IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 August 2023, accepted 17 September 2023, date of publication 2 October 2023, date of current version 5 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3321114

PERSPECTIVE

SIX-Trust for 6G: Toward a Secure and Trustworthy Future Network

YIYING WANG, (Student Member, IEEE), XIN KANG, (Senior Member, IEEE), TIEYAN LI, (Member, IEEE), HAIGUANG WANG, (Senior Member, IEEE), CHENG-KANG CHU, (Member, IEEE), AND ZHONGDING LEI, (Senior Member, IEEE)
Digital Identity and Trustworthiness Laboratory, Huawei Singapore Research Center, Singapore 138588
Corresponding author: Xin Kang (kang.xin@huawei.com)

ABSTRACT Recent years have witnessed a digital explosion in the deployment of 5G and the proliferation of 5G-enabled innovations. Compared with 5G, 6G is envisioned to achieve a much higher performance and experience a number of paradigm shifts, such as exploiting new spectrum, applying ubiquitous Machine Learning and Artificial Intelligence (ML/AI) technologies and building a space-air-ground-sea integrated network. However, these paradigm shifts may lead to numerous new security and privacy issues, that traditional security measures may not be able to address. Moreover, the expected high performance of 6G also challenges network reliability and energy efficiency. To tackle these issues and build a trustworthy 6G network, we introduce a novel trust framework called SIX-Trust. This framework is composed of three layers with an emphasis on distinct aspects: sustainable trust (S-Trust), with a particular focus on trust in applications of AI, novel trust evaluation methods and modeling of trust relationships; infrastructure trust (I-Trust), which is more focused on the trustworthiness of network infrastructure; and xenogenesis trust (X-Trust) paying special attention to the core technologies which form the backbone of 6G trust. Besides, the importance of each layer varies under different application scenarios of 6G. For each layer, we briefly introduce its related enabling technologies, and demonstrate how these technologies can be applied to enhance the trust and security of the 6G network. Finally, a use case is illustrated and analyzed. In general, SIX-Trust provides a holistic framework for defining and modeling trust in 6G, which can facilitate establishment of a trustworthy 6G network.

INDEX TERMS 6G, privacy, security, trust, trustworthiness.

I. INTRODUCTION

The rapid development of 5G has opened a world of low-latency communication, high-speed data delivery, and exponentially increased connectivity among numerous devices and sensors. The deployment of network function virtualization (NFV) in 5G offers a dynamic network architecture and enables flexible resource allocation by separating service from the hardware. Owning to the unprecedented growth in data volume and the expanding demand for ubiquitous connectivity, researchers have been driven to put much effort into developing 6G technologies. It is expected that 6G will offer at least 20 times more network capacity, and 50 times more data transmission rate than 5G. In addition, 6G is envisioned to add one more dimension to create a three-dimensional network covering from terrestrial to non-terrestrial, from space to underwater, and to form the so-called space-air-ground-sea integrated network [1]. Moreover, Artificial Intelligence (AI), an essential enabler, empowers automation of network resource allocation, anomaly detection and ubiquitous system monitoring. The proliferation of pervasive intelligence will drive the transformation of mobile communications from "connected everything" to "connected intelligence" [2]. However, the expanding connectivity and new features of 6G may introduce new security threats from multiple aspects: open interfaces, pervasive usage of NFV, the integration of sensing and computing, extensive usage of clouds and edges, complicated relationships among humans, things, and

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

connected intelligence, and the entangled relationship among various stakeholders [3]. Millions of connected devices and sensors, forming the base layer of threats, increase vulnerability to the impact of attacks. With the extensive use of AI, more threats and new types of attacks are likely to appear. For instance, the training procedure for AI models requires a substantial amount of data, which may lead to data leakage or malicious usage of sensitive and confidential information [1]. In addition to security and privacy issues raised by expanding attack surfaces and AI, the increased network connectivity as well as the proliferation of technologies pursuing high performance could pose challenges to network reliability. For example, to achieve the desired performance of federated learning, a substantial amount of energy and computing resources are required to achieve the desired performance. Besides, some critical technologies envisioned to ensure network security, such as blockchain and increasing cryptographic key length, lead to considerable amount of energy consumption [4]. Thus, how to balance the need for secure and resource-intensive networks and energy efficiency has become one of the primary concerns.

To deal with all potential threats and challenges, trust has become a pivotal factor enabling large-scale computation and ad-hoc communication across heterogenous entities [5]. Trust, in a network context, is closely related to concepts including security, reliability and availability. As proposed in ITU-T Y.3053 [6], trust in networking refers to a collection of techniques aimed at ensuring dependable and protected communications between any two network components that have trust relationships. To establish trust relationships among countless endpoints and heterogenous entities, trust needs to be evaluated across end-devices, access networks, and core networks. However, the concept of trust lacks a widely accepted definition and is still under-studied in both academia and industry. The existing works regarding trust definition, trust evaluation and trust establishment in 6G networks are further discussed in the ''related work'' section.

Thus, how to build a trustworthy 6G network becomes a challenging research problem. In this paper, we present our perspectives on how to build a trustworthy 6G network. Initially, a systematic approach is adopted to investigate and analyze the trust challenges of 6G in a layer-wise manner. To address the challenges, a three-layer trust framework for 6G is then proposed. The proposed trust framework, named as SIX-Trust, consists of Sustainable trust (S-Trust), Infrastructure trust (I-Trust) and Xenogenesis trust (X-Trust). Each layer plays a different role, and the importance of each layer varies for different application scenarios of 6G. For each layer, we share our views on relevant technologies as potential solutions to address the security and trust challenges. The proposed framework is envisioned to provide a comprehensive overview of 6G trust and offer insights into pivotal enablers as well as viable methods that can be applied to establish trust in 6G networks.

II. RELATED WORK

Owning to the growing threats posed by the emergence of the latest technologies and new application scenarios which are envisioned to come true, trust is drawing increasing attention from current research works related to 6G. In general, trust is an elastic term, and its definition varies from field to field. In [7], a thorough study was conducted on trust in various communication scenarios in the future digital world. However, this survey did not specifically address trust in 6G networks. To further understand how trust is understood in 6G context, we have explored a limited number of works which have brought forward discussions about the concept of trust in 6G. Work [8] examined trust in 6G with a specific focus on AI. It stated that in addition to security, trust was also believed to originate from certain evaluation criteria, ranging from functional to non-functional. Moreover, Veith et al. [9] primarily discussed the crucial enablers for trust in 6G and the differences between trust in 5G and that of 6G in terms of five categories: network topology, feature set, architecture, stakeholder relationships and new technologies. In the 6G White Paper proposed by Ylianttila et al. [10], trust in a network context was defined as the ''expected outcome'' during remote communication. The outcome can be either positive or negative, reflecting the other party's trustworthiness. Similarly, Li et al. [11] defined trust as the extent to which users would like to trust the trust provider, as well as reliability. Trust was modeled as a weighted sum of ''physical trust'' and ''emotional trust'' determined by trust indicators including robustness, transparency, accuracy, etc.

