IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 April 2023, accepted 17 April 2023, date of publication 24 April 2023, date of current version 5 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3270042

STANDARDS

An Overview of Trust Standards for Communication Networks and Future Digital World

HUILIN WANG, XIN KANG, (Senior Member, IEEE), TIEYAN LI, (Member, IEEE), ZHONGDING LEI, (Senior Member, IEEE), CHENG-KANG CHU, (Member, IEEE), AND HAIGUANG WANG, (Senior Member, IEEE)
Huawei Singapore Research Center, Singapore 138588

Corresponding author: Xin Kang (kang.xin@huawei.com)

ABSTRACT Trust is an essential concept in various scenarios enabled by Information and Communication Technologies (ICT). To facilitate the implementation of trust in these scenarios, different organizations have published a series of trust frameworks. However, most existing works on trust standards only focus on a specific application domain. Unlike these works, in this paper, we provide a comprehensive overview of the current available trust standards related to communication networks and future digital world from several main organizations. We categorize these trust standards into three layers: trust foundation, trust elements, and trust applications. We then analyze these trust standards and discuss their contributions in a systematic way. We also examine the motivations behind each enforced standard, analyze their frameworks and solutions, and present their role and impact on communication works and future digital world. Finally, we offer our suggestions on the trust work that needs to be standardized in the future.

INDEX TERMS Trust, trust management, trust standards.

I. INTRODUCTION

Trust has been a crucial concept in the development of modern computer science. It refers to the degree of willingness of a party to be vulnerable and take a risk in interacting with another based on specific expectations [1]. Initially, discussions on trust in computer security were centered on whether humans should trust a program to be resilient against Trojan horse attacks [2]. In other words, could users trust a program to perform its intended function without any malicious code that could cause harm to the system or user data? Over time, the concept of trust has evolved, and it now extends to various fields and aspects beyond computer security. Scholars have been inspired by how trust is established between humans, and they have explored trust relationships between humans and objects, objects and objects, and even entities and entities in the digital world. Furthermore, the trustworthiness of parties has become a popular topic of study. Trustworthiness refers to a party's ability to fulfill expectations or be dependable for others [3]. For example, how reliable is a particular software application, and will it perform as intended? Authentication and evaluation are some common methods to identify the trustworthiness of a party. Authentication verifies the identity of a party, while evaluation assesses their past behavior to determine their reliability. To quantify trust, scholars have proposed trust modeling. Trust modeling represents trust as a value that reflects the trustee's trustworthiness in a trust relationship between the trustor and trustee. Quantitative measurements of different factors influencing the trust relationship are used to produce this value. These factors may include past behavior, reputation, and authentication.

Trust and its applications have been extensively studied in academia over the past few decades. The study of trust has important implications for the development of secure and trustworthy systems. By understanding the factors that

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

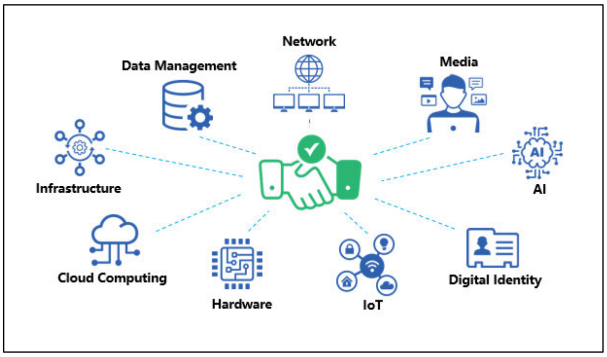

FIGURE 1. Active area of trust standards.

influence trust, developers can design systems that are more reliable, and users can make more informed decisions when interacting with digital entities. Ting et al. studied trust and trust modelling for the future digital world. Based on the deep understanding of definitions, properties, theories, and the impact of digital trust, Ting et al. provided a comprehensive study on digital trust modelling techniques, summarized exhaustive trust evaluation criteria, and analyzed extensive state-of-art methodologies and theories in trust modelling [4]. Wang et al. proposed a novel trust framework called SIX-Trust, which involves 3 layers: sustainable trust (S-Trust), infrastructure trust (I-Trust) and xenogenesis trust (X-Trust), to construct trustworthy and secure 6G networks [5]. Both Valero et al. [6] and Benzaïd et al. [7] concentrated on trust in the context of 5G networks and beyond. Valero et al. conducted an inclusive survey and comparison of standardization efforts for trust and reputation models, engaging in a thorough discussion on pre-standardization approaches, aiming to enhance trust and reputation models beyond the limitations of 5G networks [6]. Benzaïd et al. instead focused on the concept of trust in 5G and beyond networks by examining its dimensions, potential enablers, and future research directions, while proposing a blockchain-based data integrity framework to bolster trust in data used by machine learning pipelines [7]. Wang et al. provided a comprehensive survey on trust models in heterogeneous networks (HetNets) and introduced a criterion for evaluating trust models in terms of Quality of Trust (QoT) with taxonomies of trust models and their applications [8]. Although trust and trust modeling have been extensively studied, the literature focusing on trust-related standards is limited. Although trust and trust modeling have been extensively studied, the literature focusing on trust-related standards is rather limited.

