# Trust in 5G and Beyond Networks

Chafika Benzaïd*, Tarik Taleb† and Muhammad Zubair Farooqi*
*†Aalto University, Espoo, Finland
†University of Oulu, Oulu, Finland
†Sejong University, Seoul, South Korea
Email: firstname.lastname@aalto.fi

***Abstract*—5G and beyond ecosystem will be characterized by a growing set of stakeholders and an increasing number of interconnected devices and services, not necessarily under the administration of the same entity. Establishing trust in such an open and diverse ecosystem is a cornerstone for a global adoption of the technology. In this vein, it is important to tackle security and privacy risks stemming from this rich ecosystem. In this paper, we shed light on the trust concept in 5G and beyond networks and its dimensions, while pointing out potential emerging trust enablers and research directions. Furthermore, we propose a blockchain-based data integrity framework to foster trust in data used by a machine learning pipeline.**

***Index Terms*—Trust, Security, Privacy, Blockchain, Network, 5G and beyond.**

## I. Introduction

5G and beyond networks are promising unprecedented capabilities, including ultra-high data delivery rates, ultra-high reliability, ultra-low latency, and support of massive number of connected devices. These capabilities will allow for new applications, such as industry 4.0, augmented and virtual reality, teleportation, and autonomous driving. To achieve their promises, 5G and beyond networks capitalize on the potential of advanced technologies, such as Software Defined Networks (SDN), Network Function Virtualization (NFV), Multi-access Edge Computing (MEC), Network Slicing (NS), and Artificial Intelligence (AI). Leveraging these technologies, the aim is to build extremely flexible, highly programmable and autonomously manageable infrastructures that can cater to the stringent performance demands of emerging and future services.

5G and beyond ecosystem will be characterized by a growing set of stakeholders (e.g., users, mobile network operators, service providers, and infrastructure providers) and an increasing number of interconnected devices and services. This flexible and rich ecosystem will pose significant security and privacy risks [1]. A curious or malicious service provider could abuse its access privileges to steal confidential information. Vulnerable IoT devices can be exploited to launch a large-scale distributed denial of service (DDoS) attack against the access network. A vulnerable Virtual Network Function (VNF) might manipulate the received packets before forwarding them to the next VNF in the service function chain. AI systems are able to disclose sensitive private information (e.g., identity, position, personal interests) from the processed data, and can be fooled to take wrong decisions [2]. Insecure communication channels and interfaces are sources for service unavailability and data leakage. To lessen these fears and increase confidence in 5G and beyond networks, it is paramount to establish and maintain trust among involved stakeholders and network entities. Building trustworthy 5G and beyond networks is intertwined with guaranteeing that adequate measures are put in place to resist security incidents and preserve the privacy of users' personal information as well as providing continuous assurance that the implemented measures meet the required security and privacy levels.

This article aims to shed light on the trust concept in 5G and beyond networks and its dimensions, whilst pointing out potential emerging trust enablers and research directions. The rest of this article is organized as follows. The next section briefly describes our a view of a typical zero-touch management architecture for secure and trustworthy 5G and beyond networks. The definition of trust is then given. Following that, we present the different trust dimensions in a 5G and beyond ecosystem, including trust in communications, VNFs, NFV infrastructure, services, AI/ML models, data, and applications. We identify the trust requirements and the appropriate security and privacy measures to establish and maintain trust for each dimension. We then discuss the potential of some emerging trust enablers, particularly blockchain, trusted platforms, and behavioral and big data analytics. A case study is then presented to show how trust in data fed into an ML pipeline can be enabled using blockchain technology, while investigating the overhead entailed by the blockchain. Before concluding the paper, we highlight some open issues and future research directions to resolve the trust issue in 5G and beyond networks. (Table I summarizes the abbreviations used in the article.)

## II. Typical Secure and Trustworthy 5G/B5G Management Architecture

The 5G and beyond networks are expected to be highly dynamic in terms of virtualization and softwarization. They are envisioned to support heterogeneous and flexible deployment scenarios, whereby the same infrastructure is shared among multiple services/verticals. The concept is commonly known as network slicing, which consists in creating multiple virtual networks (i.e., slices) dedicated to different service types with diverse performance requirements over a common physical infrastructure. A network slice can span across multiple technological domains (e.g., radio access network (RAN), core network (CN), transport network (TN), multi-access edge network (MEC), cloud infrastructure) and different administrative domains [3].

The anticipated unprecedented complexity in operating and managing 5G and beyond networks is driving the trend

TABLE I: List of abbreviations used in the paper.

| Abbreviation | Description | Abbreviation | Description |
|---|---|---|---|
| AI | Artificial Intelligence | API | Application Programming Interface |
| CN | Core Network | COTS | Commercial Off-The-Shelf |
| DDoS | Distributed Denial of Service | FG-DPM | Focus Group on Data Processing and Management |
| HSM | Hardware Security Module | ICT | Information and Communication Technology |
| IEC | International Electrotechnical Commission | ISG SAI | Industry Specification Group on Securing Artificial Intelligence |
| KPI | Key Performance Indicator | MEC | Multi-access Edge Computing |
| MITM | Man-In-The-Middle | ML | Machine Learning |
| NFV | Network Function Virtualization | NFVO | NFV Orchestrator |
| NS | Network Slicing | PNF | Physical Network Function |
| RAN | Radio Access Network | SDN | Software Defined Networks |
| SDO | Standards Developing Organization | SG13 | Study Group 13 |
| SLA | Service Level Agreement | TC | Trusted Computing |
| TCG | Trusted Computing Group | TEE | Trusted Execution Environment |
| TLA | Trust Level Agreement | TMS | Trust Management System |
| TN | Transport network | TNC | Trusted Network Communications |
| TPM | Trusted Platform Module | VIM | Virtualized Infrastructure Manager |
| VNF | Virtual Network Function | VNFM | VNF Manager |
| ZSM | Zero-touch network and Service Management | ZT | Zero Trust |

towards enabling fully autonomous management capabilities (e.g., self-configuration, self-provisioning, self-monitoring, self-assurance and self-protecting), leveraging SDN, NFV and AI technologies [4]. NFV is recognized as a key enabler for providing flexible, scalable, agile, and cost-effective provisioning and deployment of network services. It aims to decouple network functions, such as load balancers, firewalls, routers, from the underlying hardware, allowing their implementation as VNFs running on top of Commercial Off-the-Shelf (COTS) servers. The management of the virtualized infrastructure (NFVI) as well as the orchestration of resources required by the network services and VNFs are carried out by the NFV management and orchestration functions, namely: (i) Virtualised Infrastructure Manager (VIM), which is in charge of NFVI virtual resources; (ii) VNF Manager (VNFM), which handles the VNF lifecycle; and (iii) NFV Orchestrator (NFVO), which manages network services and resources by interacting with NFVM and VIM[1]. To fulfill the challenging performance and security demands of the wide range of services, an end-to-end management automation across multiple domains is required. Fig. 1 illustrates our view of a typical zero-touch management architecture for 5G and beyond networks. To support the separation of management concerns, the management and orchestration functions are provided at both domain and cross-domain levels. Each management task (e.g., slice manager, E2E slice manager, security manager, and trust manager) is conducted in an intelligent closed-loop way, allowing to automate the generation and enforcement of management policies based on insights extracted with the help of AI/ML techniques from data collected at domain or cross-domain level. The security manager provides real-time enforcement and control of security policies throughout the network service life cycle and manages the security functions. The trust manager assesses the trustworthiness of network services, their composed functions (e.g., VNFs, physical network functions (PNFs)) and the hosting infrastructure. The trust level is determined based on trust attributes specified in the Trust Level Agreement (TLA), which may include security measures in place, compliance with regulation (e.g., privacy preservation), and fulfillment of the agreed service and security levels. While the security manager and trust manager provide, respectively, the security and trust management functions for the network service at the domain level (e.g., RAN, CN, TN), the E2E security manager and E2E trust manager coordinate between domains to manage the network service's security and trust cross domains.

The services running over a 5G network can span across multiple domains and use different physical and virtual network resources that can be either dedicated to a particular service or shared between services. Given that the involved domains and resources may have different trust levels, their interaction may be source of serious security breaches. For instance, a VNF with low trust level may be exploited by an adversary to attack a VNF with more sensitive data if the two VNFs are hosted on the same physical infrastructure. Therefore, isolation and segmentation mechanisms should be applied to control the flow of information between domains with different trust levels. For fine-grained separation, micro-segmentation should be enabled to segregate between workload functions (e.g., VNFs). Micro-segments are endowed with authentication and authorization functions to ensure that only entities with sufficient trust level can interact with each other.

