Design of an Intelligent Trust Management Architecture for 5G Service Deployment

Samra Bouakkaz[1,2][a], Luis Suárez[1][b], Nora Cuppens[1][c] and Frédéric Cuppens[2][d]
[1] Computer Engineering and Software Engineering, Polytechnique Montreal, Canada
[2] Ericsson, Saint-Laurent, Canada
{samra.bouakkaz, luis.suarez}@ericsson.com, {nora.cuppens, frederic.cuppens}@polymtl.ca

Keywords: 5G Security, Trust Management Architecture, Trustworthiness Assessment, Trust Model.

Abstract: The security of 5G networks relies on trust, but managing this is challenging due to their dynamic nature and lack of a unified trust framework. Current research focuses on trust evaluation mechanisms, neglecting a comprehensive architecture. Hyperscale Cloud Providers (HCPs) are crucial in securing 5G network deployment, especially with virtualization. To enhance cloud service adoption, HCPs must demonstrate trust and security while addressing end-user and industry concerns. This paper's primary contribution is the design of a comprehensive intelligent trust management architecture rather than focusing solely on specific implementations for particular 5G use cases. It serves as a blueprint for integrating and managing various trust evaluation methods within a single framework, making it flexible and adaptable for successful 5G service deployment. We instantiate our architecture within 5G networks to tailor it to specific methods and techniques best suited for different scenarios. Furthermore, we animate its dynamic adaptation to various 5G use cases, showcasing real-time changes in trust levels and strategies to ensure secure and reliable service delivery.

1 INTRODUCTION

The 5G network is a technology platform that enables new services and business models across various sectors. Open-source innovation, utilizing virtualization technologies, automation, and elasticity, has driven the expansion of cloud infrastructure services. Initially focusing on the enterprise market, cloud providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform offer economies of scale and flexibility in resource allocation. Communication Service Providers (CSPs) adopt a hybrid and multi-cloud approach to lower ownership costs and accelerate their market entry (Alonso et al., 2022). As cloud providers evolve into Hyperscale Cloud Providers (HCPs), they deliver faster services, greater capacity, and massive scalability, which allows network operators to optimize their service delivery and business models (Zhang et al., 2019). Telecommunication partnerships must build trust to enforce security requirements, protect information sharing, and comply with policies, while HCPs must address end-user and industry concerns in cloud service adoption. Trust management in the evolving network landscape faces challenges such as a lack of a unified architecture, inconsistencies in trust models, and difficulties accommodating emerging technologies like AI-driven automation and edge computing. Scalability issues in large-scale 5G environments and a lack of real-time solutions to security threats are also significant issues. However, trust is confidence in others' abilities, which helps facilitate smooth collaboration within a network. Trustworthiness refers to an entity's demonstrated qualifications, capabilities, and reliability (Scarfone and Hoffman, 2007). To address these, we propose a new architecture for real-time monitoring, dynamic adjustments, and scalability in the 5G ecosystem, ensuring the trustworthiness of the 5G ecosystem. To our knowledge, this paper is the first to design a comprehensive Intelligent Trust Management Architecture for 5G services, using HCPs as the primary shared infrastructure. The 5G-TMA modules addresses four key contributions, which are addressed by specific modules as follows:

1. Propose a trustworthiness assessment model for 5G stakeholders by collecting real-time data to evaluate trust in their relationships.
2. Propose a trust assessment framework that generates a dynamic trust model fostering adaptable re-

[a] https://orcid.org/0000-0001-5852-4956
[b] https://orcid.org/0000-0002-7831-9252
[c] https://orcid.org/0000-0001-8792-0413
[d] https://orcid.org/0000-0003-1124-2200

Bouakkaz, S., Suárez, L., Cuppens, N. and Cuppens, F.
Design of an Intelligent Trust Management Architecture for 5G Service Deployment.
DOI: 10.5220/0013252200003899
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 310-317
ISBN: 978-989-758-735-1; ISSN: 2184-4356
Proceedings Copyright © 2025 by SCITEPRESS – Science and Technology Publications, Lda.

lationships and permitting only trustworthy stakeholders to maintain high trust.

