from the oximeter, it can process and translate it into information useful for monitoring the patient (*Data Elaboration*); hence, the controller can perceive if an anomalous value has been detected (*Information Mining*).

3) Storage: The MEC node represents the highest level of the proposed architecture and is located in the base station. Its main function concerns the storing of information obtained from the controllers (*Information Storage*). This is an eHealth-oriented benefit offered by the proposed architecture as data, being stored in the edge, are accessible with low latency. Besides, MEC can be delegated by a CC node to perform a



(a) Layers (b) Functional Components

Fig. 1. The proposed hierarchical eHealth system architecture.

particularly computationally complex data processing (*Complex Data Elaboration*). Thanks to its strategic position, the MEC node enables two additional features: *(i)* it can collect context-awareness information; *(ii)* it can offer the possibility of quickly implementing the service models characteristic of cloud computing environments, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). For example, the Mobile Network Operator (MNO) managing the MEC server could offer a platform to software developers working for an hospital; or even, the MNO itself could develop applications useful for identifying COVID-19 or for its tracking as off-the-shelf solutions for interested Tenants.

III. Introduced Security Measures

A *Security* functional block is present in each layer of the proposed architecture as security is one the foremost requirements in the management of health data. Particularly, before establishing data transmission, IoMT devices (i.e., sensors) and controllers must accomplish an *authentication procedure* in which the MEC node is involved as a supervisor and trusted third party; in addition, the controllers should also cater for the *encryption* of data and information transmitted to the MEC node. As part of the novelty of this work, an innovative mutual authentication protocol is presented in the following.

1) A lightweight mutual authentication procedure: In order to ensure security within each cluster, sensors have to be certain of the identity and genuineness of the CC node towards which they send data and, vice versa, it is of paramount importance that only authorized devices transmit data to the controller. For this purpose, we propose LiMAD, a Lightweight Mutual Authentication procedure for D2D communications, suited to the constrained nature of IoMT sensing devices and aimed at protecting the data exchanged in D2D communications towards the CC nodes. The flow of the operations performed in the proposed LiMAD is shown in Fig. 2 and detailed in the following; used notations are listed in Table II.

Starting with the first group of operations ($GO()$), the MEC node receives the identity (ID) (e.g., the SIM serial number) both from the sensor i and the CC node j via secure channels. Then, it generates: *(i)* a secret random number sn_i associated

