IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 18, 2020, accepted January 15, 2021, date of publication January 21, 2021, date of current version February 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3053233

Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review

BELAL ALI, (Member, IEEE), MARK A. GREGORY, (Senior Member, IEEE), AND SHUO LI, (Member, IEEE)
School of Engineering, RMIT University, Melbourne, VIC 3000, Australia

Corresponding author: Mark A. Gregory (mark.gregory@rmit.edu.au)

ABSTRACT Multi-Access Edge Computing (MEC) is an extension of cloud computing that aims to provide computation, storage, and networking capabilities at the edge of the network in close proximity to end-users. The MEC architecture supports applications and services that bridge between cloud computing and end-users. The architecture includes devices and systems that are interconnected, layered, and flexibly deployed. As a result of the technological advancements, MEC is facing a myriad of highly sophisticated threats. This paper provides a review of MEC Architecture, use cases, conceptual guidelines for MEC security architecture, security and privacy techniques, and identifies current and future challenges, their implications, and approaches to overcome the challenges. This research examined significant threats, described the MEC architecture, identified the susceptible functional layers, the different categories of threats, and the potential security safeguards. The research recommends that MEC providers should implement multiple layers of security controls to mitigate targeted attacks.

INDEX TERMS Multi-access edge computing, MEC, security, privacy, SDN, 5G.

I. INTRODUCTION

Multi-Access Edge Computing (MEC) is an evolving technical solution that moves the computing and storage needed to support high-bandwidth, low-latency applications to the edge of the network and closer to end-users [1], [2]. MEC was first proposed in 2009 by Microsoft [3], and over the past decade, network operators have welcomed the additional functionality and capabilities offered by MEC. Interaction with the applications and services offered over the Internet has become a daily activity [2], [4]–[7] and over time, the applications, services, and the underlying networks have evolved [8]. The main rationale for MEC is to provide end-users with improved Quality of Service (QoS) and Quality of Experience (QoE).

MEC can be recognised as a specific case of the next generation of Mobile Cloud Computing (MCC) [2]. MEC is an emerging technology for 5G mobile networks with a decentralized computational architecture in which computing resources and application services can be spanned across the communication path from the data source to the cloud that brings forward the technical benefits of improving application performance, satisfying data privacy and security concerns as well as capacity enhancements in the backhaul and core networks [2], [8]–[10].

While a Software-Defined Edge Computing architecture solves several data traffic issues such as latency and jitter in access networks [11], it can also present new vulnerabilities [8], [10], [12], [13], resulting in a larger overall attack surface and potential security threats.

Despite the increasing acceptance of MEC as a mechanism to improve the performance of connected smart devices and end-user experience, security remains one of the most significant challenges for the creation of an edge paradigm ecosystem [8], [9], [14]. MEC's unique characteristics of highly diverse building blocks to enable the technologies and techniques for computation offloading to network architectures introduces new risks [2], [15], [16].

It is essential not only to secure the building blocks but also to orchestrate diverse security mechanisms to create an autonomous view that allows their integration and interoperability [17]. Therefore, when considering MEC security, tracking the threat landscape becomes more challenging. The use of proximate edge servers delivers a capable solution to circumvent these challenges. For instance, due to the small-scale nature of distributed deployments, and the

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

reduced concentration of valuable information, MEC servers are less prone to a security attack [18]. MEC nodes could be privately-built cloudlets, which ease the risk of information leakage. Employing ‘‘security by design’’ is substantial to securing components and communication channels within the MEC environment [19], [20].

Data security and privacy have consistently been a significant issue in the Information and Communication Technology (ICT) space. Data security and privacy become particularly severe in the MEC environment [13], [19]–[22] because data is scattered across different nodes and storage devices, including servers, PCs, mobile devices and wireless network sensors. Data security and privacy in the MEC is more complicated than conventional information systems.

To facilitate the adoption of MEC by mobile operators and enterprise customers, the security concerns should be rectified to ensure MEC environment trustworthiness. A trustworthy architecture is a fundamental prerequisite to gain the confidence of users when adopting new technologies. Security has become a substantial factor in the design of MEC architectures and modes of operation.

Identifying security risks and mitigation strategies that can be implemented in the MEC paradigm is a crucial focus for MEC research and development. For this reason, this paper provides a review of MEC related research and the development of security risk mitigation strategies for MEC. The contribution of this review is to:

- Investigate the MEC architecture, functional layers and to identify the security challenges.
- Provide a comprehensive survey of MEC data security domains and present a holistic overview of related works in each domain. In particular, access control, identity and authentication, data confidentiality, data integrity, communication security and privacy-preserving.
- Identify and examine previous work on MEC security challenges, i.e., threat vectors and actors for MEC functional layers and map the matching security safeguards and controls.
- Discuss the open challenges and present the future research directions, e.g., software-defined segmentation, cloud-native security mechanisms, security orchestration, MEC applications and services, and integrated trust management.

The rest of this paper is organized as follows. Section II presents the ETSI MEC Reference Architecture. Section III outlines MEC Security Architecture. Section IV provides a review of data security and privacy-preserving technologies and mechanisms. Section V addresses MEC security and privacy challenges. Based on our findings, Section VI describes the open issues and future research directions. Finally, Section VII concludes this paper.

II. ETSI MEC REFERENCE ARCHITECTURE

Before the data security and privacy issues are discussed, the MEC environment structure should be analyzed first. The concept of a computing platform located at the mobile network edge was carried out by the ETSI MEC ISG [15], commencing in December 2014. The primary MEC concept is to provide storage, computational capacity and service delivery at the edge of the mobile network, enabling emerging vertical business segments, applications and services for consumers and enterprise customers [8], [9].

Distinctive features of the MEC architecture [1], [2], [19], [23] are low latency, proximity, location-aware, high bandwidth, and real-time insight into radio network information. These capabilities facilitate accelerated content delivery services and applications, delivered at the mobile network's edge, closer to the end-users. The mobile subscriber's experience can be significantly improved through the more efficient network and service operations, enhanced service quality, minimized data transit costs and reduced network congestion.

A. MEC ARCHITECTURE COMPONENTS

The MEC reference architecture [15], [16] contains entities which are grouped in two mobile edge levels, namely host and system levels as depicted in Fig. 1 and are briefly introduced as follows:

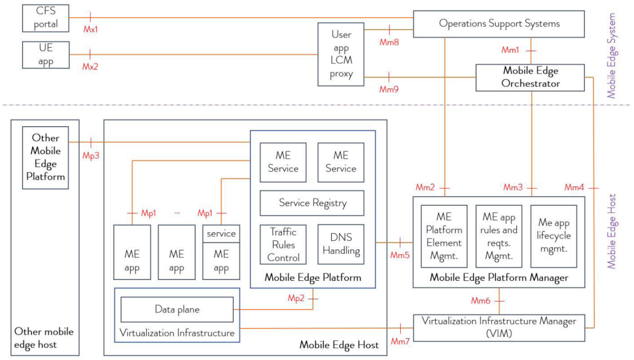

FIGURE 1. **MEC Architecture.**

- *ME host and network:* The host layer is represented by the middle level of the MEC reference architecture [15], [16]. It includes the ME Host and ME Host management entities. The MEH comprises the ME platform, applications and Virtualization Infrastructure (VI). The VI provides the computing, networking and storage infrastructure that is used to host ME applications and services. The network layer provides the connectivity between the internal and external entities.
- *MEC platform:* The MEP supports application and service hosting on virtualized infrastructure and enables ME applications as services. MEP is also responsible for the instantiation and termination of ME applications if requested by the MEC platform manager (MEPM) [15], [16].
- *MEC orchestrator:* The MEO is a system-level management layer [15], [16]; it includes a platform manager and a VI Manager (VIM). Its primary responsibilities

include application and service provisioning utilizing the ME VI resources, maintaining ME resource information such as topology, available MEH resources and services and integrity and authenticity checks for the ME application packages. The MEO also carries out policy enforcement.

- *Operation support system:* The OSS is responsible for granting access to user subscription requests forwarded from User Equipment (UE) via the User Application Life-Cycle Management Proxy [15], [16].

B. MEC FUNCTIONAL LAYERS

MEC as a technology is relatively new, nevertheless, according to 5G-PPP [24], MEC is one of the architectural concepts and prime technologies that will drive the next generation of network evolution and serve as a key enabler to edge applications leveraging 5G networks.

The MEC functional structure comprises of four functional layers [15], [16], end devices, access network, edge network and core infrastructure, as depicted in Fig. 2. The end devices layer includes the devices connected to the access network, e.g., IoT devices, IP cameras and mobile terminals [2]. The access network serves as the connection between the functional layers and the Internet [19], [20]. The edge network combines the MEC and Network Function Virtualization (NFV) concepts [8], [9], that are typically owned by the infrastructure provider through multi-tenancy VI. MEC can be deployed through multiple edge networks that continuously cooperate and remain connected to the traditional cloud [10]. Core infrastructure represents the centralized MEC control and management functions for mobile end devices.

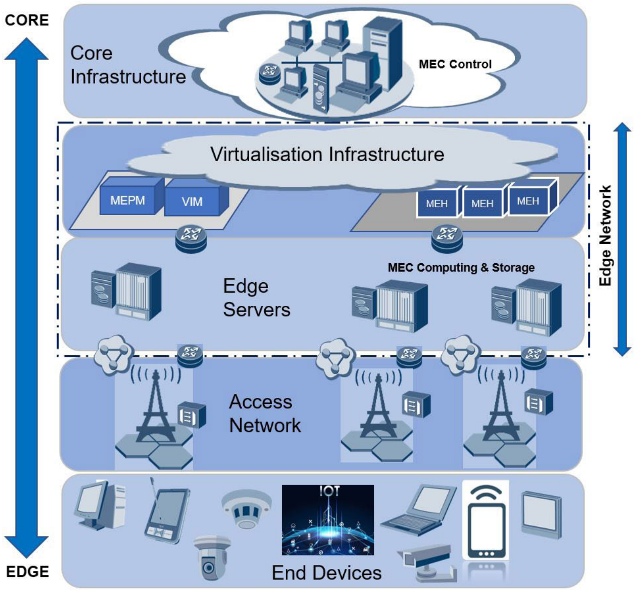

FIGURE 2. MEC Functional Structure.

