5G in the Internet of Things era: an overview on security and privacy challenges

Sabrina Sicari[*‡], Alessandra Rizzardi[*], Alberto Coen-Porisini[*]
[*]Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria,
via Mazzini 5 - 21100 Varese (Italy)
[‡]Corresponding author
Email: {sabrina.sicari; alessandra.rizzardi; alberto.coenporisini}@uninsubria.it

***Abstract*—Now reaching 2020, the world is witnessing the initial diffusion of 5G networks, which promise to revolutionize the mobile wireless communications, providing faster services, very low delays, and a very pervasive connectivity via mobile devices. It is worth to remark that the main paradigm which will take advantage from 5G is really the Internet of Things (IoT). However, the spreading of 5G technology also generates important concerns in terms of security and privacy, due to the continuous and wireless connection to the network, which hinders the reliability of the involved devices. This paper deeply analyzed the current state of the art about the existing security and privacy solutions tailored to 5G. More in detail, the following requirements are discussed: data integrity, confidentiality, authentication, access control, non-repudiation, trust, privacy, identity management, key management, policy enforcement, and intrusion detection. Furthermore, the paper aims to shed the light on future research directions towards the realization of secure and privacy aware 5G systems. To this end, the role of emerging paradigms, such as IoT, fog computing, and blockchain is investigated.**

Keywords—5G, Internet of Things, Fog Computing, Blockchain, Security, Privacy

I. Introduction

Mobile wireless communication evolved, since the late 1970s, from analog voice calls to the current modern technologies, providing end-users with high data rates to perform (multimedia) data and communication transmissions [1]. The spreading and the development of mobile wireless communication are also encouraged by the diffusion of mobile devices such as smart phones and tablets, which pave the way for the realization of mobile applications. The consequence is a huge increment of the network traffic, which naturally requires new means to support the widespread supply of ”wireless” services with high levels of Quality of Service (QoS).

To cope with such an issue, as expected, at the threshold of 2020, we are witnessing to the put in action of the next generation 5G wireless communications [2]. The 5G network architecture's components are sketched in Figure 1 and include: (i) a huge number of macro-cells and micro-cells, associated with proper base stations and/or hotspots, for guaranteeing the pervasiveness of the connectivity among end-devices/end-users; (ii) the core network, composed by routers, gateways, etc., which is responsible for gathering and transmitting the information acquired by the base stations; (iii) the final connection to the Internet, which may take place through servers, data centers, or cloud infrastructures.

Compared to the actual 4G technologies, 5G is characterized by higher bit rates, quantified in more than 10 gigabits per second, as well as by more capacity and very low latency. Such features are fundamental in a world increasingly connected, especially thanks to the continuous spreading of billions of connected objects and smart devices in the context of Internet of Things (IoT). In fact, in the emerging IoT era, 5G certainly enables to overcome the current issues in terms of network response times and network resources' management. Note that the IoT paradigm embraces heterogeneous technologies, ranging from Wireless Sensor Networks (WSNs), to RFID, NFC, actuators, and so on, which are able to communicate through different protocols and standards. The data acquired by such kinds of devices are usually collected by the so-called ”smart objects”, which act as a middleware (or fog) layer, in order to be processed and shared with the end-users, which are interested in certain services [3]. Hence, in such a scenario, also the role of fog computing [4] peeks out. Fog computing, which is also known as *fog net-*

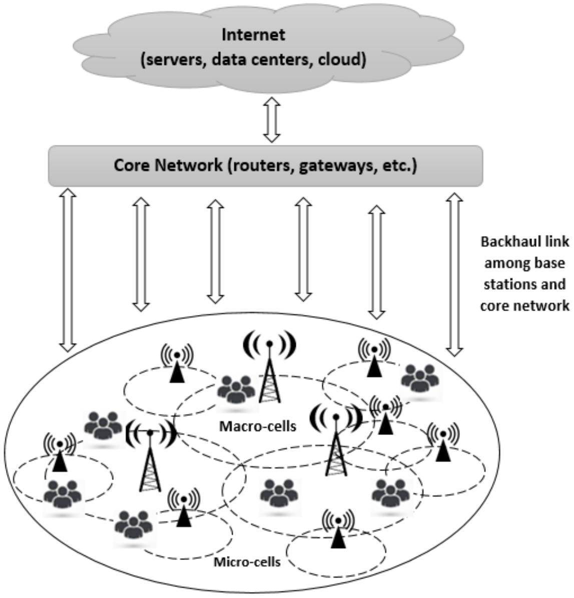
Internet
(servers, data centers, cloud)
Core Network (routers, gateways, etc.)
Backhaul link among base stations and core network
Macro-cells
Micro-cells

Fig. 1: 5G network's components

working or *fogging*, mainly consists of a decentralized networking and computing infrastructure, where data, processing tasks, storage and applications are distributed in an efficient manner among the data sources and the cloud. In few words, lightweight application processes and services are managed at the edge of the network by one or more smart devices (or smart gateways or routers), while other heavier tasks are still managed by the cloud.

However, as such devices are connected to the network all the time in a even more pervasive way, they can be more easily tracked down and are more vulnerable towards several kinds of attacks, such as: eavesdropping, impersonation, man-in-the-middle, Denial of-Service (DoS), replay, repudiation, and so on [5]. Maintaining a high level of QoS in terms of delay, when a huge amount of data is transferred inside the 5G network, while keeping, at the same time, the reliability of the network itself, is a critical and complex task. The final goal is to prevent the data violation and the improper diffusion of malicious contents among the mobile devices. Hence, the design of new security and privacy oriented solutions, targeted to the 5G network, represents now a compelling need, due to the imminent diffusion of the 5G technology in the real world.

In this paper, a broad overview of the security and privacy issues related to 5G network is provided, along with the discussion about already available solutions in literature. To this end, the following requirements are investigated: data integrity, confidentiality, authentication, access control, non-repudiation, trust, privacy, identity management, key management, policy enforcement, and intrusion detection. The final goal of such a research work is to clearly point out what is needed, what lacks, and what must be done in order to realize a secure and privacy aware 5G network in the next future, taking in mind emerging paradigms, such as IoT, fog computing, and blockchain. Concerning fog computing, it should help in enhancing the overall network performance, by moving some network's task towards the edge of the network system [6]; while blockchain would give support to ensure adequate levels of robustness to the information transmitted [7]. In fact, the blockchain approach allows applications to operate in a decentralized or peer-to-peer fashion, without the need for a central authority or for other trusted intermediaries, as now required in mostly contexts.

The rest of the paper is organized as follows. Section II presents the existing surveys and tutorials on 5G, pointing out the current state of the art in this field, both in general and with a focus on security and privacy aspects. Section III deeply investigates security and privacy challenges in the 5G network. Section IV provides a discussion about the outcomes of the conducted analysis. Section V ends the paper and draws some hints for future work.

II. Motivations and related works

5G is increasingly involving the researchers, due to the great impact it will certainly have in the Internet-based applications. In particular, it could become a major driver for the growth of IoT-related context. Many survey papers have been just proposed in literature, mainly focusing on the features and challenges of 5G protocol. As revealed by the following discussion, little attention has, until now, been paid on security and privacy requirements in the 5G communication standard.

For example, the authors in [8] mainly concerns 5G network slicing techniques, which represent a central topic in the realization of the 5G mobile network architecture and in establishing how the network's resources must be used from the physical to the higher layers. In fact, thanks to 5G network slicing, resources are split into logical or virtual networks (i.e., the slices) to address use cases with distinct features and service level agreement (SLA) requirements. In such a way, a 5G slice that supports, for example, a critical IoT use case would differ in terms of throughput, latency and reliability requirements from another 5G slice which is dedicated to a non-critical application. The main challenges, concerning 5G network slicing, which have been pointed out in the survey, are: (i) the virtualization of the radio resources; (ii) the definition of fine-grained network functions to better compose the services; (iii) how to efficiently perform and end-to-end orchestration and management of the provided services.

[9] provides a wide overview of the next 5G generation, discussing about: (i) the new architectural changes associated to the design of the radio access network (RAN); (ii) the underlying novel physical layer technologies; (iii) the details of MAC layer protocols; (iv) the new QoS and QoE features, associated with the 5G evolution; (v) the energy consumption and cost efficiency; (vi) the relevant field trials, drive tests, and simulation experiments.