In addition to the concept of 6G trust, several studies have proposed methods or developed architectures aimed at addressing 6G trust issues. Yang et al. [12] introduced an intelligent and heterogenous architecture for intelligent and distributed trust management using AI techniques. The architecture consists of three layers: intelligent sensing layer as the bottom layer, intelligent edge and intelligent control layer as the medium layer and smart application layer as top layer. It emphasized the importance of the role played by AI in solving 6G trust problems. Another architecture was designed by Stavroulaki et al [5], named as DEDICAT 6G baseline functional architecture. The architecture primarily underlined the significance of trusted information sharing and trustworthy orchestration of decision-making processes. ITU-T Y.3053 [6] presented a framework for trustworthy networking. The identification of network elements trust evaluation and trustworthy communication were highlighted to establish trust-centric networks. Nyugen et al. [4] presented a holistic and comprehensive review of the key enablers of 6G security and trust and proposed three layers: physical, connection and service layers. The enablers of service layer and connection layer are more related to our ''I-Trust'', in terms of 6G authentication protocols and network virtualization. The security in the physical layer envisioned in [4] mainly included the key communication technologies including 6G mmWave, 6G holographic radio technology,

terahertz communication, etc., while the X-Trust of our work is more focused on technologies with endogenous trust at design.

III. SIX-TRUST FOR 6G

From our perspective, to build a trustworthy 6G network, a multi-layer hierarchical trust architecture consisting of a root layer, a foundation layer and a representation layer is required. Based on this, we propose a three-layer SIX-Trust, comprising of S-Trust, I-Trust and X-Trust. The overview of the SIX-Trust framework is illustrated in Figure 2.

A. SUSTAINABLE TRUST (S-TRUST)

Sustainable trust (S-Trust) embodies trust representation, which emphasizes the degree of trust that can be perceived by users. In the context of 6G, continual and tenable trust representation and evaluation are indispensable to sustainably provide 'a sense of trust'. The sustainable trust is the most palpable layer of all layers, as trust is often presented in numerical values or visual artifacts during user's interaction with provided applications. Thus, S-Trust is closely related to application layer.

To increase perceivability, trust needs to be quantified and sustainably assessed by both static and dynamic evaluation processes, which will be facilitated by the AI technology. However, to the best of our knowledge, there are no fully complete or widely accepted trust evaluation methods established so far neither in academia or industry. To bridge this gap, we proposed an evaluation framework particularly aiming at dynamic trust evaluation in 6G context. With the capability to preserve data privacy, automate resource management, achieve better explainability, and mitigate undesirable biases, trustworthy AI has become a critical enabler for sustainable trust. Moreover, trust evaluation will foster the establishment of trust relationships, as it becomes more convenient for evolved parties to measure other parties' trustworthiness. Trust relationship represents a form of agreement or consensus reached by both parties prior to communication. Decentralized trust and federated trust are two representatives of trust relationships that are envisioned to be of great importance to 6G for achieving S-Trust.

B. INFRASTRUCTURE TRUST (I-TRUST)

Infrastructure trust (I-Trust) reinforces the trust of the bottom layer (Xenogenesis Trust, X-Trust) of SIX-Trust architecture and provides a trustworthy infrastructure for the upper layer (Sustainable Trust, S-Trust). Therefore, the focus of I-Trust has been put on both service and transport layers. Given the countless security threats posed by the involvement of various types of entities and inclusion of all kinds of cutting-edge technologies, a reliable and trustworthy network infrastructure is crucial for underpinning secure 6G networks by ensuring secure execution of upper layer applications. I-Trust reflects the trustworthiness of the network architecture, which is envisioned to be distributed and autonomous. The architecture is undergirded

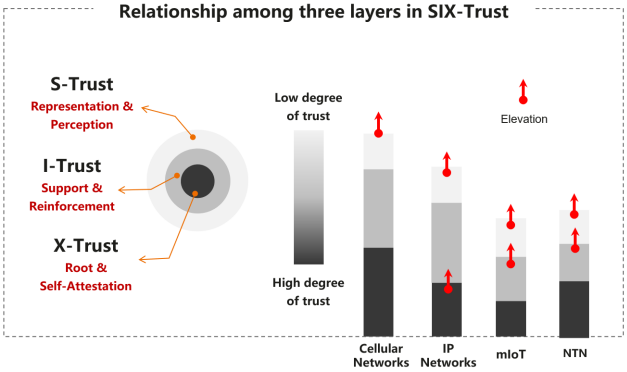

FIGURE 1. Relationship among three layers in SIX-Trust and their ratios in different 6G scenarios (Cellular Networks, IP Networks, mIoT, NTN).

by trustworthy underlays such as Decentralized Public Key Infrastructure (DPKI) and trusted Network Functions Virtualization Infrastructure (NFVI), which can be viewed as the skeleton of I-Trust, to provide decentralized authentication topology and facilitating more flexible deployment of intelligence by virtualization. DPKI is an advanced version of PKI, which embraces the concept of decentralization to address several issues faced by traditional PKI, such as the possibility of single-point-of-failure and vulnerability to network attacks [13]. NFVI consists of the necessary software and hardware components, enabling network functions to be decoupled from hardware appliances. Nevertheless, as Xue et al. [14] suggested, new security threats appear along with the multi-layer perspective and increased complexity brought about by Network Function Virtualization (NFV). Thus, a trustworthy NFVI is essential for ensuring the reliability and security of network functions. On top of the underlay, trustworthy protocols further reinforce trustworthiness during communication. As stated in [4], novel authentication methods such as 6G Authentication and Key Agreement (6G-AKA) are indispensable for 6G networks to satisfy the security requirements of open programmable networks. It is also suggested that an improved version of Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) can be deployed to support reliable device-to-device and vehicle-to-vehicle communication in diverse 6G scenarios.

C. XENOGENESIS TRUST (X-TRUST)

Xenogenesis trust (X-Trust) represents the basis of trust, which is the initial point where the chain of trust starts in the 6G networks. It is an endogenous trustworthiness originated from three aspects: trusted foundation, trusted platform, as well as trusted hardware. The technologies involved are inherently designed to be trustworthy in order to preserve the network security. For instance, Trusted Platform Module (TPM) as embedded security hardware, is inherently resistant to spoofing and tampering. Therefore, it can be used as the basis for the hardware root of trust, by providing hardware-level protection of data integrity. In other words, X-Trust

