IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 3 July 2024, accepted 30 July 2024, date of publication 7 August 2024, date of current version 20 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3439689

PERSPECTIVE

Toward an Open Trust Establishment Infrastructure for Future Network: Motivations, Models, and Technologies

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

ABSTRACT In the era of 6G, given the emergence of heterogenous devices, diverse network scenarios, along with future deployment of cutting-edge applications that require high computation ability, how to establish trust in such complex network environment has become a demanding task. Current trust establishment process mostly relies on certificates issued by certificate authority (CA) or reputation derived from interaction and behavior history. However, these approaches may not be applicable to 6G scenarios due to several reasons, including but not limited to insufficient adaptability, lack of openness and transparency, and limited scalability. Hence, this article mainly proposes a novel approach, which is based on a claim-attestation-evidence framework and leverages both blockchain and artificial intelligence (AI) to build trust in highly open and dynamic future networks. Meanwhile, we also provide an overview on current trust establishment models, discuss about the advantages of our proposed model and suggest certain parts of our current design for improvements that can be considered by future research.

INDEX TERMS 6G, privacy, security, trust, trustworthiness, claim-based trust models.

I. INTRODUCTION

With the increasingly growing demand for ubiquitous connectivity and the need for highly-efficient and low-latency communication, there has been a significant surge in network complexity and device heterogeneity over the past decade. In 2015, ITU issued International Mobile Telecommunications-2020 (IMT-2020) [1], where the requirements of 5G, such as latency, data rate, mobility etc., were specified for different usage scenarios (enhanced mobile broadband (eMBB), ultra-reliable low latency communication (URLLC) and massive machine type communication (mMTC)). To meet the requirements of IMT-2020, service-based architecture (SBA) has been deployed as a key to network flexibility and openness of 5G core network [2]. By leveraging network function virtualization (NFV), software defined network (SDN), open APIs and network slicing, 5G network is able to facilitate a secure access to network capabilities and services for communication service providers (CSPs) as well as customers.

However, a highly open and flexible network is expected to face higher risk and more susceptible to network attacks, mainly due to the introduction of numerous interfaces which are lack of sufficient protection, inherent vulnerability of data transmission between entities, and excessive use of users' data and personal information. Whereas 6G, as the successor of 5G, will embrace even more openness [3]. Compared to 5G, 6G is envisioned to have wider coverage, lower latency and higher connectivity. As the original network architecture of 5G will no longer meet 6G's requirements, a novel architecture design is essentially needed, where intelligence and privacy preservation are two indispensable factors that need to be considered. Artificial intelligence (AI) will be pervasively deployed for more efficient network management and more effective attack detection, while

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

TABLE 1. Certificate-based vs. reputation-based vs. claim-based trust models.

Metrics	Certificate-based	Reputation-based	Claim-based
Open vs. Closed	Relatively closed	Relatively open	Open
Trust Accumulation	Trust value only switches between two states: trust (1), distrust (0).	Trust value varies with time continuously	Trust value varies with time continuously.
Security	Relatively safe. Trustworthy certificate issuance and verification by trusted third party.	Relatively unsafe. Need for security mechanisms to prevent malicious attacks.	Safe. Secure data storage and reliable transmission based on blockchain technology.
Implementability	Relatively high. Refer to established and comprehensive PKI system.	Relatively high. A number of reputation-based trust models have been proposed in various scenarios including P2P network, distributed system, cloud computing.	Still in its exploratory stage. One problem is how to make self-claims trusted by other nodes in the absence of trusted third parties.
Dynamicity	Relatively low	Relatively high	Relatively high
Extensibility	Relatively low, dependent on trustworthy third parties.	Relatively high, avoid reliance on a single node.	Relatively high, avoid reliance on a single node.

privacy-preserving mechanisms, such as differential privacy, homomorphic encryption and federated learning are expected to be widely applied. To build trustworthy 6G networks, one should first consider how to establish trust among heterogeneous involved entities, including human, devices, applications and services. In the view of Gartner, continuous adaptive risk and trust assessment (CARTA) is critical to trust establishment [4]. Furthermore, Gartner suggests that robust attack protection is necessary to ''keep bad stuff out'', and a reliable access control is required to ''let good stuff in''.

Most of the research work related to 5G/6G trust can be roughly divided into 2 types: the first type of research is focused on the calculation of trust value, including definition of trust metrics and utilization of ML/DL techniques for autonomous evaluation [5], [6], [7]. Alternatively, the second type mainly discusses about enabling technologies, such as blockchain [6], trusted platform module (TPM) [8], decentralized public key infrastructure (DPKI) [9], and gives recommendations on building a trustworthy network architecture, especially stressing on the importance of decentralization, privacy preservation and automation [10], [11]. Nevertheless, little attention has been paid on the trust models that illustrate trust establishment process, known as trust establishment models.

Current trust establishment models mainly comprise certificate-based models and reputation-based models, which have already been applied in the fields of authentication and identity management, as well as formation of trust relationship in social networks. In 6G networks, it is envisioned that trust establishment models will be essentially required in diverse scenarios such as device-to-device (D2D) communication [12], cross-domain mutual authentication [13], ubiquitous edge computing [14], and distributed machine learning [15] for heterogenous network. However, existing models are facing the challenges to meet the requirements of emerging scenarios, which demand for unprecedented openness, dynamicity, flexibility and scalability. In the next section, we will give a thorough overview of current trust establishment models, explain the deficiencies inherent in each model and discuss the rationale for adopting claim-based trust models.

The main contribution of this paper is as follows:

- We provided formalizations for key concepts related to the trust establishment models, addressing gaps in existing literature.
- We proposed a novel claim-based trust establishment model targeted at future networks that enhances security by enabling decentralized attestation of self-provided proofs while utilizing the power of artificial intelligence and blockchain technology.
- We designed a comprehensive architecture for the proposed claim-based trust model, outlining its components and interactions.

II. OVERVIEW OF VARIOUS TRUST MODELS

In the context of networks, ranging from the internet to mobile networks, a number of trust models have been proposed so far as the tools to show how trust is established among different entities. Based on trust establishment process, we have categorized these trust models into 3 categories, namely, certificate-based, reputation-based, and claim-based trust models, each of which will be discussed in the following. To offer a more straightforward explanation for the models' concepts, an easy-to-understand example is presented in Figure 1.