Today, trust has become an important concept in security design, and several organizations such as ITU, NIST, ISO, and IETF have published standards to supervise and regulate the application of trust in various fields of security. These standards mainly cover seven areas of security: infrastructure, data management, network, media, AI, digital identity, IoT, hardware, and cloud computing, as shown in Fig. 1. However, there is a lack of literature that provides a comprehensive survey and overview of existing trust standards on communication networks and the future digital world. This motivated us to write this paper, which aims to present a comprehensive overview of all currently available trust standards related to communication networks from these main standard organizations. Specifically, this paper organizes and summarizes all these trust standards into three layers: trust foundation, trust elements, and trust applications. We then analyze these trust standards and discuss their contribution in a systematic way. For example, we discuss the motivations behind each enforced standard, analyze their frameworks and solutions, and present their role and impact on communication networks and the future digital world. The objective of this paper is to provide a valuable resource for researchers, practitioners, and policymakers interested in the field of trust in communication networks. By presenting a comprehensive overview of existing trust standards and analyzing their impact and potential, we hope to advance the understanding and application of trust in this field.

II. TRUST FOUNDATION

As shown in Fig.2, we summarize and categorize all the existing trust-related standards into three layers: trust foundation, trust element, and trust application. The trust foundation level comprises standards that serve as the basis for the upper layers, as they establish the fundamental concepts, definitions, and evaluation criteria for trust. This section of our paper introduces the standards that cover these fundamental aspects of trust.

A. TRUST DEFINITION AND TRUST ENVIRONMENT

Trust is a crucial concept in the development of information and communication technology (ICT). In order to establish trust between entities, a trusted environment that provides interoperability and information security within the ICT infrastructure is essential. This enables entities to reduce risk and uncertainty by using trust to predict the outcomes of their interactions.

The formal definition of a trusted environment is provided in ITU-T Y.3051, which was developed by ITU-T SG13 in 2017. This recommendation aims to offer a high level of confidence and protection to entities by defining a trusted environment as an environment that provides a set of technical and regulatory conditions that allow for the establishment of trust between interacting agents. To build a trusted environment, a number of requirements must be met, including predictability, information security, interoperability, and availability of administration services. The recommendation also outlines the basic principles of a trusted environment, both on the technical and legal aspects, which refines the concept of a trusted environment. This provides a thorough understanding of a trusted environment in the context of the ICT infrastructure and services, and can be used for the further implementation of trust in various scenarios.

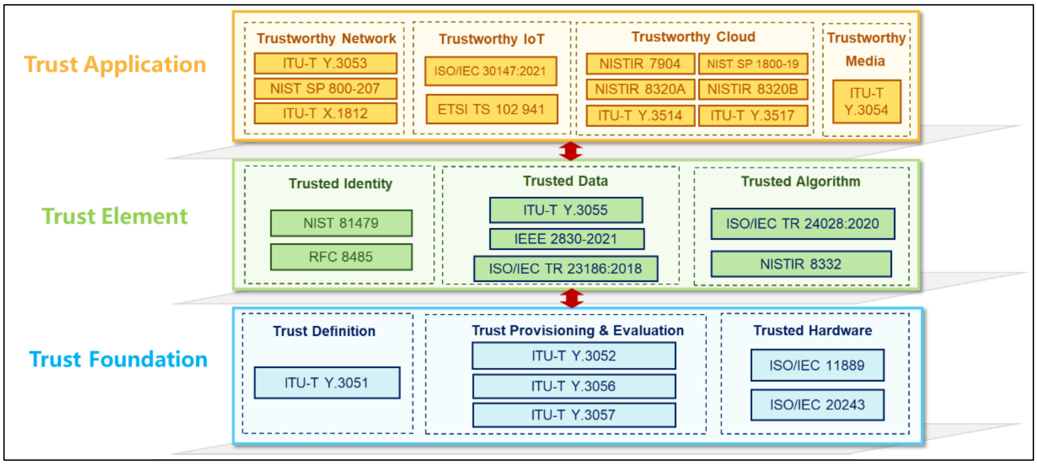

FIGURE 2. Overview of trust standards for communication networks and future digital world.