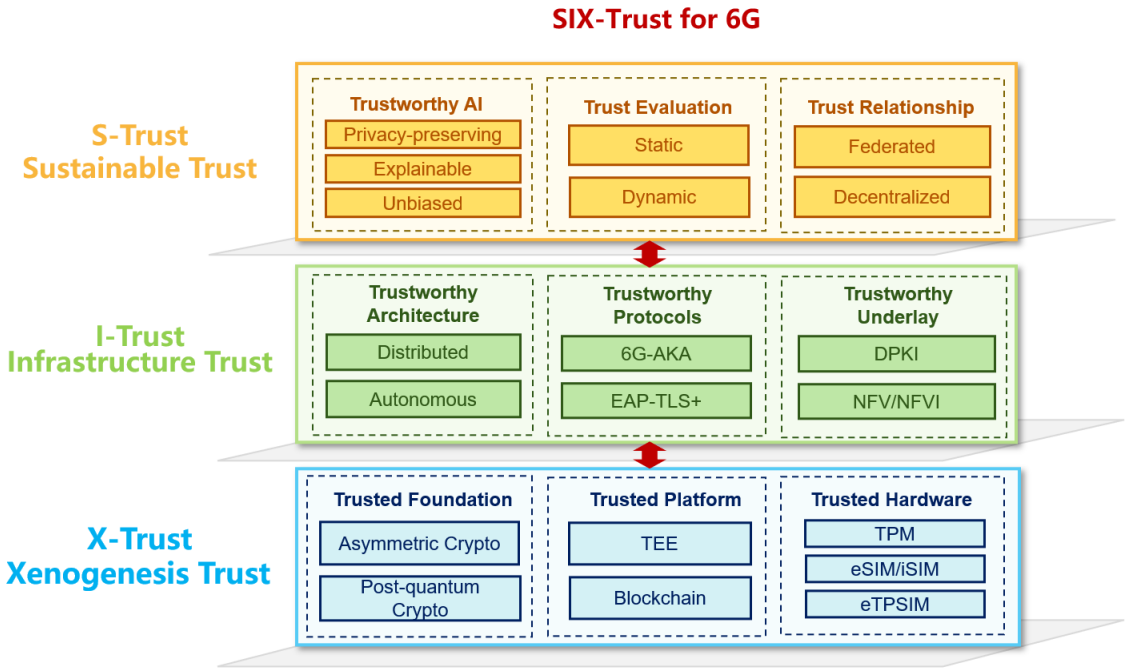

FIGURE 2. SIX-Trust framework.

stems from the beliefs about in-built security features of the related technology. Consequently, X-Trust offers higher degree of trust and forms the basis of SIX-Trust.

D. RELATIONSHIP AMONG THREE LAYERS

The three layers are stacked hierarchically, each of which possesses a different degree of trust. This three-layer model is inspired by the internal structure of the Earth [15]. The Earth's inner structure is mainly divided into three parts: the Earth's core, mantle and crust. As shown in Figure 1, X-Trust, which is born with trust, has the highest degree of trust and is the core of SIX-Trust. I-Trust, like the earth's mantle, is mainly responsible for reinforcing X-Trust and supporting the S-Trust. S-Trust, like the earth's crust, is more perceptible and directly faces the network users. For example, decentralized and autonomous network architecture of I-Trust requires decentralized trust relationships to be established as stated in S-Trust and trustworthy AI such as federated learning to empower self-healing, self-optimizing, self-configuring, etc. The security of authentication protocols and network virtualization of I-Trust will be reinforced by tamper-proofing components like TPM and trusted execution environment and highly secure cryptographic algorithms. Meanwhile, AI models and AI-supported trust evaluation of I-Trust need to be undergirded by reliable data collection and transmission enabled by trustable hardware and network infrastructure. These three-layers are tightly connected and influence one another; however, it is worth noting that the importance of each layer varies depending on the type of network. For example, IoT includes numerous devices and sensors with limited processing ability and insufficient security mechanisms [4], which significantly undermines the X-Trust. Moreover, the degree of S-Trust and I-Trust in IoT are both low and weak due to resource limitation. On the contrary, cellular networks are expected to achieve a high degree of trust in all three layers. First, advanced encryption methods and trusted algorithms will enable a strong X-Trust. Moreover, more trustworthy and secure authentication methods will be applied ensure solid I-Trust. Finally, from the users' perspective, the degree of trust representation and trust perceivability will be greatly increased (which is represented by the arrow and the term "elevation" shown on the figure), since cellular networks will shift from being device-centric to becoming user-centric [16]. The importance of each layer in IP networks and Non-Terrestrial Networks (NTN) is illustrated in Figure 1.

IV. SUSTAINABLE TRUST

In this section, the potential intelligence enablers that are crucial to achieve sustainable trust are presented. Meanwhile, a general framework of dynamic trust evaluation is proposed to enhance the perceptibility of trust.

A. TRUSTWORTHY AI

With the rapid development of network softwarization and virtualization, ubiquitous AI has become a trend of 6G to build self-adapting, self-sustaining and self-learning networks [17]. The beneficial relationship between AI and 6G networks is mutual: AI empowers 6G in terms of automation, attack detection and defense, semantic communication,

optimal resource management, trust evaluation, and efficient network maintenance, whereas 6G provides massive data and trustworthy infrastructure for AI. This relationship is also known as ''Network for AI and AI for Network'' [18]. On the one hand, trustworthy AI inevitably requires support from I-Trust and X-Trust in terms of data integrity, transmission security, identification and authentication in 6G. For example, in the I-Trust layer, distributed computing power enabled by a distributed network architecture facilitates the deployment of federated learning for better privacy preservation. Meanwhile, when a user's identity is involved, trustable protocols such as authentication and key agreement protocol can be utilized to protect the user's identity. X-Trust enablers such as trusted platform module, trusted execution environment and distributed ledger technology are particularly essential for ensuring that the data integrity has been preserved and the originality of AI models [19]. On the other hand, trustworthy AI will foster more adaptable and reliable trust evaluation from the network core to end devices. Furthermore, as mentioned in [20], Deep Learning (DL), as part of AI, is expected to bring changes and enhancements to the modules of the physical and data link layers. For example, Mahimkar et al. [21] proposed Auric as a data-driven model using a deep neural network for automatic generation of recommendation for cellular configuration parameters. The model also applies a decision tree learner to meet the needs of explainable AI. Moreover, a number of studies [22], [23], [24] have proposed approaches that apply deep learning to facilitate and optimize network resource management. Sodhro et al. [25] suggested a novel mobility management based on ML to achieve an energy-efficient communication. In this subsection, we will be discussing three key components of trustworthy AI: privacy-preserving AI, explainable AI, and unbiased AI.

1) PRIVACY-PRESERVING AI

The training process of AI models requires massive amounts of data collected through networks, which poses a significant threat to user privacy. Federated Learning (FL), being decentralized and distributed, offers a solution to privacy-preserving learning by facilitating computing on heterogenous edge devices of 6G networks [17]. FL allows on-device training, which means that data can be processed locally, and a shared model will be trained in a collaborative manner. Wireless devices with FL only need to upload their model parameters to the base station, instead of exchanging the entire training dataset. Thus, the user's data are processed in a local and distributed manner. The trustworthiness of FL can be further strengthened by robust aggregation algorithms for secure learning and differential privacy for privacy preserving [26]. For example, with application of differential privacy, the involved parties are unable to determine whether a certain instance has been used for model training even when data were publicly released. It has also been suggested that Distributed Ledger Technology (DLT) can converge with FL by securing data sharing and record retrieval to form a distributed and trustworthy machine learning system [27].

2) EXPLAINABLE AI

In the context of 6G, understanding the decision-making process is extremely important especially in fields that involve physical interactions between the human body and machines, where safety is the primary concern. However, AI models, particularly DL models, are often depicted as black boxes due to lack of transparency and explainability. To be more specific, deep neural networks cannot explain the relationship between certain features and outputs or determine the salience of each attribute [20]. In other words, users usually have no idea how and why a decision is made by the model, which will greatly undermine the model's trustworthiness and make the decision inconvincible. Explainable AI (XAI) is therefore proposed in order to help human to understand the decision-making process, provide new insights of the data from an AI's perspective, and most importantly, facilitate trust establishment between AI and people. XAI is used to explain a black-box model logically or mathematically, providing a decision of trust. As suggested by [20], an XAI model can achieve explainability using visualization, hypothesis testing, mathematical models or even providing explanation in natural language. The transparency of AI will assist 6G stakeholders in designing their strategies for AI development and integration. Moreover, since XAI will play a pivotal role as an enabler of the application layer, users are expected to sense an increased level of trust [28]. Before taking any actions advised by an AI model, a user will be provided with additional information and will then understand why a certain decision is made by AI.