A. CERTIFICATE-BASED TRUST MODELS

Certificate-based trust models establish trust through certificate verification between two entities, which is mainly facilitated by current public key infrastructure (PKI), achieving considerable implementability. The trust model has already been applied in a number of real-world scenarios of 5G: specified in 3GPP TS 33.310, one of the implementations is the application of a certificate-based trust model used to enable certificate enrollment of base stations. Another example would be Extensible Authentication Protocol-Transport

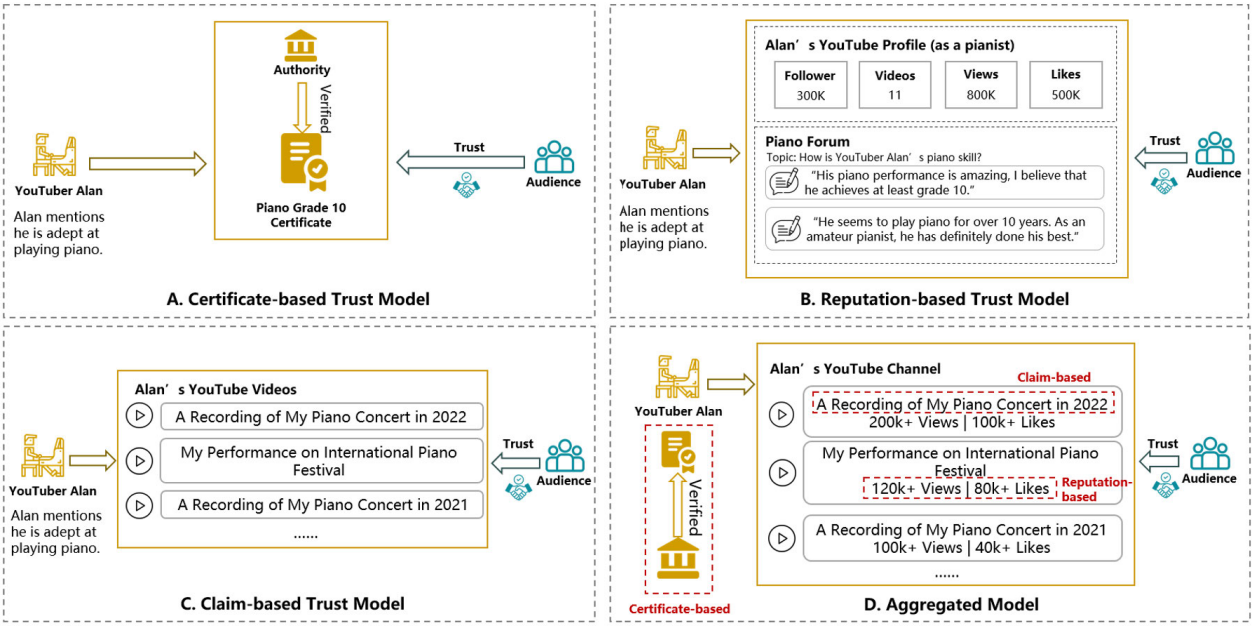

FIGURE 1. Overview of three types of trust models.

Layer Security (EAP-TLS), which provides mutual authentication by relying on PKI certificates.

In a certificate-based trust model, if entity A would like to communicate with B or get access to B's resources, a trust relationship needs to be established beforehand. In such case, A will present certificate, which is signed by a certificate authority (CA), as an evidence to justify its identity and trustworthiness [16]. After receiving A's certificate, entity B is required to verify the validity of the certificate with CA's public key. Trust will only be established if the certificate is authenticated. In our example (Figure 1A), Alan establishes trust with the audience by displaying his piano grade 10 certificate verified by trusted authority. The verified certificate alone is sufficient to prove Alan's piano proficiency.

Certificate-based trust model usually has a relatively high level of security, given that CAs are trustworthy and authoritative most of the time. Since no numerical computation is involved in the certification process, the trust value is not continuous, but binary, switching between 1 (trusted, when a certificate is verified) and 0 (distrusted, when a certificate cannot be verified or is revoked). Certificate-based trust models can be divided into a few subcategories, including single-CA, hierarchical, bridge, as well as mesh trust models [17].

Single-CA trust model, as its name suggests, only involves one CA which signs certificates for all entities [17]. The topology of single-CA model is simple but highly centralized, which is extremely prone to single-point failure. Thus, this type of trust model is not commonly to be seen in real-world scenarios.

As having a single and universal CA is not practical, a hierarchical trust model is built by several CAs structured in a hierarchical manner. The trust establishment process commences from the root CA (RCA), which is the upmost CA with greatest authority and power. The established trust relationship is unidirectional, from RCA to leaf CAs, which means that only superior CAs are allowed to issue certificates to their subordinate CAs. Although the hierarchical model involves more CAs to increase its scalability, the risk of single-point failure still exists, due to over reliance on the RCA. If RCA is compromised by malicious parties, the whole PKI will be endangered.

Compared to hierarchical trust model, mesh model, which is also called cross-certification model, has a much flatter architecture. Instead of trusting a single superior CA, CAs within the same mesh rely on each other to establish bidirectional and peer-to-peer trust relationships. In other words, a CA of mesh model is able to build trust relationship with several CAs, where each relationship generates a pair of certificates. Obviously, such mechanism solves the issue of single-point failure, but the cost of certificate management and model complexity is expected to increase at the same time [17].

Bridge trust model is designed to enable peer to peer certification process across organizations, such that different organizations may possess their distinctive trust models. For example, if organization A applies hierarchical trust model, while organization B has chosen mesh trust model, to establish a trust relationship between the two organizations, a bridge CA will be connected to both the RCA of organization A and a randomly-chosen CA of organization B. Unlike RCA or CA of mesh models, bridge CA is not responsible for direct certificate issuance. Thus, how to distribute certificates effectively across organizations becomes an unavoidable challenge to bridge model. Meanwhile, the bridge certification authority (BCA) is susceptible to single point failure. Once it is compromised by malicious attack, the

trust relationship among the connected CAs will be entirely damaged [17]. Thus, it is obvious that bridge trust models do not meet the need of highly complex, large-scale and heterogeneous future networks.