B. TRUST PROVISIONING AND TRUST EVALUATION

Trust and the related trusted environment are crucial to the development of Information and Communication Technology (ICT). In order to establish trust between entities, it is necessary to have interoperability and information security provided by a trusted environment in the ICT infrastructure. This helps entities to reduce risks and uncertainty by using trust to predict the results of interactions.

ITU-T Y.3051, defined in 2017 by ITU-T SG13, provides a formal definition of the trusted environment which aims to offer a desired level of confidence and protection to entities. This recommendation defines the trusted environment as an environment that provides a set of technical and regulatory conditions that allows the establishment of trust between interacting agents within the environment. The recommendation also highlights the requirements needed to build such a trusted environment, including concerns on predictability, information security, interoperability, and availability of administration services. Furthermore, the recommendation outlines the basic principles of trusted environment on both technical and legal aspects, which refines the concept of a trusted environment. This recommendation provides a thorough conception of the trusted environment in ICT infrastructure and services for further implementation of trust in different scenarios.

ITU-T Y.3052, on top of the trusted environment defined in ITU-T Y.3051, proposes a trust framework for trust provisioning in ICT infrastructures and services. It aims to resolve security issues caused by a lack of trust in ICT. The framework categorizes trust into direct trust and indirect trust based on the conception of trust. It introduces the obligation of trust based on the analysis of risk in several circumstances in ICT, along with the elaboration of the concept and fundamental characteristics of trust in the context of trusted ICT infrastructures and services. The recommendation then describes models for trust provisioning, including social trust, cyber trust, and physical trust. It also provides a trust evaluation framework, as well as a detailed trust provisioning process based on these models and the concept of trust.

ITU-T Y.3056 focuses on future distributed ecosystems that require open access to trusted services and mutual identification, authentication, and authorization. To meet these requirements, the security capabilities of devices and the underlying network must be considered, along with the standardization of related inferences and processes in ICT infrastructures. ITU SG 13 proposes a framework for bootstrapping devices and applications in the ecosystem by network operators, taking into account the security capability of network operators responsible for connecting users and devices to the Internet. This framework allows network operators to share their network security capabilities with users and service or equipment providers to achieve open and secure access interactions in the ecosystem. The recommendation also provides a reference model and a functional architecture beyond the requirements to illustrate the elements, functions, reference points, and security parameters of provisioning the bootstrapping capabilities. At the end, the information flow is provided to demonstrate the operation of bootstrapping processes.

Building on the trust provisioning model provided in ITU-T Y.3052, ITU SG 13 extended the concept of trust evaluation and proposed a trust index model for ICT infrastructure and services in ITU-T Y.3057. This model provides an approach for trust evaluation that covers different characteristics of trust, such as trustworthiness, reliability, and security. The trust index is an overall accumulation of trust indicators that reflects the evaluation and measurement of the trust degrees of entities. ITU SG 13 also defined a set of trust indicators based on the characteristics of trust and fundamental criteria for trust evaluation. These trust indicators are categorized into objective trust indicators and subjective trust indicators to cover both objective and subjective trust.

C. TRUST HARDWARE

The root of trust is the foundation of the chain-of-trust in a system upon which the security and reliability of high-level functions, features, and operations depend. As the root of trust is deemed absolutely trustworthy, a common approach is to implement it in hardware, which is considered immune to malware attacks due to its inalterability [9].

One system component that can enhance platform security and enable trusted computing by establishing trust is the Trusted Platform Module (TPM). The TPM-based hardware solution for roots of trust can overcome the limitations of software-based solutions in resisting malware. The Trusted Computing Group (TCG) defines the architecture, data structures, command interface, and behavior of TPM in ISO/IEC 11889, regulating the interaction between the host and the TPM.

In the trusted platform, TCG defines a mechanism for establishing trust by identifying hardware and software components on the platform to ensure the trustworthiness of the platform and the services it provides. This mechanism requires TPMs to provide three types of roots of trust (RoT) under hardware protection: measurement, storage, and reporting. These RoTs describe the characteristics that impact a platform's trustworthiness with the minimum necessary functionality. The Root of Trust for Measurement (RTM) is designed to reveal the software running on the platform in a trusted manner. The Root of Trust for Storage (RTS) is primarily responsible for creating, managing, and keeping encryption keys and other data values. The Root of Trust for Reporting (RTR) helps external entities establish trust in platform software measurements or encryption keys with the proof of the presence of a value in the TPM. These three types of RoT are implemented by TPM components.