It is worth mentioning that the envisioned management architecture is in compliance with ETSI Zero-touch network and Service Management (ZSM) recommendations[2].

## III. Trust Definition

Trust is a concept that has been considered as a key foundation for decision making in different disciplines, including philosophy, sociology, psychology, economics, law as well as computer science. Although the definitions of trust vary across disciplines, they all share the common idea that trust is "a relationship in which an entity, often called the trustor, depends

[1]ETSI GS NFV-MAN 001 (V1.1.1). Network Functions Virtualisation (NFV); Management and Orchestration.

[2]ETSI GS ZSM 002 (V1.1.1). Zero-touch Network and Service Management (ZSM); Reference Architecture.

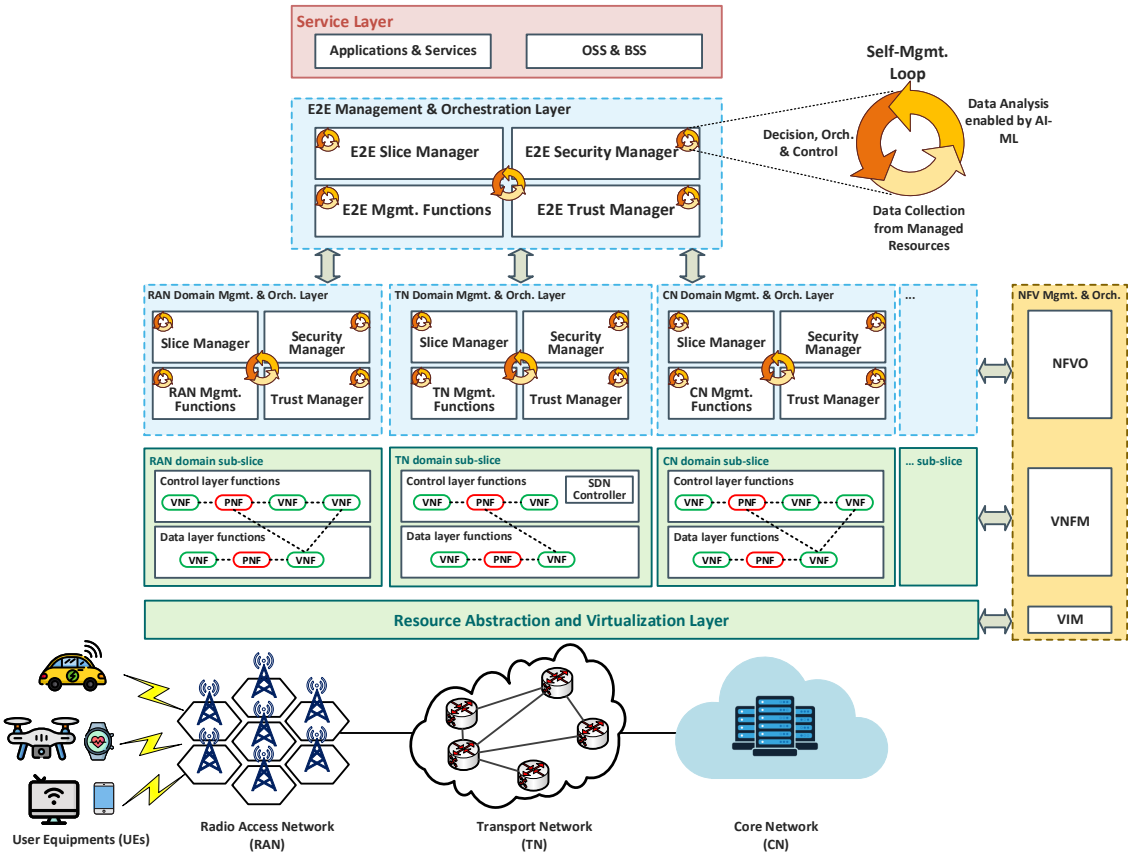



Fig. 1: A typical secure and trustworthy 5G/B5G management architecture.

on someone or something, called the trustee, based on a given criterion" [5].

In the communication and networking field, this concept of trust is used across many domains, such as artificial intelligence, telecommunication, human-computer interactions, social network analysis, communication networks, and cybersecurity [6]. According to ITU-T, trust is "the measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future". ITU-T noted that "trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of entities, value-chains among multiple stakeholders and human behaviors including decision making"[3]. ETSI defines trust as "confidence in the integrity of an entity for reliance on that entity to fulfill specific responsibilities" [7]. They stated that trust is extremely dynamic and characterized in levels of assurance based on specific measures (e.g., identity, attestation, non-repudiation) that identify when and how to rely on a relationship.

Using the aforementioned definitions as a reference, trust in 5G can be defined as an acceptance level between the entities of the 5G architecture for a precise action according to former surveillance of performances. The trust value can be measured, which is used to decide whether a component is eager and able to perform normally in the environment.

[3] ITU-T Y.3052 (03/17). Overview of Trust Provisioning for Information and Communication Technology Infrastructures and Services.

## IV. Trust Surface

The variety of actors and network entities involved in a 5G and beyond network ecosystem broadens its trust surface. In this section, we discuss the multiple trust dimensions (See Fig. 2) to be considered by a Trust Management System (TMS) in 5G and beyond networks. It is worth noting that the trust in services and applications dimension is not shown in Fig. 2 as it is considered as a composite dimension entailing the basic trust dimensions depicted in the figure.


Fig. 2: Basic Trust Dimensions in 5G and Beyond Networks.

### A. Trust in Communications

The communication protocols and established channels between the interacting entities are vulnerable to a variety of threats, including impersonation (spoofing), DDoS, Man-In-The-Middle (MITM), message replay and manipulation, and eavesdropping [8]. Thus, reliable and secure communications are paramount to ensure service availability while preventing data and privacy leakage. To this end, authentication, authorization, and transmission encryption services are required[4]. The authentication service guarantees that the communication is established among legitimate entities. It is worth mentioning that unlike 4G and previous generations, 5G extends the trust model to include the service providers, as depicted in Fig. 3. As a result, 5G introduces a new authentication framework enabling an end-user device to perform not only the primary authentication for network access, but also a secondary authentication for service access[4]. The control (signaling) messages and user data should be exchanged over encrypted and integrity-protected channels in order to ensure compliance with privacy regulations and obviate the risk of sensitive information leakage and tampering.

The communication protocols used within the 5G infrastructure can result in malicious signaling storms (e.g., excessive attach/detach requests received from a massive number of IoT devices exploited by a botnet). In addition to mutual authentication between communicating entities, mechanisms for real-time detection and mitigation of signaling DDoS attacks are vital to ensure the infrastructure availability.

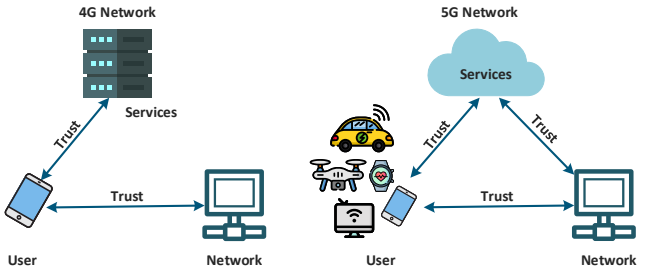



Fig. 3: 4G vs 5G Trust Model.

The 5G system is designed as a Service-Based Architecture (SBA) where the system functionality is achieved by a set of network functions exposing their services to internal network functions and external third parties via Service-Based Interfaces (SBIs). 3GPP recommends to implement SBIs as REST-based open Application Programming Interfaces (APIs). The key role played by the APIs in integrating and orchestrating services makes them an ideal target for attackers [9]. By 2022, API abuses are expected by Gartner to be the most-frequent attack vector. Such abuses may involve identity theft, DDoS and MITM. The API security can be enabled through the implementation of various security measures, including authentication (e.g., using OAuth2.0, JWT tokens), authorization (e.g., using Role Based Access Control, Attribute Based Access Control), communication encryption (e.g., using Transport Layer Security (TLS)), input validation, and throttling/rate limiting [9].

[4] 3GPP TS 33.501 (V16.4.0). Security Architecture and Procedures for 5G System (Release 16).