B. REPUTATION-BASED TRUST MODELS

There have already been a number of researches on reputation-based trust models in various scenarios, including internet of things (IoT), e-commerce, cloud services etc. [18] A node's reputation, as the indicator of its trustworthiness in a reputation-based trust model, is mainly calculated based on the goodness of the node's past behaviors and interaction records. An example of trust establishment process based on reputation is illustrated in figure 1B. It can be inferred from the statistics of Alan's YouTube profile and the comments on Alan's piano skills that he is indeed popular for his outstanding piano performance, and it is approved by a remarkable number of people. Consequently, the trust relationship from the audience to Alan is established based on Alan's good reputation. In IoT, reputation of a node will be aggregated and calculated from opinions of nodes that have interaction history with the node itself [19]. If the node's reputation value is higher than a threshold value, the trust relationship between two nodes will be established. Compared to certificate-based trust model, reputation-based trust model is more flexible, scalable, and therefore able to better capture the dynamicity of trust [19]. However, the model is susceptible to collusion attacks, such as bad-mouthing attacks and ballot stuffing attacks. These malicious attacks will impair the trustworthiness of a node's reputation, which means that a malicious node may have good reputation in a ballot stuffing attack, while a benign node receives bad reputation in a bad-mouthing attack [20]. Thus, even though there have been quite a number of researches on reputation-based trust models, the implementations in reality are quite limited, most of which are used for e-commerce and social networking services (SNS) [18].

C. CLAIM-BASED TRUST MODELS

Since claim-based trust model is a novel type of trust model, there is a paucity of research on the definition of relative concepts and the design of model architecture [21], which is one of the main motives for this paper. With reference to the claim-based identity management system of cloud computing [22], we defined a claim as a statement made by a subject, which can be judged as true or false. It usually consists of three components: a subject, an object, and the relationship between them. Meanwhile, to determine whether a claim is valid, evidences related to the claim are necessary. In our proposed claim-based model, trust relationship is established by performing attestation on evidences provided by the claim subject. As illustrated in Figure 1C, when Alan makes the claim that he is ''adept at playing piano'', he uses his published videos as self-evident proofs. After watching these videos, the audience will be convinced that Alan's claim is valid. The most significant distinction between a claim-based trust establishment model and others is that it both embodies decentralization and enables attestation with self-proofs. Compared to certificate-based model, a claim-based model does not rely on a third party, and therefore is more extensible, dynamic and open, avoiding the limitations of closed domains [23]. Thomas and Meinel [23] proposed a model that assesses trust on an individual claim basis, in which trust in a claim is determined by its perceived correctness and integrity, dependent on the issuer. Following [23], Grüner et al. [21] introduced a blockchain-empowered with larger flexibility and finer granularity for trust assessment. Instead of assessing trust on a claim-level, the authors of [21] evaluated the trust score of each attestation, and then calculated the final trust score of a claim based on the aggregated attestations. The immutability and the decentralized nature of blockchain technology make the model more anti-tampering and be more robust to malicious attacks. However, the aforementioned models are both limited to internet applications and lack of a more automated trust score evaluation process. Compared to [21] and [23], our proposed model obtains attestations directly by analyzing the existing raw data stored on public blockchains, which are generated by entities' activities. Our solution provides greater flexibility by eliminating the need for attestations from a trusted third party. The comparison of existing claim-based trust models is further elaborated in table 2.

In regard to our proposed resolution, the attestation will be performed by AI algorithms, and the obtained trust value would be continuous rather than discrete. To ensure the security of model, all involved data will be stored on blockchains so as to protect data from malicious tampering. Given that claim-based trust models are still under research and discussions, its implementability cannot be simply concluded, but it is undeniable that a real implementation will face many challenges. The most challenging part that affects the implementability of claim-based trust models is how to design the attestation process in a way that self-claims can be trusted by other nodes in the absence of a trusted third party. In the following section, a claim-based trust framework and a claim-based attestation process are proposed as our attempts to address the challenging issue. This model is particularly well-suited for future networks due to its inherent flexibility, scalability, and decentralized nature. As 6G aims to provide ubiquitous connectivity and support a wide range of applications and services, a claim-based trust model aligns well with these goals. It facilitates seamless and secure interactions among diverse and dynamic entities without the need for centralized authorities, thereby enhancing the overall efficiency and robustness of the network.

III. CLAIM-BASED TRUST ESTABLISHMENT MODEL

In this section, we will first outline the model's main structure, as well as relevant technologies that will be applied. Then, the full attestation process will be discussed, which will

TABLE 2. Comparison of claim-based trust models.

Models	Application Scenario	Trust Score	Security Level	Trust Score Evaluation	Granularity	Flexibility
Thomas et al. [23]	Internet	Binary	Low	Simple mathematical model	Claim-level	Low
Gruner et al. [21]	Internet	Continuous	High	Complex mathematical model	Attestation-level	Medium
Ours	Future networks	Continuous	High	AI-assisted mathematical model	Attestation-level	High

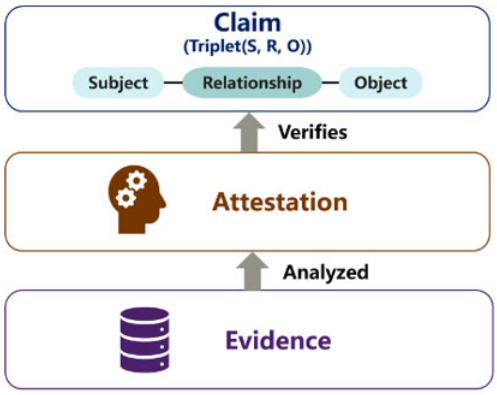

FIGURE 2. An illustration of Claim-Attestation-Evidence (CAE) framework.

illustrate how an entity's self-claims can be verified by data generated by the entity in an autonomous manner.