The survey proposed in [10], after presenting the limitations of the current cellular systems, discusses about some challenges in the development of 5G networks, such as: (i) data rate and network capacity expansion with energy optimization; (ii) scalability and flexibility; (iii) handling interference; (iv) low latency and high reliability; (v) high mobility and hand-off; (vi) self-healing infrastructures; (vii) QoS; (viii) security and privacy; (ix) economical impacts. Concerning security and privacy issues, the authors focus their attention on authentication, whose actuation is hindered by the fast and frequent handover promised by 5G networks' components. Hence, novel efficient solutions must be defined, in order to guarantee the end-devices authentication in the 5G scenario.

Instead, a particular focus on RAN, core network, and caching in 5G networks is provided in [11], in order to reveal how to achieve low latency, mainly in critical services, such as those belonging to the following contexts: factory automation, intelligent transportation systems, robotics and telepresence, virtual and augmented reality, e-health, gaming, smart grid, remote learning/education.

Other surveys focus on particular aspects of 5G networks, such as:

- The millimeter wave (mmWave) bands [12], which act an important role in guaranteeing high propagation loss, directivity, and sensitivity to blockage in 5G communications
- The non-orthogonal multiple access (NOMA) at the radio access layer [13] [14], which ensures more than one user can be served in each orthogonal resource block, such as a time slot, a frequency channel, a spreading code, or an orthogonal spatial degree of freedom; note that, in such a work, security is mentioned as an open challenge and it was not considered when the NOMA principle was developed
- The backhaul, which is pointed out as a bottleneck by the authors in [15], due to the ultra-dense and heavy traffic cells connected to the core network through the backhaul itself
- Multi-access edge computing (MEC) [16], which could represent a viable solution to the just mentioned issues related to the 5G backhaul; in fact, MEC aims at providing a cloud computing platform at the edge of the radio access network, offering, at the same time, storage and computational resources at the edge, reducing latency for mobile end users
- User association mechanisms [17], which play a pivotal role in enhancing the load balancing, the spectrum efficiency, and the energy efficiency of networks; they mainly aim to determine whether a user is associated with a particular base station (BS), before initiating data transmission
- Energy efficient techniques [18], which inevitably influence the resources' allocation, both at the physical and at the radio access layer
- Cooperative localization [19], which should contribute to decrease communications' delay.

Specifically tailored to the link between 5G and IoT, the survey, presented by the authors in [20], reveals that one fundamental challenge is the realization of a 5G-IoT architecture; the second challenge is how to guarantee security and privacy concerns, which can be listed as follows: identity, authentication, key management, encryption, secure mobility, and secure storage. A third challenge is, instead, related to standardization, which involves: (i) technology standards, including wireless communication, network protocols, data aggregation standards; (ii) regulatory standards, including data security and privacy, such as general data protection regulation, cryptographic primitives, unstructured data, and data analysis algorithms.

Seamlessly, the work in [21] deeply analyzes the communication technologies and challenges for the adoption of 5G networks for the IoT. It discusses the IoT application requirements, in the fields of smart homes, intelligent transportation systems, smart cities, industries, and e-health, further revealing the new 5G radio enhancement in terms of multi-cast, mobility, and service continuity.

[22] promotes the adoption of security solutions at the physical layer security by means of different techniques, including: physical layer security coding, massive Multi-Input Multi-Output (MIMO) systems, mmWave communications, heterogeneous networks, and NOMA.

Finally, the work in [23] presents a comprehensive survey of existing authentication and privacy-preserving schemes for 4G and 5G cellular networks. The authors outlined the threat model, by highlighting the attacks which can occur in a 5G network, and a categorization of authentication and privacy models. Their analysis is very deep and accurate, but leaves out some important issues, such as trust and access control.

The scope of the work presented hereby is to investigate all the requirements related to security and privacy in the field of 5G, also with respect to the last emerging Internet-based technologies, such as IoT paradigm, fog computing, and blockchain [24]. Already available solutions, along with hints for future research directions will be clearly pointed out, in order to pave the way for a broader discussion on security and privacy in such a field. More in detail, the following secure and privacy related features will be considered:

- Integrity, confidentiality and non-repudiation
- Authentication and access control
- Key management
- Privacy and identity management
- Trust
- Policy enforcement
- Intrusion detection.

Table I summarizes the topics covered by the just mentioned surveys on 5G. In this way, the differences among the existing works and the one proposed in this paper are clarified. More in detail, what emerge from the comparison is that the present paper entirely focuses on security and privacy issues related to 5G, while other papers are tailored to investigate other aspects, such as network resources' management, architectural components, or performance metrics. Note that security requirements are only partially covered in other works.

Note that some works available in literature refer only on IoT security and could be used as starting points for addressing security issues in the 5G-IoT domain. In such a direction should be interesting to analyze the following works [25] [26] [27].

III. Security and privacy in the 5G

In this section, the issues mentioned in Section II, which are related to security and privacy in 5G networks, will be separately discussed with respect to available solutions and taking in mind the 5G network scheme, proposed in Figure 2. Such a figure represents a high level overview of a 5G-based system, where IoT devices are included and fog computing principles are applied. It is worth to remark that, in the considered analysis, only the existing approaches strictly targeted to 5G security and privacy are investigated, in order to clearly point out what has been already realized and what, instead, still lacks.

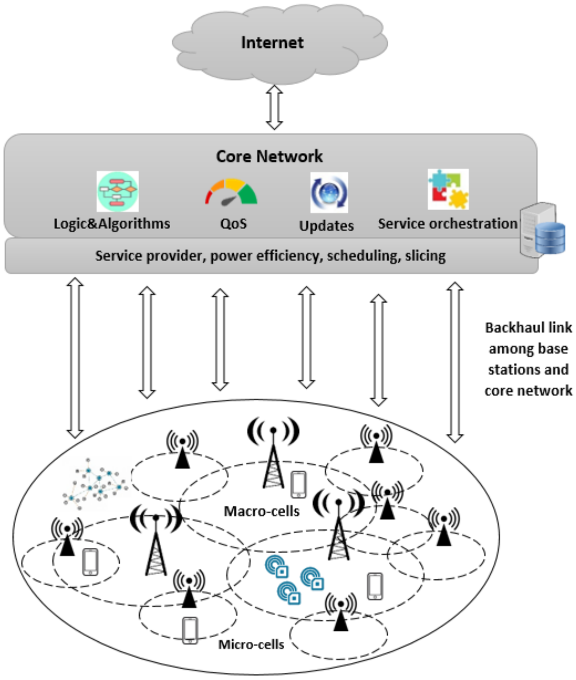
Internet
Core Network
Logic&Algorithms
QoS
Updates
Service orchestration
Service provider, power efficiency, scheduling, slicing
Backhaul link among base stations and core network
Macro-cells
Micro-cells

Fig. 2: Scheme of a 5G network, including IoT and fog computing

More in detail, the following sections will deeply discuss, respectively, about: (i) integrity, confidentiality and non-repudiation; (ii) authentication and access control; (iii) key management; (iv) privacy and identity management; (v) trust; (vi) policy enforcement; (vii) intrusion detection.

A. *Integrity, confidentiality and non-repudiation*

Integrity and confidentiality requirements are guaranteed if the content and the owner of the data cannot be

TABLE I: Comparison of surveys on 5G

Work	network resources' management	architectural aspects	performance	IoT	authentication	physical security
[8]	yes	no	no	no	no	no
[9] [12] [11] [13] [14]	no	yes	yes	no	no	no
[10]	no	no	yes	no	yes	no
[15] [16]	yes	yes	yes	no	no	no
[17] [18] [19]	yes	no	yes	no	no	no
[20] [21]	no	yes	no	yes	no	no
[22]	no	no	no	no	no	yes
[23]	no	no	no	no	yes	no
our paper	no	yes	no	yes	yes	no

Work	privacy	trust	access control	key management	enforcement	intrusion detection	integrity/confidentiality
[8]	no	no	no	no	no	no	no
[9] [12] [11] [13] [14]	no	no	no	no	no	no	no
[10]	no	no	no	no	no	no	no
[15] [16]	no	no	no	no	no	no	no
[17] [18] [19]	no	no	no	no	no	no	no
[20] [21]	no	no	no	no	no	no	no
[22]	no	no	no	no	no	no	no
[23]	no	no	no	no	no	no	no
our paper	yes	yes	yes	yes	yes	yes	yes

tampered or eavesdropped by a non-authorized entity. Finally, non-repudiation implies that a device cannot declare to not be the owner of its generated information. Encryption techniques are usually adopted to deal with such issues.