### B. Trust in VNFs

Despite its potential to empower flexible, scalable, agile, and cost-effective provisioning and deployment of network services, the virtualization of network functions introduces new security challenges. Indeed, a malicious or compromised VNF has the potential to escalate privilege, escape isolation, disclose and tamper data, spread malware, and carry out DoS attacks. For instance, a malicious VNF may manipulate the received packets before forwarding them to the next VNF in the service function chain or deny resources to co-located VNFs by exhausting shared resources. Thus, mechanisms to build and assess the trustworthiness of VNFs along their lifecycle are paramount [7]. The validation and certification of the VNF software should be performed during both the on-boarding and subsequent instantiation of a VNF. The validation is a procedure that applies authenticity and integrity mechanisms to ascertain the provenance of the VNF software from a trusted vendor/supplier and that its content has not been tampered with. A VNF is certified by conducting quality and security assurance tests to ensure that the VNF software functions as expected and it is free from vulnerabilities. Furthermore, the assurance of the VNF instance identity and the monitoring of its behavior and performance throughout its lifespan are key requirements for establishing trust between instantiated VNFs.

### C. Trust in Management and Orchestration

Given the key role played by NFV management and orchestration (NFV-MANO) functions (i.e., NFVO, VNFM, VIM), their compromise or unavailability can jeopardize the security and functioning of the entire network [10]. For instance, a compromised or impersonated NFVO may perform malicious actions on VIM to cause resource exhaustion leading to DoS. Thus, it is imperative to ensure the resiliency, reliability and availability of MANO's components in order to build trust in them. Mechanisms to ascertain the identity and integrity of MANO components are vital to prevent masquerade attacks. A continuous analysis and auditing of their behavior and resilience to attacks is necessary to trust in their actions. Finally, appropriate redundancy procedures are also required to meet the availability and geographic restriction requirements.

### D. Trust in NFV Infrastructure

The NFV Infrastructure (NFVI) is the set of physical compute, storage and network resources and the virtualization software which build up the virtual environment in which VNFs are deployed. Given that VNFs can run mission-critical functions, it is crucial to trust its virtualized hosting infrastructure. In fact, improperly secured and/or malicious NFVI can pose serious security risks to hosted VNFs, such as isolation failure and introspection attack. A vulnerable hypervisor may allow a malicious VNF to break isolation, putting into danger the confidentiality, integrity and/or availability of co-resident VNFs [11]. Furthermore, a malicious hypervisor with introspection capabilities can view, inject, and/or change

operational state information (i.e., code + data) associated with a VNF. In order to be trusted, a NFVI should provide the assurance of its own security as well as its capabilities to meet security and performance requirements of hosted VNFs. Secured boot is a key enabler to prove the integrity of the hypervisor and VNFs at load time [7]. Measured boot (i.e., load time integrity status) and hardware-based roots of trust (e.g., Hardware Security Module (HSM), Trusted Platform Module (TPM)) are pre-requisite to enable remote attestation of the platform. The capability of a NFVI to provide an isolated and trusted environment for executing critical software components is paramount to prevent introspection risk. Trusted Execution Environments (TEE) are hardware-based solutions that can be leveraged to achieve this goal. As the NFVI can span several geographic areas, the location assertion is essential to meet the operating location rules. Indeed, some VNFs may need to operate only in a specific geographical, logical or jurisdictional location. For example, VNFs for lawful interception are mandated to be in-country; that is, they are allowed to run only in the country that issued the authorization. The NFVI should also ensure the availability of resources required to meet the performance requirements of the hosted services according to the Service Level Agreement (SLA).

### *E. Trust in AI/ML Models*

AI is vital for embodying cognitive and self-managing capabilities to 5G and beyond networks, enabling fully autonomous networks that can cater to the stringent requirements in terms of latency and reliability. However, the integration of AI systems raises reliability, security, safety and transparency concerns. On one hand, AI systems are prone to several adversarial attacks [12] that can influence them to learn wrong models, make erroneous decisions, or leak confidential information. On the other hand, the domain experts (e.g., telecommunication operators, verticals) need guarantees to trust the decisions taken by an AI system. Thus, without enforcing its trustworthiness, AI may become intentionally malevolent endangering not only the performance expectations of 5G and beyond networks but also the people's lives. An AI system must be able to explain its reasoning in order to foster trust in its decisions. For instance, it is necessary for a telecommunication operator to explain the decision taken by an AI-powered network optimization solution that has led to not achieving the ultra-latency requirements. An explainable AI looks at what, how and why a decision was made, allowing to establish accountability, reliability and transparency of AI systems [13]. The AI systems must guarantee that the data is processed in compliance with privacy protection regulations. Differential privacy, homomorphic encryption and decentralized learning (e.g., federated learning) are among the most promising approaches to achieve privacy-preserving AI [2]. Another key requirement for trustworthy AI is the attestation of robustness and resiliency of AI/ML models to adversarial attacks. Possible defense mechanisms that could be adopted to enable robust AI/ML models include input validation, adversarial training, ensemble methods and moving target defense [2].

### *F. Trust in Data*

AI is poised as a key enabler to empower intelligent self-managing capabilities in 5G and beyond networks. However, the success of AI in enabling those capabilities is heavily reliant on the quality of underlying data. In fact, inaccurate and manipulated data can have a substantial impact on the accuracy of decisions taken by the analytics and intelligence services. For instance, imprecise historical traces of a user's location can lead to wrong forecasting of his next position, which may mislead the caching service into taking the right decision on whether and where to cache the user's content beforehand. It is therefore crucial to ensure the trustworthiness of data. Many factors contribute to establishing trust in data, including data quality, data provenance, and data security. The data quality refers to data that are fit for use by data consumers [14]. The primary metrics used to quantify the quality of data include accuracy, completeness, timeliness, validity, and consistency. To maximize data trustworthiness, the fulfillment of the required data quality should be measured and monitored over the entire data lifecycle. The data provenance promotes trust in data by tracking its sources and derivation history. Data security aims to safeguard data against tampering by performing integrity checks.

### *G. Trust in Services and Applications*

5G and beyond networks are expected to enable and support a wide range of applications and services, such as augmented and virtual reality, teleportation, industry 4.0, remote healthcare, and autonomous driving. The deployment and use of these services and applications may affect the security, safety and privacy of network and users. For instance, a vulnerable or malicious IoT application may allow an attacker to conduct a signaling storm attack against the RAN resources [2]. The failure of mission- and safety-critical applications, such as unmanned communications and remote surgery, to provide the ultra-latency requirements may put human lives in danger. Thus, it is vital to ensure the trustworthiness of the delivered services and applications. in fact, a trustworthy application/service, including a network slice service, should operate in adherence to SLA, security, and privacy requirements. Continuous monitoring and assessment of Quality of Service (QoS) and Quality of Experience (QoE) is required to provide the assurance that the agreed SLA is guaranteed. The fulfillment of security requirements can be attested through the implementation of (i) integrity checks to ascertain that the application/service is genuine, (ii) authentication and authorization mechanisms to ensure that the application/service is protected from unauthorized access. This is particularly relevant to critical services/applications; (iii) quality and security assurance tests to ensure that the application/service is operating as intended and it is free from vulnerabilities. The user privacy assurance can be provided by adopting adequate methods to empower the security and privacy of data in rest or transit[5]. Besides encrypted communication channels, access control and data integrity mechanisms are necessary to

[5]ETSI TS 103 485 (V1.1.1). CYBER; Mechanisms for Privacy Assurance and Verification.

ensure that the sensitive data are disclosed only to legitimate entities and have not yet tampered with. Privacy protection measures, such as anonymity, pseudonymity and obfuscation, are required to prevent reidentification of a service/application user from his Personally Identifiable Information (PII) (e.g., identity and location information). Moreover, it is important to provide an accurate audit trail on which PII is collected and for what purposes, how it is processed and used, and by whom. Such audit trails allow to guarantee that the PII is handled on the basis of users' consent and in accordance with laws and regulations.

## V. Emerging Trust Enablers

This section promotes the potential of blockchain, trusted platforms, and behavioral and Big data analytics in implementing some of the aforementioned security measures to enable trust in 5G and beyond network ecosystem.

### A. Blockchain

The Blockchain's intrinsic features of decentralization, security, transparency and auditability make it a promising candidate to foster trust in 5G and beyond networks without relying on a trusted third party. These characteristics ensue from the fact that a blockchain is designed as a distributed, shared digital ledger for storing records in an immutable and tamper-proof way. Once a new block - or record - is created, it is validated by peers on the blockchain network using a consensus protocol before being added to the ledger. The blocks are chained together by including in each block the cryptographic hash of the preceding block. The use of crypto-hashing guarantees the integrity property, making the blocks tamper-proof. Blockchains can be roughly divided into two types, namely: (i) permissionless blockchains (e.g., Bitcoin, Ethereum) which are public and anyone can participate in the consensus process to add blocks; and (ii) permissioned blockchains (e.g., Hyperledger Fabric) which are accessible only by authorized entities.