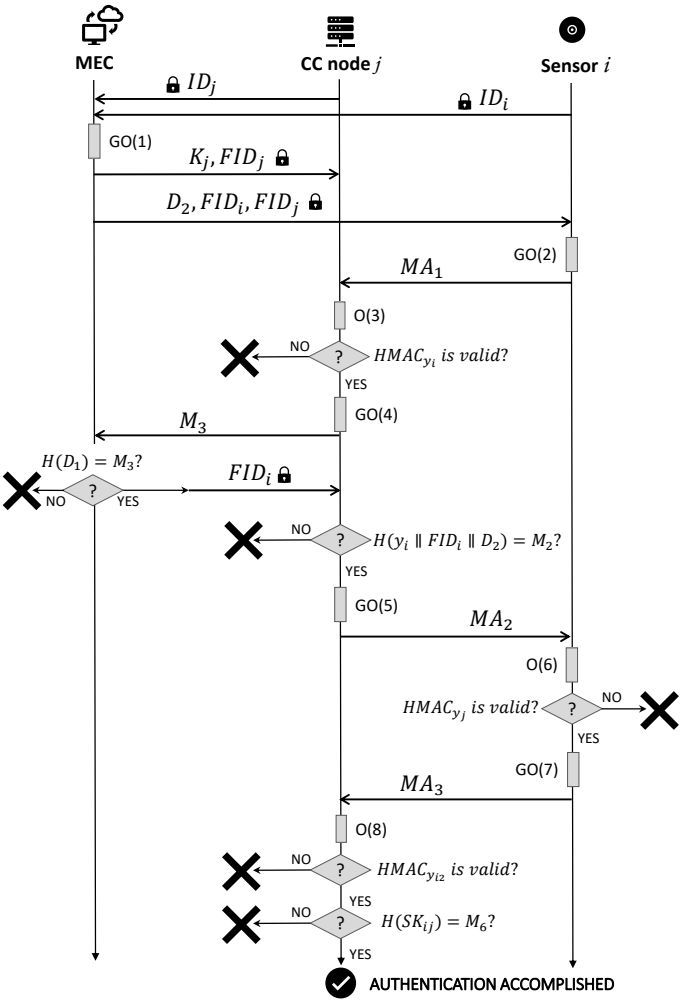


Fig. 2. Authentication procedure.

to the sensor i; *(ii)* a secret key K_j which it will securely share with the CC node j; a key for the ID encryption of both *(iii)* the sensor i (i.e., KI_i) and *(iv)* the CC node j (i.e., KI_j). Consequently, it computes $GO(1)$:

$$D_1 = H(ID_i||sn_i);$$
$$D_2 = D_1 \oplus K_j;$$
$$eID_j = ID_j \oplus KI_j;$$
$$eID_i = ID_i \oplus KI_i;$$
$$FID_j = H(eID_j);$$
$$FID_i = H(eID_i); \quad (1)$$

where, D indicates preliminary data, $H()$ is a secure hash function, eID represents an encrypted ID, and FID stands for a fake identity.

After that, the MEC node sends, via secure channels, K_j, FID_j to the CC node j and D_2, FID_i, FID_j to the sensor i. The latter generates a secret random number y_i and executes the second group of operations $GO(2)$:

$$M_1 = FID_j \oplus y_i;$$
$$M_2 = H(y_i||FID_i||D_2);$$
$$MA_1 = D_2||M_1||M_2||HMAC_{y_i}(D_2||M_1||M_2), \quad (2)$$

where, M discloses a generic message and MA_1 denotes the first message used for the mutual authentication. Subsequently, it sends MA_1 to the CC node which performs the following operation $O(3)$:

$$y_i = M_1 \oplus FID_j, \quad (3)$$

necessary to continue the authentication procedure because it is preparatory to the check of the Hashed Message Authentication Code (HMAC) previously computed by the sensor i with y_i. In fact, if the CC node computes $HMAC_{y_i}(D_2||M_1||M_2)$ and obtains a different value from the one received by the sensor in MA_1, then the procedure fails because, clearly, the integrity and authenticity of the message have been breached. Differently, if the HMAC check is successful, the CC node accomplishes the fourth group of operations $GO(4)$:

$$D_1 = D_2 \oplus K_j;$$
$$M_3 = H(D_1). \quad (4)$$

Therefore, it sends M_3 to the MEC which can check that this matches with its computation of $H(D_1)$; if the check is successful, the MEC sends the FID_i to the CC node over a secure channel. This step allows the controller to verify the integrity of M_2 to proceed with the generation of y_j and the execution of the fifth group of operations $GO(5)$:

$$SK_{ij} = H(y_i||y_j);$$
$$M_4 = FID_i \oplus y_j;$$
$$MA_2 = M_4||HMAC_{y_j}(M_4), \quad (5)$$

where, SK_{ij} is the secret key that must be shared only between the two authenticating entities. Thereby, the CC node sends MA_2 to the sensor, which performs the operation $O(6)$ with the aim of computing y_j and checking the HMAC included in MA_2:

$$y_j = M_4 \oplus FID_i. \quad (6)$$

If the control of the HMAC is successful, the sensor generates a different y_{i2} to compute the HMAC of a new message. In fact, according to LiMAD, sensor and CC node must use a unique HMAC key for each message exchange session. Then, the sensor executes the seventh group of operations $GO(7)$:

$$SK_{ij} = H(y_i||y_j);$$
$$M_5 = FID_j \oplus y_{i2};$$
$$M_6 = H(SK_{ij});$$
$$MA_3 = M_5||M_6||HMAC_{y_{i2}}(M_5||M_6), \quad (7)$$

sending the resulting MA_3 to the CC node. By now, the final operations of the procedure begin. In order to verify the validity of the HMAC, the CC node carries out the operation $O(8)$:

$$y_{i2} = M_5 \oplus FID_j. \quad (8)$$

If the HMAC is valid, it performs the last check for the assessment of the SK_{ij}: if the key is the legitimate one, then the authentication procedure is successfully accomplished.