A. PRELIMINARIES

1) BLOCKCHAIN

Blockchain is a decentralized, distributed ledger system that is designed to ensure the integrity, transparency, and security of data transactions being posted on chains. Each chain is organized as a chain of blocks, with new blocks added only after verification through a consensus mechanism. Due to its unidirectional structure, operations on the blockchain are irreversible, and the recorded data cannot be modified. There are three types of blockchains, namely, public blockchain, private blockchain, and consortium blockchain. Different from a public blockchain, where anyone is allowed to participate by reading or writing data, a private chain only has a single participant, in which access is rigorously controlled. A consortium blockchain is often regarded as a balanced type when compared to both private and public blockchains [7]. It is controlled by a group of enterprises or organizations, each organization of which is in control of several nodes. The existing research works of 'blockchain for 6G' primarily focus on two aspects: more secure services and smart and reliable IoT applications [24]. The nature of decentralization, traceability, distribution, and tamper resistance makes blockchain an ideal technology for future networks.

2) ARTIFICIAL INTELLIGENCE

AI is an advancing technology that aims to emulate human intelligence through the use of machines. The concept of AI can be further narrowed down to machine learning (ML) and deep learning (DL). The main difference between ML and DL is that the latter one applies deep neural networks, which simulate human brains. It is believed that AI technology is of much importance for dynamic and highly complex future networks [24]. Given that massive volumes of data will be produced along with enhanced capabilities of future networks (low data latency, high security, reliability, etc.), AI is expected to converge both computing and communication networks, enabling more automated, efficient and intelligent networks. The integration of AI and 6G have attracted significant attention from researchers, resulting in a substantial body of published research, the main focuses of which include channel estimation [25], channel decoding [26], resource optimization [27], etc.

B. MAIN STRUCTURE

As shown in Figure 2, the proposed model is comprised of three components: claim, attestation and evidence. Claim, as defined previously, represents a verifiable statement made by an entity. In order to achieve interoperability, claims made by different entities for various purposes should be constructed according to certain commonly accepted standards. In other words, the syntactics of a valid claim should be pre-defined by trustworthy authorities. Instead of being merely syntactic, a claim should also be semantically meaningful. Inspired by the representation of knowledge graph, each claim will be converted into the form of a triple: (S, R, O), where S stands for subject, O means object, and R represents the relationship between the subject and the object. In most of cases, S can be ignored by default, since the subject of the triple is usually the same as the entity who generated the claim. The relationship R is extracted from the entity's original claim, and the extraction process can be facilitated by making use of natural language processing (NLP) tools.

Prior to introducing the attestation process, evidence, as an indispensable resource to support attestation, should be discussed first. Evidence is mainly originated from raw data generated and also published by the claim's subject, which may include the subject's attributes, past behaviors, or interaction history. However, as 6G networks are expected to include many more open interfaces, data generated by each identity become more susceptible to be compromised by malicious parties. Traditional approach of data storage heavily relies on trusted third parties, while this kind of over reliance can lead to problems caused by centralization: First, users are forced to renounce their control over data, and how the data will be used in the future cannot be guaranteed. Furthermore, if the trusted third party has been compromised, all data stored in it will be endangered. To preserve data's integrity, blockchain is a promising technology that can

empower secure, transparent and trustworthy data storage. It is by nature decentralized, which means that there does not exist a central authority that manages all the data. In addition, the blockchain is also immutable, realized by the well-known consensus mechanism and cryptographic hashes. With the use of blockchain, the users are able to take control of their own data, which means that it is up to the user to decide what can be shared and how it should be used. Moreover, since everything published on a public chain is visible to every node within the blockchain, the authenticity of evidences belonged to one node can be verified by other nodes. This will ensure that if a malicious entity deliberately uploads fake data in order to validate its claim, which is supposed to be invalid, the dishonest behavior will be detected and the entity will be marked as anomaly.

Attestation is the process that verifies an entity's claims based on provided evidences of the entity. The key to a reliable attestation process is trustworthy algorithms, which will decide how to match a claim with evidences relevant to a claim and how to determine if the claim is valid. Having regard to the pervasive use of AI in 6G, it is unavoidable to leverage ML/DL models to enable system autonomy. In traditional programming, the program logic is mainly rule-based, consisting of a number of predefined rules. However, in the highly open and dynamic future networks, this paradigm will face numerous problems, due to its lack of flexibility and heavy reliance on human intelligence. Given the massive amount of data produced by heterogeneous entities, as well as challenges posed by various usage scenarios and demands, it is impossible to define a set of universal rules for attestation process to make adaptations reactively according to current situation. On the contrary, AI models can be trained to accommodate for different claims and evidences provided by diverse entities both proactively, and they usually have better capability of processing large scale of data in a relatively short time. Thus, in order to achieve higher degree of flexibility and openness, AI algorithms are taken as one of the core elements of attestation process, and AI trustworthiness should also be viewed as the essential cornerstone.

From our point of view, trustworthy AI algorithms should embody several indispensable attributes, including but not limited to security, transparency, explainability, openness, impartiality. First and foremost, AI security, as the most important element, represents several aspects, such as privacy preservation, data integrity and confidentiality. Besides, the algorithms also need to be robust against adversarial attacks like data/model poisoning, evasion attacks etc. To achieve transparency, an AI model is required to have its parameters, algorithms and model structure accessible to external parties. This attribute is commonly related to explainability, which measures the extent to which the model's decisions can be explained, and openness, which requires an AI model to be open-source and publicly available. Impartiality stresses the importance of AI fairness, representing that the model does not have a particular preference for or discriminate against certain sensitive attributes of an entity's evidences.

C. CLAIM-BASED TRUST ATTESTATION PROCESS

In this section, we introduce the complete attestation process of a claim-based trust establishment model. The process mainly involves 5 steps: claim triple generation, rule extraction, evidence collection, claim attestation and knowledge graph (KG) updates, which are discussed in the following (Figure 3).

1) CLAIM TRIPLE GENERATION

At the initial stage, before an entity makes a claim, a claim template should be chosen for the purpose of standardization. The claim template, which is obtained from a consortium blockchain, defines the format and required elements of a valid claim. Given the distinctive features of aforementioned blockchains, consortium blockchain would be the optimal choice for storing claim templates, as it retains both partial openness and access control mechanism. The word "partial" means that the blockchain is open in a way that external entities are able to read the data, while write operation is only allowed for several authorized entities. The access control mechanism is achieved by involving pre-selected nodes in charge of the consensus protocol. To put it in 6G context, the consortium blockchain is expected to include main mobile network operators as well as telecommunication infrastructure companies. In our proposed process, a standardized claim template will only be produced after the majority of involved enterprises have reached a consensus.