A blockchain can play the role of a distributed trust authority. Indeed, it can be used to empower software and data integrity assurance. Furthermore, its immutability property can be leveraged to maintain comprehensive audit trails of all events and changes related to VNFs, data and applications, allowing to ascertain their provenance from trusted sources [15] and that PII is processed on the basis of the user's consent and in compliance with regulation. Finally, blockchain smart contracts are an ideal tool to enable authentication and access control, and establish service level agreements (SLA) with an automatic liability enforcement in case of violation.

### B. Trusted Platforms

Hardware-based security modules (e.g., TPM) and hardware-mediated execution enclaves (e.g., TEE) are considered key enablers to promote trust in NFVI [7], by providing hardware-based root of trust. TPM can be used to safeguard integrity measurements, cryptographic keys and certificates that are needed to empower measured boot and remote attestation of hosted VNFs. While remote attestation shelters the integrity of VNF instances at load time, it falls short in preventing introspection risk. TEE is recognized as a promising solution to guarantee the integrity and confidentiality of VNFs at run-time [9]. In fact, TEE is an isolated, secure execution environment having the capabilities of protecting its content (i.e., code and data loaded) from unauthorized access and tampering even in the presence of a high-privileged malicious hypervisor or operator, allowing to address the introspection issue.

### C. Behavioral and Big data Analytics

The trust is likely to decay over time due to various factors, such as SLA violations, new vulnerabilities being reported, changes in configuration and intended behavior, security breaches, and failures. For instance, an initially trusted VNF can become compromised by exploiting zero-day vulnerabilities, which requires to revisit its trust level. Thus, a continuous trust assessment is essential to maintain the desired trust level between stakeholders and network entities involved in the 5G and beyond ecosystem. Nevertheless, the diversity of trust parameters and the growing volume of trust-related data makes the constant and timely evaluation of trust a challenging task. Big data analytics is a promising enabler to address this challenge, thanks to its potential to correlate and analyze a tremendous amount of time-varying multi-dimensional data to uncover hidden patterns. In fact, leveraging data analytics enables identification and modeling of security posture and behavior, real-time measurement and adjustment of trust levels, as well as prediction of future trustworthiness values. The use of AI has also the potential to automatically generate quality and security assurance tests.

Table II summarizes the main security threats discussed in the previous section as well as the emerging enablers that could be leveraged to implement their potential security measures in order to build trust between network entities involved in a 5G ecosystem.

## VI. Trust and Standardization

This section provides an overview of the relevant efforts and initiatives of Standards Developing Organizations (SDOs) to foster the different dimensions of trust in future networks.

ITU-T Study Group 13 (SG13) published different recommendations related to trust in future networks. The recommendation ITU-T Y.3052[3] provides an overview of trust provisioning in information and communication technology (ICT) infrastructure and services. Y.3052 explains the concept of trust provisioning, and introduces a trust relationship model and trust evaluation based on trust indicators and trust index. The recommendation ITU-T Y.3517[6] focuses on inter-cloud trust management, where a trust model and a reputation-based trust management are specified. The recommendation ITU-T Y.3053[7] introduces a conceptual model for trustworthy networking in trust-centric network domains. The model encompasses features of identification and trust evaluation of

[6]ITU-T Y.3517 (12/2018). Cloud Computing – Overview of Inter-Cloud Trust Management.

[7]ITU-T Y.3053 Amendment 1 (12/18). Framework of Trustworthy Networking with Trust- centric Network Domains.

TABLE II: Summary of trust dimensions, the related security threats, the potential measures and the emerging enablers to establish trust between entities in a 5G ecosystem.

| Trust Dimension | Potential Security Threats | Potential Security Measures | Emerging Enabler |
|---|---|---|---|
| Communication | - Spoofing<br>- DDoS<br>- MITM<br>- Message reply<br>- Eavesdropping<br>- API abuses | - Authentication and authorisation controls | Blockchain |
| | | - Encrypted transmission services (e.g., TLS) | Trusted platforms (Protect encryption keys) |
| | | - Throttling/rate limiting APIs usage | Behavioral & Big data analytics |
| VNF | - Privilege escalation<br>- Escape isolation<br>- Data exposure and exploitation<br>- Malware dissemination<br>- DDoS attacks | - VNF software validation (authenticity and integrity) | Blockchain |
| | | - VNF software certification (Quality and security tests) | Behavioral & Big data analytics |
| | | - VNF instance identity assurance | Blockchain |
| | | - VNF instances's behaviour and performance monitoring | Behavioral & Big data analytics |
| NFVI | - Isolation failure<br>- Introspection attacks | - Secured boot<br>- Measured boot | Trusted platforms |
| MANO | - Impersonation<br>- DDoS (resource depletion) | - Identity and integrity mechanisms | Blockchain |
| | | - Continuous assessment of MANO's activities and resiliency to attacks | Behavioral & Big data analytics |
| | | - Redundancy procedures | |
| AI/ML | - Incorrect patterns learning<br>- Wrong decision making<br>- Sensitive data leakage | - Explainable AI | |
| | | - Privacy-preserving AI/ML | |
| | | - AI/ML models resilient to adversarial attacks | Blockchain (Prevent poisoning attacks) |
| Data | - Manipulated and inaccurate data | - Data quality (accuracy, completeness, timeliness, validity, consistency) | |
| | | - Data provenance (track its sources and derivation history)<br>- Data security (integrity checks) | Blockchain |
| Applications & Services | - Endanger user safety<br>- Impact network security (e.g., DoS)<br>- Data security and privacy violation | - Continuous monitoring and assessment of QoS and QoE | Behavioral & Big data analytics |
| | | - Application/service integrity check | Blockchain |
| | | - Authentication and authorization mechanisms | Blockchain |
| | | - Quality and security assurance tests | Behavioral & Big data analytics |
| | | - Audit trails on use of PII | Blockchain |

network elements and trustworthy communication between them. A security framework based on trust relationship among stakeholders in 5G ecosystem is under development in ITU-T SG17[8].

NIST proposes Zero Trust Architecture (ZTA)[9], an enterprise's resource and data security strategy that is based on zero trust (ZT) principles. ZT is a cybersecurity paradigm centered on the assumption of mistrust; that is, everyone can be a threat and the network is hostile. The core tenets of ZT is to never trust, always verify, enforce least privilege-access, and maintain dynamic risk-based access policies. ZTA encompasses "identity, credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure".

The Industry Specification Group (ISG) NFV[10] focuses on security and trust challenges related to virtualization. In this regard, different reports and specifications have been developed, providing security and trust guidance that is unique to NFV, and addressing VNF Package security, MANO components security, certification management, remote attestation, multi-layer host administration, and execution of sensitive NFV components.

The Trusted Computing Group (TCG)[11] develops specifications and standards for the Trusted Platform Module (TPM), Trusted Network Communications (TNC), and Trusted Computing (TC). TPM focuses on the establishment of hardware-based root of trust. TCN architecture offers compliance, orchestration and access control capabilities, aiming to address network visibility, endpoint compliance, network enforcement, and security automation problems. TC revolves around trust establishment, platform information exchange, and policies compliance assurance for cloud users. A trusted multi-tenant

[8]X.5Gsec-t: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14786
[9]https://csrc.nist.gov/publications/detail/sp/800-207/draft
[10]https://www.etsi.org/committee/1427-nfv
[11]https://trustedcomputinggroup.org

infrastructure reference framework is proposed to build a trusted computing base using shared multi-tenant infrastructure. Recently, a work group is created by TCG to extend the trust concepts into vritualized platforms.

The trust in data has also attracted the attention of SDOs. The International Organization for Standardization (ISO) develops several standards on software and data quality (ISO/IEC 25000 series[12]) and records/archives management (ISO/TC46/SC11[13]). The ITU-T Focus Group on Data Processing and Management (FG-DPM[14]) proposes a trusted data enabling process model in line with the requirements from ISO/TC46/SC11. In another specification, FG-DPM defines the requirements, functional models, a platform and deployment modes of blockchain-based data exchange and sharing.

Recognizing the key role that AI will play in the digital transformation, different standardization initiatives are underway to promote trust in AI. The ISO and IEC (International Electrotechnical Commission) joint technical committee on artificial intelligence (ISO/IEC JTC 1/SC 42[15]) has very recently published a technical report providing an overview of trustworthiness in AI and is developing standards on risk management for AI and assessment of the robustness of neural networks. ETSI initiated a new Industry Specification Group on Securing Artificial Intelligence (ISG SAI[16]). The group aims to develop standards to safeguard and improve the security of AI in ICT field.