2) Security measures for multi-tenancy: The layers of the proposed architecture can be managed by different stakeholders. For example, it is reasonable to assume that an MNO owns and operates the MEC node, while the Hospital, as a Tenant, could administer the Processing and Sensing levels. We refer to [18] for the definition of stakeholders; the MNO is defined as *the entity operating its mobile network infrastructure to provide connectivity to end-users*, while a Tenant is *a service provider which acquires the virtual network services to make them available to its users*. As also stated in [18], numerous actors can populate cellular environments with the effect that the deployment of different stakeholders in a virtualized architecture makes the system vulnerable to many security threats. Among these, the problem of storing data relating to hospital and patients on a MEC managed by an external entity is one of the most concerning. The use of homomorphic encryption can be a valid solution to this problem, as it allows processing on encrypted data while keeping plaintext hidden. Referring to our architecture, cluster controllers could apply homomorphic encryption on the data before sending them to the MEC, so that it stores encrypted information and cannot operate on plaintext. This represents a proper countermeasure to the threat of Data Breach in multi-tenant environments.

IV. Results

A. Security analysis

Similarly to [19] [20] [21], we perform a security analysis of the proposed LiMAD authentication protocol by discussing the security requirements it is able to guarantee.

TABLE II
NOTATIONS USED IN THE AUTHENTICATION PROCEDURE.

Notation	Description
MEC	Multi-Access Edge Computing node
CC node	Cluster Controller
sn_i	A Secret random Number generated by the MEC node and associated to sensor i
y	A secret random number (e.g. y_i is the one generated by sensor i)
K_j	A secret key generated by the MEC node and shared only with the legitimate CC node j
KI	The Key used for the encryption of the ID (e.g. KI_i is the key used for ID_i)
ID	Identity (e.g. ID_i is the identity of sensor i)
eID	Encrypted Identity (e.g. eID_i is the encrypted identity of sensor i)
FID	Fake Identity (e.g. FID_i is the fake identity of sensor i)
$H()$	A secure hash function
$HMAC$	Hashed Message Authentication Code (e.g. $HMAC_{y_i}$ is computed using the key y_i)
D	Preliminary Data
$GO()$	Group of Operations (e.g. $GO(1)$ is the group of operations number (1))
MA	Message for Authentication
$O()$	Operation (e.g. $O(3)$ is operation number 3)
M	Generic Message
SK_{ij}	The Secret Key shared only between the two authenticating entities

1) Identity privacy protection: This is a requirement of paramount importance in the health ecosystem, also when dealing with COVID-19 [22]. Indeed, the fear of a violation of patient data privacy represented a big obstacle to the use of ICT to fight against the COVID-19. The proposed LiMAD is aimed at the protection of the privacy through the definition of a secure method for identifying nodes in the network even apart from the authentication procedure. In fact, the MEC computes an encrypted version of IDs of both sensor and controller, by means of secret keys, and further protects their privacy by computing fake identities. In our proposal, we charged the MEC of performing all operations required for the safeguard of the privacy in order to move, as much as possible, the computational burden of security towards the network.

2) Message authentication: The implementation of message authentication is important to foster the assurance of two remarkable properties for the exchanged messages: integrity and authenticity. The former implies that who does not know the key used for message authentication cannot modify the message; the latter guarantees that the key generator is the sender of the message. HMAC is a message authentication method that is well suited to lightweight authentication protocols; for example, it is used in the protocol for low-end IoT devices introduced in [23]. Also in LiMAD, the HMAC is implemented by network nodes in all the messages for authentication (MAs) in order to ensure their integrity and authenticity. For example, the sensor i inserts in MA_1 the HMAC computed with the random number y_i, previously selected and never exchanged in clear; only the legitimate receiver, associated to the FID_j, is able to compute y_i in $O(3)$, then to calculate $HMAC_{y_i}(D_2||M_1||M_2)$ and to verify that this matches the one received by the sensor. As regards messages coming from the MEC node, it represents a trusted third party, from which, along with receiving a wide range of beneficial properties, nodes obtain information that are considered undoubtedly true. Actually, the MEC establishes only secure connections with the nodes so as to deliver unbreakable messages.