Afterwards, the entity will submit a claim based on the chosen claim template, and the claim will be passed to semantic-processing algorithms. Embedding semantic aspects in 6G has become a future trend, envisioned to enable 6G networks to accommodate for higher data rate, boarder spectrum and wider bandwidth [28]. The semantic-processing algorithms empowered by NLP models will parse and encode a claim into triples, by recognizing and extracting three main components of the claim: the object of the claim, the subject of the claim, and relationship between the two entities. In [29], the authors divided the triple generation task into two sub-tasks: entity tagging, aimed at identifying main entities (e.g., the object and the subject), and entity relation classification, combining BERT model with a convolutional layer which is used to obtain higher-level features. The extracted claim triple not only provides keywords as crucial information, but also compresses and condenses claims of different qualities in order to achieve higher transmission efficiency as well as strive for fairness and uniformity among heterogeneous entities.

2) RULE EXTRACTION

Knowledge Graph (KG) is gaining increasingly growing attention and popularity in the studies of diverse fields

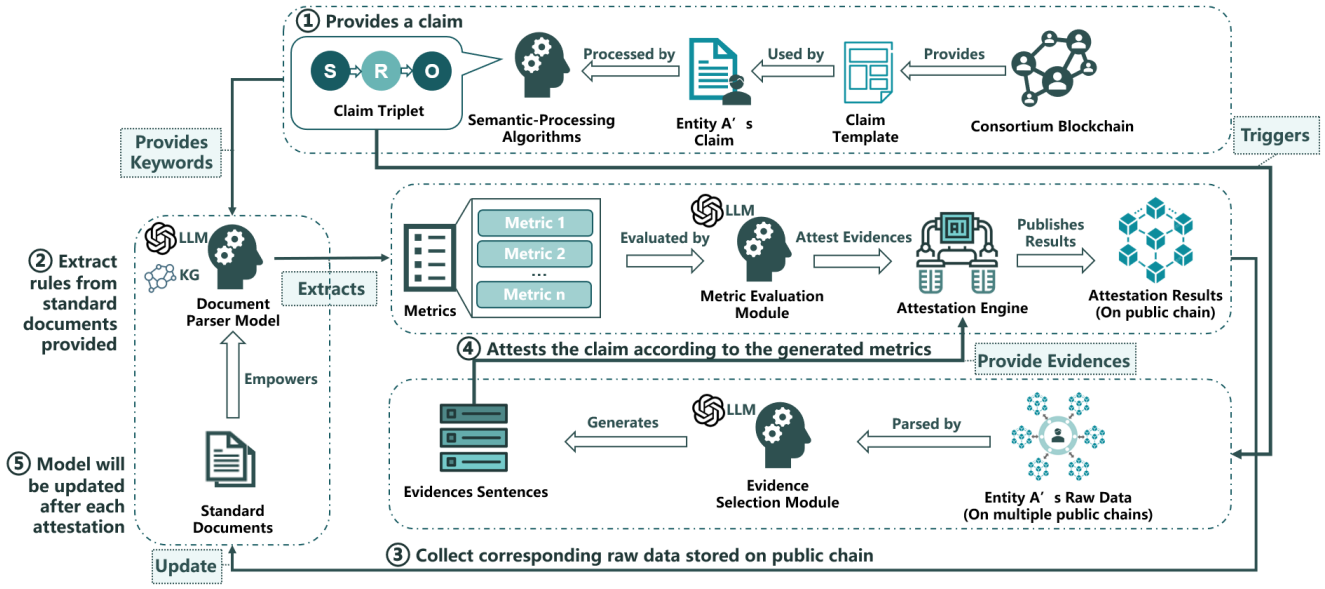

FIGURE 3. An overview of our claim-based approach to establish trust.

recently, since it can represent massive human knowledge as an extensible structured graph, which facilitates the application of DL algorithms on knowledge representation and reasoning, such as graph neural networks (GNN), attention mechanisms, recurrent neural networks (RNN) and reinforcement learning (RL).

Rule mining is one of the sub-tasks belonging to the knowledge acquisition task of KG. A rule is defined as body→head, where body stands for body predicates which may include several atoms, while head only consists of a single atom. For instance, as described in Fig. 1, to verify whether Alan's claim is true, one possible mined rule could be performance (X, piano concert) and hasVideo (X, piano concert) → play (X, piano). Rule mining algorithms usually contains two stages: the first stage is to generate all possible rules, and the second stage is to filter out low-quality rules by calculating confidence score of each generated rule. Considering that it will be time-consuming to generate rules based on a large-scale KG in the first step, Chen et al. [30] proposed a RL-based framework to reduce the cost of rule generation and rule evaluation. It has suggested that RL is quite effective in shortening the time needed for rule extraction, by providing a trained value function as a guidance for the agent to make wise decisions.

Besides KG, the rapid development of large language models (LLM) further facilitates the automation of rule mining process, given that LLM has demonstrated impressive capabilities on various tasks, including text comprehension as well as logical reasoning [31]. LLM consist of a series of large-sized pretrained language models (PLM), which contain billions of parameters and have been pretrained on massive amount of text corpus. It has been discovered that increasing the size of the PLM and training datasets eventually led to significant improvements on the model's performance on downstream tasks [32]. Given the remarkable performance of LLM on a variety of reasoning tasks, [33] proposed a framework for building a rule library with LLM by utilizing the deductive reasoning and inductive reasoning methods. The framework has proved the feasibility of mining as well as verifying rules with LLM. Sharma and Yegneswaran [34] developed a framework named PROSPER to understand request for comments (RFC) documents and extract protocol finite state machine (FSM) state and transition. It showed the high potential of utilizing LLM to automate the process of understanding protocol RFC documents.