TCG provides a generic library of commands, cryptographic algorithms, and TPM capabilities in the remaining standards for flexible implementation and to meet various global requirements in different deployment scenarios. However, the factors that affect trustworthiness in hardware can be the product of vulnerabilities or lack of robust hardware support [9]. These two issues can be traced back to the supply chain, where products are initially designed and produced. Maliciously tainted products may have backdoors that allow adversaries to launch attacks, while the integrity of counterfeit products cannot be verified. To mitigate the risks posed by tainted and counterfeit products, The Open Group has proposed the Open Trusted Technology Provider Standard (O-TTPS) in ISO/IEC 20243. The standard addresses a set of guidelines, requirements, and recommendations for suppliers and providers to resolve problems arising from tainting and counterfeiting that may threaten the integrity of Commercial Off-the-Shelf (COTS) ICT products throughout their life cycle.

III. TRUST ELEMENT

The trust element layer encompasses standards related to the three essential components of the future digital world and communication networks. In our view, all activities in the future communication networks and digital world can be considered as a form of digital "transaction" in a broad sense. Such a transaction comprises three elements: identity, data, and algorithm. As illustrated in Fig. 3, a digital transaction is carried out by a designed algorithm that processes input data and generates output data, involving different entities with unique identities. The successful execution of a digital transaction heavily relies on trust and trust relationships among various components and parties. Therefore, trusted identity, trusted data, and trusted algorithm are crucial in ensuring the trustworthiness of future communication networks and digital transaction.

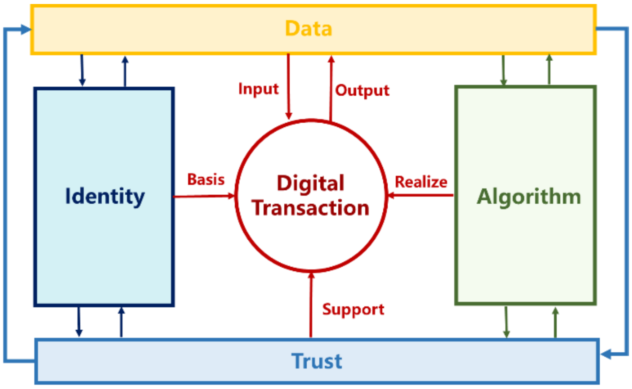

FIGURE 3. Illustration of a digital transaction.

A. TRUSTED IDENTITY

Identity is a crucial element in the digital world, as every entity must be authenticated before being granted access. However, managing digital identities can be complicated and burdensome for current systems. Federated identity is a solution that centralizes user trust in a federated identity provider and uses a single-use token from a trusted identity provider to grant users access to services. This simplifies user access and mitigates the risk of identity theft, as users only need to register their personal information once with the identity provider. However, trust among entities in the identity ecosystem is still vital, and different service providers may have different risk management procedures, making it challenging to manage identity federation risks [10].

To address these challenges, NISTIR 8149 introduces the concept of a trust framework that supports the establishment of mutual trust among entities in identity federations. The trust framework has four components: system rules, legal structure, establishing conformance, and recognizing conformance. System rules specify technical requirements, security requirements, and required identity management operations in identity federations, while the legal structure ensures that members of federations are legally bound. Establishing conformance provides assessments and methodologies for members to evaluate their conformances, and recognizing conformance describes several mechanisms, including registry or listing services, trust marks, and digital certificates, for communication, conformance recognition, and trust establishment in federations.

Another important standard related to digital identity is IETF RFC 8485. This RFC focuses on the measurement of trust in digital transactions. There are two approaches to measuring trust in digital identity transactions: combining all indicators to a single scalar value or evaluating the detailed set of attribute data locally to make trust decisions. However, these approaches have limitations, such as limited information trust values and the requirement for identity providers and rely parties to process data. To address these limitations, RFC 8485 presents the Vector of Trust (VoT) framework. A VoT contains four orthogonal components: identity proofing, primary credential usage, primary credential management, and assertion presentation. The sample applications and metrics of VoT are also provided in the document.