3) Mutual authentication: In [24], mutual authentication is considered a necessary measure for the realization of edge computing integration in time-sensitive IoT applications expected for future 6G networks. The LiMAD is effective in mutual authentication between sensor and controller thanks to the exchange of a set of MAs. In particular, the sensor is authenticated thanks to MA_1 and to the check on M_3 performed by the MEC, as only the legal node can own information on D_2. The controller is authenticated trough the exchange of M_3 with the MEC node, because only a legitimate controller can compute the correct D_1, and thanks to MA_2, as it contains the FID_i only sent by the MEC to the licit CC node. The further steps, including MA_3, are aimed at generating a shared secret key between sensor and controller able to strengthen their mutual authentication.

4) Resistance to replay attacks: A replay attack occurs when a malicious entity intercepts the communication between two parties and delays the sending of messages (or replicates them) to manipulate the receiver. The susceptibility to this type of attack of some contact tracing apps used to thwart the spread of COVID-19 is known and declared in the literature, for example in [25], where authors state that authentication procedures represent a valid countermeasure to these attacks. The LiMAD is resistant to replay attacks thanks to the use of unique random session keys. In fact, during the authentication procedure, in each communication between sensor and controller, a different secret random number y is used which also acts as a session token useful to prevent someone else from replying the message. If a receiver gets two messages containing the same session token, it knows that a replay attack has occurred.

5) Resistance to man-in-the-middle (MITM) attack: The MITM attack allows a malicious entity to meddle in a communication between parties without being noticed, for example, by pretending to be one of them and sending messages on its behalf. This threat represents a significant vulnerability of D2D communications, so, it is important to face it, as in [26], where an innovative model for the assessment of the trustworthiness of nodes possibly involved in D2D communications is defined to deal with the D2D security problem. The occurrence of such an attack during the authentication process would pose a serious threat to the protection of health data. Actually, an attacker could be able to impersonate a controller, thus receiving data sent by the sensing nodes and using the obtained

information at its own discretion. To prevent this, LiMAD provides for the implementation of several measures. First of all, the impossibility for malicious entities to replicate the MAs thanks to the intervention of the trusted third party, which ensures that only legitimate nodes have important information for authentication purposes (e.g., D_2 and K_j).

B. Communication and Computational Overhead

Likewise other papers in the literature that present security proposals [27], a measurement of the communication and computational overhead due to LiMAD is provided in this work. The operations referred hereinafter are represented in Fig. 2 and detailed in Section III.

Starting with the *Communication Overhead*, our evaluation is based on the hypothesis of using SHA-256 as hash function, also for the computation of the HMAC. Actually, thanks to an interesting comparison among three well-known hashing algorithms (i.e., SHA-256, SHA-1, and MD5) probed by authors of [28], we can infer that SHA-256 represents the best trade-off in terms of latency, energy consumption, and security level. In view of this, the assessment of the bytes required by the messages exchanged in LiMAD follows. The transmission of the IDs by the sensor and the CC node requires roughly $16B$ each. The MEC node has to deliver the message with K_j, FID_j (i.e., $64B$) to the CC node and the one with D_2, FID_i, FID_j (i.e., $96B$) to the sensor, hence it has to send $64 + 96 = 160B$. The MA_1 costs $128B$ to the sensor. The CC node sends $32B$ for M_3 to the MEC, which replies with the $32B$ of FID_i. Finally, the MA_2 requires $64B$ to the CC node to which the sensor responds with $96B$ for the MA_3. The authentication protocol described in [19] uses security mechanisms comparable with those implemented by LiMAD, therefore it represents the best benchmark in the literature. To carry out the comparison, we assume: to use the same parameter setting for the IDs and for the hash function; to consider the router of the architecture of [19] as the equivalent of the CC node of our architecture and the authentication server as our MEC. In so doing, LiMAD results in an overall bandwidth overhead of $288B$, against $240B$ of [19]. The greater overhead of LiMAD affects only the MEC node, as it is due to additional security controls that require the involvement of the trusted third party, hence are aimed at increasing the security of the authentication procedure. The resulting comparison is shown in Table III.