In our proposed framework, the document parser model (which can be LLM or KG) extracts the rules from standard documents provided. It can be further fine-tuned by the latest standard documents to ensure that the knowledge learned by the parser model aligns with up-to-date information. Given the keywords provided by a claim triple, the document parser model will produce a set of rules that are closely related to the claim. The generated rules are also named as metrics, which will be used in the following procedure to measure the claim's veracity and trustworthiness.

To further ensure the trustworthiness of our generated metrics, a metric evaluation module is therefore needed to filter out insignificant metrics or misleading ones. In [35], the authors proposed an effective pipeline to remove generated questions and answers of bad quality using a quality filter, which can assess data points on multiple dimensions, to guarantee that the final question and answer pairs obtained at the end of the pipeline will be reliable and of high quality. Inspired by it, the metric evaluation module also needs to be designed to enable multi-dimensional assessment

(e.g., format quality, significance, relevance) of the extracted rules.

3) EVIDENCE COLLECTION

The evidence collection process is triggered by the creation of a claim triple, which implies the need for evidences to attest the proposed claim. Nevertheless, the collection of evidences can be quite risky and may pose formidable threats to an entity's data integrity. As mentioned previously, blockchain is a promising technology that can be deployed as an underlying infrastructure to defend against data integrity attacks that mainly involve unauthorized data modification, injection and deletion [36]. If the integrity of raw data is compromised, the evidences generated from the compromised will subsequently become untrustworthy, which may even imperil the entire attestation process.

As 6G is envisioned to include heterogeneous mobile devices as well as diverse scenarios, an entity's data can be classified into different categories, and sometimes need to be stored on different public blockchains [37]. For example, Polkadot is a sharded multi-chain and seeks to establish connections among multiple previously-isolated blockchains [38]. Each shard, also named as a parachain, might belong to different types, including private, consortium, and public blockchain. The data generated by an entity can be dispersed among parachains, due to various data provenances. All parachains are coalesced by a relay chain, which bears the responsibility for offering cross-chain interoperability, resolving disputes and providing the network's shared security.

After the claim triple is generated, the identity information of the object will be passed to the multi-chain system for retrieving publicly accessible data, that are relevant to the object, stored on different parachains. The retrieved data will then be processed by an evidence selection module, which is responsible for parsing, filtering, and reorganizing the data and finally transforming it to valid evidence sentences. The evidence selection module. One way of generating evidences in the form of structured and machine-readable data is to use knowledge embedding algorithms. However, the derived embeddings need to be aligned with previously generated metrics before the evidence can be verified. To tackle this issue, using LLM becomes an ideal approach, since a single LLM can support multiple functions, including sentence parsing, information extraction, filtering, and text reorganization. The generated evidence sentences will eventually be passed to attestation engine and assessed by formerly extracted evaluation metrics.

4) CLAIM ATTESTATION

At claim attestation stage, the attestation engine applies evaluation metrics generated by rule-mining algorithms of former stages to verify the validity of a claim. As stated in previous sections, both evidence and metrics will be transformed into sets of embeddings for the purpose of quantitative comparison.

In the context of using KG as rule extraction tool, since evidence embeddings have already been aligned with the established KG, when calculating cosine similarity between an evidence embedding and a metric embedding, highly correlated pair should receive a high attestation score, which means that the evidence has effectively supported the corresponding claim. Zhong et al. [39] have proposed a graph-based fact checking approach to check the validity of a given claim based on provided evidences: the embeddings of evidences are first aggregated into claim-centric representations with the use of graph attention mechanism, and the representations will be aligned with original claim embeddings in order to measure the similarity as the degree of coherence between the claim and evidence.

If it is an LLM which has been applied to extract rules from standard documents, it will provide human-readable rules instead of embeddings. In this scenario, LLM can be directly used as the attestation engine with tailored prompts containing task requirements. Different from the former approach, using LLM provides a fast, efficient and more generalizable way of validating the provided claims [40]. Meanwhile, it avoids costly training procedure while retaining high generalizability across various domains.

In our proposed procedure, the attestation results of claims will be uploaded to a public chain, where everyone is able to check published results, which cannot be deleted or tampered.

5) KNOWLEDGE UPDATES

If the claim passes the attestation process, the evidences that support the claim will be used to update the document parser model. If the model is a KG, the update can be done by adding new entities and defining new relations based on knowledge extracted from raw data of the claim owner. However, most of the current research are only applicable to static KG, which means that KG representation is deterministic, and will not evolve over time. As a result, in a conventional way of constructing KG, the addition of new triples unavoidably alters the embeddings of original KG, which will require a costly re-training process including all existing triples afterwards and cause a waste of computational resource. To better reflect dynamicity and reduce computational cost at the same time, a novel approach proposed by [41] applies anchors-based incremental embedding (ABIE) to address the issues brought by the growth of dynamic KG. The ABIE model is built based on the assumption that every KG has nodes of great importance, which are also known as the ''backbone'' of KG or the ''embedding anchors''. The embeddings of anchor nodes are affected by inclusion of new triples, and thus can be leveraged as the baseline for deriving embeddings of added knowledge.

Motivated by the method of [41], in our proposed process, only after each successful attestation, the evidences (in the

form of KG) used by the claim will be aligned to current fundamental KG based on anchors that represent the core knowledge elements. The aligned embeddings of evidences will then be incorporated into the fundamental KG as an incremental KG (IKG). The proactive updating mechanism ensures our fundamental KG is continuously evolving to meet real-time and varying demands.

Nevertheless, when the document parser model is an LLM, fine-tuning the LLM requires considerable amount of computing resources. Considering the recent findings and application of prompt engineering, instead of directly fine-tuning the model, the latest knowledge can be stored in a library and will be injected into the reasoning process by including it in the input prompts, which is similar to what has been done in the deduction stage of [33]. Another advantage of using prompt engineering is that the input knowledge can be filtered based on the relevance to the current claim. This approach narrows down the range of knowledge learned from standard documents, and thus is envisioned to enhance the capability of the document parser model.

D. DISCUSSION

In our design of a claim-based trust model, AI, especially LLM, and blockchain are two core technologies that have been applied for three elemental components of trust establishment framework: identity, algorithm as well as data. User identities of claim-based models are mainly encapsulated in triples generated by AI. Meanwhile, the full attestation process, including rule mining and evidence generation, is powered by AI algorithms that facilitate automation. The trustworthiness of the third component, user data, is guaranteed by blockchain given its transparency, decentralization and immutability.