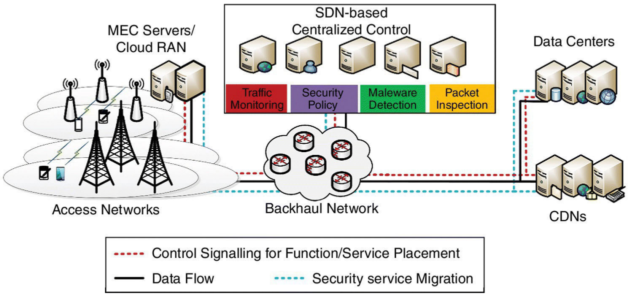

FIGURE 3. Centralized Security Architecture for MEC [10].

C. MEC CHARACTERISTICS AND USE CASES

The MEC architecture is a complementary unification of information technology, and telecommunication domains in a virtualized platform serving computation and storage capabilities at the edge of the network [2], [15], [25], as shown in Fig 1. MEC integrates application server platforms into the edge servers, its key features being proximity to a data source, mobile users, application services and connectivity technologies. MEC offers the following benefits:

- *Low latency:* Extending computing resources to the edge of the network means faster packet arrival, and reduced delay before content streaming commences [2], [26]. Networks with MEC are more suitable for delay-sensitive applications, and lower latency translates into improved QoE for the end-users [2].
- *High-efficiency:* By processing and storing content in proximity to user applications at the edge, the data forwarding through the backhaul network is significantly reduced [2], [6]; therefore, efficiency gains can be achieved [20], [27].
- *Backhaul capacity:* Data destined for the backhaul links are efficiently transmitted through designated channels, thus minimizing the signal load on the core network [19], [20].
- *User context and network status awareness:* MEC deployed at the edge facilitates access to a real-time network and channel information. Intelligent applications [2], [26] can leverage location and user context locally to process and aggregate data at the edge of the network [28], [29].
- *Cost savings:* We cannot overlook the economic elements; MEC leverages a distributed server architecture [2], [15], which reduces or eliminates the need to pay for expensive data center upgrades, reconfiguration and equipment replacement. Additionally, the backhaul configuration removes the costs associated with truck rolls to the data centers [8], [14].

The MEC open architecture makes it fitting for novel applications and specific use cases [2], [25]. However, given that MEC is still in its infancy [8], most of its potential use cases and scenarios are not typical in the current networking environment. With existing network infrastructure, several use cases are being tested and verified; among these are augmented reality [30], Location-Based Services (LBSs) [28], distributed content and caching [20], video analytics [2], [26] and Connected and Autonomous Vehicles (CAVs) [19], [27], [31].

- *Augmented reality:* The MEC servers use real-time tracking and content caching to support augmented reality on mobile devices. The MEC architecture provides low latency packet transmission to devices and high rates of local data processing. The key driver for this use case is the demand for higher throughput and reduced Round-Trip-Time [30].
- *Location-based services:* The active device location tracking, also known as LBS, use case consists of a MEC-based application and third-party geolocation algorithm to perform real-time network measurement [28]. The geolocation service operates independently of the conventional Global Positioning System (GPS) and provides a low cost and low power alternative.
- *Distributed content and caching:* Mobile users at a given location and time tend to watch a remarkably consistent and narrow set of content, and the amount of traffic is rapidly growing, but it is often concentrated in specific locations and times [20]. Hence, shifting the computational process and storage to the edge minimizes the load on the core servers and systems through local caching at the edge and subsequently providing faster service delivery to customers [2].
- *Video analytics:* This use case uses a distributed video management platform, predefined codecs and live-stream analytics application to process, analyze and store video data [2], [26]. The solution is capable of collecting new video streams and comparing with pre-recorded streams to detect abnormalities in the environment and trigger corrective actions. Typical scenarios are safe city and public security [2], [25].
- *Connected and autonomous vehicles:* A prerequisite for autonomous vehicles is the capability to comprehend their ambient environments in real-time [19], [20], [31]. Autonomous vehicles rely on a combination of sensors, cameras, lidar and radars, to observe their surroundings and make appropriate driving decisions. Vehicles exchange information with nearby infrastructure and vehicles through Vehicle-to-Infrastructure (V2I) communications and Vehicle-to-Vehicle (V2V) [27]. The MEC paradigm enhances communication networks to improve the reliability and quality of autonomous driving.

III. MEC SECURITY ARCHITECTURE

MEC security architecture connects the breadth of the MEC integrated security controls and the entire security infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens the security across the network, users, devices, and applications [32], [33]. High-level guidelines are described for key security features, requirements and options for MEC deployments in [18]. This paper highlights the following security requirements: entity authentication, identity verification, network security with traffic separation, application integrity assurance, malware detection within the MEC layer, data encryption, and tamper-proof MEC equipment. Some of these aspects are built-in, inherent, secure characteristics of the MEC architecture itself [5], [18]. With the advent of 5G networks, myriads of new businesses, new mobile technologies and new service delivery models will gain momentum on a global scale [2], [8]–[10]. As a result of the MEC boom and its critical role in the 5G evolution, this technology model will soon become a prime target for malicious actors who want to leverage this platform to disrupt its growth and in turn, use it to launch attacks against a broader user base of mobile networks [8], [10], [13]. Impacts of breaches in this new generation of the connected world can be vast and impactful [1], [10], [12], [23], [34]. The MEC environment inherits risks from cloud computing and virtualized network security [2], [25], [35], by introducing the security threat vectors related to physical devices, network functions, the MEC platform and its applications [14], [23], [35], [36]. In the MEC framework [15], [16] security management is required to achieve interoperability among the layers (Communication Technology (CT) capabilities, IT applications, MEC platform, devices, and edge cloud). MEC encounters security risks associated with its deployment [1], [18]. MEC can be implemented at the network level using the same principles as a Mobile Packet Core [32]. The external connections are secured using security protocols, e.g., TLS, IPsec or SNMPv3. The Security Gateway (SeGW) can be used to terminate IPsec tunnels from the radio network elements, as depicted in Fig. 4.

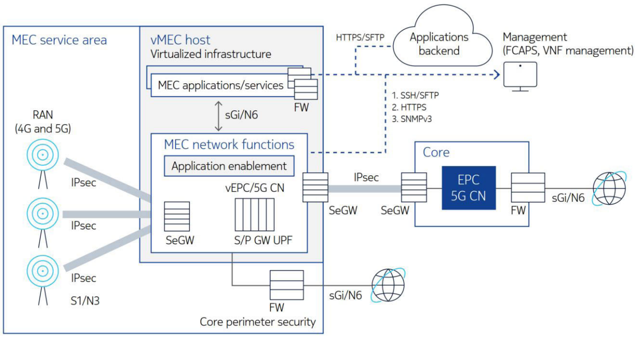

FIGURE 4. MEC Security Network Architecture [32].

In an attempt to mitigate the security risks, a centralized security architecture is needed to address a hierarchical MEC security framework that covers the physical facility layer, virtual facility layer, applications lifecycle, MEC platform, user plane function and management system security [10]. A benefit of centralization is the global view of computing and network resource usage and policy synchronization [5], [31]. A centralized control plane coupled with programmability and automation enables real-time network control to achieve business requirements [10], [33], as depicted in Fig. 3. Software-Defined Networking (SDN) has been adopted to provide a centralized control plane with programmability and automation [31], [37], [38].

By integrating SDN control with the Edge Computing processing and storage, the unified control plane interfaces are provided by decoupling the control plane from the data plane without additional infrastructure [10]. As a result of global network control [31], intelligent traffic steering and efficient resource management can be used to improve overall resource utilization. SDN enables dynamism in network security systems by harvesting intelligence from the network devices through programmable interfaces [31]. By enabling NFV in MEC, virtual security functions can be provisioned on servers flexibly and enforced at any network perimeter with reduced provisioning cost, utilizing SDN's programmable interfaces. Latif *et al.* [39] presented a detailed and systematic survey of different types of SDN models' interfaces.

Peng *et al.* [31] proposed a novel MEC architecture based on the collaborative technologies, SDN and NFV to meet computing and communication demands at the edge. The proposed architecture demonstrates the effectiveness of intelligent traffic steering and efficient resource management techniques; however, secure communication channels is an essential research issue.

IV. DATA SECURITY AND PRIVACY

The security threat vectors in MEC will be multi-dimensional [10], [12], [23], [34], from the end devices up to the core infrastructure. MEC networks will connect critical infrastructure, interconnect multiple cloud providers and integrate new models of service delivery. Employing multiple layers of security is crucial for data protection at all MEC levels and across numerous devices, applications and nodes [33]. Network security, inter-MEC communication, communication with the cloud and data security are key requirements [18].

A. SECURITY DIMENSIONS

Security dimensions, also known as security controls, are proposed by International Telecommunication Union's Telecommunication (ITU-T) in its security recommendation X.805 [40] to address the overall security-related architectural elements that, when appropriately applied, can provide comprehensive security protection. The security dimensions encompass a set of security controls to promote the interweaving of security capabilities in the overall end-to-end (E2E) security solution.