TABLE III
COMMUNICATION OVERHEAD AND COMPARISON.

	LiMAD	**[19]**
MEC	$256 + 384 + 128 = 768b = 96B$	$256b = 32B$
CC node	$128 + 128 + 256 = 512b = 64B$	$640b = 80B$
Sensor	$128 + 512 + 384 = 1024b = 128B$	$1024b = 128B$

With regard to the *Computational Overhead*, we distinguish the computational cost required by: the XOR operation (i.e., c_x), the computation of hash function including HMAC (i.e., c_h), and the generation of a random number (i.e., c_r). Starting with the MEC, it has to spend $4 * c_r + 3 * c_h + 3 * c_x$ for the execution of $GO(1)$. Then, the sensor performs $GO(2)$, which requires $c_r + c_x + 2 * c_h$. In reply, $2 * c_x + 2 * c_h$ are needed to the CC node to carry out: $O(3)$, one HMAC check, and $GO(4)$. After that, one c_h is required to the MEC node for the M_3 check, followed by the $3 * c_h + c_r + c_x$ yielded for the CC node to obtain MA_2. The last operations performed by the sensor cost $2 * c_x + 4 * c_h + c_r$. The CC node reaches the accomplishment of the authentication procedure by spending $c_x + 2 * c_h$. The total computational overhead for each node is shown in Table IV, which also includes the comparison with the lightweight authentication mechanism presented in [19]. As with the communication overhead, we consider the router of the architecture in [19] as the equivalent of the CC node of our architecture and the authentication server as our MEC. The resulting comparison evidences that the protocol presented in this work satisfies the requirement of lightness imposed by IoT devices. In fact, LiMAD ensures an overall saving of the computational overhead on the constrained nodes of the network by slightly increasing the load on the central and most powerful node of the architecture (i.e., the MEC).

TABLE IV
COMPUTATIONAL OVERHEAD AND COMPARISON.

	LiMAD	**[19]**
MEC	$4 * c_r + 3 * c_x + 4 * c_h$	$2 * c_x + 2 * c_h$
CC node	$c_r + 4 * c_x + 7 * c_h$	$c_r + 6 * c_x + 7 * c_h$
Sensor	$2 * c_r + 3 * c_x + 6 * c_h$	$c_r + 4 * c_x + 7 * c_h$

C. Performance Evaluation

In order to prove the benefit of our proposal, we carried out a performance evaluation concerning both the authentication protocol and the proposed architecture.

As previously stated, LiMAD causes a higher communication overhead than the approach presented in [19] due to the messages exchange with the trusted third party during the authentication phase. Although this step causes a greater exchange of information compared to [19], it can foster bandwidth saving thanks to a prompt detection of any attacks against the CC node. Fig. 3 depicts the amount of bandwidth loss under varying percentage of malicious CC nodes and considering different numbers of sensors controlled by each CC. Specifically, if a controller is malicious it sends an M_3 bogus message to the MEC node, which immediately identifies the attack and blocks the authentication procedure, thus allowing bandwidth savings to the involved nodes, with benefits especially for resource-constrained sensors. In [19], there is not any involvement of a trusted third party during the authentication phase as only the two authenticating nodes participate to the procedure; this justifies the higher bandwidth loss.