To ensure that the model conforms to 6G's openness, the attestation process should be accessible and auditable to external parties. Moreover, despite that data integrity has been guaranteed by the use of blockchain, user privacy is still an important factor to be considered. Data that contain confidential information should never be disclosed to other entities without user's acknowledgement or authorization.

IV. CONCLUSION

This article mainly provides a claim-based trust model, which is mainly enabled by AI models and blockchains, as a novel approach to establish trust in the context of future 6G networks. The claim-based model embodies several essential characteristics of trust establishment, including openness, transparency, automation and data security. Besides, an overview of three trust establishment models is also discussed and compared with one and another in the early section. We hope that our approach would provide inspirations or offer feasible suggestions to future research on the trust establishment approaches, facing a highly open, dynamic and heterogeneous network environment of 6G.

REFERENCES

[1] *IMT for 2020 and Beyond*, Int. Telecommun. Union Radiocommunication Sector (ITU-R), Geneva, Switzerland, 2020.
[2] K. Du, L. Wang, Z. Zhu, Y. Yan, and X. Wen, "Converged service-based architecture for next-generation mobile communication networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Glasgow, U.K., Mar. 2023, pp. 1–6, doi: 10.1109/WCNC55385.2023.10118793.
[3] M. Polese, M. Dohler, F. Dressler, M. Erol-Kantarci, R. Jana, R. Knopp, and T. Melodia, "Empowering the 6G cellular architecture with open RAN," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 2, pp. 245–262, Feb. 2024.
[4] K. Panetta. (2017). *The Gartner IT Security Approach for the Digital Age*. [Online]. Available: https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age
[5] E. L. C. Macedo, R. S. Silva, L. F. M. de Moraes, and G. Fortino, "Trust aspects of Internet of Things in the context of 5G and beyond," in *Proc. 4th Conf. Cloud Internet Things (CIoT)*, Niteroi, Brazil, Oct. 2020, pp. 59–66.
[6] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Toward blockchain-based trust and reputation management for trustworthy 6G networks," *IEEE Netw.*, vol. 36, no. 4, pp. 112–119, Jul./Aug. 2022, doi: 10.1109/MNET.011.2100746.
[7] S. Wong, "The fifth generation (5G) trust model," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Marrakesh, Morocco, Apr. 2019, pp. 1–5, doi: 10.1109/WCNC.2019.8885697.
[8] 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, doi: 10.1109/OJCOMS.2023.3244274.
[9] 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.
[10] 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.
[11] C. Benzaïd, T. Taleb, and M. Z. Farooqi, "Trust in 5G and beyond networks," *IEEE Netw.*, vol. 35, no. 3, pp. 212–222, May 2021.
[12] M. Omar, Y. Challal, and A. Bouabdallah, "Certification-based trust models in mobile ad hoc networks: A survey and taxonomy," *J. Netw. Comput. Appl.*, vol. 35, no. 1, pp. 268–286, Jan. 2012.
[13] S. R. Garzon, H. Yildiz, and A. Küpper, "Towards decentralized identity management in multi-stakeholder 6G networks," in *Proc. 1st Int. Conf. 6G Netw. (6GNet)*, Paris, France, Jul. 2022, pp. 1–8, doi: 10.1109/6GNet54646.2022.9830163.
[14] X. Zhu, F. Ma, F. Ding, Z. Guo, J. Yang, and K. Yu, "A low-latency edge computation offloading scheme for trust evaluation in finance-level artificial intelligence of things," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 114–124, Jan. 2024.
[15] W. Ye, C. Qian, X. An, X. Yan, and G. Carle, "Advancing federated learning in 6G: A trusted architecture with graph-based analysis," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Kuala Lumpur, Malaysia, Dec. 2023, pp. 56–61.
[16] A. S. Wazan, R. Laborde, D. W. Chadwick, F. Barrere, and A. Benzekri, "How can i trust an X.509 certificate? An analysis of the existing trust approaches," in *Proc. IEEE 41st Conf. Local Comput. Netw. (LCN)*, Dubai, United Arab Emirates, Nov. 2016, pp. 531–534.
[17] Z. El Uahhabi and H. El Bakkali, "A comparative study of PKI trust models," in *Proc. Int. Conf. Next Gener. Netw. Services (NGNS)*, Casablanca, Morocco, May 2014, pp. 255–261.
[18] S. Zishen, P. Jie, J. Lingyu, W. Fazhuan, and W. Dong, "A reputation-based dynamic trust model in P2P e-commerce environment," in *Proc. China Autom. Congr. (CAC)*, Oct. 2021, pp. 6432–6438.
[19] F. Ullah, A. Salam, F. Amin, I. A. Khan, J. Ahmed, S. A. Zaib, and G. S. Choi, "Deep trust: A novel framework for dynamic trust and reputation management in the Internet of Things (IoT)-based networks," *IEEE Access*, vol. 12, pp. 87407–87419, 2024, doi: 10.1109/ACCESS.2024.3409273.
[20] N. Saini, A. Chaturvedi, and I. Jha, "Identifying collusion attacks in P2P trust and reputation systems," *Int. J. Comput. Appl. (IJCA)*, vol. 2, pp. 36–41, Apr. 2014.
[21] A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 1475–1482.