B. TRUSTED DATA

The importance of data, especially personal data, has been growing rapidly with the development of related technologies. However, the increasing frequency of data breaches has posed a significant challenge to the trust relationships between different stakeholders involved in data management. For instance, users expect that the parties collecting and processing their personal data are trustworthy and capable of safeguarding their privacy. At the same time, companies rely on user data to make decisions and provide better services [11]. The mistrust between stakeholders regarding data integrity and privacy has resulted in an overall untrustworthy personal data ecosystem.

To address this issue, ITU-T has published the recommendation Y.3055, which proposes a trust-based personal data management framework (TPDM). The framework categorizes stakeholders into personal data principles, personal data controller, personal data processor, and third parties. It defines the phases of personal data flow as the personal data management phase, data collection phase, and data management phase. The TPDM framework outlines the architecture and requirements for each function involved and proposes a trust provisioning mechanism to enhance trust between stakeholders in data management. The objective is to achieve a trustworthy personal data ecosystem by balancing data utilization and privacy protection.

Another critical issue related to trusted data is the isolated data island problem, which arises due to regulations, competition, or ethical considerations that prevent different datasets from being combined. IEEE 2830-2021 proposes a framework for trusted execution environment (TEE)-based shared machine learning (SML) to enable large-scale, multi-source data sharing and analysis. This framework enables multiple participants to collaborate in machine learning model training and provides technical and security requirements for TEE-based SML to ensure trust and security.

Isolated data also exists in cloud computing due to regulations and policies, especially as industrial cloud for common purposes is taking shape. ISO/IEC TR 23186:2018 presents a trust framework for the cloud processing of multi-sourced data, which mitigates trust issues between cloud service providers (CSP), cloud service customers (CSC), and cloud service users (CSU) in the processing of multi-sourced data. It outlines the data use obligations and controls, data provenance, chain of custody, security, and immutable proof of compliance as elements of trust and provides a data flow for trusted processing of multi-source data. The trust framework also demonstrates the importance of trust in critical areas such as transportation and automation.

C. TRUSTED ALGORITM

The reliability and trustworthiness of the future digital world are dependent on the algorithms that power it. Most algorithms in use today are based on artificial intelligence (AI), but users struggle to trust the decisions made by AI because of the lack of transparency in the decision-making process. AI is often considered a ''black box'' that users cannot understand. As a result, trusted algorithms face challenges such as transparency, explainability, accuracy, and reliability [12].

To address these challenges, current standards regulate AI from both the user and AI's perspective. ISO/IEC TR 24028:2020 provides an overview of trustworthiness in AI, discussing possible approaches to mitigating vulnerabilities and challenges while improving trustworthiness of AI systems. The standard identifies specific standardization gaps in the field and surveys current threats and risks to AI systems that may impact overall trustworthiness. The standard suggests that trust can be established through transparency, explainability, controllability, and more. Trustworthiness assessments are recommended based on the characteristics of trustworthy AI, which include availability, resiliency, reliability, accuracy, safety, security, and privacy.

On the other hand, NISTIR 8332 focuses on user trust in AI. It analyzes trust challenges in AI systems and introduces an approach to calculate user trust in AI. The calculation involves the pertinence and sufficiency of AI trustworthy characteristics, as well as user experience in AI systems. The ranking of each characteristic may differ based on the occasion of AI systems. NIST believes that accountability, objectivity, and explainability are also important characteristics to consider, while availability is considered less important. Usability is measured by efficiency, effectiveness, and user satisfaction.

IV. TYPICAL TRUST APPLICATION SCENARIOS

At the top of the trust framework is the trust application layer, and numerous standard organizations have published a range of standards to guide and regulate the application of trust. In this section, we will discuss four typical trust application scenarios covered by existing standard.

A. TRUSTWORTHY NETWORK

The traditional network security model assumes that all entities inside the network are trusted, while entities outside the network are untrusted and require authorization to access the network [13]. However, this approach is vulnerable to internal attacks since adversaries who have gained access to the network are considered trusted. To address this issue, ITU SG 13 proposed a framework of trustworthy networking with trust-centric network domains in ITU-T Y.3053. This recommendation describes a conceptual model of trustworthy networking that involves identification, trust evaluation, and trustworthy communication. Entities within the network domain rely on identification and trust evaluation to authenticate the entities they interact with and perform trustworthy communication. In contrast, NIST introduces the idea of zero trust and proposes a framework of zero trust architecture (ZTA) deployment in enterprise environments in NIST SP 800-207. Zero trust assumes that there is no implicit trust granted to network elements based on their physical or network location or ownership. Instead, strict verification is required for every entity before accessing the network or resources. ITU-T X.1812 is another standard closely related to trust networking, which describes application scenarios of 5G systems and analyzes the stakeholders and their trust relationships for each scenario. X.1812 proposes a security framework supported by a trust model that is designed based on trust relationship mapping, and the trust level and criteria for the trust model are also clarified in the recommendation.