For example, the approach presented in [28] claims to have potential to achieve confidentiality, integrity, availability and non-repudiation across the 5G based IoT networks, by integrating Elliptic Curve Cryptography (ECC) and Quantum Cryptography, in order to encrypt the information transmitted within the devices and base stations involved in the 5G system. Such a proposed solution is not evaluated with respect to its real feasibility and performance.

A solution based on the integration of ECC and Identity-Based Encryption (IBE) mechanisms is proposed in [29], in order to avoid the non-repudiation of the messages, exchanged in device-to-device (D2D) 2D communications, during the discovery and transmission phases. A key derivation mechanism, targeted to group communication, has also been integrated.

Instead, a simulation environment based on ns-3 simulator and a simple test-bed are put in place in [30] for assessing the efficiency of the envisioned secure multi-hop D2D solution for 5G mobile networks. The workflow is conceived as follows: (i) users' subscription; (ii) devices' discovery and authentication, based on public keys and certificates; (iii) session keys' distribution; (iv) communication. Results are encouraging to maintain low the overhead, while guaranteeing integrity and confidentiality to the transmitted data.

An integration of LoRaWAN, an open and standardized LPWAN (low-power wide area networks) technology, with 4G/5G mobile networks, is proposed in [31], in order to enable the mobile network operators to re-use their current infrastructures. As security is crucial for the IoT applications, it has been included just from the initial versions of the LoRaWAN standard. More in detail, the main properties of LoRaWAN security are: mutual authentication, integrity protection, and confidentiality. Data packets, transported over the core network, are both encrypted and integrity is protected, thus achieving end-to-end security, by means of a system based on the exchange of session keys and authentication codes. The adopted encryption scheme is based on AES with a key length of 128 bits. What does not emerge from the proposed approach is its real feasibility in a wide 5G network, since the architecture considered by the authors is essentially composed by devices, gateways, and network's servers.

Two signcryption schemes are, instead, developed in [32], to achieve secure mutual heterogeneous communications of 5G network slicing, thus guaranteeing integrity, confidentiality, and non-repudiation. More in detail, when the end-users in the 5G slicing based on PKI environment (such as a mobile internet slicing) try to communicate with the end-users in the 5G slicing based on CLC (Cryptography with Low Complexity, such as a vehicle internet slicing), the signcryption schemes allow the interoperability between the two encryption methods.

[33] states that the best way to guarantee data integrity and non-repudiation in 5G service orchestration is by means of a hash chain (which is a concept very close to blockchain). Since such a method provides one-time signatures, it is well suited for protecting management information (e.g., keeping track of management activities, history logs). Instead, connection-oriented interactions, including control information exchange, could be better secured by means of public-key cryptography schemes, used for producing digital signatures.

Outcomes. Summarizing, the literature is still divergent if adopting more traditional cryptographic algorithms, such as AES, RSA, PKI, or if moving towards more recent methods, such as ECC or Quantum Cryptography, or solutions based on blockchain. Probably, the well-suited approaches for 5G are those able to support the resources' constraints of end-devices as long as guaranteeing the robustness of the system and, at the same time, preserving the performance of the 5G network. It is worth to remark that is very widespread the use of session's keys to secure the communications among end-devices and service providers, but proper mechanisms must be designed for the wide 5G area. Finally, an important role is also acted by certificates, which must be also managed accordingly to the needs and functionalities of the 5G network. Maybe, in this direction, a trade-off must be established towards an efficient and a standardized solution. What currently lacks is a standard for the 5G, since, mainly when 5G is coupled with the IoT, different protocols and technologies are involved; furthermore, such protocols and technologies expose diverse security and privacy levels, as well as different constraints in terms of power and computational resources. As a consequence, the certificates' management must deal with such new requirements.

B. Authentication and access control

Authentication mechanisms include all the methods adopted for recognizing the identity of a generic device, in order to allow or deny the access to a certain system or resource. Once an entity is authenticated to a service, for example, the information to be disclosed may depend on specific access control rules, which could prevent the access to certain kinds of sensitive or non-authorized data.

As introduced in Section II, the survey proposed in [23] is almost exhaustive with respect to authentication in the 5G context (it cites more than 200 papers on such a topic). Hence, we recommend to refer to such a work for obtaining a complete bibliography and a detailed analysis with respect to such a requirement. Summarizing, the analysis conducted on authorization mechanisms targeted to 5G points out that they commonly use three factors for authentication, including: (i) what you know (e.g., passwords); (ii) what you have (e.g., smart cards); (iii) who are you (e.g., biometrics). Furthermore, based on the categorization of authentication models, the surveyed schemes have been classified in seven types, including: handover authentication, mutual authentication, RFID authentication, deniable authentication, authentication with mutual anonymity, authentication and key agreement, and three-factor authentication.

Some more recent works, not cited in [23], include the cross-layer authentication protocol, designed in [34] for ultra-dense 5G networks. A channel-based fingerprinting mechanism is employed to enhance the authentication procedure, generating an unpredictable secret key. Subsequently, a cryptographic mechanism, based upon the authentication and key agreement protocol, by employing the generated secret key, is performed for improving the confidentiality and integrity of the authentication handover. Furthermore, a radio trusted zone database, aiming to enhance the frequent authentication of radio devices, which are present in the network, is put in action. The proposed approach is evaluated in a limited scenario, thus not allowing to infer something about scalability.

Instead, concerning access control, the work, which is proposed in [35], presents the adoption of fog computing paradigm, for efficiently managing the resources' requests in presence of caching systems. In fact, revealing that fog-based caching systems may suffer from malicious access, to protect caching from violation and to further ensure its reliability, a new lightweight label-based access control scheme, able to authenticates the authorized fog nodes is provided. More in detail, fog nodes are authenticated by verifying the integrity of the shared files, which consist in embedded label values, and only the authenticated fog nodes can access the caching service.

Also inspired to fog computing, [36] presents a service-oriented authentication framework, supporting network slicing and fog nodes for 5G-enabled IoT services. End-users can establish connections with the 5G core network and anonymously access IoT services through proper network slices of 5G infrastructure, selected by fog nodes, by means of a group-based signature method. More in detail, neither service providers nor local fogs can gain any information about the subscribers (i.e., the end-users) of IoT services, but both are aware of whether end-users are legitimate to access IoT services. Furthermore, a three-party key agreement mechanism (based on Diffie-Hellman scheme), using session keys negotiated among users, local fogs and IoT servers, is put in place to guarantee secure access of service data in fog cache and remote servers.

Also based on group-based authentication is the handover protocol detailed in [37] for 5G wireless networks. Another solution for the handovers in 5G consists in adopting an anonymous mutual authentication with key agreement, by exploiting the trapdoor collision property of chameleon hash functions and the tamper-resistance of blockchains [38]. Blockchain technology is also employed in [39], for the realization of an authentication scheme in 5G ultra-dense networks, and in [40], where consortium blockchain is employed. Note that, in the consortium blockchain, a selected set of nodes can determine the final decision on the consensus of a block, instead of including all the network's participants in the consensus process.

Other authentication schemes are based on pseudonymous, which have been proposed, fox example, for VANET (i.e., vehicular ad hoc networks), but frequently suffer of expensive cost for their initial authentication, which may foster DoS attacks. To cope with such an issue, a hash puzzle-based co-authentication scheme is proposed in [41]. The hash puzzle is designed to restrict the attacker's capability to forge fake pseudonymous certificates; moreover, collaborative verification is used to integrate the computing resources among legitimate vehicles, either as the certificate verifier or the certificate owner.

The data access control scheme, presented in [42], makes also use of pseudonyms, but, in addition, it applies CP-ABE to encrypt and decrypt data encryption keys and the access policies are regulated by trust levels (see Section III-D). A main goal achieved by such an approach is flexibility, which implies that the proposed scheme can control communication data access no matter if the core network functionalities are available or not.

A reputation system-based lightweight message, based on ECC, batch authentication framework and protocol for 5G-enabled vehicular networks is also presented in [43]. A Trusted Authority (TA) is in charge of reputation management. In general, a vehicle with a reputation score below the given threshold cannot obtain a credit reference from the TA for participating in the communication; therefore, the number of untrusted messages in vehicular networks is reduced just from the source.