3) UNBIASED AI

There are two major concerns related to fairness in the AI models in 6G: bias and discrimination. Bias mainly originates from inappropriate data collection or flawed design of algorithms, while discrimination is often caused by stereotypes towards certain sensitive features and can be derived from existing biases [29]. The existence of bias in the training data can lead to a biased training process, and eventually produce a biased AI model. This type of bias is likely to cause the model to be discriminative against certain attributes, which will downgrade the model's performance. Hence, assuring an unbiased dataset in the data collection and pre-processing stages is critical for building a fair trust evaluation model.

Biased AI models significantly affect the trustworthiness of the 6G network and reduce the reliability of trust evaluation processes. To tackle this issue, two solutions have been proposed: fairness toolkits, which can be accessed as functions to detect and evaluate bias in a model quantitatively, and a fairness checklist, which offers comprehensive guide to ensure fairness [30].

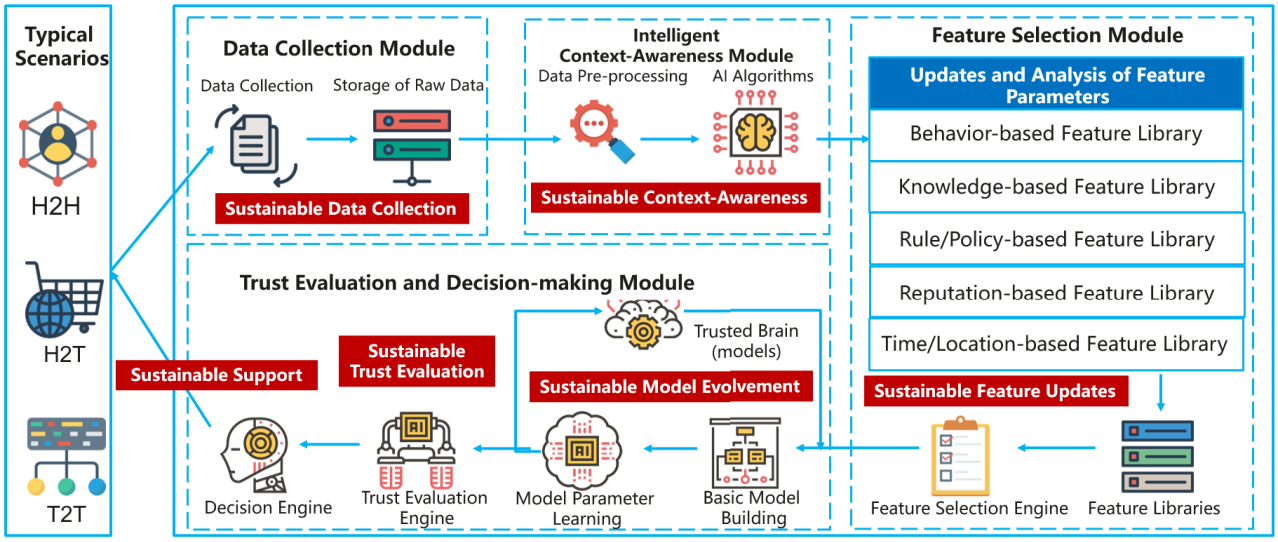

FIGURE 3. Envisioned dynamic trust evaluation framework.

B. TRUST EVALUATION

To build trustworthy 6G networks, trust needs to be evaluated across numerous devices and heterogenous networks in both static and dynamic ways. Evaluation methods can be further applied to measure the trustworthiness and reputation of the enablers of I-Trust.

1) STATIC TRUST EVALUATION

Static trust is often measured for network hardware. Since devices have static properties, such as their manufacturer, their hardware firmware, their software configuration, they will not change quickly over time. In 6G networks, large amount of these kinds of information will be collected from devices for the purpose of static trust evaluation. Thus, static trust of the devices will have a significant impact on the overall trust of the entire network.

An example of static trust evaluation is the Common Criteria (CC) for Information Technology Security Evaluation, which is an international standard for security evaluation. The standard evaluates the reliability of a device mainly based on security functions provided by the device. A systematic review was presented in [31] with a thorough analysis of the current implementations of CC. Existing categories of CC applications include mobile devices, trusted computing, databases, access control systems, to name a few [31]. The applications further imply the feasibility and necessity of performing trust assessment on network infrastructure entities to reinforce I-Trust.

2) DYNAMIC TRUST EVALUATION

Dynamic trust evaluation is typically used for continuously monitoring the behaviors of users, devices, and applications. To assure security and trustworthiness of communication in a highly connected and heterogenous environment, an integrated real-time dynamic trust evaluation framework that is applicable in diverse scenarios is essentially needed. As shown in Figure 3, in our opinion, the dynamic trust evaluation framework can be divided into four interconnected modules: The data collection module continually collects data generated by the evaluatee and stores raw data in database. The intelligent context-awareness module pre-processes the stored data, and then applies AI/ML algorithms for feature extraction. The feature selection module contains multiple feature libraries that are updated by previously extracted features. Appropriate feature parameters for the current scenario are selected by feature selection engine, and passed to next module to build and train the AI/ML models. Trust evaluation and decision-making module takes in selected feature parameters and finetunes AI/ML models for trust evaluation. Decisions will be made based on trust values after evaluation and will be used to support the policy control for different 6G scenarios.

C. TRUST RELATIONSHIP

In this subsection, we discuss two promising trust relationships for secure and seamless 6G identity management: decentralized trust and federated trust.

1) DECENTRALIZED TRUST

In existing networks, the Identity Management (IDM) of network devices is mainly supported by a centralized PKI where certificates are issued by a Certificate Authority (CA). The trust relationship between the CA and related entities is highly centralized, which may lead to many security issues, such as single-point-of-failure [32]. For instance, a compromised root CA will result in sharp decrease in the trustworthiness of sub-CAs as well as issued certificates.

To build a more trustworthy 6G network, the IDM for network devices should be structured in a decentralized manner. One promising enabler is the Decentralized Identifiers (DID),

which has been announced by W3C as an official Web standard [33]. DID is not dependent on any central issuing agency (e.g., CA), and are verifiable cryptographically. The decentralized IDM is envisioned to enable key management without CAs across network slices, facilitate trustworthy and secure mutual authentication for massive IoT devices, with interoperability provided, and offer better privacy protection [34].