B. DATA SECURITY TECHNOLOGIES AND MECHANISMS

In this section, a description is provided of the five key security dimensions: Access Control IV-B1; Identity and Authentication IV-B2; Data Confidentiality IV-B3; Data Integrity IV-B4; and Communication Security IV-B5. Summary tables are provided to address scalability for each security dimension in terms of manageable, effective, and efficient mechanisms to support MEC distributed nodes and the automate dynamic scaling needs of various interacting services and applications.

1) ACCESS CONTROL

The MEC architecture is a shared open environment and distributed system [25]; therefore, certain levels of access sharing on both MEC entities and data are mandatory [41]. The primary function of access control is to monitor and protect against unauthorized use of MEC resources [41]–[43]. The major access controls for MEC will be explained.

- *Attribute-Based Access Control (ABAC) model:* This model makes access decisions based on a set of attributes associated with the device making a request or a target resource [44]. There are several ways to use or define attributes in the ABAC model. An attribute can be a user role, a user location, a user's work start date, or all of them [45]. Models similar to ABAC are known as either Claims Based Access Control (CBAC) or Policy-Based Access Control (PBAC).
- *Role-Based Access Control (RBAC) model:* In this model, a subject can have more than one role or be a member of multiple groups [46]. The roles are based on several factors, including authorization, responsibility and job designation [41].
- *Dynamic Risk-Based Access Control (DRBAC) model:* was proposed to cope with multinational organizations that face various policies and regulations in different jurisdictions, allowing greater flexibility to access control [45]. It employs the notion of quantifying risk metrics and aggregating them. This model uses different types of risk levels with environmental conditions and leverage the principle of "operational need" to make access decisions.
- *Access Control for Cloud Computing (AC3) model:* is a novel access control model for cloud computing. It fulfills access control requirements for diverse cloud-based users who share resources in a multi-tenancy environment [41]. Under the model, users are classified according to their actual jobs.

The success of any access control solution for MEC will depend on its ability to analyze and accurately identify a list of requirements [43]. Table 1 summarizes the capability-based access control mechanisms. There are other mechanisms such as TPM-based access control [47] that might be suitable for a particular MEC environment.

2) IDENTITY AND AUTHENTICATION

In the MEC paradigm [15], [16] there are several functional actors (end-users, infrastructure providers and service providers), infrastructure layers (end devices, edge network and core infrastructure) and virtualization platforms (data containers, VM) coexisting and cooperating in an ecosystem.

In this heterogeneous environment, identity is assigned to each entity in a single trust domain but permits entities

TABLE 1. Access-Control Techniques.

Capability	DAC	MAC	RBAC [46]	ABAC [44]	DRBAC [45]	AC3 [41]
Least privilege principle	✗	✗	✓	✓	✓	✓
Separation of duties	✗	✗	✓	✓	N/A	✓
Auditing	✓	✓	✓	✓	✓	✓
Policy management	✗	✗	✗	✗	✓	✓
Flexibility of configuration	✗	✗	✓	✗	✓	✓
Operational and situational awareness	✗	✗	✗	✗	✓	✓
Integrated with authentication functions	✗	✗	✗	✗	✗	✓
Supporting passive and active workflows	✗	✗	✗	✗	✗	✓
Delegation of capabilities	✓	✗	✗	✗	✓	✓
Dealing with heterogeneity	✗	✗	✗	✗	✓	✓
Scalability	✗	✗	✓	N/A	N/A	✓

to mutually authenticate other entities across different trust domains [47]–[49]. At the same time, considering the flexibility of the MEC architecture, achieving mutual authentication with anonymity and untraceability are crucial for data security and user privacy [50], [51]. Authentication methods include single-domain authentication [41], cross-domain authentication [52], and the SDN-based handover authentication scheme [53].

Additionally, existing adopted methods for authentication in MEC environments are user authentication ([5], [43], [54], [55]), application authentication [5] and cloudlet and server authentication ([55], [56]).

Jia *et al.* [57] presented the identity-based Anonymous Authenticated Key Agreement (AAKA) cryptographic protocol that is tailored to be explicitly deployed in MEC environment; the authors show how it meets both user anonymity and untraceability requirements. The AAKA protocol permits a registered mobile user to access multiple MEC servers with a single registration. A summary of identity and authentication related works are listed in Table 2.

3) DATA CONFIDENTIALITY

Data confidentiality is a fundamental requirement in the MEC paradigm [62]–[64]. Confidentiality is a significant hindrance for mobile users that wish to utilize mobile apps and services. The MEC paradigm introduces limitations affecting data confidentiality [21], [65], [66]. As the data is transmitted and received within shared and sometimes public networks and stored or processed in distributed and shared edge networks, the likelihood of unauthorized access to sensitive data by service providers is relatively high [12], [23], [34], [35]. Solving the data confidentiality challenge is crucial as data leaks continue unabated [1]. In recent years, techniques have been developed to provide data confidentiality by preventing unauthorized access [41], [48], [67], [68]. A summary of data confidentiality related works are provided in Table 3.

4) DATA INTEGRITY

Data integrity is known to be one of the essential elements of security frameworks. The objective of integrity models [25], [71]–[73] is to maintain data by preventing intentional or accidental modifications.

The MEC ecosystem integrates multiple actors [8], [15], [16], and data integrity challenges remain unresolved [12], [23], [34], [35]. Data integrity schemes have been developed that maintain the integrity of outsourced data [71].

5) COMMUNICATION SECURITY

As depicted in Fig. 2, the MEC environment includes end devices and the edge network [15], [16]. The communication channel between UE and base stations (BS) are established and logically isolated by the air interface [19], [20]. The need for reliable and secure wireless links is a prerequisite to building a robust MEC architecture [17], [40], [77].

- *Communication channels within the access network:* Communication channels in the access network are established between UE and BS or between UEs in an ad-hoc method that can use Device-to-Device (D2D) channels [78]. Malicious attacks on D2D communications are a plausible attack vector [2]. A summary of works related to communication channel security is provided in Table 5.
- *Communication channels among edge and core entities:* The MEC paradigm identifies threat vectors related to the links within the edge and core layers [19], [20]. Therefore, transmission technologies are susceptible to threat vectors such as Sybil, fibre tapping, electromagnetic pulses, hidden pulse, Distributed Denial of Service DDoS) and jamming [12], [13]. Although the long-distance transmission links are often secured with encryption and encoding mechanisms, successful exploitation of the MEC ecosystem could result in the network being compromised [5], [13]. Therefore, encrypted communication methods such as Virtual Private Networks (VPNs) could be employed to provide secure communications between edge and core entities [32].
- *Communication channels in NFV:* The ETSI NFV Reference Framework [16] defines NFV and Virtual Network Functions (VNFs). NFV is abstracting and automating many of the operational and business processes by software; as such, it requires operators to redefine trust relationships between existing components and roles [37], [38]. VNFs enable a data center to provide the most

TABLE 2. Identity and Authentication Techniques.

Technical Approach	Scalability	Security Features	Summary
Single-Domain Authentication Bilinear Pairing Cryptosystem Dynamic Nonce Generation [58]	Moderate	Privacy-preserving Anonymous authentication	This paper presented a new anonymous authentication scheme for a distributed mobile cloud services environment based on a bilinear pairing cryptosystem and dynamic nonce generation. The proposed scheme supports mutual authentication, key exchange, user anonymity, and user untraceability.
Single-Domain Authentication Bilinear Pairing Cryptosystem Identity-Based Signature [59]	High	Privacy-preserving Anonymous authentication	This paper constructs a new Privacy-Aware Authentication (PAA) scheme for MCC services by using anonymous authentication an identity-based signature scheme.
Single-Domain Authentication ECC Identity-Based Signature [60]	High	Privacy-preserving Batch verification	A new efficient identity-based (ID-based) batch signature scheme based on the Elliptic Curve Cryptosystem (ECC) is first introduced, and then a new conditional privacy-preserving authentication scheme is developed based on the invented signature scheme for Vehicular Sensor Networks (VSNs) to provide a secure authentication process for messages transmitted between vehicles and Roadside Units (RSUs).
Single-Domain Authentication ECC [61]	High	Lightweight authentication	This paper presents an ECC based lightweight authentication scheme for Smart Grids (SG). The proposed scheme was tested using the automated tool ProVerif. It was found not to require a trusted third-party during the authentication phase.
Cross-domain Access Revocation System Attribute Certificate [52]	Moderate	Privacy-preserving Certificate revocation	This paper presents a new framework for authorisation in structured P2P networks based on attribute certificates and a fully distributed certificate revocation system. This proposal enables a more flexible and secure authorisation scheme for authorisation in structured P2P networks while improving the efficiency of privilege assignment.
Cross-domain Access ECC Hierarchical Tree Structure Key Revocation [50]	Moderate	Anonymous authentication Privacy-preserving Key revocation	This paper presents a novel cross-domain dynamic anonymous authenticated group key management system with symptom-matching (CD-AGKMS). The proposed system is a hierarchical architecture that enables anonymity and traceability for end-users and organisations.
Handover Authentication ECC Identity-Based Authentication [49]	High	Anonymous authentication Privacy-preserving Untraceability	This paper presents a novel protocol based on an identity-based elliptic curve algorithm to achieve an efficient handover authentication process for mobile cloud computing.

TABLE 3. Data Confidentiality Techniques.