Outcomes. What emerged is that authentication and access control are widely explored concepts already in the 5G era. The most recent solutions make use of three techniques: (i) group-based authentication; (ii) pseudonymous; (iii) ABE. Hence, it is possible to envision the definition of a system where such three approaches work together, in order to enable a reliable authorization scheme and the protection of users' and devices' identities, for example, in the different macro and micro cells. Note that group signature has been widely adopted in literature, just from the diffusion of security and privacy protocols for WSN [44] and Information Centric Networking (ICN) [45]. Essentially, only the members of a defined group (i.e., the devices which belong to a cluster or to a portion of the network) can sign the transmitted messages with a previously agreed group signature. Such members, when receive a message, can verify that it contains a valid group signature, but they cannot discover which group member made it; such a feature prevents the identities' disclosure by the group members. In fact, only the group manager can open the signature and trace the original signer. Furthermore, the aforementioned analysis also pointed out the emerging role of fog computing and blockchain in the IoT-5G environment. Since they are novel techniques, their application still deserves further studies and evaluation, mainly to cope with the heterogeneity of the involved entities.

C. *Key management*

Often the realization of clever key management mechanisms is overlooked, especially with respect to the definition of encryption methods. However, the adoption of robust key distribution and replacement algorithms has the scope to improve the resilience of any networking-based system, thus enhancing the reliability of the services provided to the end-users. In fact, the availability of mechanisms in charge of revoking the actual keys and replacing them with new ones would help in counteracting the theft of credentials. Reaching such a goal is a complex task, due to dynamic and heterogeneous nature of the devices involved in 5G and, even more, in hybrid 5G-IoT networks.

The aspect of key management is currently mainly treated, as regard the 5G context, in D2D communication and at the physical layer. In fact, [46] proposes a key distribution mechanism for D2D communication in 5G, for counteracting, in particular, the man-in-the-middle attack; the target scenario is composed by two devices belonging to the same cellular network and coverage. The proposed key exchange protocols are based on the standard Diffie-Hellman based key exchange and other lightweight cryptographic functions.

Instead, the authors, in [47], believe that physical layer security can be used to either provide direct secure data communication or facilitate the distribution of cryptographic keys in the 5G network. However, no practical solution is provided and key management at the physical layer is until now reduced to credentials, which are pre-installed on the devices.

The protocol presented in [48] aims at guaranteeing the privacy for the protected identification of end-users' devices and the mutual authentication, among such devices and the core network. The whole system is based on public keys and on IBE paradigm, but it is worth to remark that a key revocation mechanism is also provided. Such a mechanism depends on an expiration time, to prevent possible attacks.

Outcomes. Clearly, the key management area in the IoT and, even more, in the 5G-based systems, still requires more attention by the research community, since few solutions specifically address such a concern. However, what emerges is the importance of the Diffie-Hellman scheme, which is a well-known certified and robust mechanism for key negotiation in wireless systems. Moreover, it also scales, if integrated, for example with a group key exchange system [49], which has been just introducted in Section III-B. Instead, to really consider the possibility to demand the key management and preservation at the physical layer, it is fundamental to assess the tamper-resistance of the involved devices and of the 5G network components.

D. Privacy and identity management

Privacy is intended as the preservation of users' sensitive information, which can also be derived from habits, profiling, tracing, or inferred from other information, such as location or services' preferences. Some application domains are more affected by the presence of sensitive data, such as health monitoring and services, traffic analysis, smart retail, and so on.

Vehicular networks, for example, could potentially gain a great advantage with the diffusion of 5G, since scalability and latency are the major drawbacks of current vehicular systems. However, security and privacy seamlessly represent critical issues, due to the kind of managed data (e.g., vehicles location, vehicles behavior). [50] proposes a secure and privacy-aware cloud-assisted video reporting service, whose scope is to instantly report the videos of traffic accidents to the nearest official vehicle in order to improve safety on the roads. Great attention is paid to preserve the participating vehicle's identity and the contents of the reported accident videos. The whole system is based on pseudonymous certificates and on public/private keys, which should guarantee the vehicles' authentication, the non-repudiation of the video sent by vehicles, and traceability. Its main drawback is the presence of a TA, which is assumed to be fully trusted and strongly protected so as to be difficult for any adversary to compromise it. The TA is a centralized entity, thus it potentially represents a single point of failure. A similar solution is outlined in [51].

Another application field is that of 5G-based Vehicular Social Network (VSN), which needs to manage the privacy for vehicle's location and trajectory, in an environment characterize by high mobility and multiple hops. Therefore, [52] constructs an architecture of 5G-based VSN with the Mobile Femtocell, and, then, proposes the Dynamic Group Division algorithm for privacy preserving, since it increases the chance of pseudonym exchanging with the proposed group generating protocol and pseudonym exchanging protocol.

The work in [53] proposes a scheme based on a blockchain, with the scope of solving the privacy issues in content-centric mobile networks for 5G. Content-centric networks suffer of huge range of content requests, which also hinders the reliability of the whole system. Hence, the openness and tamper-resistant of the blockchain ledger is exploited to ensure the access control and privacy of the services' provider; while the miner is selected by the users, so as to implement a sort of mutual trust among content providers and users. It is worth to remark that blockchain potentialities are really emerging in the last years; hence, such a technology, mainly due to its distributed nature, seems very promising in the 5G field, as long as issues related to the workload of blockchain itself are overcome. Another work which also exploits blockchain functionalities for content-centric networks, towards the realization of a trusted 5G vehicular networks, is [54].

The purpose of [55] is to present how to achieve secure users' digital interactions for ensuring privacy in the future 5G networks. The paper concludes that a distributed ecosystem consisting of a Trusted Third Party (TTP) among the end-user and the service providers could be integrated to secure the perspective of user controlled privacy. However, the effective feasibility and limitations of such a system does not really emerge.

Moving towards IoT context, another aspect to be considered is that, in order to allow an IoT application or digital service to use the network and its resources, the end-user must authenticate itself towards the service/application respective provider. To do this, a set of user credentials (i.e., username and password) is usually adopted to allow the user himself/herself to prove its authenticity towards the providers. However, the increasing number of available services and the need of increased security force the user to make various different combinations with strict rules to remember. To address such an issue and alleviate both users and service providers, mechanisms called *identity federations* were introduced, providing single sign-on solutions, which allow to simplify the registration and login processes for the user as well as reducing the costs for service providers, while handling with their Identity Management Systems. Following such principles, [56] presents an identity federation solution.

Fog computing is, instead, considered in [57], in order to reduce the load of computational overhead for enhanced security protection at the user side. Here, a list of options should be available at the side of fog nodes, so that they can intelligently and dynamically adjust the desired level of security protection for users' data. Note that cloud is perceived as an untrusted entity. Hence, such an idea of Quality of Protection (QoP) can be applied at the fog nodes in 5G networks, so that fog nodes can supply different levels of security protection to different data protection demands by users.

Outcomes. Also with respect to privacy, there is a variety of strategies which can be put in action, in particular the use of pseudonymous and of identity federations. As also emerged in Section III-A, blockchain appears as viable solution, along with fog computing, for supporting the definition of a privacy-aware 5G system. The main drawback related to many privacy techniques is due to the presence of a TA or TTP, which potentially represent single points of failure for the whole system. Hence, a distributed approach should be envisioned, mainly due to the wide area covered by 5G networks. As an alternative, combining federation techniques with fog computing and blockchain could represent an opportunity. It is worth to remark that efficiency, scalability and decentralization are the main requirements to take into account towards the definition of solutions tailored to the 5G environment in order to not weigh down the network.

E. Trust

The trust concept is used in various contexts and with different meanings. What is important is "how much" an entity "knows" another one. Such a relationship can be direct among the involved entities, or mediated by a certification (and, so, trusted) authority. In general, trust is a complex notion about which no definitive consensus exists in the scientific literature, although its importance is widely recognized. A main problem with many approaches towards trust definition is that they do not lend themselves to the establishment of metrics and evaluation methodologies. For such a reason, the need of trust models is often overlooked, since the 4G era. Now that 5G is coming, it is fundamental to ensure a certain level of 5G networks trustworthiness towards the end-users, in order to encourage 5G diffusion and adoption at a large scale. In general, people want to feel that they can trust the means by which they communicate their personal data.

The authors, in [58], mention trust, along with privacy protection and identity management, as critical challenges to be addressed in the 5G context, due to the fact that the promised 24/7 connectivity, involving heterogeneous devices, may generate a high number of attacks to be faced. Moreover, 5G enables immersive experiences, such as context-aware services, augmented reality, and concepts of anything-as-a-service and user customization, towards the provision of ubiquitous connectivity for smart objects in the IoT. These are the main motivation behind the need of a novel trust model tailored to the 5G domain, which still lacks.