2) FEDERATED TRUST

As 6G networks encompass an unprecedented number of heterogenous devices and diversified services, federated trust becomes extremely critical to network security. To address the issue of cumbersome management of numerous user credentials, identity federation has been proposed as a feasible solution to provide a more cohesive authentication process. More importantly, it establishes federated trust relationship between an Identity Provider (IdP) and a Service Provider (SP). The SPs do not need to handle users' credentials directly, but rather authenticate users based on federated trust on the IdP. Shuhan et al. [35] proposed block-chain based identity federations to overcome the shortcomings of current Security Assertion Markup Language (SAML)-based federated identity management caused by centralization. It indicated the possibility of utilizing blockchain, a trust platform of X-Trust, to foster the formation of federated trust relationships. Related standards include OAuth 2.0 and OpenID Connect, both of which can be applied to implement Single Sign-On (SSO) scheme. Another way to build federated trust is to form a network service federation by orchestrating network services across multiple domains.

Establishing a federated trust relationship will bring numerous benefits to 6G networks, one of which is that network security will be strengthened, since simplification of registration process will reduce security breaches caused by numerous user credentials and login interfaces. In addition, users will have a seamless experience across multiple domains and applications, as the operators are projected to orchestrate external domain services. The federation also facilitates secure and effective resource sharing among different entities, increases network flexibility, as well as reduces operational cost.

V. INFRASTRUCTURE TRUST

In this section, we present the potential technologies that are crucial for reinforcing I-Trust.

A. TRUSTWORTHY ARCHITECTURE

With the exponentially increasing demand for ubiquitous connectivity, traditional centralized network architectures may no longer be applicable. The network architecture of 6G is envisioned to be highly distributed and autonomous [36].

Compared to the former centralized architecture, distributed and decentralized architectures will be more resilient to external threats. As 6G networks need ubiquitous and uniform coverage, cell-free MIMO has been advocated to elevate the uplink capacity and avoid inter-cell interference. Cell-free massive MIMO deploys antennas in a distributed manner, where cells and cell boundaries no longer exist. It takes the advantages of both massive MIMO and distributed systems to create more reliable and user-centric communication networks. The 6G network architecture will also be more widely distributed in the form of distributed computing (e.g., edge computing), decentralized data storage, decentralized identity management, and decentralized AI (e.g., federated learning).

Meanwhile, it is envisioned that 6G networks will adopt an autonomous network architecture to achieve self-provisioning, self-recovering and self-evolving abilities. Autonomous Networks (AN) are supposed to benefit both 6G stakeholders and users, by providing optimized resource allocation, enhanced network scalability, and increased operations and maintenance efficiency. Meanwhile, AN can facilitate flexible network deployment in diverse scenarios, which presents a solution to the complex control plane of a distributed architecture. It is expected that network operators will gradually entrust their control authority as well as management duties to self-sustaining AN of 6G.

B. TRUSTWORTHY PROTOCOLS

In this subsection, two emerging authentication protocols for ensuring secure communications are presented.

1) 6G AUTHENTICATION AND KEY AGREEMENT (6G-AKA)

AKA is a security protocol specified by 3GPP which enables mutual authentication between end-users and the core network. Given the complexity of the 6G network and a number of novel applications (e.g., tele-medical, tele-presence holography, tele-operation of industry machines), 6G-AKA is required to provide faster, more reliable, and trustworthy authentication. As a precedent of 6G-AKA, 5G-AKA is found to be vulnerable to several attacks, including linkability attacks, DDoS attacks, single-point-of-failure problems, and forward/post-compromise secrecy. 6G-AKA is expected to strengthen authentication between The Home Network (HN) and Serving Network (SN) in order to prevent the attacks mentioned earlier, enable direct device-to-device authentication, bridge the gaps among heterogenous devices for their incompatible security capabilities, and revise its design for new subscriber identifier privacy model [4]. Besides, as DDoS attacks are becoming more complicated and threatening, it is crucial to make 6G-AKA more robust and equipped with security mechanisms to defend against DDoS attacks.

2) EXTENSIBLE AUTHENTICATION PROTOCOL – TRANSPORT LAYER SECURITY PLUS (EAP-TLS+)

EAP serves as an authentication framework used to support various authentication methods. TLS is one of the methods, which enables certificate-based mutual authentication within a private network. EAP-TLS is regarded as a promising authentication protocol and has been included in the annex of 5G security standard (TS 33.501). However, due to the size

of current certificates (such as X.509v3), transmission of such certificates for authentication may cause excessive overhead for infrequent data transmission in IoT scenarios. Thus, EAP-TLS+ is expected to support certificateless authentication methods, such as identity-based signature (IBS), implicit certificate. The IBS-supported EAP-TLS+ is able to establish a Device-to-Device (D2D) mutual connection without the need for certificates. This feature will greatly benefit and facilitate Vehicle-to-Vehicle (V2V) and D2D wireless communications. In 6G, EAP-TLS+ is expected to be further developed from 5G EAP-TLS and incorporate more advanced features to offer a secure and seamless communication experience.

C. TRUSTWORTHY UNDERLAY

Trustworthy undelay is indispensable for providing the necessary support for higher level applications. Two types of underlay, decentralized authentication and network virtualization, are discussed as follows.

1) DECENTRALIZED PKI (DPKI)

PKI serves as an underlying framework that enables data encryption, digital signature creation and certificate-based authentication, thereby propelling the establishment of trust among the involved entities. However, PKI in 5G is deployed in a centralized manner, which suffers from single-point-of-failure.

PKI in 6G is expected to become more decentralized, which can be realized by blockchain, to avoid single point of failure caused by excessive dependence on a single root CA [13] and minimize the control of third parties. The integration of blockchain will enable transparency and immutability in PKI, which means that certificate issuing can be observed by all entities, and issued certificates are traceable. In decentralized PKI, trust is decentralized, and built on consensus protocols. Developing an effective and decentralized PKI is critical for establishing a trustworthy identity management process in 6G networks.

2) NETWORK FUNCTION VIRTUALIZATION/NETWORK FUNCTION VIRTUALIZATION INFRASTRUCTURE (NFV/NFVI)

Owing to the emergence of numerous heterogeneous devices, countless novel applications and various scenarios that require high flexibility and low latency, 6G is expected to incorporate NFV as an enabling technology for network virtualization. It is supported by NFVI, which consists of components of networking, computing and storage, and serves as a platform for VNFs. NFV enables services of different types to run on top of commonly shared hardware appliances by decoupling network functions from proprietary hardware and empowering a service-orientated networking. This feature will significantly increase network flexibility, scalability and reduce cost of network deployment [37]. Full virtualized 6G networks are expected to expedite harmonization, with core network, radio access networks and network edge underpinned by uniform underlying hardware. Furthermore, as AI pervades every corner of 6G networks, NFV can partner with AI to facilitate network automation, optimize resource utilization, and enhance the Quality of Service (QoS).

VI. XENOGENESIS TRUST

In this section, we list the prospective technologies that can be used to undergird xenogenesis trust.

A. TRUSTED FOUNDATION

Cryptography forms the foundation for trustworthy communication. Common application cryptographic techniques include symmetric and asymmetric cryptography. Given that symmetric cryptography decrypts and encrypts messages with the same key (which needs to be pre-shared before communication), it involves complicated key management problem. In contrast, asymmetric cryptography does not need to share the key, and can enable direct authentication and secure communication among devices without the help of the core network device (such as Home Subscriber Server (HSS) in 4G, Unified Data Management (UDM) in 5G). Hence, cryptography in 6G is expected to gradually move from symmetric encryption to asymmetric encryption, serving as a strong foundation of xenogenesis trust.