Fig. 4 analyses the capability of the proposed architecture to improve the data delivery delay with respect to traditional sensors-to-MEC communication. In particular, the use of D2D combined with the execution of the authentication protocol

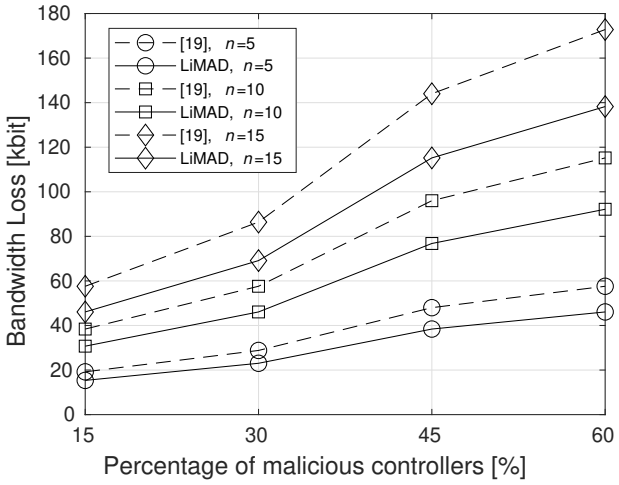


Fig. 3. Bandwidth loss under varying percentage of malicious controllers (n is the number of sensors managed by each CC node).

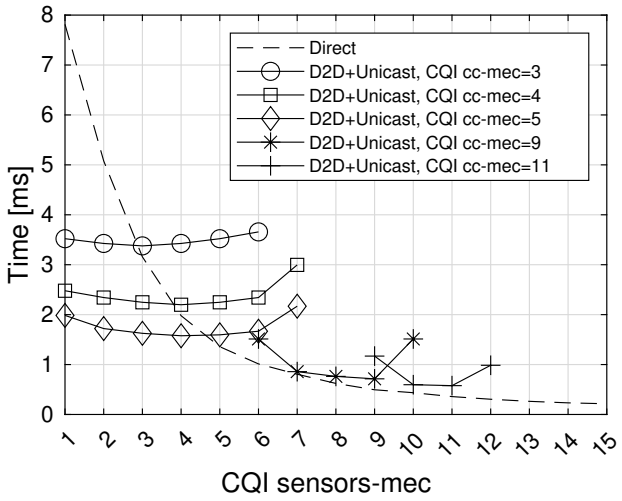


Fig. 4. Data delivery delay experimented by means of the proposed architecture w.r.t. traditional sensors-to-MEC communication.

proves to be mostly more effective than the direct data transmission to MEC. Two macro-scenarios are compared as the Channel Quality Indicator (CQI) of the sensors towards MEC increases (i.e., MEC-to-sensors distance decreases):

- **Direct:** sensing devices send data directly to the MEC, without going through the controllers.
- **D2D+Unicast:** the proposed architecture is implemented, therefore the use of cluster controllers as intermediaries for the communication between MEC and sensors is considered. The latter, following the execution of LiMAD, transmit the data in D2D to the controllers, which then forward them to the MEC. For this scenario, different cases are compared obtained by varying the position of the controller: CQI controller-MEC (cc-mec)$= 3, 4, 5, 9, 11$. We remark that the communication via the controllers, due to the nature of proximity communications, is not feasible for devices that are too far from the controllers. For this reason, D2D+Unicast curves report non-zero values only if D2D communication is possible.

The graph highlights the gain that the implementation of the procedures envisaged by the proposed architecture brings in terms of transmission time savings. In particular, Fig. 4 serves as a guidance to understand under which conditions the use of our approach is beneficial. As an example, in the case of the CQI cc-mec is equal to 3 (see the curve with circles), the proposed approach is able to guarantee a significantly lower data delivery delay w.r.t. the benchmark approach when CQI sensors-mec is lower than 3.