Dimensions of trust levels, instead of a hierarchical attribute structure, are adopted in [42] (just presented in Section III-B). More in detail, a number of trust impact factor, such as communication times or users' vote, is considered to evaluate trust levels, which are further used to simplify the access policy by making it only based on such trust levels. On the basis of trust evaluation, CP-ABE primitives are exploited for the secret attributes' key generation.

The framework, proposed in [59], applies adaptive trust evaluation and management, and sustainable trusted computing technologies to ensure the computing platform trust and achieve security with the 5G core network. More in detail, it adopts cloud computing to securely deploy various trustworthy security services over the virtualized 5G networks. The main idea is to allow an authorized party to certificate a networking device's trustworthiness, and to embed the authorized party's policies/criteria/rules into the trust insurance component of the device, to serve as a proof for the device itself.

Tailored to the slicing service, the network slice trust degree concept, proposed in [60], establishes the following trust degree calculation model: the network slice trust value is divided into three parts, namely, the network slice subjective trust value calculation based on the cloud model algorithm, the network slice history trust value calculation based user evaluation, the reward and punishment calculation when the slice runs. Such a task is performed by the network slice manager, which, during the process, sets reasonable weighting parameters for the above three parts, according to the different security requirements of the network slices.

Outcomes. Note that the satisfaction of trust requirements is strictly related to the identity management and to the access control issues, treated in Sections III-D and III-B, respectively, because the profiles' protection and the supervisioning on the information's disclosure must be considered as pillars, since information of any kind can travel across the 5G network. Usually, a score is assigned to the trustworthiness grade of each network's actor, and its communication ability is suspended or denied in case the assigned score is lower than an established threshold. The main challenge is how to define which parameters, in a 5G environment, concur in the trust's calculation. In fact, the actors, services, and information involved in the 5G network are so various and dynamic during the time that the trust model must, consequently, adapt to such rapid environment's changes. Hence, conventional trust models must evolve towards a more flexible organization of the thresholds and efficient trust's calculation algorithms must be put in action.

F. *Policy enforcement*

Policy enforcement embraces the methods which are in charge of ensuring the actuation of well-defined security and privacy policies on the data in a system. Policy enforcement is often represented by a module of the system itself, able to filter the end-users' requests and enable only the disclosure of authorized resources. As the key management, presented in Section III-C, also policy enforcement is often overlooked by the research community, which fosters the definition of encryption and authentication schemes. However, the definition of accurate policies is fundamental for guaranteeing an adequate protection of the information managed within the network.

The authors of [61] advocate that 5G must do its best to eliminate malicious traffic, which is the main cause of failure of legitimate services (e.g., source address spoofing, DoS). Therefore, they propose that all communications in 5G should be controlled by policies, which should facilitate the cooperation of customer networks against misbehaving entities and the collection of evidence of malicious activity in real time. Dynamic policies can also react to hosts that are used in attacks. More in detail, contrary to the current Internet model, where any host can send a packet to any address, in [61], all communications are granted depending on the policy, which allows the receiver to decide what traffic it wants to receive, thus minimizing its risk. The policy effectively puts the receiver in charge of managing the flow admission, so as to balance the needs of the receiver with those of the sender. The underlying architecture is composed of edge switches, thus following the fog computing concept.

Seamlessly, the architecture described in [62] aims to automatically manage the network anomaly detection by using policies. By means of three types of policies and an orchestration process, in charge of making policy actions, the proposed system can deploy different actions to assure an effective anomaly detection process in real time. Note that policy actions establish the behavior of the network resources according to parameters, such as: network traffic, detection of anomalies, amount and mobility of users, and current state of the network resources.

The authors, in [63], propose to actuate policy enforcement mechanisms in 5G by means of Network Function Virtualization (NFV). However, no hints for a concrete design of a such a kind of architecture are provided.

Similarly, the service-oriented network resource slicing scheme, presented in [64], includes an inter-slice policy enforcement, which should ensures that each slice receives the corresponding network orchestration policy, traffic priority and frame configuration. The format of the policies is, however, not clearly defined.

Outcomes. With respect to policy enforcement, the proposed approaches are not presented in a clear way, mainly concerning the policy format and definition. Another crucial aspect regards how policies are managed and updated, mainly due to the dynamicity of IoT-5G network, which is higher than current existing application domains. In fact, a policy update should be extended to the whole network for being effective.. As emerged by the conducted analysis, policies are currently adopted to support anomaly detection processes (which will be discussed in the next Section III-G) and, therefore, to recognize and react to possible network's attack. Instead, policies should also have the role or regulating the access to the 5G network's resources, in combination with a proper access control framework, as presented in Section III-B.

G. Intrusion detection

The intrusion detection systems (IDS) involve all the mechanisms aimed at preventing, recognizing, and, sometimes, counteracting possible attacks, which can occur within the network (e.g., DoS, man-in-the-middle, tampering, etc.). IDS can be also put in relation with policies' definition and management, as emerged in the previous Section III-F.

The need of extending the coverage region of connectivity, required the introduction of new wireless components in the 5G networks, such as small cell access points and hotspots. However, such components are highly vulnerable to security breaches and provides an easy entry point for the intruder to enter into the network. The work in [65] focuses on the implementation of an IDS using an adaptive neuro-fuzzy inference system.

A neural network model is, also, employed in [66], for intrusion classification and prediction in 5G-IoT networks. Such a method uses the capability of learning complex patterns and behaviors to differentiate between normal traffic and network attacks.

A similar approach adopts an adaptive IDS using a hidden Markov Model for detecting an intrusion on small cell access points in the 5G wireless communication networks [67]. Also, the work in [68] follows an adaptive approach to recognize intrusions on the relay, small cell access point and base station, which realize a multistage 5G wireless communication network.

Instead, location-aware mobile intrusion prevention system, envisaged for 5G, is proposed in [69]. The Intrusion Detection Message Exchange Format (IDMEF) is used for activating the IDS alerts, and, in conjunction with the Intrusion Detection Exchange Protocol (IDXP), for transmitting the alerts from the mobile IDS sensors to a security operations center. The Security Assertion Markup Language (SAML) is used for authentication in a federated environment, and the well-known dynamic eXtensible Access Control Markup Language (XACML) based policies are used for authorization and security obligations in the mobile devices. Note that the alerts are anonymized along with location data, to avoid that sensitive information leaks out. Such a shrewdness avoids that location information can easily be linked to the device being monitored. Such an approach seems very promising, but neither a test-bed has been developed to perform some analysis, nor the scalability of the conceived system has been considered.

Finally, [70] proposes a high level framework, for securing mobile cloud computing by adopting IDS techniques, tailored to 5G networks. In such a framework, all data transmissions are delivered by the heterogeneous 5G networks, which provides the flexibility of networking choices for mobile users. Then, all data processing, required by intrusion detection, is migrated into cloud. Hence, such an approach does not take into account, for example, fog computing to pursue a more distributed solution.

Outcomes. The adoption of intrusion detection mechanisms is mainly fundamental to avoid misbehavior of the network's participants or DoS/DDos attacks, which could block the functionalities of a part of the network. As emerged, current conceived approaches are based on artificial intelligence methods or on location-aware techniques. The main issue is how to manage the IDS itself in the wide 5G environment, in a capillary way, without hindering the service provision to the more constrained devices.

IV. Discussion

The analysis, conducted in Section III, on existing recent papers on 5G security and privacy requirements has emerged many peculiarities and leads to make some important thoughts, examined in the following. Table II summarizes the topics addressed by the works discussed in Section III, split on the basis of the treated security and privacy features. What clearly emerges looking at Table II (and also confirmed in Section III) is that authentication methods are the most investigated in literature, along with privacy and identity management; while other topics still deserve much more attention by the research community.

Moreover, Table III shows the role of fog computing and blockchain timidly emerge. Such an aspect will be deeply treated in the next Sections IV-A and IV-B.

A. The role of fog computing

Inevitably, the security and privacy issues and solutions strictly depend on the network's infrastructure to manage and on the entities involved, which include, in the 5G-IoT scenario, heterogeneous devices, so as a multitude of different kinds of information has to be handled. As shown in Figure 2, 5G is conceived as a network composed of macro-cells and micro-cells, where proper base stations and/or hotspots must be installed, in order to guarantee a pervasive connectivity. Such components may be further connected to a cloud, thus requiring an efficient management of the IoT request at fog layer, in order to reduce communication and computation at the cloud as much as possible, while supporting scalability of service provision, as discussed in [71].