On the other hand, with the powerful computing ability of quantum computers, the time needed to decrypt a key can be significantly reduced. Owing to the security threats posed by quantum computing in future 6G network, a transformation: from traditional cryptography to post-quantum cryptography is being fostered [3]. This upgraded version will benefit asymmetric cryptography-based technologies, by preventing them from being compromised by quantum attacks.

B. TRUSTED PLATFORM

The trusted platform in this subsection mainly embodies X-Trust in terms of confidential computing and reliable data storage.

1) TRUSTED EXECUTION ENVIRONMENT (TEE)

TEE, as a tamper-proof environment, is targeted to preserve code authenticity and data integrity within a device. It serves as an isolated secure zone in the main processors, where unauthorized data access and malicious modification are prevented [38]. TEE is a key enabler for confidential computing. Current encryption methods mainly focus on ensuring integrity of data in storage and data in transmit, most of which do not focus on preserving the integrity of the data in use. Confidential computing, empowered by TEE, is targeted at preserving both data-in-use integrity and code confidentiality on device, facilitating establishment of end-to-end trustworthiness. Existing TEE solutions include ARM TrustZone, Intel SGX, as well as AMD Secure Encrypted Virtualization (SEV). Besides, TEE can be leveraged to ensure data privacy of cloud computing. As encrypted data needs to be decrypted in cloud services to facilitate data

processing, the data in use becomes vulnerable. TEE offers a trustworthy execution environment such that data privacy is preserved even the data is being handled by third parties. It is also envisioned to be combined with network functions.

2) BLOCKCHAIN

Blockchain is a distributed ledger characterized by its immutability. Blockchain is structured by a chain of blocks, to which a new block will be added only after being verified through a consensus mechanism. Because the chain is unidirectional, an operation on the blockchain is irreversible, and the recorded data cannot be modified. The irreversible nature of blockchain facilitates the establishment of mutual trust between different parties and enhances privacy preservation. For instance, as spectrum sharing, automated orchestration, and decentralized computation will be widely applied in 6G networks, blockchain will be able to facilitate distribution and management of resources in a secure manner. Beyond this, it can also be embedded in authentication and authorization process for key management and access control. The application of blockchain in 6G networks will increase the security level, in terms of data integrity and service availability, and enable massive connectivity with assurance of trustworthiness [39].

C. TRUSTED HARDWARE

In this subsection, we present a significant component of X-Trust: the trusted hardware, including TPM and various SIMs.

1) TAMPER PROOF MODULE (TPM)

TPM is a tamper-proof module dedicatedly designed to establish the hardware Root of Trust (RoT) by securing hardware and securely storing encryption keys, certificates, or other confidential information for platform authentication. In the highly distributed and virtualized network environment of the 6G era, hardware RoT becomes critical for ensuring communication security especially on untrusted platforms. TPM is envisioned to empower trusted computing in NFV in two ways: integrity preservation with secure storage, as well as trustworthy verification with remote attestation [40]. During the boot process, measurement values of system components will be sheltered and cannot be modified during run time. Remote attestation is then applied to remotely verify whether the booting process of the system can be trusted given its measurement values at the load time. Furthermore, recognizing the increasing number of heterogenous devices on the edge, the deployment of trustworthy TPM is able to enhance their tamper resistance and efficiently reduce vulnerability.

2) ESIM/ISIM

In 6G, reliable and trustworthy massive Machine-to-Machine (M2M) communication is of great importance. A traditional approach is SIM, a removable smartcard used for subscriber identification and authentication. However, as a physical object, it needs to be plugged in and out for every IoT device, which makes it troublesome to deploy massive IoT networks. To overcome the limitations of the traditional SIM, embedded SIM was subsequently proposed and deployed [41]. Compared to removable SIM, eSIM enables operator profiles to be provisioned ''over the air''. This underlying feature offers a seamless communication process for heterogenous devices deployed worldwide. Apart from eSIM, another type of SIM is integrated SIM (iSIM), supported by System-on-Chip (SoC). eSIM and iSIM are predicted to become enabling technologies in many 6G IoT verticals, including but not limited to smart factories, eHealth, smart grids and connected autonomous vehicles, and will facilitate cellular M2M communication, secure updates of firmware, and ensure flexible and trusted IoT connectivity [41].

3) ETPSIM

As mentioned previously, traditional SIMs may be no longer suitable for large-scale devices. TPM, as a trustworthy and secure chip, is envisioned to be integrated with SIM to develop embedded TPSIM (eTPSIM), especially for mobile devices. The integration provides a unified solution for device identity authentication, trust booting, and platform integrity. eTPSIM can be soldered into a device's circuit board, which facilitates the establishment of physical binding between root of trust for measurement of the platform and eTPSIM. This will become beneficial for many large-scale 6G applications: Internet of Vehicles (IoV), smart cities, Industrial Internet of Things (IIoT), etc. It can effectively reduce the cost of SIM deployment among numerous mobile devices, enhance the security and trustworthiness of IoT terminals, empower trusted computing for IoT devices, and assure information security for critical information infrastructure.

VII. 6G USE CASE STUDY

6G is expected to support demanding network requirements, including low transmission latency, high network capacity, efficiency and reliability in diverse scenarios with heterogeneous devices. Numerous emerging use cases have also appeared given the enhanced capabilities of 6G networks. In this section one of the key use cases of 6G is discussed and we further analyze the feasibility of our SIX-Trust framework based on the use case being studied.

eHealth, as presented in [42], is envisioned to optimize workflow in the healthcare sector and provide healthcare services remotely in 6G. However, due to individuals' lack of trust in privacy preservation in eHealth and several security concerns, eHealth has not been widely applied across the whole society. eHealth system can be embodied by a hierarchical architecture, consisting of a storage layer, processing layer and sensing layer [43], where the processing layer includes device management and coordination. SIX-Trust framework can potentially be applied to establish, reinforce, and evaluate trust of the eHealth system architecture.

To begin with, enablers of X-Trust such as eTPSIM and trustworthy encryption algorithms are responsible for ensuring security, privacy, and data integrity on the sensing layer. The eHealth system relies heavily on a plethora of heterogeneous IoT devices which are leveraged to collect highly sensitive medical data of patients, such as heart rate, blood pressure and body temperature. Consequently, the end devices are vulnerable to several security threats, such as data leakage, identity spoofing attacks and tampering [44]. Since eTPSIM combines both TPM and SIM, soldered into the circuit board of a device, it can be used to mitigate tampering authenticate each device's identity, and prevent spoofing attacks. Meanwhile, DPKI and DID increase the level of decentralization of device identity management, thereby addressing the single-point-of-failure issue. Moreover, asymmetric encryption (e.g., Rivest-Shamir-Adleman (RSA) encryption) also helps to foster secure data transmission from end devices to servers for data processing. Trustworthy protocols such as 6G-AKA and EAP-TLS+ guarantee a secure authentication process under the D2D scenario while reducing some overheads which presented in the previous authentication protocols.