## VII. Case Study - Blockchain-based Trust in Data

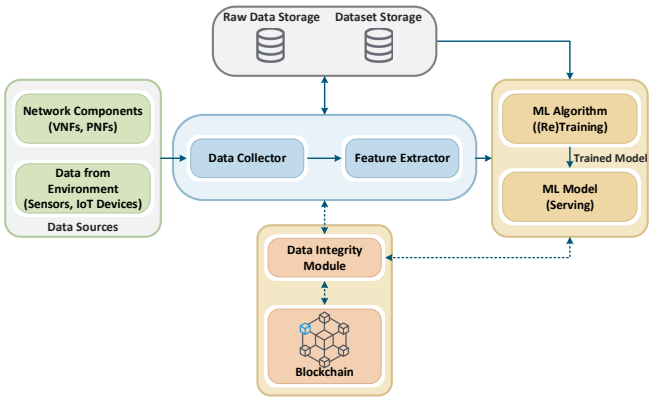



Fig. 4: Learning Pipeline with Blockchain-based Trustworthy Data.

Data is the fuel powering AI and Machine Learning (ML) algorithms. Its manipulation may result in drastic change in the decisions made by AI/ML models. Thus, the importance of protecting the data integrity cannot be overlooked. Different enablers can be leveraged to enforce the integrity of data. Traditionally, cryptographic mechanisms such as Message Authentication Codes (MAC) and digital signatures have been used to achieve data integrity protection. However, a major challenge with those mechanisms is their reliance on trust in a third party for public/private key generation. Consequently, if the key generator is compromised, the whole system will be compromised. As aforementioned, Blockchain is emerging as an ideal alternative to develop advanced methods for guaranteeing data integrity in an exposed environment without relying on a trusted third party. Indeed, it can be used to enable data integrity assurance. In this section, we present a case study demonstrating how the integrity of data fed into a ML algorithm (during training phase) or ML model (during inference phase) can be empowered using blockchain technology.

Figure 4 depicts the proposed learning pipeline with blockchain-based trustworthy data. The pipeline encompasses the following components: (1) a *data collector* which collects the raw data from various sources (e.g., network traffic from vSwitch); (2) a *feature extractor* which processes raw data to retrieve features relevant to learning task; (3) a *data integrity module* which is in charge of maintaining and assessing the integrity of data using blockchain smart contracts; and (4) ML algorithm and model which leverage the extracted data for training and inference purposes, respectively.

For each acquired raw data file, the data collector assigns a unique identifier (ID), records its hash along side its ID in the blockchain leveraging the hashing service provided by the data integrity module, and uploads the file to the raw data storage. It is worth noting that given the huge amount of data that can be collected from the network, only the raw data hashes are stored in the blockchain, which allows to improve the blockchain's scalability and performance. The data extractor can either fetch the raw data file from the storage (during training phase) or receive it in real-time from the data collector (during the inference phase). In both cases, the data extractor utilizes the integrity checking service provided by the data integrity module to assess the integrity of the raw data file. The raw data file integrity is validated by calculating and comparing its hash with the one retrieved from the blockchain. After proving its integrity, the raw data file is processed by the feature extractor to retrieve the feature vectors. Once extracted, the set of feature vectors is split into multiple chunks. For each chunk, the feature extractor assigns a unique ID, records its hash along side its ID and the ID of the raw data file from which it has been extracted in the blockchain using the hashing service provided by the data integrity module, and uploads the chunk to the dataset storage. The rationale behind breaking data down into chunks is to prevent losing the whole data in case of data integrity breaches; only the altered chunks will be lost. Similar to raw data files, the ML algorithm (during the training phase) or the ML model (during the inference phase) conducts an integrity check before using the chunks. It is worth mentioning that the interaction with the blockchain is performed through a smart contract including functions to add and retrieve hashes.

The data integrity assurance and the audit trails provided by the blockchain comes at the price of an increased latency to access data, which will certainly impact the training time as well as the inference time of the ML algorithm and ML model, respectively. To investigate the time overhead entailed by the

[12]https://iso25000.com/index.php/en/iso-25000-standards
[13]https://www.iso.org/committee/48856.html
[14]https://www.itu.int/en/ITU-T/focusgroups/dpm/Pages/default.aspx
[15]https://www.iso.org/committee/6794475.html
[16]https://www.etsi.org/commit- tee/1640-sai

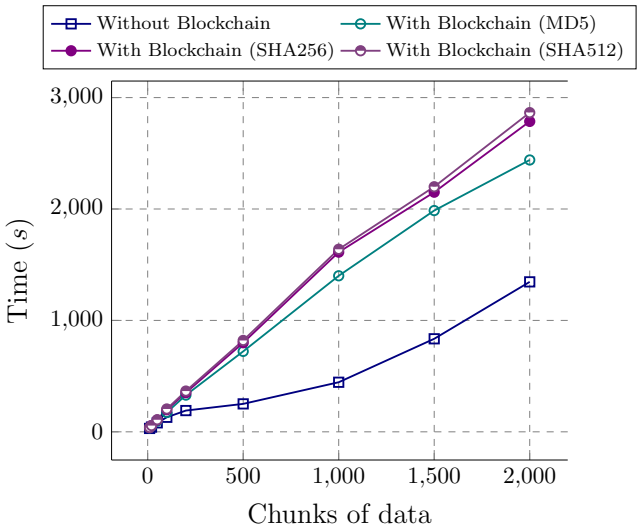



Fig. 5: Comparison of overhead induced by the use of Blockchain using different Hashing Algorithms.

blockchain, we implemented a permissioned blockchain using Hyperledger Fabric[17]. We used a dataset [18] containing 800000 samples [16], where each sample represents either a legitimate or a DDoS network flow defined by a feature vector containing 79 features. The dataset is used to train a deep learning model for detecting application-layer DDoS attacks. The data access time is measured with and without the use of blockchain for varied number of chunks and different hashing algorithms (i.e., MD5, SHA256 and SHA512). The data access time is defined as the time elapsed between when the ML algorithm requests the data chunk and when this chunk is ready to be used for training. The comparative results depicted in Fig. 5 show that while the access time increases with the increase in the number of chunks, the use of blockchain exhibits a significant impact on the access time. The access time is also influenced by the hashing algorithm used. In fact, the more robust the hashing algorithm is, the longer the hashing time will be.

## VIII. Open Issues and Research Directions

Although trust in 5G and beyond networks has recently attracted increasing research interest, addressing the trust issue in these networks is still far from being resolved. With the growing set of stakeholders and the increasing number of interconnected devices and services, a zero-trust approach is an attractive solution for building an effective end-to-end security posture in future networks. In fact, the "never trust, always verify" principle, underlying the ZT paradigm, requires explicit authentication and authorization of each access request, which allows to reduce the risk of data breaches and reduce the risk of lateral movement within the network. However, a zero-trust model for 5G and beyond networks is not yet defined. A potential research direction is to investigate how to accommodate the ZTA to the complex 5G and beyond ecosystem. The adoption of a zero-trust model entails a continuous monitoring and assessment of risks, which may impact the network performance. Thus, further researches are needed to evaluate this impact and propose mechanisms to reduce it.

It is widely recognized that what is "measurable is manageable". Therefore, an effective management of trust in 5G and beyond ecosystem entails the identification of relevant trust Key Performance Indicators (KPIs) and metrics that need to be measured for each entity involved in this ecosystem (e.g., services/applications, VNFs, AI/ML models, data, infrastructure, management & orchestration functions). The trust KPIs can broadly be categorized into security related KPIs (e.g., confidentiality, integrity, robustness, privacy, safety), performance related KPIs (e.g., availability, precision) and transparency related KPIs (e.g., explainability, interpretability). For example, the trust KPIs for a VNF include its integrity and its source credibility, its robustness which can be measured by e.g. the security measures in place and their strength, the number of detected vulnerabilities and the impact of their exploitation, and the number of security breaches, and its capability of providing the intended functionality. In the case of an AI/ML model, the trust KPIs may include its transparency which can be computed by the degree of its explainability, its robustness to adversarial attacks which can be measured by the defense mechanisms adopted and their effectiveness, its privacy preservation, and its performance which can be quantified using e.g. precision, accuracy and F1 score metrics. In a more abstract level (e.g., service, slice or domain), measuring the trust KPIs is more challenging as it depends on the trustworthiness of all involved components. For instance, the safety of a remote surgery service can be related to the performance and security of AI/ML models and VNFs used, the reliability of communication channels, and the availability of the infrastructure resources. How to appropriately combine the trust metrics of composing entities to derive the end-to-end trust metrics is still an open issue. Besides, to the best of our knowledge, a framework for defining and measuring the trust KPIs and their target values in 5G and beyond networks has not yet been defined. Moreover, the trust and risk assessment in 5G and beyond networks becomes a very challenging task due to the increasing number of trust metrics and the high complexity and dynamics of the network. Approaches that leverage AI, big data analytics and automation capabilities are desirable to deal with the complexity of 5G and beyond networks. Furthermore, the use of AI-powered analytics for trust level prediction based on the historical behavior of network entities is an important topic to investigate.