V. Conclusions

The digital Health represents a future that the current global pandemic is showing not to be long in coming. The ICT is rich in means exploitable in support of the development of eHealth. Among the technologies that mostly attracted attention in the evolution process of the 5G network are *D2D* and *MEC*. As regards the major imperative requirements of the 5G network, *security* really caught the eye. The integration of these three factors (i.e., D2D, MEC, and security) can lead to a 6G-oriented implementation, given the requirements asked by the services that 6G will have to support. All these considerations led to the elaboration of the proposal of this work which introduces a MEC-based hierarchical architecture for the execution of eHealth services in a 6G-oriented system. The proposal includes the use of D2D communications to improve the performance of data transmission and involves the accomplishment of a proposed lightweight authentication protocol suitable for resource-constrained IoMT devices that could be used, for example, for a telemonitoring service. Our proposal meets some of the main requirements that an eHealth system should have: *(i)* low latency in data transmission and processing, thanks to the use of D2D and MEC; *(ii)* availability of context-awareness information, offered by the use of the MEC; *(iii)* devices authentication and privacy protection, thanks to the proposed security protocol.

References

[1] A. Sedik, M. Hammad, F.E. Abd El-Samie et al., *Efficient deep learning approach for augmented detection of Coronavirus disease,* Neural Comput & Applic (2021).

[2] L. Mucchi et al., *How 6G Technology Can Change the Future Wireless Healthcare,* 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 2020, pp. 1-6.

[3] A. Shahraki et al., *A Comprehensive Survey on 6G Networks:Applications, Core Services, Enabling Technologies, and Future Challenges*, 2021, available at: arXiv:2101.12475v2.

[4] F. Tariq, M. R. A. Khandaker, K. -K. Wong, M. A. Imran, M. Bennis, and M. Debbah, *A Speculative Study on 6G,* in IEEE Wireless Communications, vol. 27, no. 4, pp. 118-125, August 2020.

[5] S. Pizzi, C. Suraci, A. Iera, A. Molinaro, and G. Araniti, *A Sidelink-Aided Approach for Secure Multicast Service Delivery: From Human-Oriented Multimedia Traffic to Machine Type Communications,* in IEEE Transactions on Broadcasting, vol. 67, no. 1, pp. 313-323, March 2021.

[6] J. Cao et al., *A Survey on Security Aspects for 3GPP 5G Networks,* in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170-195, Firstquarter 2020.

[7] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, *6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence,* in IEEE Wireless Communications, vol. 27, no. 5, pp. 126-132, October 2020.