3. Propose Trust Lifecycle Management (TLM) among trustworthy entities by establishing, assessing, and revoking trust relationships, ensuring trust stays dynamic and responsive.
4. Finally, it enhances decision-making, entity behavior understanding, system reliability by enabling proactive responses to trust issues.

This paper is organized as follows: Section 2 offers an overview of related research. Section 3 presents a use-case scenario. In Section 4, we explain the proposed 5G-TMA; in this section, 5, we discover the integration of 5G-TMA within the 5G architecture. Section 6 provides an example of how this 5G-TMA can be instantiated, followed by a demonstration of its animation in Section 7. We discuss future directions in Section 8, and Section 9 presents our final thoughts.

2 RELATED WORK

Network operators can collaborate with cloud infrastructure and specialized service providers to enhance service delivery and make network capabilities available to third-party providers (Maman et al., 2021). This collaboration will significantly impact business models and the dynamics of the mobile market, necessitating the establishment of new trust relationships in security design. Trust, defined as the belief that one entity excels in a specific task or action, is essential in communication and networking to mitigate risks (Svare et al., 2020). Zhang et al. (Zhang et al., 2019) highlighted the importance of trust management in 5G systems, emphasizing collaboration between network operators and vertical service providers to create and manage trust. This collaboration is essential for enabling secure and efficient identity management. The new trust model requires additional security measures, including authentication, accountability, and non-repudiation. Valero et al. (Valero et al., 2023) developed a reputation-based trust framework using PeerTrust that predicts trust scores based on stakeholder behavior patterns. These scores are adjusted according to breach predictions, detections, and violations. It emphasizes trust in deployment services, highlighting its importance in 5G adoption, reliability, transparency, and stakeholder accountability, as it is a strategic goal for the ecosystem's success. Wary et al. (Wary et al., 2019) point out the complexity of managing trust in 5G, as it involves monitoring both the network's and the service's reliability. The competition among providers offering various guarantees and trust levels makes implementing a dynamic and intelligent system necessary. Collaboration between CSPs and HCPs is crucial for deploying cloud-native 5G Network Functions (NFs), focusing on trust to enhance stakeholder cooperation and data exchange. Current trust management approaches are inconsistency-prone and lack scalability for multi-tenant and multi-domain scenarios. A more sophisticated trust management architecture and scalable mechanisms are needed to address these issues to adapt to evolving conditions and emerging threats.

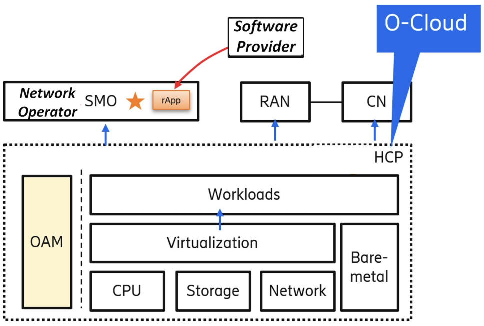


Figure 1: Use case: instantiating an rAPP within an SMO.

3 USE CASE: rApp IN SMO

In this motivating scenario (refer to Figure 1), a Mobile Network Operator (MNO), which is a telecommunications service provider, utilizes a Service Management and Orchestration (SMO) system to manage its Radio Access Network (RAN). The SMO hosts rApps, software applications designed to operate on the Non-Real Time RAN Intelligent Controller (Non-RT RIC). These applications aim to automate various RAN management and optimization tasks, functioning with control loops that take effect over a time scale of one second or longer. The MNO plans to deploy a rApp developed by a software provider through its instantiation over the HCP. The SMO components are instantiated in the HCP, allowing the rApp to access the Network Functions (NFs) within the RAN. In this context, several interesting questions arise:

- How to assess trustworthiness evidence from HCPs?
- How does the MNO choose the appropriate HCP based on high confidence?
- How can a relationship of trust can be built continuously between trustworthy parties?