B. TRUSTWORTHY IOT

Compared to traditional devices, IoT devices, such as sensors, have unique ways of interacting with the physical world and require different management and security approaches due to hardware and architectural limitations [14]. The current common security approach for IoT is to create closed networks that only allow devices from the same manufacturer to join, which ensures trust based on the manufacturer's reputation but goes against the idea of an interconnected world. To address this issue, the concept of trustworthy IoT has been proposed as a promising solution.

The ISO/IEC JTC 1/SC 41 has proposed a trust framework for IoT systems and services in ISO/IEC 30147:2021 to achieve trustworthy IoT systems by introducing system life cycle processes in the implementation and maintenance of trustworthiness in IoT systems. The document focuses on the challenges in IoT systems that were not covered previously and specifies the characteristics of trustworthiness, including security, reliability, safety, privacy, and resilience, as well as the risks associated with each characteristic in IoT systems. By refining and customizing the implementation of system life cycle processes in IoT systems based on ISO/IEC/IEEE 15288:2015, IoT systems can achieve trustworthiness from the dimensions of the above characteristics.

As an important use case of IoT systems, Intelligent Transport Systems (ITS) face a trade-off between user data utilization and privacy protection. Therefore, TC ITS presents a framework of trust and privacy management in ITS communication in ETSI TS 102 941 V2.1.1 to enhance security and build trust and security in ITS environments. The document summarizes the required trust establishment and privacy management for supporting a secure ITS environment, clarifies the relationships between entities and elements of the ITS reference architecture, and lists required security services for privacy management in ITS, such as ITS lifecycle management, Public Key Infrastructure (PKI), and trust provision. For each security service, the document classifies the considerations, requirements, and implementation details in actual deployment scenarios.

C. TRUSTWORTHY CLOUD

As one of the service delivery models, Infrastructure as a Service (IaaS) greatly simplifies provisioning and management by abstracting hardware and allowing users to purchase server, network, storage, and more as a service without worrying about deployment complexities [15]. However, security and privacy of workloads have been a concern in the current multi-tenant cloud environment. Each workload needs to be isolated to avoid mutual interference and access. Also, the migration of workloads between different cloud servers is sometimes restricted by local relevant policies and laws, which demands trusted geolocation to determine the restriction of cloud servers.

Therefore, NIST proposed a solution that combines hardware root of trust and trusted compute pool to realize trusted geolocation while deploying and migrating workloads between different cloud servers within a cloud. NIST suggested that organizations implement an automated hardware root of trust, along with the host's unique identifier and platform metadata in the hardware of cloud servers to access geolocation information and enforce and monitor geolocation restrictions. Such an approach could guarantee the integrity of geolocation information and platform with the assumption of tamper-resistant hardware and firmware. Besides, a trusted compute pool is required to achieve different workloads' isolation by aggregating trusted systems and separating them from untrusted resources. The proof of concept implementation of the solution is proposed in NISTIR 7904. Based on this solution, National Cybersecurity Center of Excellence (NCCoE) develops NIST SP 1800-19, which describes the approach, architecture, and security characteristics of this solution in detail with an evaluation of how such a solution could provide the necessary security capabilities. It also provides a sample solution with deployment details and prototype. NISTIR 8320A and NISTIR 8320B elaborate on how the solution of trusted compute pool leveraging hardware root of trust with workload orchestration could be implemented to protect application container deployments in multi-tenant cloud environments instead. Workload orchestration could ensure that containers can only be instantiated on server platforms from satisfactory locations that meet trustworthiness. Issues of decryption keys and initial encryption of container images may also be involved in orchestration.

ITU-T Y.3514 published by ITU SG 13 specifies the required security mechanisms and overall trust framework to support the establishment of trusted inter-cloud relationships among multiple cloud service providers (CSPs). The concept of interconnected multiple clouds, or "cloud of clouds," addresses the issue of limited resources in a single cloud. Such a concept allows CSPs to cooperate with one or more CSPs with relationship patterns of peering, federation, or intermediary to maximize utilization of cloud resources. Interoperability and portability are highlighted for CSPs. Trusted relationships between CSPs and cloud service consumers (CSCs) or within multiple CSPs are essential to achieve trusted inter-cloud computing successfully. Also, different security levels shall be considered in the management of trusted inter-cloud depends on the technology that CSCs and CSPs deploy. In Y.3514, the necessities and properties of trusted inter-cloud relationships are specified. The requirements according to the characteristics of governance, management, resiliency, security, and confidentiality of trusted inter-cloud computing are included.