Encryption Techniques	Scalability	Security Features	Summary
CP-ABE Hierarchy access structure [69]	High	Data confidentiality Data Sharing	This paper presents a variant of CP-ABE to efficiently share hierarchical files in a cloud computing environment. The proposed scheme has the advantage that users can decrypt authorization files by computing a secret key once.
CP-ABE All-or-Nothing principle [62]	Moderate	Data confidentiality	This paper presents a comprehensive proxy-assisted approach based on an all-or-nothing principle to overcome the limitation of needing to trust the cloud server not to disclose user proxy keys inherent in mediator assisted proxy user revocation techniques.
HE-based Scheme Homomorphic Encryption [63]	High	Data confidentiality Lightweight encryption	This paper presents a new LHE scheme that permits mobile users to outsource their data in a secure and privacy-preserved manner with improved efficiency while enabling homomorphism under both addition and multiplication.
PRE-based Scheme Workload distribution model [64]	High	Data confidentiality Proxy re-encryption	This paper presents a proxy re-encryption scheme that offloads the encryption, decryption, and re-encryption operation. Hence, it puts a minimum load on a mobile device during the execution of security operations. The technique permits the data owner to encrypt the message using a personal private key before uploading it to cloud storage.
Attribute-Based Proxy re-encryption with Keyword Search (ABRKS) [70]	High	Data confidentiality Keyword search	This paper presents a novel attribute-based proxy re-encryption with keyword search (ABRKS) that supports keyword search on encrypted data. It enables data owners to delegate the keyword search capability to other data users complying with the specific access control policy.
Cross-domain Access RSA algorithm CP-ABE [48]	High	Data sharing CP-ABE scheme RSA algorithm	This paper presents a cross-domain access technique for MEC. The RSA algorithm and CP-ABE are used for information confidentiality and one-to-many data sharing.
Lightweight data access control scheme SL-CP-ABE [42]	High	Data confidentiality Fine-grained data access control	This paper presents a secure and lightweight data access control scheme that preserves the confidentiality of outsourced data and achieves fine-grained data access control efficiently in MCC.

suitable and efficient routing capability for cloud applications and to control the network configuration as conditions warrant via software-based management [37], [81], [82]. At the core of NFV are VNFs that handle specific network functions including routing, firewalls or load balancing as illustrated in Fig. 5.

When a physical network device is introduced into an operational network, trusted communication channels

TABLE 4. Data Integrity Technical Approaches.

Encryption Techniques	Scalability	Security Features	Summary
Cryptography Method Bilinearity Property [74]	High	Dynamic auditing Privacy-preserving	This paper presents an efficient and inherently secure dynamic auditing protocol. It protects the data privacy against the auditor by combining the cryptography method with the bilinearity property of bilinear paring, rather than using the masking technique.
Algebraic Signature Divide and Conquer Table [75]	Moderate	Dynamic auditing Low-complexity	This paper develops a remote dynamic auditing method based on low computational complexity an algebraic signature and Divide and Conquer Table that can be used to check the integrity of the outsourced data in cloud computing and minimise computational and communication cost of frequent data auditing.
Online/Offline Signatures Merkle Hash Tree [76]	High	Batch auditing Lightweight privacy-preserving	This paper presents two privacy-preserving public auditing protocols that support batch auditing and data dynamics for secure storage in a cloud environment. These protocols are based on online/offline signature and utilised Merkle Hash Tree, by which a user only needs to perform lightweight computing when a data file to be outsourced is given.
Mobile provable data possession BLS Short Signature [71]	Moderate	Dynamic auditing Low-complexity	This paper presents a synthesised scheme based on low computational complexity that supports block-less, stateless, data outsourcing verification, and dynamic data operations based on provable data possession (PDP) and BLS short signature scheme to achieve high accurate data integrity verification.
ECC based lightweight authentication scheme [61]	High	Mutual authentication Low-complexity	This paper presents an ECC based lightweight authentication scheme for Smart Grid (SG) system. The Proposed scheme is secure under the threat model of automated tool ProVerif and sustains data integrity.
Multi-tier trust security model [5]	High	Data processing offloading Digital signatures Reputation mechanisms	This paper presents a security model for MEC that can adapt the security level of the different elements in the architecture to the degree of trust of each of those elements.

TABLE 5. Access Network Communication Channel Security.

Technical Approach	Scalability	Security Features	Summary
Rogue eNodeB MitM Relay Battery Draining [13], [79]	High	Data encryption VPN Public Key-Pair based authentication	This paper presents a novel mitigation approach that explores mandatory security protection for UE and core networks that is mutually verified and utilises a Non-Access Stratum (NAS) security setup.
Eavesdropping Computation Offloading [7]	Moderate	Multiuser multicarrier method Weighted sum-energy consumption scheme	This paper presents a Physical Layer Security (PLS) method that is used to secure the mobile communication and computation task offloading channels.
Spoofing Replay Integrity Messages [5]	High	Symmetric key scheme Authentication	This paper presents a new protocol based on cryptographic systems for authentication and establishment of secure sessions between UE and Machine Type Communication devices without any prior trust relationship.
D2D communications [80]	High	Asymmetric cryptography-based authentication scheme Integrated PHY-ID	This paper presents an enhanced E2E IoT device authentication approach using PHY-aided cross-layer design.
D2D communications [80]	High	Asymmetric cryptography-based authentication scheme Integrated PHY-ID	This paper presents an enhanced E2E IoT device authentication approach using PHY-aided cross-layer design.

are used to achieve full automation in a Continuous Integration/Continuous Deployment (CI/CD) chain [8], [9], [36]. For VNFs, this chain of trust relationships needs to be created and maintained in an NFV environment throughout its lifecycle [82]. The potential solutions to mitigate communication challenges include NFV-based network security, in the form of firewalls, Deep Packet Inspection (DPI), Intrusion Detection Systems (IDSs) or Intrusion Prevention Systems (IPSs) and VPN access [37]. Secondly, Machine learning for NFV-based security services [81] is a policy-based security approach that tends to favor deductive reasoning by building models and analyzing the models based on logical rules. SDN and NFV [83] promise rapid provisioning, greater flexibility, and reduced operational costs [8]. The integration of SDN/NFV-based security solutions into network infrastructure [38] offers enhanced monitoring, automation and resources provisioning capabilities, in addition to the prospect of dynamic packet manipulation and re-routing [31], [37], [53].

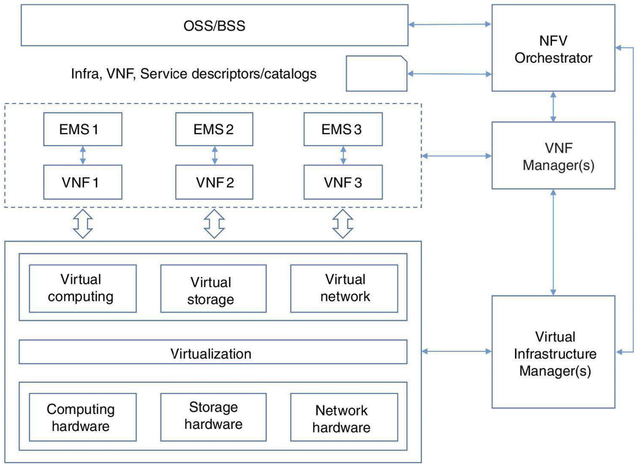

FIGURE 5. ETSI NFV Reference Framework [16].

C. PRIVACY-PRESERVING TECHNOLOGIES AND MECHANISMS

The privacy of mobile user data, as it is processed and moved between a mobile device and the distributed MEC nodes while availing different cloud applications or services, is a critical challenge [21], [22], [35]. Moura and Hutchison [25] introduce the game theory, which addresses the defender's strategy, cooperative behavior and action towards the attacker, and vice versa, in cybersecurity. This approach relies on a distributed reliable defense, timely action and proven mathematics. Private information can be characterized into three domains: data, identity, and location [1]. Reviews of the state of data privacy protection ([21], [84]) and identity privacy ([22], [57]) can be found in the literature. An extensive review of privacy protection methods from various disciplines is provided in Table 6.

The purpose of including multiple layers in MEC network security is to ensure that the defense controls have a backup in the case of a flaw or missing coverage [18]. The individual strengths of each layer should cover any gaps in other defenses. With this assumption in mind, individual layers in a multi-layered security approach focus on a specific area where vulnerabilities may exist [33]. By working in concert, the security layers have a better chance of preventing intruders from breaching MEC networks [5].

V. SECURITY THREAT CHALLENGES

This section presents the MEC related security threats for the functional layers in the order of their severity and identifies the proposed controls. Threats can be targeted or opportunistic, the aim is to take advantage of a security vulnerability to erase, alter, or harm objects of interest [13], [23], [95]. The MEC architecture [15], [16] comprises multiple technologies, including wireless networks, distributed computing servers and storage, and the virtualization of networking equipment. The MEC architecture components inter-operate in an open ecosystem that permits service providers to deploy applications and services into the MEC nodes. The hierarchy and heterogeneity of the MEC environment [2], [22], constitutes a significant threat; hence robust security and privacy measures should be implemented [5], [21], [37], [40]. Privacy is one of the fundamental motivations for security [21], [84]. The ITU-T defines privacy [17] as the right of individuals to control what information related to them may be collected, analyzed and stored and by whom and to whom that information may be revealed. By extension, privacy is also associated with specific technical means such as cryptography [61], [66]. Privacy mechanism will ensure information is not disclosed to any party other than the intended parties so that only the explicitly authorized parties can interpret the content being exchanged. Security and privacy challenges related to data management remain open, and a discussion on how the challenges are being tackled is provided.

A. EDGE DEVICE SECURITY THREATS

User-controlled device content sensitivity is a factor that is used when determining the security and privacy requirements [23]. Users not only consume services but also can become active contributors that generate data and participate in the distribution of information [87]. However, there will also be rogue users that maliciously attempt to disrupt services and detrimentally affect the operation of edge devices [22], [53].