As security risks cannot be eradicated even with a zero-trust model in place, addressing the question of liability and responsibility when security breaches occurs is necessary to foster confidence between parties and compliance with regulation. Therefore, liability-aware trust schemes need to be designed to enable liable end-to-end service delivery in future networks. Smart contracts are a potential candidate to define Trust Level Agreement (TLA) and enforce duty of involved parties in case of TLA violation.

Intent-based technologies and AI are identified as key

[17]https://www.hyperledger.org/use/fabric

[18]https://drive.google.com/drive/folders/1h-b7px3RmgvzXS1notQl2dl9RobHko8x?usp=sharing

drivers to enable zero-touch management capabilities in 5G and beyond networks. However, without appropriate measures to address security issues brought by those enablers, the full automation could indisputably become a weapon that may endanger the entire ecosystem [9]. Thus, it is paramount to devise mechanisms to guarantee the security and trustworthiness of intent and AI techniques in order to build trust in network automation.

As aforementioned, blockchain is a promising technology to promote trust in 5G and beyond networks, by enabling authentication and access control, integrity and provenance assurance, and SLA definition. Nevertheless, its adoption poses scalability, performance, and privacy challenges. The scalability and performance issues stem mainly from the decentralization of the consensus protocol, which, while provides the security guarantees, limits the transaction throughput and speed, and increases the computation, storage and communication overhead to process transactions. Several solutions have been proposed to deal with the scalability and performance problems, including increase in block size, sharding, faster consensus algorithms, and off-chain methods. Increasing the block size would allow for a higher transaction throughput but at the price of increased block propagation time which may prevent the blockchain network from reaching a globally consistent state. The key idea behind sharding is to partition the network into multiple committees (or shards), each of which is in charge of approving a disjoint set of transactions, resulting in improved throughput and reduced communication, computation and storage overhead. However, sharding introduces security challenges where the entire network can be compromised by only compromising one shard. Even though lightweight and faster consensus protocols such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT) can increase the transaction throughput, they pose security concerns and/or fail to achieve adequate decentralization. The off-chain methods improve scalability by offloading the time-consuming operations outside the main blockchain and then writing the results back to the main chain. Nevertheless, the use of off-chaining may impact the blockchain's trustlessness property. Thus, improved or new approaches are required to cater to the stringent scalability and performance requirements of 5G and beyond networks without sacrificing the blockchain security. AI can play a key role in achieving this goal, where its potential can be leveraged to dynamically adjust the block size as well as design efficient sharding and off-chaining solutions [17]. Moreover, how to reconcile privacy and data protection rights with transparency and immutability of blockchain is still an open question.

## IX. Conclusion

This paper identified the different trust dimensions to be considered by a trust management system in 5G and beyond networks. We discussed the security measures needed to establish and maintain trust for each dimension. We then advocated some emerging enablements (e.g., blockchain, trusted platforms, big data analytics) and concepts (e.g., zero-trust models) that can be leveraged to foster trust in a 5G and beyond ecosystem. However, the adoption of these enablements and concepts will open up new issues in terms of privacy, performance and scalability. Achieving the balance between the desired trust level and the induced cost is of utmost importance.

## Acknowledgment

This work was supported in part by the European Union's Horizon 2020 research and innovation programme under the MonB5G project (Grant No. 871780); the Academy of Finland Project 6Genesis Flagship (Grant No. 318927); and CSN (Grant No. 311654).

## References

[1] C. Benzaid and P. Alemany and D. Ayed, G. Chollon and M. Christopoulou and G. Gür and V. Lefebvre and E. Montes de Oca and R. Muñoz, J. Ortiz and A. Pastor and R. Sanchez-Iborra and T. Taleb and R. Vilalta and G. Xilouris, "White Paper: Intelligent Security Architecture for 5G and Beyond Networks," Nov. 2020.

[2] C. Benzaid and T. Taleb, "AI for Beyond 5G Networks: A Cyber-SecurityDefense or Offense Enabler?" *IEEE Network Magazine*, To appear.

[3] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On Multi-domain Network Slicing Orchestration Architecture and Federated Resource Control," *IEEE Network Magazine*, vol. 33, no. 5, pp. 242 – 252, Sept. 2019.

[4] M. Bagaa and T. Taleb and J. B. Bernabe and A. Skarmeta, "QoS and Resource-aware Security Orchestration and Life Cycle Management," *IEEE Trans. on Mobile Computing*, to appear.

[5] J.-H. Cho, K. Chan, and S. Adali, "A survey on Trust Modeling," *ACM Comput. Surv.*, vol. 48, no. 2, Oct. 2015. [Online]. Available: https://doi.org/10.1145/2815595

[6] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[7] ETSI GS NFV-SEC 003, "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance," Dec. 2014.

[8] ENISA, "ENISA Threat Landscape for 5G Networks; Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)," , Nov. 2019.

[9] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Network Magazine*, vol. 34, no. 3, pp. 124 – 133, May/June 2020.

[10] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "SecMANO: Towards Network Functions Virtualization (NFV) based Security Management and Orchestration," in *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016, pp. 598–605.

[11] S. Lal, T. Taleb, and A. Dutta, "Nfv: Security Threats and Best Practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211 – 217, Aug. 2017.

[12] C. Benzaid and T. Taleb, "AI-driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions," *IEEE Network Magazine*, vol. 34, no. 2, pp. 186 – 194, March/April 2020.

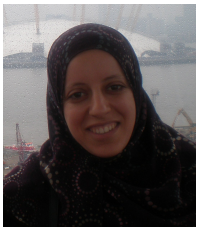
[13] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti and D. Pedreschi, "A Survey of Methods for Explaining Black Box Models," *ACM Computing Surveys*, vol. 51, no. 5, pp. 93:1 – 93:42, Aug. 2018.

[14] R. Y. Wang and D. M. Strong, "Beyond Accuracy: What Data Quality Means to Data Consumers," *Journal of Management Information Systems*, vol. 12, no. 4, pp. 5 – 33, March 1996.

[15] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and Beyond Networks: A State of the Art Survey," *Journal of Network and Computer Applications*, vol. 166, Sept. 2020.

[16] C. Benzaid and M. Boukhalfa and T. Taleb, "Robust Self-Protection Against Application-Layer (D)DoS Attacks in SDN Environment," in *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC)*, May 2020.

[17] Y. Liu, F. R. Yu, X. Li, H. Ji and V. C. M. Leung, "Blockchain and Machine Learning for Communications and Networking Systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392 – 1431, Secondquarter 2020.



**Chafika Benzaïd** is currently a PostDoc researcher at MOSA!C Lab, Aalto University. She is an associate professor and research fellow in Computer Science Department at University of Sciences and Technology Houari Boumediene (USTHB). She obtained her PhD degree in Computer Sciences from USTHB in 2009. Her current research interests include AI-driven network security and AI security. She serves/served as a TPC member for several international conferences and as a reviewer for multiple international journals.

**Tarik Taleb** is Professor at Aalto University and University of Oulu. He is the founder and director of the MOSA!C Lab (www.mosaic-lab.org). Prior to that, he was a senior researcher and 3GPP standards expert at NEC Europe Ltd., Germany. He also worked as assistant professor at Tohoku University, Japan. He received his B.E. degree in information engineering, and his M.Sc. and Ph.D. degrees in information sciences from Tohoku University in 2001, 2003, and 2005, respectively.

**Muhammad Zubair Farooqi** is currently working as a Research Assistant at MOSA!C Lab, AALTO University Finland. He received his M.Sc. degree from FAST-NUCES, Islamabad, Pakistan, and Bachelor degree from COMSATS University Islamabad. His research interests include wireless sensor networks, software defined networks, and network security.