After being collected by the end devices, the patient data will then be processed in servers with higher computational capability (the processing layer). In this case, TEE, a key trusted platform of X-Trust, can be applied to achieve secure and privacy-preserving data processing and analysis. Unbiased AI of S-Trust will help to mitigate possible biases towards certain patients to ensure that the analysis or AI-made decisions are just and fair. As suggested by Kalapaaking et al. [45], federated learning allows each hospital to train its local model for data analysis. A global model (usually located in clouds) is formed by aggregating encrypted local models based on Secure Multi-Party Computation (SMPC), which prevents the disclosure of sensitive information as the models have been encrypted. Moreover, NFV, as a trustworthy underlay of I-Trust, empowers network monitoring and enhances overall security through network intelligence. The trust evaluation methods of S-Trust, including both static and dynamic trust evaluation, can be leveraged to assess the trustworthiness of every device, database, or server in the network. The trust score of an entity will help network administrators to decide whether to allow the entity to join the network, or whether to grant the entity access rights. Meanwhile, because the trust relationship between two entities is established based on the entities' level of trustworthiness, the dependability of trust evaluation methods and device identification becomes crucial. In the case where user interaction is involved, explainable AI will explain the decision-making process or medical data analysis results in a user-friendly manner. For example, explainable AI can produce a saliency map of a CT image, from which the patient will be able to see which part of the CT image makes the AI model generate the current prediction. In such a case, the user is likely to perceive an increased level of trust owing to the presence of explanations.

VIII. CONCLUSION

In this article, we proposed a novel trust framework SIX-Trust to build a more secure and trustworthy 6G networks. The framework consists of three layers: sustainable trust layer, infrastructure trust layer, and xenogenesis trust layer. For each layer, emphasis has been placed on a different aspect of trust, and we have provided our insights into how the potential technologies can be used, how the technologies can facilitate the establishment of trustworthiness in 6G, and why they are crucial for future trustworthy 6G networks. X-Trust stresses the importance of applying enablers with endogenous trust to establish the root of trust in 6G. As for I-Trust layer, the trust enablers of X-Trust such as TPM or trustworthy cryptographic algorithms will reinforce the overall trust of network devices, network communication protocols, and thus increase the trust, security and privacy of network infrastructure, undergirding trustable network architecture featuring autonomy and decentralization. Trustworthy AI is leveraged for network autonomy, thereby increasing the explainability of the network decision-making process to make network trust more perceivable. Trust evaluation empowered by AI models is used to form trust relationships between different entities and facilitate trustworthy communication. Finally, the proposed framework is applied to the use case of eHealth in 6G and then analyzed. Further research needs to be carried out to explore other potential use cases to which SIX-Trust framework can be well applied to enhance network trust. Besides, the energy consumption of several enablers like Blockchain and AI models requires further investigations to better balance the trade-offs between trust and environmental sustainability.

REFERENCES

[1] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6G: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 905–974, 1st Quart., 2023.

[2] Y. Chen, P. Zhu, G. He, X. Yan, H. Baligh, and J. Wu, "From connected people, connected things, to connected intelligence," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–7.

[3] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6G era," *IEEE Access*, vol. 9, pp. 142314–142327, 2021.

[4] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[5] V. Stavroulaki, E. C. Strinati, F. Carrez, Y. Carlinet, M. Maman, D. Draskovic, D. Ribar, A. Lallet, K. Mößner, M. Tosic, M. Uitto, S. A. Hadiwardoyo x, J. Marquez-Barja, E. Garrido, M. Stamatelatos, K. Sarayeddine, P. Sánchez Vivas, A. Mämmelä, and P. Demestichas, "DEDICAT 6G–Dynamic coverage extension and distributed intelligence for human centric applications with assured security, privacy and trust: From 5G to 6G," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 556–561.

[6] *Framework of Trustworthy Networking With Trust-Centric Network Domains*, Standard ITU-T Y.3053, 2018.

[7] H. L. J. Ting, X. Kang, T. Li, H. Wang, and C.-K. Chu, "On the trust and trust modeling for the future fully-connected digital world: A comprehensive study," *IEEE Access*, vol. 9, pp. 106743–106783, 2021.

[8] S. Barmpounakis and P. Demestichas, "Framework for trustworthy AI/ML in B5G/6G," in *Proc. 1st Int. Conf. 6G Netw. (6GNet)*, Jul. 2022, pp. 1–6.

[9] B. Veith, D. Krummacker, and H. D. Schotten, "The road to trustworthy 6G: A survey on trust anchor technologies," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 581–595, 2023.

[10] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, and I. Oppermann, "6G white paper: Research challenges for trust, security and privacy," 6G Flagship, Univ. Oulu, Oulu, Finland, 6G Res. Vis. 9, Apr. 2020.

[11] C. Li, W. Guo, S. C. Sun, S. Al-Rubaye, and A. Tsourdos, "Trustworthy deep learning in 6G-enabled mass autonomy: From concept to quality-of-trust key performance indicators," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 112–121, Dec. 2020.

[12] L. Yang, Y. Li, S. X. Yang, Y. Lu, T. Guo, and K. Yu, "Generative adversarial learning for intelligent trust management in 6G wireless networks," *IEEE Netw.*, vol. 36, no. 4, pp. 134–140, Jul. 2022.

[13] Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, "Decentralized public key infrastructures atop blockchain," *IEEE Netw.*, vol. 34, no. 6, pp. 133–139, Nov. 2020.

[14] P. Xue and Z. Jiang, "SecRouting: Secure routing for network functions virtualization (NFV) technology," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 3, pp. 1727–1731, Mar. 2022.

[15] M. Båth, "Internal structure of the earth," in *Introduction to Seismology* (Wissenschaft und Kultur), vol. 27. Basel, Switzerland: Birkhäuser, 1979.

[16] D. Simeonidou and R. Nejabati, "Human-centric networking: From device-centric 5G networks to full cyber-physical convergence in 6G," in *Proc. Eur. Conf. Opt. Commun. (ECOC)*, Sep. 2021, pp. 1–2.

[17] Y. Xiao, G. Shi, and M. Krunz, "Towards ubiquitous AI in 6G with federated learning," 2020, *arXiv:2004.13563*.

[18] J. Pan, L. Cai, S. Yan, and X. S. Shen, "Network for AI and AI for network: Challenges and opportunities for learning-oriented networks," *IEEE Netw.*, vol. 35, no. 6, pp. 270–277, Nov. 2021.

[19] D. Krummacker, B. Veith, D. Lindenschmitt, and H. D. Schotten, "DLT architectures for trust anchors in 6G," *Ann. Telecommun.*, vol. 78, nos. 9–10, pp. 551–560, Jan. 2023.

[20] W. Guo, "Explainable artificial intelligence for 6G: Improving trust between human and machine," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 39–45, Jun. 2020.

[21] A. Mahimkar, A. Sivakumar, Z. Ge, S. Pathak, and K. Biswas, "Auric: Using data-driven recommendation to automatically generate cellular configuration," in *Proc. ACM SIGCOMM Conf.* New York, NY, USA: ACM, Aug. 2021, pp. 807–820.

[22] P. Kamble, D. A. Shaikh, and A. Shaikh, "Optimization of base station for 6G wireless networks for efficient resource allocation using deep learning," K.J. Somaiya Inst. Eng. Inf. Technol., Mumbai, India, Apr. 2022.