- *Information injection:* An adversary can inject malicious data into any compromised device to distribute false information when queried [23]. Poisoning [93] is an act whereby adversaries maliciously inject false data into a system. Outside forgery [96] occurs when deceptive messages are generated with forged information to compromise the privacy of victim nodes. E.g., in smart manufacturing space, an attacker injects incorrect pressure measurements to delay valve actuation with the intent to cause equipment damage [97].
- *Eavesdropping:* Adversaries capture transmissions over communication channels, thereby gaining access to private information [98].
- *Side-channel attacks:* The aim is to capture sensitive private information via surreptitious access to UEs. The focus of this type of attack are passwords, login credentials, email, and location information [99]. To detect the malware in a UE, a low-resource environmental IDS or IPS with ML techniques might be a potential solution [28].

B. ACCESS NETWORK SECURITY THREATS

Access network security is a key factor for the efficient operation of MEC nodes and provides a platform for secure integration with UE and cloud infrastructure [15], [16]. Failure to implement robust access network security controls introduces attack vectors for malicious parties, resulting in severe network threats [5], [17], [40]. Access networks consist of infrastructure, including network devices and systems that facilitate message flows between the devices found

TABLE 6. Privacy Protection Methods.

Technology	Works	Proposed Techniques	Technical Approaches	Scalability
Cryptography	[63]	Lightweight and computationally efficient protocol called CLOAK based on Cryptographically Secure Pseudo-Random Number (CSPRN).	Symmetric key Stream cipher	High
	[66]	A context-aware encryption protocol which adapts the encryption algorithm based on the information sensitivity as well as the available device resources.	Adaptive encryption algorithm profiling	High
	[85]	An efficient statistical authentication protocol using lattice-based primitives for smart cards through zero-knowledge proofs.	Post-quantum cryptography Zero-knowledge authentication	Moderate
Biometrics	[86]	An inference-based framework for privacy-preserving biometric schemes to prevent adversaries from inferring biometric identities.	Randomized Montgomery domains Hamming distance Hash-based indexing	Moderate
Differential Privacy	[21]	Strict mathematical proof for privacy-preserving by adding randomisation noise to aggregated query results to protect individual entries without significant change in query results.	Machine learning Output perturbation Objective perturbation Laplacian noise Data mining	High
Blockchain	[87]	A reputation-based crowdsourcing Federated Learning (FL) system leveraging the power of blockchain technology to construct a secure, decentralised and privacy-preserving MEC system.	Crowdsourcing FL Federated training Differential privacy	High
	[88]	TrustChain distributed architecture based on the permissible blockchain concepts to match with the requirements at each layer of the model.	Lightweight consensus management protocol BFT protocol ROOF	High
	[89]	A high-performance permissible blockchain system. Two authorisations were involved for node validations.	Covert Channel Authorization (CCA) RL-based method	Moderate
	[90]	A dynamic and privacy-preserving reputation management scheme based on blockchain for mobile crowdsensing to overcome the defects of existing schemes.	Mobile crowdsensing (MCS) Dynamic reputation management scheme Hyperledger Sawtooth	High
Game Theory	[91]	Implement the game theory algorithm on FPGA, which especially shows the value of game theory for autonomous driving.	Lemke-Howson FPGA Accelerator	High
	[29]	A distributed approach for LBS privacy protection by developing a dummy-based k-anonymity method for preserving location privacy of users.	Dummy-based k-anonymity method Bayesian game	Moderate
	[92]	A bidding-based resource allocation and consolidation technique "epcAware" enables various applications across various service providers.	Time factors Non-cooperative game "epcAware" resource management	high
Machine Learning (ML)	[93]	A learning model to construct the inferred social graph without any domain experts' knowledge to protect against poisoning attacks in MEC.	Inferred social graph Feature learning Loc-Gwalla and loc-Brightkite data sets	High
Data Mining (DM)	[94]	A privacy-preserving data mining (PPDM) technology based on an iterative algorithm (k-means clustering) to protect both, users and community from privacy leakage.	Homomorphic encryption Social participatory sensing Pattern clustering	High
Data Mining (DM)	[94]	A privacy-preserving data mining (PPDM) technology based on an iterative algorithm (k-means clustering) to protect both, users and community from privacy leakage.	Homomorphic encryption Social participatory sensing Pattern clustering	High

connecting to the access network, MEC and core networks [5], [13]. An adversary can target the access network infrastructure, connected devices or communication channels [100]. Threats to the MEC applications and services include device, application or service hijacking [93], [96], and DDoS attacks [12], [13].

- *Denial of Service:* Digital networks are vulnerable to DoS attacks that may be implemented, e.g., as DDoS attacks or wireless jamming [13]. The co-existence of Virtual Machines (VMs), spread across multiple MEHs, increases the likelihood of compromised VMs coordinating in a large-scale attack, e.g., DDoS [12]. This form of attack occurs when an application or service is compromised, and the corrupted application or service consumes MEC resources, e.g., network bandwidth, computation power or memory [8], [14]. The attack creates a delay in application or service responsiveness or completely disrupts the functionality of the MEC node and ultimately leads to an application or service outage [21], [78]. The security industry offers Security Orchestration, Automation and Response (SOAR) frameworks to provide an automated and proactive security approach to this type of critical threat [33].
- *Man-in-the-Middle:* The MitM attack is characterized by the presence of a malicious third party interposed between two or more communicating parties, and secretly relaying or intercepting the communication between the parties [79], [101]. For the MEC scenario, a MitM attack is categorized as an infrastructure attack, where the malicious attacker tries to hijack a specific

network segment and begins to launch attacks, such as eavesdropping and phishing, on connected devices [98], [100]. Since MEC applications and services rely primarily on virtualization, launching a MitM attack on multiple VMs could affect other elements on both sides of the attack [37], [82].

- *Rogue gateway:* The distributed MEC architecture creates a scenario where malicious adversaries can implement unauthorized gateways and deploy them to perform unprivileged activities [10], [36]. With access to network equipment, applications and edge services; unauthorized gateways can pose a significant threat by creating backdoor access to sensitive resources [13].
- *Inconsistent security policy enforcement:* A challenge for mobile network operators, is the alignment and shared compliance of security services when mobile users shift from one operator network to another [24]. This activity exhibits the need for security policy sharing among network operators on an agile scale, to ensure that user traffic across the access networks is securely managed, including when UE connectivity is shifting from MEC on one operator network to MEC on another operator network [2], [8].
- *Communication channels:* Mobile network radio channels are established over an air interface, which is the most insecure link in a mobile network [5], [13], [77]. Mobile communication attack vectors include MitM, Sybil, eavesdropping, replay, spoofing, smurf and DoS [12], [96], [98], [100]. During the offloading process, there is a potential risk of unauthorized access to offloaded content [7]. The risk factors highlight interoperability and compatibility concerns related to UE connections to BS [5], [6]. Further details of the communication channel security approaches are provided in Section IV-B5.

C. EDGE NETWORK THREATS

The edge network hosts computational capability, data storage, VI and management services [15], [16]. It enables the provisioning of applications and services by sharing infrastructure, platform and management planes [8], [9]. However, components may not offer the equivalent to the cloud security requirements, e.g., isolation [12], [34], [35]. Applications or services may not be designed using trusted computing practices, and this introduces risk in a MEC and edge network environment [47].

- *Privacy leak:* Unauthorized access to MEC nodes could result in information privacy being compromised [88], [102], [103]. On the edge network, the MEC paradigm limits the scope of privacy leaks by partitioning information and access [1], [35]. However, edge networks might exfiltrate sensitive information and rich network context information, such as client status information, traffic statistics and local network conditions that are used by applications to offer context-aware optimization [12].
- *Privilege escalation:* Privilege escalation arises when a bad actor exploits a design flaw, bug, or configuration error in an operating system or application to gain elevated access to protected resources that would typically be restricted to that user [51], [104]. The malicious user can then use the newly acquired unauthorized privileges to steal confidential data, run administrative commands or deploy malware, and potentially do severe damage to server applications [5], [13], [77].
- *Service manipulation:* Unlike cyber-criminals that attempt to steal data or hold it hostage with ransomware, service manipulation attacks can be hard to detect. Hackers can insert erroneous changes to the information that can have potentially catastrophic effects [100], [104]. A device that participates in service provisioning in a cluster deployed in an edge network can act as a distributed computing platform, and if the device is compromised, the entire cluster can be manipulated [93]. An internal adversary with appropriate privileges can manipulate not only the information flow but also instantiate rogue services that can provide false management information and historical data to other parties [96].
- *Rogue data center:* The edge network is less manageable and secure than conventional cloud computing environments [13]. In this threat environment, an adversary might take control of an entire edge network using, e.g., privilege escalation, or deploying malicious infrastructure disguised as an edge network device that resides between a data center located in the core and UE to manipulate interactions with external systems [88], [102], [103].
- *Physical damage:* Cyber-Physical Security (CPS) integrates multiple technical disciplines such as physical, computing and networking resources on different spatial scales controlled by computational algorithms [36], [53], [105]. The systems are often connected to an IP network. In the case of attack, the full ecosystem could be disrupted or potentially brought to a halt by physical damage [13], [53], [77]. The possible security controls to safeguard the internal constructs of the MEC nodes against this attack is to monitor the computational resources for unexpected consumption or load [36], [53].
- *Resource misuse:* Malicious actors may leverage MEC resources to target users, organizations or other service providers [57]. The threat actors can be a large-scale automated click fraud, ''mining'' for digital currency, or brute-force computer attacks of stolen credential databases [13], [102], [103]. Resource misuse represents a different form of attack, e.g., a malicious VM can scan for vulnerable IoT devices in the local network and host botnet servers [2], [37], [95].
- *VM manipulation:* In MEC, the host layer, is a prominent functional element. It comprises the MEPM, VIM, and MEHs that launch resources and provisioning services for the MEC subscribers using virtualization techniques such as VM and VNF [16], [37], [81]. However,

virtualization techniques, when applied to MEC generate several security challenges including VM manipulation, VM escape, Domain Name System (DNS) amplification, VNF location shift, security-log auditing and monitoring [23]. The attack vectors impact the operations of orchestration entities in the host layer [37]. Solutions such as Virtual Machine Introspection (VMI) and Trusted Platform Manager TPM) are two countermeasures proposed for addressing the virtualization interposing security threat [95].