[8] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, *IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network,* in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5164-5171, April 2021.
[9] M. Masud et al., *A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care,* in IEEE Internet of Things Journal (Early Access).
[10] Mamta, B. B. Gupta, K. -C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, *Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System,* in IEEE/CAA Journal of Automatica Sinica (Early Access).
[11] M. Kumar and S. Chand, *A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System With Public Verifiability,* in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10650-10659, Oct. 2020
[12] A. P. G. Lopes and P. R. L. Gondim, *Mutual Authentication Protocol for D2D Communications in a Cloud-Based E-Health System,* Sensors, vol. 20, no. 7, p. 2072, Apr. 2020.
[13] A. Feriani, A. Refaey, and E. Hossain, *Tracking Pandemics: A MEC-Enabled IoT Ecosystem with Learning Capability,* in IEEE Internet of Things Magazine, vol. 3, no. 3, pp. 40-45, September 2020.
[14] Y. Zhang, G. Chen, H. Du, X. Yuan, M. Kadoch, and M. Cheriet, *Real-Time Remote Health Monitoring System Driven by 5G MEC-IoT,* in Electronics, vol. 9(11):1753, no. 3, pp. 40-45, October 2020.
[15] Z. Ma et al., *Lightweight Privacy-preserving Medical Diagnosis in Edge Computing,* in IEEE Transactions on Services Computing, 2020.
[16] Z. Xue et al., *A Resource-Constrained and Privacy-Preserving Edge Computing Enabled Clinical Decision System: A Federated Reinforcement Learning Approach,* in IEEE Internet of Things Journal, 2021 (Early Access).
[17] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, *Envisioning Device-to-Device Communications in 6G,* in IEEE Network, vol. 34, no. 3, pp. 86-91, May/June 2020.
[18] C. Suraci, G. Araniti, A. Abrardo, G. Bianchi, and A. Iera, *A stakeholder-oriented security analysis in virtualized 5G cellular networks,* in Computer Networks, vol. 184, Jan. 2021.
[19] A. Esfahani et al., *A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment,* in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 288-296, Feb. 2019.
[20] M. Chuang and J. Lee, *TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks,* in IEEE Systems Journal, vol. 8, no. 3, pp. 749-758, Sept. 2014.
[21] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, *SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks,* in IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2659-2672, April 2016.
[22] M. Whaiduzzaman et al., *A Privacy-Preserving Mobile and Fog Computing Framework to Trace and Prevent COVID-19 Community Transmission,* in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 12, pp. 3564-3575, Dec. 2020.
[23] M. Nakkar, R. Altawy, and A. Youssef, *Lightweight Broadcast Authentication Protocol for Edge-Based Applications,* in IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11766-11777, Dec. 2020.
[24] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, *Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment,* in IEEE Consumer Electronics Magazine, 2021 (Early Access).
[25] M. Casagrande, M. Conti, and E. Losiouk, *Contact Tracing Made Unrelay-able*, Nov. 2020, available at: arXiv:2010.12641v2.
[26] C. Suraci, S. Pizzi, D. Garompolo, G. Araniti, A. Molinaro, and A. Iera, *Trusted and secured D2D-aided communications in 5G networks,* in Ad Hoc Networks, vol. 114, 2021.
[27] Y-H Chuang, N-W Lo, C-Y Yang, and S-W Tang, *A Lightweight Continuous Authentication Protocol for the Internet of Things,* in Sensors, 18(4):1104, 2018.
[28] A. V. Mota, S. Azam, B. Shanmugam, K. C. Yeo, and K. Kannoorpatti, *Comparative analysis of different techniques of encryption for secured data transmission,* 2017 IEEE ICPCSI, Chennai, India, 2017.

Chiara Suraci (chiara.suraci@unirc.it) received her M.Sc. degree in Telecommunications Engineering from University Mediterranea of Reggio Calabria, Italy, in 2018. Currently, she is a Ph.D. student at the University Mediterranea of Reggio Calabria, with Scholarship supported by Vodafone Italia and CNIT (National Inter-University Consortium for Telecommunications) to investigate potentially harmful security risks for 5G networks. Her current research topics include 5G, D2D, network security, and virtualization technologies.

Sara Pizzi (sara.pizzi@unirc.it) is an assistant professor in telecommunications at University Mediterranea of Reggio Calabria, Italy. From the same university she received the 1st (2002) and 2nd (2005) level Laurea Degree, both cum laude, in Telecommunication Engineering and the Ph.D. degree (2009) in Computer, Biomedical and Telecommunication Engineering. In 2005, she received a Master's degree in IT from CEFRIEL/Politecnico di Milano. She was a visiting PhD student at the Department of Computer Science of Alma Mater Studiorum-University of Bologna in 2008. Her current research interests focus on radio resource management for multicast service delivery, D2D and MTC over 5G networks, integration of NTNs in the IoT.

Antonella Molinaro (antonella.molinaro@unirc.it) graduated in Computer Engineering (1991) at the University of Calabria, received a Master degree in Information Technology from CEFRIEL/Polytechnic of Milano (1992), and a Ph.D. degree in Multimedia Technologies and Communications Systems (1996). She is currently an associate professor of telecommunications at the University Mediterranea of Reggio Calabria, Italy, and has a double affiliation at CentraleSupelec, Paris-Saclay University, France. Her research activity mainly focuses on wireless and mobile networking, vehicular networks, and future Internet.

Giuseppe Araniti (araniti@unirc.it) received the Ph.D. degree in electronic engineering in 2004 from the University Mediterranea of Reggio Calabria, Italy, where he is Assistant Professor of telecommunications. His major area of research is on 5G/6G networks and includes personal communications, enhanced wireless and satellite systems, traffic and radio resource management, eMBMS, D2D and M2M/MTC.