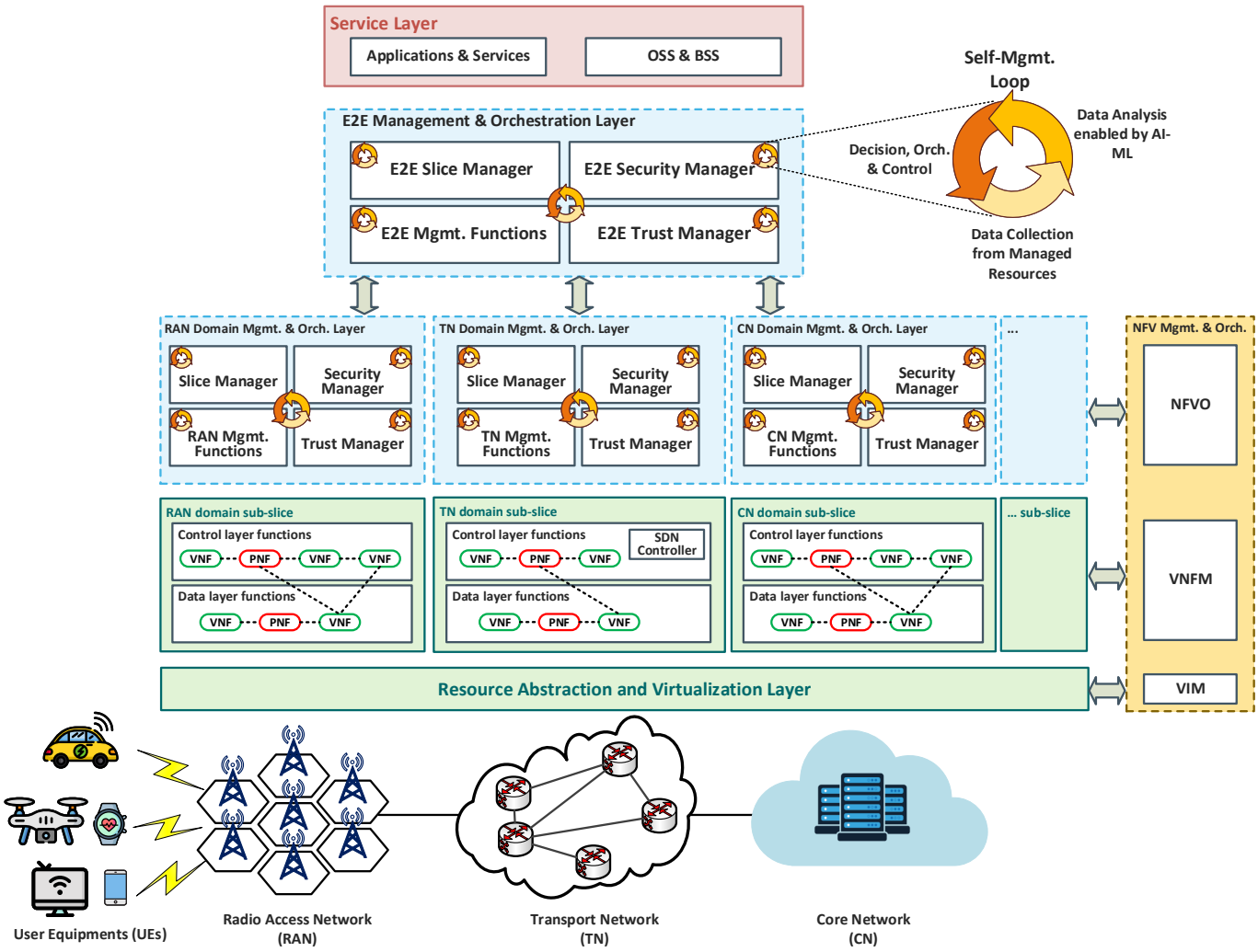



Fig. 1: A typical secure and trustworthy 5G/B5G management architecture.

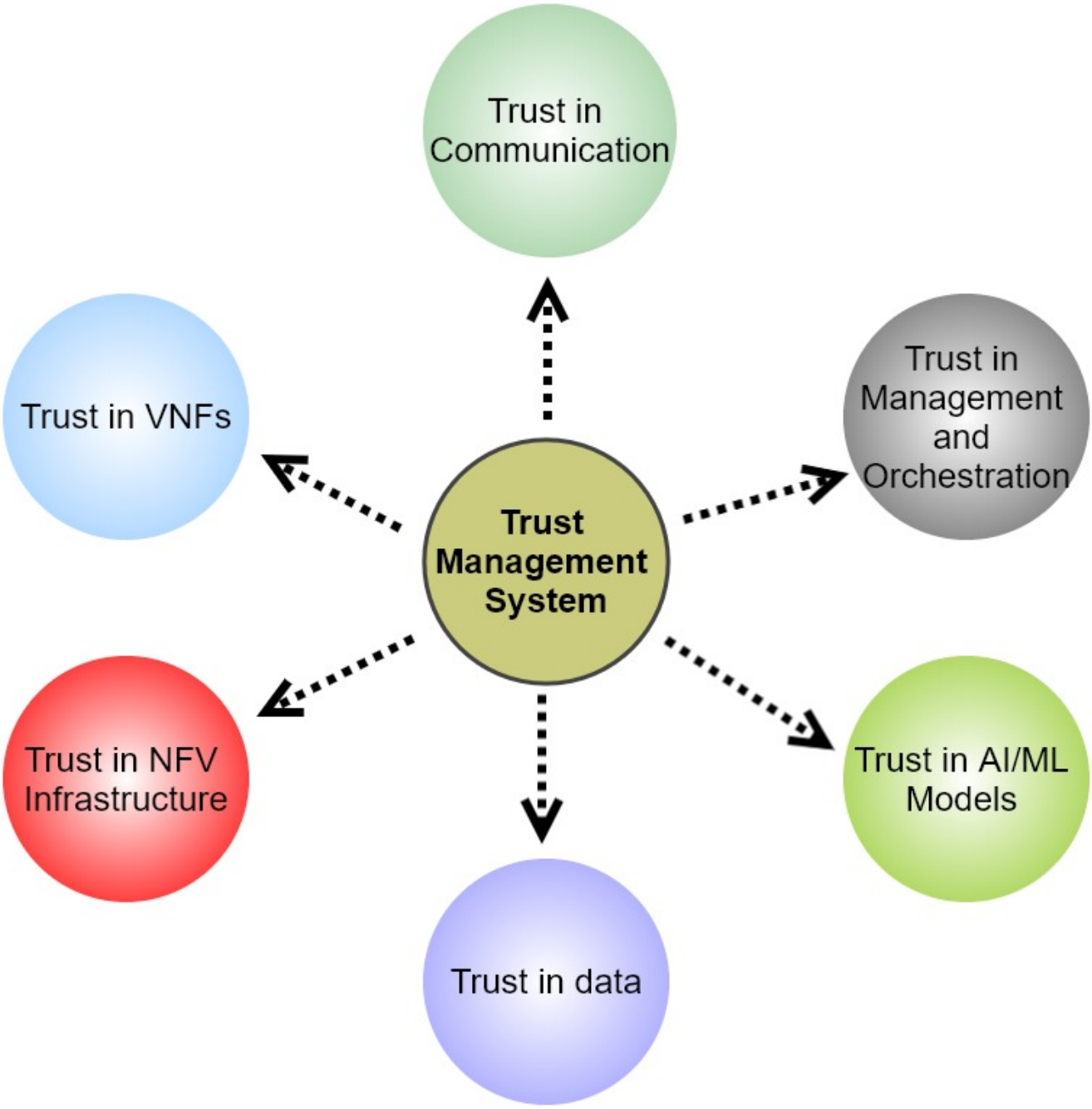



Fig. 2: Basic Trust Dimensions in 5G and Beyond Networks.

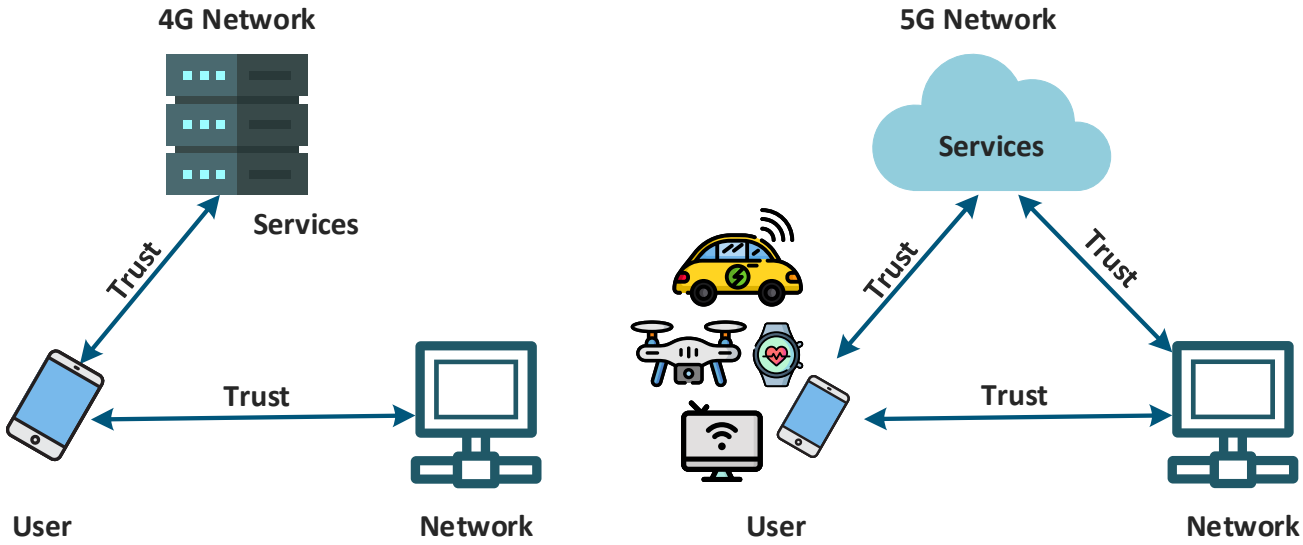



Fig. 3: 4G vs 5G Trust Model.