Isolation and confidentiality issues are the main security threats in inter-cloud systems. The potential problem from the CSP's perspective is a malicious user who threatens the virtualization layer, isolation, server, and more. The potential problem from the CSC's perspective is data security and privacy. On top of ITU-T Y.3514, ITU-T SG13 expands the management framework of trusted inter-cloud computing and provides an overview of trust management in an inter-cloud environment in ITU-T Y.3517 to mitigate risk from the threats mentioned above. This framework involves isolation and security management mechanisms based on distributed cloud management and enumerates scenarios for the implementation of such solution.

D. TRUSTWORTHY MEDIA

The modern media environment has undergone significant changes with the development of ICT, resulting in various content sharing methods. In the past, the media environment was more like broadcasting, with users participating as receivers, and media service providers such as broadcast and mass media acting as senders. This limited content sharing to the users, while the senders were mostly trusted and reliable by the mass audience [16]. However, today's platforms such as YouTube and TikTok allow users to participate as both senders and receivers, making content sharing more open and accessible. This freedom has made the environment highly complicated and risky, as it is difficult for users to evaluate the trustworthiness of those they interact with. Even adversaries could be users themselves and act maliciously. This situation not only affects the relationship between sender and receiver but also impacts the trust relationship between service provider and service consumer (user).

ITU-T SG 13 has identified potential risks in three categories: threats to media services, threats to content, and threats to user privacy in ITU-T Y.3054. Current media service providers are not equipped to counter these risks and create a trustworthy and safe content sharing environment, as most of them rely on limited rating and comment mechanisms. Therefore, ITU-T SG 13 proposed a framework for trust-based media services to overcome these limitations. The objective is to identify and mitigate potential risks by preventing potential adversaries from performing malicious actions, which requires predictability and reliability from media service providers. This framework enables media service providers to evaluate and utilize user trust by collecting, analyzing, and modeling user data with trust management and trust models.

V. FUTURE WORK AND CONCLUSION

The persistent efforts towards standardizing trust have laid the foundation for shaping the future digital world. However, despite the progress made, there are still gaps that require resolution and implementation. It's evident from the available information that most of the current trust-related standardization works primarily focus on network and computing, but the specific fields that each standard emphasizes are distinct. ITU and IETF are working on standardization in different fields, with ITU mainly focusing on trust in networks and IETF on TEE and related protocols. Nevertheless, there are still several standardization gaps that need to be addressed.

For example, present standards in media only offer a solution to mitigate risks in the trust relationship between different stakeholders in the media environment. The content on media platforms also plays a vital role in influencing the trust of service providers and content providers, and standardization is needed to evaluate the trustworthiness of content. In addition, the popularity of trust modeling has led to the development of various trust models with different approaches. However, the performance of these trust models may be impacted by different circumstances, and a general metric is therefore required to standardize these trust models' quality evaluation. Furthermore, the rapid evolution of satellite networks has introduced new challenges in trust management and trust modeling for future space-air-ground integrated networks. In this context, standardization becomes essential to ensure consistent trust evaluation and management across various network components, fostering a secure and reliable communication infrastructure among space, aerial, and ground systems.

In conclusion, this paper has provided a comprehensive overview of the state of the art in trust standardization by grouping trust-related standards by fields and evaluating the critical issues they have resolved. Furthermore, this paper offers suggestions and discussions beyond the overview to address the gaps in trust standardization.

REFERENCES

[1] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrated model of organizational trust," *Acad. Manage. Rev.*, vol. 20, no. 3, pp. 709–734, Jul. 1995.

[2] K. Thompson, "Reflections on trusting trust," *Commun. ACM*, vol. 27, no. 8, pp. 761–763, Aug. 1984.

[3] R. Hardin, *Trust and Trustworthiness*. Newbury Park, CA, USA: Sage, 2002, pp. 29–32.

[4] 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.

[5] Y. Wang, X. Kang, T. Li, H. Wang, C.-K. Chu, and Z. Lei, ''SIX-trust for 6G: Towards a secure and trustworthy 6G network,'' 2022, *arXiv:2210.17291*.