[22] A. Singh and K. Chatterjee, "Identity management in cloud computing through claim-based solution," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Technol.*, Haryana, India, Feb. 2015, pp. 524–529.
[23] I. Thomas and C. Meinel, "Enhancing claim-based identity management by adding a credibility level to the notion of claims," in *Proc. IEEE Int. Conf. Services Comput.*, Bangalore, India, Sep. 2009, pp. 243–250.
[24] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6G wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2494–2528, 1st Quart., 2023.
[25] H. W. Oleiwi, D. N. Mhawi, and H. S. Al-Raweshidy, "A secure deep autoencoder-based 6G channel estimation to detect/mitigate adversarial attacks," in *Proc. 5th Global Power, Energy Commun. Conf. (GPECOM)*, Jun. 2023, pp. 530–535.
[26] A. K. Ahmed and H. S. Al-Raweshidy, "Deep learning polar convolutional parallel concatenated (DL-PCPC) channel decoding for 6G communications," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Genoa, Italy, Jul. 2023, pp. 1–5, doi: 10.1109/cits58301.2023.10188712.
[27] M. Li, F. R. Yu, P. Si, Y. Zhang, and Y. Qian, "Intelligent resource optimization for blockchain-enabled IoT in 6G via collective reinforcement learning," *IEEE Netw.*, vol. 36, no. 6, pp. 175–182, Nov./Dec. 2022.
[28] E. Calvanese Strinati and S. Barbarossa, "6G networks: Beyond Shannon towards semantic and goal-oriented communications," *Comput. Netw.*, vol. 190, May 2021, Art. no. 107930.
[29] W. Deng and Y. Liu, "Chinese triple extraction based on BERT model," in *Proc. 15th Int. Conf. Ubiquitous Inf. Manage. Commun. (IMCOM)*, Jan. 2021, pp. 1–5, doi: 10.1109/IMCOM51814.2021.9377404.
[30] L. Chen, S. Jiang, J. Liu, C. Wang, S. Zhang, C. Xie, J. Liang, Y. Xiao, and R. Song, "Rule mining over knowledge graphs via reinforcement learning," *Knowl.-Based Syst.*, vol. 242, Apr. 2022, Art. no. 108371, doi: 10.1016/j.knosys.2022.108371.
[31] S. Bubeck, V. Chandrasekaran, R. Eldan, J. Gehrke, E. Horvitz, E. Kamar, P. Lee, Y. Tat Lee, Y. Li, S. Lundberg, H. Nori, H. Palangi, M. Tulio Ribeiro, and Y. Zhang, "Sparks of artificial general intelligence: Early experiments with GPT-4," 2023, *arXiv:2303.12712*.
[32] W. X. Zhao, K. Zhou, J. Li, T. Tang, X. Wang, Y. Hou, Y. Min, B. Zhang, J. Zhang, Z. Dong, and Y. Du, "A survey of large language models," 2023, *arXiv:2303.18223*.
[33] Z. Zhu, Y. Xue, X. Chen, D. Zhou, J. Tang, D. Schuurmans, and H. Dai, "Large language models can learn rules," 2023, *arXiv:2310.07064*.
[34] P. Sharma and V. Yegneswaran, "PROSPER: Extracting protocol specifications using large language models," in *Proc. 22nd ACM Workshop Hot Topics Netw.*, Cambridge, MA, USA, Nov. 2023, pp. 41–47.
[35] T. Schimanski, J. Ni, M. Kraus, E. Ash, and M. Leippold, "Towards faithful and robust LLM specialists for evidence-based question-answering," 2024, *arXiv:2402.08277*.
[36] A. H. Khan, N. Ul Hassan, C. Yuen, J. Zhao, D. Niyato, Y. Zhang, and H. V. Poor, "Blockchain and 6G: The future of secure and ubiquitous communication," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 194–201, Feb. 2022.
[37] J. Chang, J. Ni, J. Xiao, X. Dai, and H. Jin, "SynergyChain: A multichain-based data-sharing framework with hierarchical access control," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14767–14778, Aug. 2022.
[38] H. Abbas, M. Caprolu, and R. Di Pietro, "Analysis of polkadot: Architecture, internals, and contradictions," 2022, *arXiv:2207.14128*.
[39] W. Zhong, J. Xu, D. Tang, Z. Xu, N. Duan, M. Zhou, J. Wang, and J. Yin, "Reasoning over semantic-level graph for fact checking," in *Proc. 58th Annu. Meeting Assoc. Comput. Linguistics*, Jul. 2020, pp. 6170–6180.
[40] M. Li, B. Peng, M. Galley, J. Gao, and Z. Zhang, "Self-checker: Plug-and-play modules for fact-checking with large language models," 2023, *arXiv:2305.14623*.
[41] L. Dong, D. Zhao, X. Zhang, X. Li, X. Kang, and H. Yao, "Anchors-based incremental embedding for growing knowledge graphs," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3458–3470, Apr. 2023.

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

XIN KANG (Senior Member, IEEE) received the B.Eng. degree from Xi'an Jiaotong University, in 2005, and the Ph.D. degree from the National University of Singapore, in 2011. He was a Research Scientist with the Institute for Infocomm Research, A*STAR, Singapore, from 2011 to 2014. After that, he joined Shield Laboratory, Huawei Singapore Research Center as a Senior Researcher. He is currently a Chief Research Scientist in trust and security with Huawei Singapore Research Center. He is also an Honored Full Professor with the University of Electronic Science and Technology of China. He has published more than 70 top-tier journal and conference papers, and lots of them are listed as SCI highly cited research papers. He has filed more than 70 patents on trust and security protocol designs. Besides, he is very active in standardization. He has contributed more than 30 technical proposals to 3GPP SA3. He is the leading key contributor to Huawei 5G security white paper series. He has more than 15 years' of research experience. His research interests include but not limited to trust modeling, trust networking, trustworthy AI and machine learning, trusted AI agent, network security, optimization, wireless communications, digital identity, blockchain, security protocol design, and applied cryptography. He has received the Best Paper Award from IEEE ICC 2017, and the Best 50 Papers Award from IEEE GlobeCom 2014. He is the Vice Chair of IEEE SA AIGC Technology Working Group, and the main contributor of IEEE P3429. He is also the Initiator and main contributor of ISO JPEG Trust. He is also very active in IETF ANIMA and TLS Working Group. He is an Initiator and the Chief Editor for ITU-T standard X.1365, X.1353, Y.3260, and the on-going work item Y.Trust-AI.

TIEYAN LI (Member, IEEE) received the Ph.D. degree in computer science from the National University of Singapore. He is currently leading the Digital Trust Research, on building the trust infrastructure for future digital world, and previously on mobile security, the IoT security, and AI security at Shield Laboratory, Singapore Research Center, Huawei Technologies. He is also the Director of the Trustworthy AI C-TMG. He has more than 20 years of experiences and 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 and is an influential speaker in industrial security forums. He is the Vice-Chair of ETSI ISG SAI.