Moreover, the transmitted data also require to be processed in some ways and, to this end, the introduction of a ”fog layer” seems to be a viable solution, mainly due to the advent of IoT applications, which require to handle, as much as possible close to the end-devices, the huge amount of acquired information to be further shared with interested users. Hence, the fog computing concept expects that a number of smart devices belonging to the ”fog” layer of the network acts as intermediaries between the end-users/sources, and the core network. They are essentially conceived as powerful devices, routers, or gateways, owning processing capabilities to be exploited to perform specific computing tasks, such as data elaboration or aggregation, algorithms' execution, and security tasks [4]. Hence, fog nodes can be represented as proxies, which are also able to provide cryptographic computations; while the underlying IoT devices and sensors lack the necessary resources to do such tasks. Hence, fog computing not only provides additional computational resources to the network, but also a further level of security that could help in preventing, minimizing, and also counteracting attacks in the 5G-IoT environment. Furthermore, the adoption of fog computing paradigm could help in preserving privacy of IoT data and in protecting users' sensitive information by reducing the need to transmit certain kinds of data to the core network. However, such an approach also introduces several challenges concerning data, location's, and users' security and privacy. The following aspects deserve particular attention:

- How 5G network' components, which are integrated in a fog layer, could efficiently cooperate, in order to fulfill the desired goals of ensuring the reliability of communications within the 5G network?
- How to ensure end-to-end security from data acquisition by data producers and their reception to data consumers, taking into account all the involved network's components, including heterogeneous IoT devices, the core network's participants and the global network?
- How to regulate the access control and authentication of end-users' devices or data sources in such an heterogeneous environment? Should a hierarchy be established among fog nodes, core networks, and end-devices?
- How to put in action an efficient key management system, in order to protect the handled information?
- How to guarantee anonymization, privacy and trust throughout the whole data life-cycle?
- How to support policies' enforcement definition, update, and synchronization, even across different application realms?
- Is it possible to integrate, in the wide 5G-IoT network, a policy enforcement framework?
- How to prevent and monitor internal and external attacks both to end-devices and to network's components? And, how is it possible to react against violation attempts?
- How to put in action logging and reporting systems about the 5G network activities, in order to reveal anomalies? And, which information is useful for being logged?

Other key challenges are represented by mobility and QoS. To cope with such issues, a promising technology, which is recently emerging, is network slicing [72]. In fact, driven by the increased massive wireless data traffic from different application scenarios, efficient resource allocation schemes should be exploited to improve the flexibility of network resource allocation and capacity of

TABLE II: Security and privacy requirements treated by works about 5G

Requirement	Related work	Total
Integrity, confidentiality and non-repudiation	[28] [29] [30] [31] [32] [33] [50]	7 works
Authentication and access control	[23] [30] [31] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [48] [50] [53]	16 works
Key management	[29] [46] [47] [48]	4 works
Privacy and identity management	[23] [48] [50] [52] [53] [54] [55] [56] [57] [58] [69]	11 works
Trust	[42] [54] [58] [59] [60]	5 works
Policy enforcement	[61] [62] [63] [64]	4 works
Intrusion detection	[23] [62] [65] [66] [67] [68] [69] [70]	8 works

TABLE III: Use of blockchain and fog computing in 5G

Paradigm	Related work	Total
Fog computing	[35] [36] [57] [61]	4 works
Blockchain	[33] [38] [39] [40] [53] [54]	6 works

5G networks, based on network slicing. Moreover, new mobility management schemes are needed to guarantee seamless handover in 5G systems. Such aspects, jointly with the adoption of fog computing, may also affect security and privacy requirements, since IoT-devices frequently join to, leave from, and move into the network, in a highly dynamic way. The following questions naturally emerge:

- How to continuously guarantee adequate QoS levels, in presence of both mobility and security&privacy mechanisms?
- How to protect the information related to IoT-devices' location?
- How to manage the authentication in presence of multiple services, network's densification, and considering the mobility of end-devices?
- How to manage encryption/decryption keys' update or revocation, in presence of cryptography algorithms?

The answers to such questions would require an effort both in terms of hardware and protocols. Moreover, new proposed approaches must take into account the energy and computational constraints of end IoT devices.

B. The role of blockchain

Blockchain technology has recently attracted the interest of stakeholders across different industrial activities, ranging from finance (the first and most famous use is in cryptocurrency), healthcare, product traceability, real estate, smart cities, smart homes, and so on [7], thus paving the way for its adoption in various application context and, more specifically, in the IoT [73]. But, as emerged in Section III, a limited role for blockchain is also emerging in the 5G environment.

A block in a blockchain contains the following information:

- A set of transactions (i.e., the data content)
- A timestamp
- A cryptographic hash function, such as merkle tree or binary hash tree, which is exploited by the blockchain in order to address block's integrity; in such a way, a further level of security is introduced
- A reference to the preceding block, so as to identify the current block's place in the blockchain; note that, since each block references the hash of the block that came before it, a link between the blocks is established, thus creating a chain of blocks, named blockchain
- If needed, the so-called smart contracts, which are scripts that allow the coding and execution of computing programs on the blockchain itself; note that such scripts may contains access policies, which can be specified and enforced by the blockchain itself, preventing unauthorized operations on data.

The advantages of blockchain, obviously in terms of security, can be summarized as follows:

- **Decentralization**: blockchain does not need a centralized authority in charge of supervisioning the system's behavior and dictating the rules or policies to be applied at each time; moreover, the transactions are validated by all (or by a group of) the network's components, thus avoiding to delegate such a task to a central entity

- **Distribution of the information**: since each network's components holds a copy of the blockchain, there is (again) no need of a centralized authority which keep such information privately
- **Data transparency and auditability**: since a full copy of each transaction executed within the system is stored in the blockchain and since the blockchain is public to all the peers, then it is always possible to trace and monitor what happens in the network, guaranteeing that operations are legitimate
- **Robustness**: the blockchain is tamper-proof, hence it cannot be manipulated by malicious parties.

Ad a consequence, by adopting a blockchain, applications that usually run only through a trusted intermediary, can now operate in a decentralized fashion, without the need for a central authority, and achieve the same functionalities. Furthermore, it is worth to remark that some blockchain's features provide an answer to some of the questions raised in Section IV-A, such as the monitoring of network's activities, and end-to-end security. Even if blockchain seems to be the perfect solution to solve the some of the proposed challenges, it also suffers of some drawbacks [7], which are: (i) high resource demand for verifying the validity of a block; (ii) long latency for transactions' confirmation; (iii) low scalability, due to the broadcasting transactions and blocks to the whole network. Such limits can be faced by integrating the blockchain mechanism in the fog layer, so as to delegate to fog nodes the heaviest tasks, but future solutions must seriously pay attention to maintain the efficiency of 5G technology with respect to the adopted security and privacy methods.

C. Challenges and future directions

The previous Sections IV-A and IV-B pointed out the importance of the recent fog computing and blockchain paradigms and also raised some important questions, which deserve responses in order to ensure a proper level of reliability to 5G-IoT systems. In light of the analysis conducted in Sections III, it is now possible to summarize the open challenges and future research directions in the field of security and privacy in 5G-IoT networks. Note that the implementation of 5G will be pursued by many current and developing technologies, such as: (i) Heterogeneous Networks (HetNets); (ii) Software Defined Networks (SDNs); (iii) Massive MIMO; (iv) Multiple Radio Access. All such technologies come with their own security challenges. For example, HetNets require frequent handover, which directly affects the authentication process in the network, especially with the small latency requirement of 5G. Also, cloud computing and SDNs cause an increment in the number of DDoS attacks due to the On-Demand Self-Service feature of cloud computing. Although the authentication and robustness of SDN are addressed by having a decentralized control and exploiting user-dependent security context, the security of 5G and all the emerging technologies involved in 5G must be more extensively addressed, in order to ensure security and privacy to be guaranteed to the end-users.