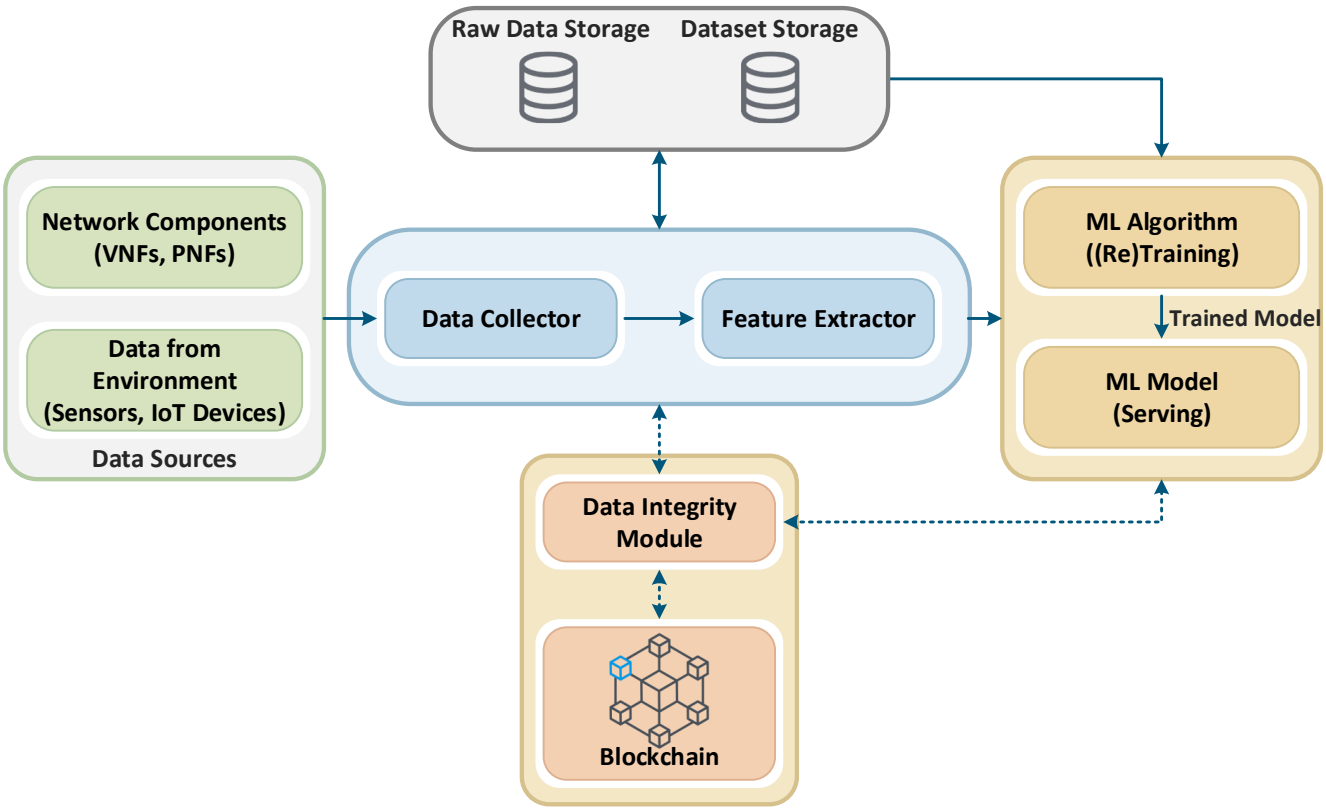



Fig. 4: Learning Pipeline with Blockchain-based Trustworthy Data.

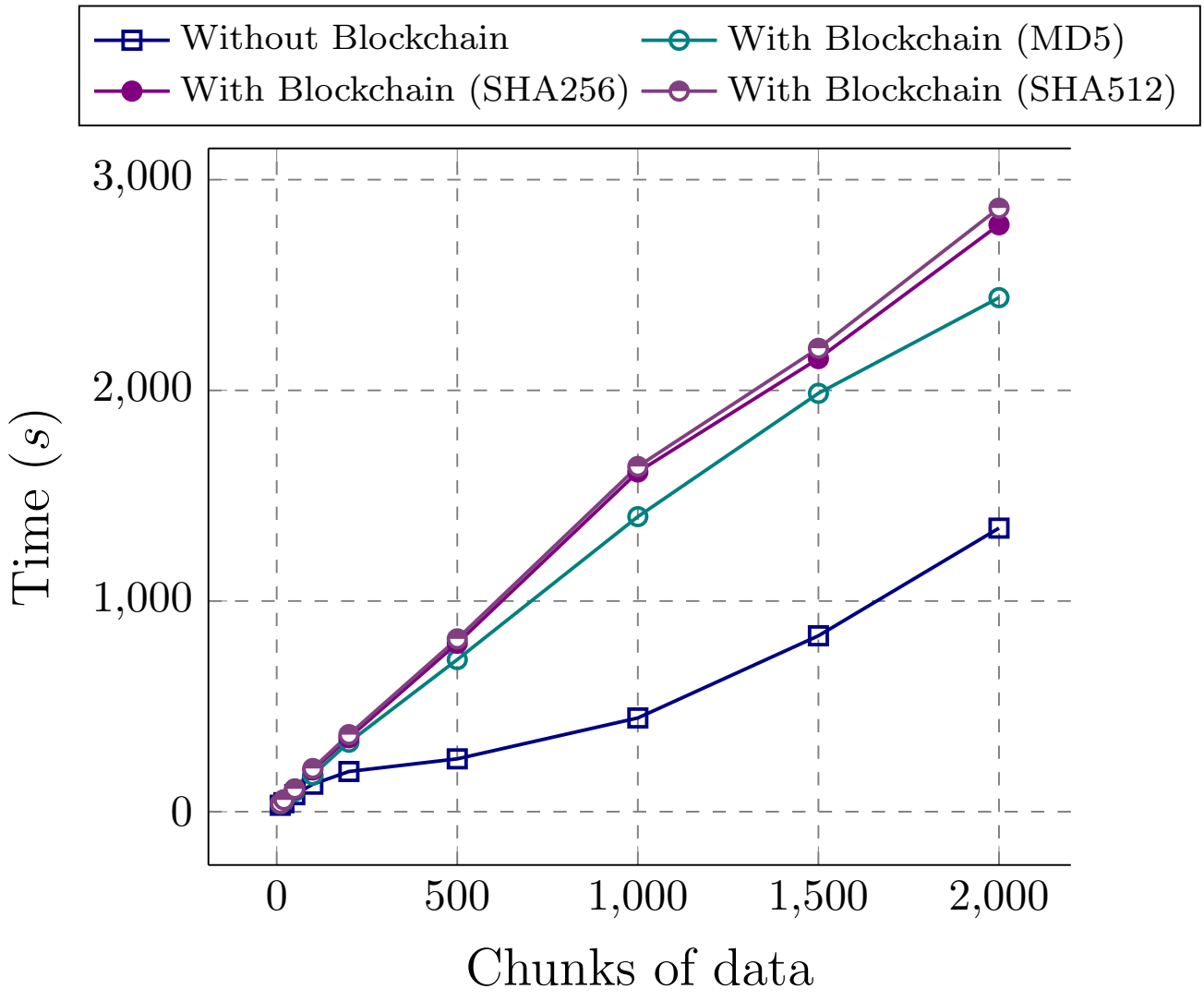



Fig. 5: Comparison of overhead induced by the use of Blockchain using different Hashing Algorithms.