- *Injection attacks:* Injection attacks are still amongst the oldest and most harmful web application attacks. They can result in data loss, data theft, loss of data integrity, DoS, as well as compromising a device or system [12], [13]. Injection attack refers to a large class of attack vectors that enable an adversary to input untrusted code into a program, which gets processed by an interpreter as part of a query or commands and leads to modifying the course of execution of the infected program [93], [96], [104].

D. CORE INFRASTRUCTURE SECURITY THREATS

Core infrastructure is used to support and manage edge and access network operations, including MEC [8], [10]. The security of the core infrastructure can have a linked effect on associated systems, e.g., the cloud [47]. It is essential to investigate the specific threats that target the core infrastructure in this particular context.

- *Privacy leaks:* By utilizing access to core infrastructure the likelihood of adversaries accessing the information stored on edge infrastructure increases and this warrants concerns about privacy leakage. For edge network security breaches V-C the potential damage of a privacy breach is limited to the class of information the adversary has gained access to [1], [35]. ‘‘Privacy by design’’ is a specific strategy to improve MEC security. The principles include privacy functionality protection embedded into the design, proactive action rather than a remedial protection strategy after privacy violations and data privacy throughout its lifecycle [14], [25]. Further details of privacy mechanisms are outlined in Section IV-C.
- *ICT attacks:* An ICT attack is characterized by the attacker attempting to break into a device or system to manipulate data deliberately and control the hardware it resides on [93], [100]. It includes attacks such as data tampering [93], background knowledge [88], collusion [102], [103], outside forgery [96], Sybil [104], likability [100], eavesdropping [98] and identity attacks [57].
- *Software-based attacks:* Security in NFV raises significant concerns about its adaptability and the security of the underlying telecommunication infrastructure [37]. It primarily impacts on system resilience as well as the overall quality of the accessible services [37]. The majority of the security threats apply to the key architectural elements of NFV infrastructure, e.g., VNF manipulation, VNF location shift and data exfiltration or destruction [95]. An SDN-based logically centralized control solution proposed by Okwuibe *et al.* [10] enables dynamism in network security systems by harvesting intelligence from the network equipment through programmable APIs and by leveraging NFV. Virtual security functions can be applied at the network perimeter to detect potential threats, isolate insecure network devices and stop them from adversely threatening the security posture [38].
- *Rogue infrastructure:* This threat assumes that adversaries target specific elements of the core infrastructure [13] and in a similar outcome to that identified for rogue infrastructure in the edge network V-C, a successful attack could enable control of applications and services found in MEC nodes. Although the likelihood of an adversary successfully launching this attack is extremely low, it is still essential to have adequate security controls and measures in place for sensitive MEC resources [17], [37], [38], [40].

VI. DISCUSSION AND OPEN ISSUES

The security of MEC nodes, applications and services is a current research area. Scalable, reliable and low complexity security solutions are a focus, due to MEC node resource availability being limited. This section briefly discusses possible future directions for MEC security solutions [2], [8], [25].

A. TRAFFIC ISOLATION AND SOFTWARE-DEFINED SEGMENTATION

MEC nodes are located on the network edge and integrate with the underlying network systems and security practices. New and innovative approaches are required to fully secure the applications and services that utilize the resources afforded by MEC nodes. Research into traffic isolation and software-defined segmentation is ongoing. Security policies are needed that consider identity and contextual information from the users, application and devices where appropriate. Software-defined segmentation can reduce the attack surface by segmenting resources and only granting permissions that are strictly needed [32], [37].

B. CLOUD-NATIVE SECURITY MECHANISMS

The cloud-native architecture adds complexity and consequently, risks associated with the number of hosted NFVs, boundaries between hardware and different software layers occur. A possible solution is to adopt cloud-native architecture based on containers and micro-services [8], [38]. Cloud-native architecture entails additional security requirements and the need for managed software element and hardware updates. Selected security mechanisms related to the MEC cloud-native architecture are:

- *Internal communication host protection:* The challenge is to use a lightweight mechanism that is sufficient to protect the host but does not introduce latency or overload computing resources.
- *Container-based application protection:* Privilege escalation from container to host, such as gaining unauthorized root access on the host system via a root process in the container.

C. SECURITY ENFORCEMENT, MONITORING AND MANAGEMENT CAPABILITIES

There is a need for pervasive visibility, and deep insights into the application, devices, packets, processes, network flows, and workload communications within a MEC environment [8], [16]. Distributed network hardware and software-based sensors might be a feasible solution [2], [5]. A high-level policy engine that manages the sprawl of access control devices across MEC environments can simplify and improve visibility. Current security approaches include Security Orchestration, Automation and Response (SOAR) frameworks to deliver proactive, integrated and automated security [33].

D. APPLICATIONS AND SERVICES

Security considerations related to deploying applications and services to MEC infrastructure include access, authentication and verification [5], [35]. Ensuring that only trusted and verified applications and services are deployed to MEC nodes remains a challenge when third parties are provided with the access rights to deploy applications and services to MEC nodes. Considerations related to the management and control of MEC deployed applications and services include:

- *Authentication:* The MEC platform includes a management entity that facilitates the deployment of authorized applications and controls network access. Authentication may be verified utilizing digital signing techniques, e.g., digitally signing software modules [5], [8].
- *Authorization:* New low complexity authorization procedures and policies that facilitate application and service operation and utilization of network resources and information, e.g., user plane traffic and Radio Network Information Service (RNIS) information are needed. Current solutions are either certificate-based authorization or OAuth 2.0 token-based authorization [32].
- *Application mobility:* Application user context mobility is a significant challenge for stateful applications that operate on MEC nodes. It remains an area of current research as new approaches are needed that reduce the time taken and network load associated with moving application user context from one MEC node to an adjacent MEC node [32], [54].
- *Certificate management:* A certificate management capability is required to ensure that the MEC architecture supports encryption standards. The certificate management capability should include monitoring and control capability to ensure that certificates are being correctly installed and utilized by the MEC node and by the applications and services operating from the MEC node [5], [88].

E. TRUST MANAGEMENT

Trust management is an important requirement for MEC, especially when the MEC nodes are made available by a provider for the third party managed applications and services. Secure access to applications and devices remains a challenge that involves the use of adaptive policies, trust in user identities, and device trustworthiness [47]. Trust management should continuously reassess the posture of applications, users, and devices [51]. The original design trusted every entity in the ecosystem, i.e., users, devices and services. Each entity was free to send information packets to every other entity at any time. Trust management may be moving to a state of affairs in which access to MEC resources must be barred by default until authorization is proved [5]. One implementation approach is to shift access decisions from the network layer to the application layer, which is a core tenet of a trust security model [51]. Selected cybersecurity challenges related to current MEC trust management architecture are:

- *Scale:* MEC will involve a massive number of connected devices. MEC operators need to authenticate, identify and keep track of all connected entities' activities for any malpractice within the network.
- *Latency break:* There might be the likelihood of an adverse effect on latency between network applications. Trust management should involve continuous monitoring and analysis of each entity connected to the network. An appropriate trust model might hamper latency as it involves remote monitoring applications, collecting and sending data to core trust management applications.
- *Heterogeneous networks interoperability:* An integrated trust model needs maturity to handle a wide variety of technologies, infrastructures, people, processes and policies.
- *Privilege access management:* All connected entities get restricted access to a particular segment of the network to perform a specified set of tasks.

VII. CONCLUSION

MEC is set to play a pivotal role in future network design and service delivery. The evolving network architectures shift towards computing and storage are being placed in the network as close to UE as possible whilst benefiting from improvements in transport technologies to facilitate reliable and high-speed connectivity to cloud computing facilities. This paper has presented the ETSI MEC reference architecture and provided a discussion on how MEC functions. MEC security technologies and management principles remain to be standardized and, as a result, the MEC architecture does not fully detail how

MEC security should be implemented. The security of the MEC node to node interaction and MEC node interaction with cloud systems is overly dependent on the communications systems' security. Research into MEC infrastructure's security, the applications and services operating on MEC nodes is ongoing and selected challenges have been identified. Security threats and proposed responses for the MEC environment have been provided along with a description of the attack vectors. The potential impact of MEC on future network operations is significant. Hence, it should be anticipated that MEC related to threat risk mitigation will grow in importance.

REFERENCES

[1] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[2] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, Jun. 2018.

[3] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervas. Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009. [Online]. Available: https://www.microsoft.com/en-us/research/publication/the-case-for-vm-based-cloudlets-in-mobile-computing/

[4] E. J. Helsper, "Gendered Internet use across generations and life stages," *Commun. Res.*, vol. 37, no. 3, pp. 352–374, Jun. 2010, doi: 10.1177/0093650209356439.

[5] F. Mora-Gimeno, H. Mora-Mora, D. Marcos-Jorquera, and B. Volckaert, "A secure multi-tier mobile edge computing model for data processing offloading based on degree of trust," *Sensors*, vol. 18, no. 10, p. 3211, Sep. 2018.