Data protection. With respect to data protection, as emerged in Sections III-A, sec:sec4 and III-F, a central role is acted by the encryption mechanisms. Some ciphering techniques have been specified in the proposed solutions, which range from AES and RSA to other more recent, maybe more suitable for resource constrained devices, ECC and Quantum Cryptography. Such mechanisms can be adopted to encrypt both data contents and location's information, in order to preserve their confidentiality and integrity and to guarantee privacy for the users' sensitive information. It is worth to remark that ECC provides short key lengths, reduced message sizes and lower resource usages; hence, ECC should not compromise the efficiency of 5G communications. The small size of the keys, with respect, for example, to RSA, makes the ECC an ideal choice for devices with limited storage or data processing resources, which are increasingly common in the field of IoT. Moreover, if fog nodes offload some of computation and storage overheads from devices in proximity, then a better scalability is achieved; also, less overhead in storage and communications is provided with respect, as just mentioned, to RSA based schemes, employed in SSL/TSL, guaranteeing the same level of security. Another fundamental issue is how to distribute and protect the credentials, owned by the involved devices, and recover the system in case of violation.

Resource disclosure. Concerning access control and authentication, some promising approaches have been cited and could represent relevant starting points for further investigations in the area, such as the adoption of group signatures or pseudonyms. Traditional public key infrastructure-based authentication schemes may provide networks with identity authentication and conditional privacy protection, which are not enough for assessing the reliability of information. Additionally, although 5G can dramatically improve the data transmission efficiency, many existing authentication schemes are based on complex bilinear pairing operations, and the calculation time is too long to be suitable for delay-sensitive 5G-enabled networks, as emerged in Section III-B. To cope with such an issue, ABE mechanisms could be adapted to 5G needs. In fact, ABE mechanisms allow to encrypt data for multiple recipients, in such a way that only those recipients whose attributes satisfy a given access policy can decrypt afterwards. A distributed architecture, resulting from the combination of 5G and fog computing, is an ideal candidate to actuate proper measures to grant access tokens to authorized parties, who use them to perform given actions (e.g., data decryption). Also, a fog computing platform can be used as a sort of distributed trust authority to authorize access and disclose data among authorized parties and end-devices. New solutions should enable and encourage the control on the data by the owners themselves, which should be provided with the necessary means for establishing, in an autonomous or semi-autonomous way, how to share their information. Such an approach is mainly due to the dimension of future 5G-IoT networks, which should distribute as much as possible the tasks to perform. In such a direction, another feasible approach is that of sticky policies [74]. Sticky policies are transmitted along with the data they refer to throughout the entire data life cycle. The concept of sticky policy is to attach security and privacy policies to owners' data and drive access control decisions and policy enforcement. Sticky policies allow specifying access rule in an extremely fine-grained manner: in principle every data unit could have its own, unique, policy. Furthermore, as policies 'travel' with the data across the entire system, they could provide protection over the entire data life cycle, independently from the network dimension. In this sense, sticky policies could help users to pursue their rights and actively manage the rules to be applied to their own information. Such an approach represents a fundamental step for improving the trustworthiness of the users with respect to the future 5G service providers and for avoiding improper resources' use or disclosure. Furthermore, ABE or sticky policy based mechanisms could be integrated in a blockchain, to provide a further level of security to the transmitted information.

Trust and rogue node detection. As emerged from Sections III-B and III-E, some access control systems typically require the presence of a TA or TTP in order to manage access permissions to resources. Moreover, there is usually the presence of an entity responsible for managing, in some ways, the reputation of the network's participants. But, in such a scenario, is it possible to envision a system, where parties are only partially trusted (e.g., honest-but-curious)? Or the end-devices must trust the fog nodes and, in turn, the fog nodes must trust the core network? Summarizing, a sort of ”chain of trust” must be specifically designed for 5G environments, taking into account all the entities involved and the parameters to be evaluated. Moreover, the end-devices are vulnerable to physical attacks, since they are far from the core network and communications take place over the 5G network. To ensure end-to-end security, it is also essential to protect the devices against hardware tampering or electromagnetic eavesdropping. Another fundamental concern is that most end-devices and fog nodes are usually remotely managed. The remote management offers opportunities for adversaries to conduct various network-based attacks, and makes the detection and mitigation of such attacks more difficult and expensive.

Monitoring, logging, reporting. Monitoring, logging, and reporting represent crucial requirements for any security system, since they also allow to detect attacks (Section III-G) and check the ability of the system to behave as expected, in response of occurring situations. In the case of 5G, and even more if it is integrated with fog nodes, such a monitoring should cover the whole data life-cycle. Such an aspect represents a distinctive feature with respect to traditional monitoring and detection solutions, which usually involve a limited area. In a 5G based system, the most part of the network is not considered trusty, thus forcing to run the monitoring, logging, and reporting tasks towards the end-devices and network's components. Recognizing issues will allow to trigger proper notifications for allowing the system to promptly react to violations and threats. Also, the attacks propagation should be inhibited.

Further considerations. Other relevant aspects, which are not treated in this work because they are not directly tailored to security and privacy, are: (i) the definition of **performance and low-overhead mechanisms** for 5G communications, able to preserve bandwidth and network's resources [75] or to save energy (i.e., towards green 5G networks) [76]; (ii) the put in action of **standardization** processes, which are already active thanks to the 3rd Generation Partnership Project (3GPP) [77], which should help in finding common interfaces and protocols, to guarantee the maximum interoperability within the 5G network; (iii) existing **platform and tools**, which can be used to evaluate and test new contribution in the 5G field [16]; (iv) **ongoing projects** and activities all over the world, which are discussed in [2].

V. Conclusion

As emerged from the analysis conducted in this paper, the real spreading of 5G network, and the consequent services provision, require the design of novel security and privacy solutions, in order to guarantee, in a capillary way, the reliability and the robustness over the whole system. The overview provided with such a survey arises many open issues, and sheds some light on research directions in the 5G security field. More in detail, a unified vision regarding the insurance of security and privacy requirements in such an environment, mainly characterized by very low latency, is still missing. Suitable solutions need to be developed; they should be independent from the involved devices, but should take into account the architecture of the 5G-based system itself. Moreover, the new proposed approaches must guarantee: integrity, confidentiality, non-repudiation, authentication methods, access control, privacy for information and devices, trustworthiness among the 5G network's components and end-users, and compliance with defined security and privacy policies. Much efforts are being spent by the worldwide scientific community to address aforementioned topics, but there are still many open challenges to be faced. We do hope that the discussion we provided can be of interest for various audiences, including most notably PhD candidates, research consortia and IT industry, in order to pursue in the realization of secure and privacy-aware 5G infrastructures.

References

[1] P. Sharma, "Evolution of mobile wireless communication networks-1g to 5g as well as future prospective of next generation communication network," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 8, pp. 47–53, 2013.

[2] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," *IEEE access*, vol. 3, pp. 1206–1232, 2015.

[3] S.Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, "A secure and quality-aware prototypical architecture for the Internet of Things," *Information Systems*, vol. 58, pp. 43–55, 2016.

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

[5] P. Schneider and G. Horn, "Towards 5g security," in *IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1165–1170.

[6] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464, 2017.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[8] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5g: Survey and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, 2017.

[9] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–655, 2016.

[10] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5g: The next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[11] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5g: Ran, core network and caching solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3098–3130, 2018.

[12] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmwave) for 5g: opportunities and challenges," *Wireless networks*, vol. 21, no. 8, pp. 2657–2676, 2015.

[13] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5g networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, 2017.

[14] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5g," *IEEE communications surveys & tutorials*, vol. 20, no. 3, pp. 2294–2323, 2018.

[15] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, "5g backhaul challenges and emerging research directions: A survey," *IEEE access*, vol. 4, pp. 1743–1766, 2016.

[16] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5g network edge cloud architecture and orchestration," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017.

[17] D. Liu, L. Wang, Y. Chen, M. Elkashlan, K.-K. Wong, R. Schober, and L. Hanzo, "User association in 5g networks:

A survey and an outlook," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1018–1044, 2016.

[18] S. Buzzi, I. Chih-Lin, T. E. Klein, H. V. Poor, C. Yang, and A. Zappone, "A survey of energy-efficient techniques for 5g networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 4, pp. 697–709, 2016.

[19] P. Zhang, J. Lu, Y. Wang, and Q. Wang, "Cooperative localization in 5g networks: A survey," *ICT Express*, vol. 3, no. 1, pp. 27–32, 2017.

[20] S. Li, L. Da Xu, and S. Zhao, "5g internet of things: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, 2018.

[21] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5g networks for the internet of things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2017.