[23] M. Ashwin, A. S. Alqahtani, A. Mubarakali, and B. Sivakumar, "Efficient resource management in 6G communication networks using hybrid quantum deep learning model," *Comput. Electr. Eng.*, vol. 106, Mar. 2023, Art. no. 108565.

[24] V. Ponnusamy and A. Vasuki, "AI-enabled intelligent resource management in 6G," in *AI and Blockchain Technology in 6G Wireless Network*. Singapore: Springer, Aug. 2022, pp. 71–92.

[25] A. H. Sodhro, N. Zahid, L. Wang, S. Pirbhulal, Y. Ouzrout, A. S. Seklouli, A. V. L. Neto, A. R. L. D. Macêdo, and V. H. C. D. Albuquerque, "Toward ML-based energy-efficient mechanism for 6G enabled industrial network in box systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7185–7192, Oct. 2021.

[26] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3347–3366, Apr. 2023.

[27] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[28] S. Wang, M. A. Qureshi, L. Miralles-Pechuán, T. Huynh-The, T. R. Gadekallu, and M. Liyanage, "Applications of explainable AI for 6G: Technical aspects, use cases, and research challenges," 2023, *arxiv:2112.04698*.

[29] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A survey on bias and fairness in machine learning," 2022, *arxiv:1908.09635*.

[30] B. Richardson and J. E. Gilbert, "A framework for fairness: A systematic review of existing fair AI solutions," 2021, *arXiv:2112.05700*.

[31] N. Sun, C.-T. Li, H. Chan, B. Dung Le, M. Z. Islam, L. Y. Zhang, M. R. Islam, and W. Armstrong, "Defining security requirements with the common criteria: Applications, adoptions, and challenges," *IEEE Access*, vol. 10, pp. 44756–44777, 2022.

[32] J. Won, A. Singla, E. Bertino, and G. Bollella, "Decentralized public key infrastructure for Internet-of-Things," in *Proc. IEEE Milit. Commun. Conf. (MILCOM)*, Oct. 2018, pp. 907–913.

[33] World Wide Web Consortium (W3C). (Jul. 19, 2022). *Decentralized Identifiers v1.0*. [Online]. Available: https://www.w3.org/TR/did-core/

[34] S. Rodriguez Garzon, H. Yildiz, and A. Küpper, "Decentralized identifiers and self-sovereign identity in 6G," 2022, *arXiv:2112.09450*.

[35] M. K. B. Shuhan, S. M. Hasnayeen, T. K. Das, M. N. Sakib, and M. S. Ferdous, "Decentralised identity federations using blockchain," 2023, *arXiv:2305.00315*.

[36] S. Wang, "6G network: Towards a distributed and autonomous system," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[37] X. Shen, J. Gao, W. Wu, M. Li, C. Zhou, and W. Zhuang, "Holistic network virtualization and pervasive network intelligence for 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 1–30, 1st Quart., 2022.

[38] M. Sabt, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 57–64.

[39] T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. 2nd Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[40] H. Lauer and N. Kuntze, "Hypervisor-based attestation of virtual environments," in *Proc. Intl IEEE Conferences Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul. 2016, pp. 333–340.

[41] C. Silva, "eSIM suitability for 5G and B5G enabled IoT verticals," in *Proc. 8th Int. Conf. FiCloud*, Aug. 2021, pp. 210–216.

[42] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Towards 6G networks: Use cases and technologies," 2020, *arXiv:1903.12216*.

[43] C. Suraci, S. Pizzi, A. Molinaro, and G. Araniti, "A trust-based selection mechanism for the support of 6G eHealth multimedia services," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Jun. 2022, pp. 1–6.

[44] P. Harvey, O. Toutsop, K. Kornegay, E. Alale, and D. Reaves, "Security and privacy of medical Internet of Things devices for smart homes," in *Proc. 7th Int. Conf. Internet Things, Syst., Manage. Secur. (IOTSMS)*, Dec. 2020, pp. 1–6.

[45] A. P. Kalapaaking, V. Stephanie, I. Khalil, M. Atiquzzaman, X. Yi, and M. Almashor, "SMPC-based federated learning for 6G enabled Internet of Medical Things," *IEEE Netw.*, vol. 36, no. 4, pp. 182–189, Jul. 2022.

YIYING WANG (Student Member, IEEE) is currently pursuing the B.S. degree in computer science with Nanyang Technological University, Singapore. She has interned at the Digital Identity and Trustworthiness Laboratory, Huawei Singapore Research Center for seven months. The article is accomplished during her internship which is mainly focused on 6G and trust modeling in future networks. Her research interests include artificial intelligence and digital security and plans to pursue further studies in the areas.

XIN KANG (Senior Member, IEEE) received the Ph.D. degree from the National University of Singapore. He is currently a Senior Researcher with the Huawei Singapore Research Center. He has more than 15 years research experience in wireless communication and network security. He is the key contributor to Huawei's white paper series on 5G security. He has published more than 70 IEEE top journals and conference papers. He received the Best Paper Award from IEEE ICC 2017 and the Best 50 Papers Award from IEEE Globecom 2014. He has also filed more than 60 patents on security protocol designs, and contributed more than 30 technical proposals to 3GPP SA3. He is also an Initiator and the Chief Editor for ITU-T Standard X.1365, X.1353, and the on-going work item Y.atem-tn.

TIEYAN LI (Member, IEEE) received the Ph.D. degree in computer science from the National University of Singapore. He is currently leading Digital Trust research, on building the trust infrastructure for future digital world, and previously on mobile security, the IoT security, and AI security with the Shield Laboratory, Singapore Research Center, Huawei Technologies. He is also the Director of Trustworthy AI C-TMG and the Vice-Chairperson of ETSI ISG SAI. He has more than 20 years experiences and he is proficient in security design, architect, innovation, and practical development. He was also active in academic security fields with tens of publications and patents. He has served as the PC members for many security conferences. He is an influential speaker in industrial security forums.

HAIGUANG WANG (Senior Member, IEEE) received the bachelor's degree from Peking University, in 1996, and the Ph.D. degree in computer engineering from the National University of Singapore, in 2009. He is currently a Senior Researcher on identity, trust and network security with Huawei International Pte Ltd. He joined Huawei, in 2013, where he is also a Senior Researcher. He has been a Research Engineer/Scientist with I2R Singapore, since 2001.

CHENG-KANG CHU (Member, IEEE) received the Ph.D. degree in computer science from National Chiao Tung University, Taiwan. He is currently a Senior Researcher with Huawei International, Singapore. He has a long-term interest in the development of new technologies in applied cryptography, cloud computing security, and the IoT security. His research interests include mobile security, the IoT security, decentralized digital identity, and web 3.0. He has published many research papers in major conferences and journals, such as PKC, CT-RSA, AsiaCCS, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He received the Best Student Paper Award in ISC, in 2007.

ZHONGDING LEI (Senior Member, IEEE) is currently a Senior Researcher with the Huawei Singapore Research Center. He has been working on 5G network security, since 2016. Prior to joining Huawei, he was the Laboratory Head and a Senior Scientist with the Agency for Science, Technology, and Research (A-STAR), Singapore, involved in research and development of 3GPP and IEEE standards in wireless systems and networks. He has been the Editor-in-Chief of *IEEE Communications Standards Magazine*, since 2019.