[6] Y. Hao, M. Chen, L. Hu, M. S. Hossain, and A. Ghoneim, "Energy efficient task caching and offloading for mobile edge computing," *IEEE Access*, vol. 6, pp. 11365–11373, 2018.

[7] J. Xu and J. Yao, "Exploiting physical-layer security for multiuser multicarrier computation offloading," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 9–12, Feb. 2019.

[8] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[9] B. Blanco, J. O. Fajardo, I. Giannoulakis, E. Kafetzakis, S. Peng, J. Pérez-Romero, I. Trajkovska, P. S. Khodashenas, L. Goratti, M. Paolino, E. Sfakianakis, F. Liberal, and G. Xilouris, "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," *Comput. Standards Interfaces*, vol. 54, pp. 216–228, Nov. 2017.

[10] J. Okwuibe, M. Liyanage, I. Ahmad, and M. Ylianttila, *Cloud and MEC Security*. Hoboken, NJ, USA: Wiley, 2018.

[11] A. Wang, Z. Zha, Y. Guo, and S. Chen, "Software-defined networking enhanced edge computing: A network-centric survey," *Proc. IEEE*, vol. 107, no. 8, pp. 1500–1519, Aug. 2019.

[12] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Realizing multi-access edge computing feasibility: Security perspective," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2019, pp. 1–7.

[13] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.* New York, NY, USA: ACM, May 2019, pp. 221–231.

[14] B. Liang, "Mobile edge computing," in *Key Technologies for 5G Wireless Systems*, V. W. S. Wong, R. Schober, D. W. K. Ng, and L.-C. Wang, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2017, ch. 4, pp. 76–91.

[15] ETSI, "Multi-access edge computing (MEC); framework and reference architecture," ETSI, Sophia Antipolis, France, Tech. Rep. GS MEC 003, 2020.

[16] ETSI, "Multi-access edge computing (MEC); architectural framework," ETSI, Sophia Antipolis, France, Tech. Rep. GR MEC 002, 2013.

[17] ITU-T, "Security in telecommunications and information technology—An overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications," Geneva, Switzerland, Tech. Rep. ITU-T/85097, 2003. [Online]. Available: https://www.itu.int/itudoc/itu-t/85097.pdf

[18] *Security Requirements for Deploying MEC at Scale*, NOKIA, Espoo, Finland, 2019. [Online]. Available: https://open-ecosystem.org/assets/security-requirements-deploying-mec-scale

[19] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[20] A. Ndikumana, N. H. Tran, T. M. Ho, Z. Han, W. Saad, D. Niyato, and C. S. Hong, "Joint communication, computation, caching, and control in big data multi-access edge computing," *IEEE Trans. Mobile Comput.*, vol. 19, no. 6, pp. 1359–1374, Jun. 2020.

[21] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 62–67, Aug. 2018.

[22] P. Zhang, M. Durresi, and A. Durresi, "Mobile privacy protection enhanced with multi-access edge computing," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 724–731.

[23] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[24] O. Queseth, Ö. Bulakci, P. B. P. Spapis, P. Marsch, P. Arnold, P. Rost, Q. Wang, R. Blom, S. Salsano, T. Chen, T. S. Buda, U. Herzog, V. Frascolla, X. Li, and Z. Yousaf, "5G PPP architecture working group: View on 5G architecture, version 2.0," Eur. Commission, Brussels, Belgium, White Paper, Dec. 2017. [Online]. Available: https://research-portal.uws.ac.uk/en/publications/5g-ppp-architecture-working-group-view-on-5g-architecture-version

[25] J. Moura and D. Hutchison, "Game theory for multi-access edge computing: Survey, use cases, and future trends," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 260–288, 1st Quart., 2019.

[26] S. Yi, Z. Hao, Q. Zhang, Q. Zhang, W. Shi, and Q. Li, "LAVEA: Latency-aware video analytics on edge computing platform," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*. New York, NY, USA: ACM, Jun. 2017, pp. 1–13.

[27] Q. Yuan, H. Zhou, J. Li, Z. Liu, F. Yang, and X. S. Shen, "Toward efficient content delivery for automated driving services: An edge computing solution," *IEEE Netw.*, vol. 32, no. 1, pp. 80–86, Jan. 2018.

[28] Z. Tian, Y. Wang, Y. Sun, and J. Qiu, "Location privacy challenges in mobile edge computing: Classification and exploration," *IEEE Netw.*, vol. 34, no. 2, pp. 52–56, Mar. 2020.

[29] J. Wang, Z. Cai, Y. Li, D. Yang, J. Li, and H. Gao, "Protecting query privacy with differentially private k-anonymity in location-based services," *Pers. Ubiquitous Comput.*, vol. 22, no. 3, pp. 453–469, Jun. 2018.

[30] X. Yang, Z. Chen, K. Li, Y. Sun, N. Liu, W. Xie, and Y. Zhao, "Communication-constrained mobile edge computing systems for wireless virtual reality: Scheduling and tradeoff," *IEEE Access*, vol. 6, pp. 16665–16677, 2018.

[31] H. Peng, Q. Ye, and X. S. Shen, "SDN-based resource management for autonomous vehicular networks: A multi-access edge computing approach," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 156–162, Aug. 2019.

[32] *Security Considerations for 5G MEC and Disaggregated Core Functions*, NOKIA, Tampere, Finland, 2020. [Online]. Available: https://onestore.nokia.com/asset/207572

[33] *From Complex to Cohesive: How a Platform Approach Can Solve Today's Security Conundrum*, Cisco System, San Francisco, CA, USA, 2020. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/white-paper-c11-744498.html

[34] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2586–2595, Nov. 2017.

[35] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, Apr. 2017.

[36] H. Ge, D. Yue, X. Xie, S. Deng, and C. Dou, "A unified modeling of muti-sources cyber-attacks with uncertainties for CPS security control," *J. Franklin Inst.*, vol. 358, no. 1, pp. 89–113, Jan. 2021.

[37] A. Molina Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, and P. Gouvas, "Security management architecture for NFV/SDN-aware IoT systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8005–8020, Oct. 2019.

[38] C. Lorenz, D. Hock, J. Scherer, R. Durner, W. Kellerer, S. Gebert, N. Gray, T. Zinner, and P. Tran-Gia, "An SDN/NFV-enabled enterprise network architecture offering fine-grained security policy enforcement," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 217–223, Mar. 2017.

[39] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *J. Netw. Comput. Appl.*, vol. 156, Apr. 2020, Art. no. 102563.

[40] *Security Architecture for Systems Providing End-to-End Communications*, document Rec. ITU-T X.805, 2003. [Online]. Available: https://www.itu.int/rec/T-REC-X.805-200310-I/en

[41] Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin, and M. S. Hossain, "A data security enhanced access control mechanism in mobile edge computing," *IEEE Access*, vol. 8, pp. 136119–136130, 2020.

[42] Y. Jin, C. Tian, H. He, and F. Wang, "A secure and lightweight data access control scheme for mobile cloud computing," in *Proc. IEEE 5th Int. Conf. Big Data Cloud Comput.*, Aug. 2015, pp. 172–179.

[43] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 1020–1026, Jan. 2018.

[44] M. A. Al-Kahtani and R. Sandhu, "A model for attribute-based user-role assignment," in *Proc. 18th Annu. Comput. Secur. Appl. Conf.*, 2002, pp. 353–362.

[45] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an adaptive risk-based access control model for the Internet of Things," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 1, pp. 26–35, Jan. 2018.

[46] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Trans. Inf. Syst. Secur.*, vol. 4, no. 3, pp. 224–274, Aug. 2001.

[47] Y. Ruan, A. Durresi, and S. Uslu, "Trust assessment for Internet of Things in multi-access edge computing," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 1155–1161.

[48] K. Fan, Q. Pan, J. Wang, T. Liu, H. Li, and Y. Yang, "Cross-domain based data sharing scheme in cooperative edge computing," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Jul. 2018, pp. 87–92.

[49] Y. Yang, X. Zheng, X. Liu, S. Zhong, and V. Chang, "Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system," *Future Gener. Comput. Syst.*, vol. 84, pp. 160–176, Jul. 2018.

[50] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for mobile cloud computing," *Future Gener. Comput. Syst.*, vol. 62, pp. 190–195, Sep. 2016.

[51] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-207, 2020.

[52] D. S. Touceda, J. M. S. Cámara, S. Zeadally, and M. Soriano, "Attribute-based authorization for structured peer-to-peer (P2P) networks," *Comput. Standards Interfaces*, vol. 42, pp. 71–83, Nov. 2015.

[53] C. Wang, Y. Zhang, X. Chen, K. Liang, and Z. Wang, "SDN-based handover authentication scheme for mobile edge computing in cyber-physical systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8692–8701, Oct. 2019.

[54] B. Han, S. Wong, C. Mannweiler, M. R. Crippa, and H. D. Schotten, "Context-awareness enhances 5G multi-access edge computing reliability," *IEEE Access*, vol. 7, pp. 21290–21299, 2019.

[55] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, vol. 74, no. 12, pp. 6428–6453, Dec. 2018.

[56] L. Khandare and D. K. Sreekantha, "Analysis on privacy protection in cloudlet and edge technology," in *Proc. 5th Int. Conf. Comput., Commun., Control Autom. (ICCUBEA)*, Sep. 2019, pp. 1–5.

[57] X. Jia, D. He, N. Kumar, and K.-K.-R. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," *IEEE Syst. J.*, vol. 14, no. 1, pp. 560–571, Mar. 2020.