[6] J. M. J. Valero, P. M. S. Sánchez, M. G. Pérez, A. H. Celdrán, and G. M. Pérez, ''Toward pre-standardization of reputation-based trust models beyond 5G,'' *Comput. Standards Interfaces*, vol. 81, Apr. 2022, Art. no. 103596, doi: 10.1016/j.csi.2021.103596.

[7] C. Benzaïd, T. Taleb, and M. Z. Farooqi, ''Trust in 5G and beyond networks,'' *IEEE Netw.*, vol. 35, no. 3, pp. 212–222, May/Jun. 2021, doi: 10.1109/MNET.011.2000508.

[8] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, ''A survey on trust models in heterogeneous networks,'' *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2127–2162, 4th Quart., 2022, doi: 10.1109/COMST.2022.3192978.

[9] Y. Jin, ''Introduction to hardware security,'' *Electronics*, vol. 4, no. 4, pp. 763–784, Oct. 2015.

[10] T. K. Frederiksen, J. Hesse, A. Lehmann, and R. T. Moreno, ''Identity management: State of the art, challenges and perspectives,'' in *Proc. IFIP Int. Summer School Privacy Identity Manage.*, Mar. 2020, pp. 45–62.

[11] L. L. Pipino, Y. W. Lee, and R. Y. Wang, ''Data quality assessment,'' *Commun. ACM*, vol. 45, no. 4, pp. 211–218, Apr. 2002.

[12] S. Lockey, N. Gillespie, D. Holm, and I. A. Someh, ''A review of trust in artificial intelligence: Challenges, vulnerabilities and future directions,'' in *Proc. 54th Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2021, pp. 5463–5472.

[13] C. Leuprecht, D. B. Skillicorn, and V. E. Tait, ''Beyond the castle model of cyber-risk and cyber-security,'' *Government Inf. Quart.*, vol. 33, no. 2, pp. 250–257, Apr. 2016.

[14] J. Voas, R. Kuhn, P. Laplante, and S. Applebaum, ''Internet of Things (IoT) trust concerns,'' NIST, Gaithersburg, MD, USA, Tech. Rep. 1, 2018, pp. 1–50.

[15] S. Iqbal, M. L. M. Kiah, N. B. Anuar, B. Daghighi, A. W. A. Wahab, and S. Khan, ''Service delivery models of cloud computing: Security issues and open challenges,'' *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4726–4750, Nov. 2016.

[16] J. Strömbäck, Y. Tsfati, H. Boomgaarden, A. Damstra, E. Lindgren, R. Vliegenthart, and T. Lindholm, ''News media trust and its impact on media use: Toward a framework for future research,'' *Ann. Int. Commun. Assoc.*, vol. 44, no. 2, pp. 139–156, Apr. 2020.

HUILIN WANG is currently pursuing the B.Comp. degree in information security with the National University of Singapore. The article was accomplished during her internship which mainly focused on trust and trust modeling in communication network with the Digital Identity and Trustworthiness Laboratory, Huawei Singapore. Her research interests include digital security and network security.

XIN KANG (Senior Member, IEEE) received the Ph.D. degree from the National University of Singapore. He is a Senior Researcher with the Huawei Singapore Research Center. He has more than 15 years of 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 has also filed more than 60 patents on security protocol designs and has contributed more than 30 technical proposals to 3GPP SA3. He received the Best Paper Award from IEEE ICC, in 2017, and the Best 50 Papers Award from IEEE GlobeCom, in 2014. He is an Initiator and the Chief Editor of 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 of experience. 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 a PC member for many security conferences. He is an influential speaker in industrial security forums.

ZHONGDING LEI (Senior Member, IEEE) is 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 a Laboratory Head and a Senior Scientist with the Agency for Science, Technology, and Research (A-STAR) of Singapore, where he has 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.

CHENG-KANG CHU (Member, IEEE) received the Ph.D. degree in computer science from the National Chiao Tung University, Taiwan. He is a Senior Researcher with Huawei International, Singapore. Before joining Huawei, he was a Research Scientist with the Cryptography and Security Department, Institute for Infocomm Research (I2R), Singapore. He has a long-term interest in the development of new technologies in applied cryptography, cloud computing security, and the IoT security. He has published many research papers in major conferences and journals. His current research interests include mobile security, the IoT security, and decentralized digital identity. He received the Best Student Paper Award in ISC 2007. He also served as the program committee member for many international conferences.

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 was a Research Engineer/Scientist with I2R Singapore, in 2001. He is an Expert on identity management and network security. He joined Huawei, in 2013, where he is currently a Senior Researcher.