[22] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[23] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[24] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[25] A. Tewari and B. Gupta, "Security, privacy and trust of different layers in internet-of-things (iots) framework," *Future generation computer systems*, 2018.

[26] V. Adat and B. Gupta, "Security in internet of things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, no. 3, pp. 423–441, 2018.

[27] B. Gupta and M. Quamara, "An overview of internet of things (iot): Architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience*, p. e4946, 2018.

[28] A. Khan, J. Abdullah, N. Khan, A. Julahi, and S. Tarmizi, "Quantum-elliptic curve cryptography for multihop communication in 5g networks," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 17, no. 5, pp. 357–365, 2017.

[29] E. Abd-Elrahman, H. Ibn-Khedher, H. Afifi, and T. Toukabri, "Fast group discovery and non-repudiation in d2d communications using ibe," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2015, pp. 616–621.

[30] M. Schmittner, A. Asadi, and M. Hollick, "Semud: Secure multi-hop device-to-device communication for 5g public safety networks," in *IFIP Networking Conference (IFIP Networking) and Workshops*. IEEE, 2017, pp. 1–9.

[31] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of lorawan and 4g/5g for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60–67, 2018.

[32] J. Liu, L. Zhang, R. Sun, X. Du, and M. Guizani, "Mutual heterogeneous signcryption schemes for 5g network slicings," *IEEE Access*, vol. 6, pp. 7854–7863, 2018.

[33] M. A. S. Santos, A. Ranjbar, G. Biczók, B. Martini, and F. Paolucci, "Security requirements for multi-operator virtualized network and service orchestration for 5g," in *Guide to Security in SDN and NFV*. Springer, 2017, pp. 253–272.

[34] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-layer authentication protocol design for ultra-dense 5g hetnets," in *IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[35] Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, "Lacs: A lightweight label-based access control scheme in iot-based 5g caching context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.

[36] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.

[37] J. Cao, M. Ma, H. Li, Y. Fu, and X. Liu, "Eghr: Efficient group-based handover authentication protocols for mmtc in 5g wireless networks," *Journal of Network and Computer Applications*, vol. 102, pp. 1–16, 2018.

[38] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5g hetnets," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[39] Z. Chen, S. Chen, H. Xu, and B. Hu, "A security authentication scheme of 5g ultra-dense network based on block chain," *IEEE Access*, vol. 6, pp. 55 372–55 379, 2018.

[40] V. Messié, G. Fromentoux, X. Marjou, and N. L. Omnes, "Baladin for blockchain-based 5g networks," in *22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2019, pp. 201–205.

[41] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating dos attacks against pseudonymous authentication through puzzle-based co-authentication in 5g-vanet," *IEEE Access*, vol. 6, pp. 20 795–20 806, 2018.

[42] Z. Yan, H. Xie, P. Zhang, and B. B. Gupta, "Flexible data access control in d2d communications," *Future Generation Computer Systems*, vol. 82, pp. 738–751, 2018.

[43] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "Rsma: Reputation system-based lightweight message authentication framework and protocol for 5g-enabled vehicular networks," *IEEE Internet of Things Journal*, 2019.

[44] D. Chaum and E. Van Heyst, "Group signatures," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1991, pp. 257–265.

[45] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "A secure icn-iot architecture," in *2017 IEEE international conference on communications workshops (ICC workshops)*, 2017, pp. 259–264.

[46] R. Sedidi and A. Kumar, "Key exchange protocols for secure device-to-device (d2d) communication in 5g," in *2016 Wireless Days (WD)*. IEEE, 2016, pp. 1–6.

[47] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5g wireless communication net-

works using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[48] M. Khan, V. Niemi *et al.*, "Privacy enhanced fast mutual authentication in 5g network using identity based encryption," *Journal of ICT Standardization*, 2017.

[49] M. Burmester and Y. Desmedt, "A secure and scalable group key exchange system," *Information Processing Letters*, vol. 94, no. 3, pp. 137–143, 2005.

[50] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5g-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7868–7881, 2016.

[51] A. Mohseni-Ejiyeh and M. Ashouri-Talouki, "Sevr+: Secure and privacy-aware cloud-assisted video reporting service for 5g vehicular networks," in *Iranian Conference on Electrical Engineering (ICEE)*. IEEE, 2017, pp. 2159–2164.

[52] D. Liao, G. Sun, M. Zhang, V. Chang, and H. Li, "Towards location and trajectory privacy preservation in 5g vehicular social network," in *IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 2, 2017, pp. 63–69.

[53] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2017.

[54] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5g vehicular networks: Blockchains and content-centric networking," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 121–127, 2018.

[55] L. T. Sorensen, S. Khajuria, and K. E. Skouby, "5g visions of user privacy," in *IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–4.

[56] B. Santos, B. Feng, T. van Do *et al.*, "Towards a standardized identity federation for internet of things in 5g networks," in *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2018, pp. 2082–2088.

[57] S. Xu, Y. Qian, and R. Q. Hu, "Privacy-preserving data preprocessing for fog computing in 5g network security," in *IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[58] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User privacy, identity and trust in 5g," *A Comprehensive Guide to 5G Security*, p. 267, 2018.

[59] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security and communication networks*, vol. 9, no. 16, pp. 3059–3069, 2016.

[60] B. Niu, W. You, H. Tang, and X. Wang, "5g network slice security trust degree calculation model," in *3rd IEEE International Conference on Computer and Communications (ICCC)*, 2017, pp. 1150–1157.

[61] R. Kantola, J. Llorente Santos, and N. Beijar, "Policy-based communications for 5g mobile with customer edge switching," *Security and Communication Networks*, vol. 9, no. 16, pp. 3070–3082, 2016.

[62] L. F. Maimó, A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, and G. M. Pérez, "Dynamic management of a deep learning-based anomaly detection system for 5g networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 8, pp. 3083–3097, 2019.

[63] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, "Network function virtualization in 5g," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 84–91, 2016.

[64] S. Costanzo, R. Shrivastava, K. Sarndanis, D. Xenakis, X. Costa-Pérez, and D. Grace, "Service-oriented resource virtualization for evolving tdd networks towards 5g," in *IEEE Wireless Communications and Networking Conference*, 2016, pp. 1–6.

[65] R. Devi, R. K. Jha, A. Gupta, S. Jain, and P. Kumar, "Implementation of intrusion detection system using adaptive neuro-fuzzy inference system for 5g wireless communication network," *AEU-International Journal of Electronics and Communications*, vol. 74, pp. 94–106, 2017.

[66] S. Rezvy, Y. Luo, M. Petridis, A. Lasebae, and T. Zebin, "An efficient deep learning model for intrusion classification and prediction in 5g and iot networks," in *2019 53rd Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2019, pp. 1–6.

[67] A. Gupta, R. K. Jha, and S. Jain, "Attack modeling and intrusion detection system for 5g wireless communication network," *International Journal of Communication Systems*, vol. 30, no. 10, p. e3237, 2017.

[68] A. Gupta, R. K. Jha, P. Gandotra, and S. Jain, "Bandwidth spoofing and intrusion detection system for multistage 5g wireless communication network," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 618–632, 2017.

[69] N. Ulltveit-Moe, V. A. Oleshchuk, and G. M. Køien, "Location-aware mobile intrusion detection with enhanced privacy in a 5g context," *Wireless Personal Communications*, vol. 57, no. 3, pp. 317–338, 2011.

[70] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5g," *Security and Communication Networks*, vol. 9, no. 16, pp. 3049–3058, 2016.

[71] A. Al-Qerem, M. Alauthman, A. Almomani, and B. Gupta, "Iot transaction processing through cooperative concurrency control on fog-cloud computing environment," *Soft Computing*, pp. 1–17, 2019.

[72] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. Leung, "Network slicing based 5g and future mobile networks: mobility, resource management, and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[73] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[74] S. Pearson and M. Casassa-Mont, "Sticky policies: An approach for managing privacy across multiple parties," *Computer*, vol. 44, no. 9, pp. 60–68, 2011.

[75] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, “Internet of things in the 5g era: Enablers, architecture, and business models,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[76] U. K. Dutta, M. A. Razzaque, M. A. Al-Wadud, M. S. Islam, M. S. Hossain, and B. Gupta, “Self-adaptive scheduling of base transceiver stations in green 5g networks,” *IEEE Access*, vol. 6, pp. 7958–7969, 2018.

[77] A. Morgado, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, “A survey of 5g technologies: Regulatory, standardization and industrial perspectives,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 87–97, 2018.