[58] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Syst. J.*, vol. 9, no. 3, pp. 805–815, Sep. 2015.

[59] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1621–1631, Jun. 2018.

[60] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[61] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Gener. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[62] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in *Computer Security—ESORICS*. Cham, Switzerland: Springer, 2015.

[63] A. Banerjee, M. Hasan, M. A. Rahman, and R. Chapagain, "CLOAK: A stream cipher based encryption protocol for mobile cloud computing," *IEEE Access*, vol. 5, pp. 17678–17691, 2017.

[64] A. N. Khan, M. Ali, A. U. R. Khan, F. G. Khan, I. A. Khan, W. Jadoon, S. Shamshirband, and A. T. Chronopoulos, "A comparative study and workload distribution model for re-encryption schemes in a mobile cloud computing environment," *Int. J. Commun. Syst.*, vol. 30, no. 16, p. e3308, Nov. 2017.

[65] J. Li, R. Ma, and H. Guan, "TEES: An efficient search scheme over encrypted data on mobile cloud," *IEEE Trans. Cloud Comput.*, vol. 5, no. 1, pp. 126–139, Jan. 2017.

[66] Z. Dar, A. Ahmad, F. A. Khan, F. Zeshan, R. Iqbal, H. H. R. Sherazi, and A. K. Bashir, "A context-aware encryption protocol suite for edge computing-based IoT devices," *J. Supercomput.*, no. 76, pp. 2548–2567, 2019.

[67] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941–12950, 2017.

[68] R. C. Lunardi, R. A. Michelin, C. V. Neu, and A. F. Zorzo, "Distributed access control on IoT ledger-based architecture," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2018, pp. 1–7.

[69] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.

[70] Y. Shi, J. Liu, Z. Han, Q. Zheng, R. Zhang, and S. Qiu, "Attribute-based proxy re-encryption with keyword search," *PLoS ONE*, vol. 9, no. 12, Dec. 2014, Art. no. e116325.

[71] C. Lin, Z. Shen, Q. Chen, and F. T. Sheldon, "A data integrity verification scheme in mobile cloud computing," *J. Netw. Comput. Appl.*, vol. 77, pp. 146–151, Jan. 2017.

[72] J. J. Kang, K. Fahd, and S. Venkatraman, "An enhanced inference algorithm for data sampling efficiency and accuracy using periodic beacons and optimization," *Big Data Cognit. Comput.*, vol. 3, no. 1, p. 7, Jan. 2019.

[73] C. K. M. Lee, Y. Z. Huo, S. Z. Zhang, and K. K. H. Ng, "Design of a smart manufacturing system with the application of multi-access edge computing and blockchain technology," *IEEE Access*, vol. 8, pp. 28659–28667, 2020.

[74] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[75] M. Sookhak, "Dynamic remote data auditing for securing big data storage in cloud computing," Ph.D. dissertation, Dept. Comput. Sci. Inf. Technol., Univ. Malaya, Kuala Lumpur, Malaysia, 2015.

[76] J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, "Privacy-preserving public auditing protocol for low-performance end devices in cloud," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2572–2583, Nov. 2016.

[77] F. Conceicao, N. Oualha, and D. Zeghlache, "Security establishment for IoT environments in 5G: Direct MTC-UE communications," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.

[78] X. Diao, J. Zheng, Y. Wu, and Y. Cai, "Joint computing resource, power, and channel allocations for D2D-assisted and NOMA-based mobile edge computing," *IEEE Access*, vol. 7, pp. 9243–9257, 2019.

[79] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," *Cyberspace, Jurnal Pendidikan Teknologi Informasi*, vol. 2, no. 2, p. 109, Jan. 2019.

[80] P. Hao, X. Wang, and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.

[81] A. M. Zarca, M. Bagaa, J. B. Bernabe, T. Taleb, and A. F. Skarmeta, "Semantic-aware security orchestration in SDN/NFV-enabled IoT systems," *Sensors*, vol. 20, no. 13, p. 3622, Jun. 2020.

[82] W. Chu, "NFV and NFV-based security services," in *A Comprehensive Guide to 5G Security*, M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, Eds. Victoria, SA, Australia: Wiley, 2018, ch. 15.

[83] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, *Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions*. Cham, Switzerland: Springer, 2020.

[84] S. Rajesh, V. Paul, V. Menon, and M. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, Feb. 2019.

[85] M. S. Dousti and R. Jalili, "An efficient statistical zero-knowledge authentication protocol for smart cards," *Int. J. Comput. Math.*, vol. 93, no. 3, pp. 453–481, Mar. 2016.

[86] Y. Wang, J. Wan, J. Guo, Y.-M. Cheung, and P. C. Yuen, "Inference-based similarity search in randomized montgomery domains for privacy-preserving biometric identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 7, pp. 1611–1624, Jul. 2018.

[87] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for IoT devices," 2019, *arXiv:1906.10893*. [Online]. Available: http://arxiv.org/abs/1906.10893

[88] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "TrustChain: A privacy preserving blockchain with edge computing," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–17, Jul. 2019.

[89] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[90] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing," *IEEE Access*, vol. 7, pp. 74694–74710, 2019.

[91] S. Du, T. Huang, J. Hou, S. Song, and Y. Song, "FPGA based acceleration of game theory algorithm in edge computing for autonomous driving," *J. Syst. Archit.*, vol. 93, pp. 33–39, Feb. 2019.

[92] M. Zakarya, L. Gillam, H. Ali, I. Rahman, K. Salah, R. Khan, O. Rana, and R. Buyya, "EpcAware: A game-based, energy, performance and cost efficient resource management technique for multi-access edge computing," *IEEE Trans. Services Comput.*, early access, Jun. 26, 2020, doi: 10.1109/TSC.2020.3005347.

[93] P. Zhao, H. Huang, X. Zhao, and D. Huang, "P^3: Privacy-preserving scheme against poisoning attacks in mobile-edge computing," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 3, pp. 818–826, Jun. 2020.

[94] K. Xing, C. Hu, J. Yu, X. Cheng, and F. Zhang, "Mutual privacy preserving k-means clustering in social participatory sensing," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 2066–2076, Aug. 2017.

[95] H.-C. Hsieh, J.-L. Chen, and A. Benslimane, "5G virtualized multi-access edge computing platform for IoT applications," *J. Netw. Comput. Appl.*, vol. 115, pp. 94–102, Aug. 2018.

[96] M. Durresi, A. Subashi, A. Durresi, L. Barolli, and K. Uchida, "Secure communication architecture for Internet of Things using smartphones and multi-access edge computing in environment monitoring," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 4, pp. 1631–1640, Apr. 2019.

[97] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things supported by mobile edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 56–61, Aug. 2018.

[98] M. A. Khan, I. M. Qureshi, I. Ullah, S. Khan, F. Khanzada, and F. Noor, "An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing," *Electronics*, vol. 9, no. 1, p. 30, Dec. 2019.

[99] M. Liyanage, P. Porambage, and A. Y. Ding, "Five driving forces of multi-access edge computing," 2018, *arXiv:1810.00827*. [Online]. Available: http://arxiv.org/abs/1810.00827

[100] T. Orekondy, S. J. Oh, Y. Zhang, B. Schiele, and M. Fritz, "Gradient-leaks: Understanding and controlling deanonymization in federated learning," 2018, *arXiv:1805.05838*. [Online]. Available: http://arxiv.org/abs/1805.05838

[101] P. Kumar and M. Liyanage, "Efficient and anonymous mutual authentication protocol in multi-access edge computing (MEC) environments," in *IoT Security: Advances in Authentication*, M. Liyanage, A. B. P. Kumar, and M. Ylianttila, Eds. Victoria, SA, Australia: Wiley, 2020, ch. 6.

[102] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. S. Hossain, "A secure data aggregation strategy in edge computing and blockchain empowered Internet of Things," *IEEE Internet Things J.*, early access, Sep. 11, 2020, doi: 10.1109/JIOT.2020.3023588.

[103] F. Koufogiannis and G. J. Pappas, "Diffusing private data over networks," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1027–1037, Sep. 2018.

[104] A. Tandon and P. Srivastava, "Trust-based enhanced secure routing against rank and sybil attacks in IoT," in *Proc. 12th Int. Conf. Contemp. Comput. (IC)*, Aug. 2019, pp. 1–7.

[105] K. C. Okafor, "Dynamic reliability modeling of cyber-physical edge computing network," *Int. J. Comput. Appl.*, pp. 1–11, 2019.

BELAL ALI (Member, IEEE) received the bachelor's degree in electronics and telecommunications engineering from Applied Science University, in 2004. He is currently pursuing the Ph.D. degree with the School of Engineering, RMIT University, Melbourne, Australia. He has more than 15 years of working experience in enterprise network design, architecture, and cybersecurity solutions. His research interests include SDx, MEC, and associated cybersecurity solutions.

MARK A. GREGORY (Senior Member, IEEE) received the Ph.D. degree from RMIT University, Melbourne, Australia, in 2008. In 2009, he received an Australian Learning and Teaching Council Citation for an outstanding contribution to teaching and learning. He is currently an Associate Professor with the School of Engineering, RMIT University. His research interests include telecommunications, network design, and technical risk. He is a Fellow of the Institute of Engineers Australia. He is the Managing Editor of two international journals (JTDE and IJICTA) and the General Co-Chair of ITNAC.

SHUO LI (Member, IEEE) received the bachelor's and Ph.D. degrees from the City University of Hong Kong, Hong Kong, in 2009 and 2014, respectively. She is currently a Lecturer with the School of Engineering, RMIT University, Australia. Her research interests include analysis and design of telecommunications, as well as analysis and design of optical networks and core networks.