4 THE PROPOSED 5G-TMA

We design a generic trust management architecture for a 5G network (5G-TMA) to support various use cases requiring different levels of trust, security, and reliability, consisting of four main modules (M1, M2, M3, and M4), each making specific contributions, as illustrated in Figure 2.

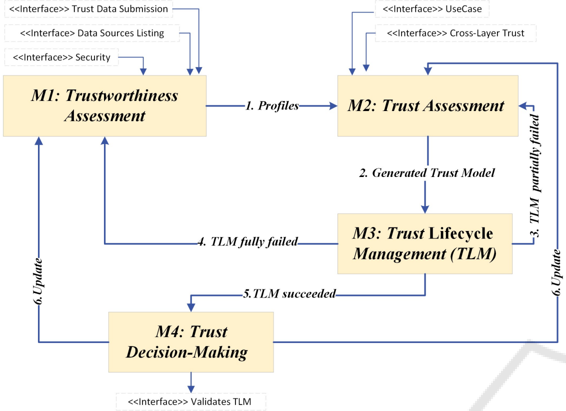

<<Interface>> Trust Data Submission
<<Interface> Data Sources Listing
<<Interface>> Security
<<Interface>> UseCase
<<Interface>> Cross-Layer Trust
M1: Trustworthiness Assessment
1. Profiles
M2: Trust Assessment
2. Generated Trust Model
3. TLM partially failed
M3: Trust Lifecycle Management (TLM)
4. TLM fully failed
5.TLM succeeded
6.Update
6.Update
M4: Trust Decision-Making
<<Interface>> Validates TLM

Figure 2: The Proposed 5G-TMA.

1. The Trustworthiness Assessment Module. The 5G ecosystem requires meticulous collection and analysis of trust evidence to promote global technology adoption and mitigate security and privacy risks. We begin with the first sub-contribution, which is proposing the trustworthiness model of 5G stakeholders. The model uses a trust-based fuzzy logic system to gather, assess, and organize evidence on trust metrics, security, and data sources through various interfaces to create trust profiles with all scores related to trust for each stakeholder. The trustworthiness assessment module consists of three interfaces: Trust Data Submission Interface, Data Source Listing Interface, and Interface Security Mechanisms. The Trust Data Submission Interface allows nodes to share information about their interactions with network providers or services, enabling third-party recommendations and indirect trust assessments. The Data Source Listing Interface presents available data sources related to trust, helping stakeholders determine how to utilize the trust framework effectively. The Interface Security Mechanisms ensure secure interactions between network functions using secure API access tokens and endpoint protection. However, the model's effectiveness in identifying trust strategies and relationships among HCPs for 5G service deployment is limited, necessitating an additional assessment for improvement. The first module collects trust information from each 5G stakeholder, compiles it into a trust profile, and sends it to the second module for further analysis.

2. The Trust Assessment Module. We propose a trust assessment framework that integrates game theory (GT) predictive capabilities with reinforcement learning (RL) adaptability. The framework evaluates the trust relationships among 5G stakeholders and creates a trust model to determine their eligibility for partnerships in deploying 5G services. This model adapts to the evolving landscape of 5G technology, allowing stakeholders to adjust trust strategies in real-time for successful deployment and operation. It supports a dynamic trust decision-making process, fostering strong stakeholder relationships. It includes several key interfaces. The UseCase interface for 5G-TMA demonstrates how different layers and components interact with 5G-TMA for trust validation, scoring, and policy enforcement. The Cross-layer Trust interface also allows communication between the service layer and 5G-TMA, facilitating dynamic policy enforcement and adjustments to trust scores.

3. The Trust Lifecycle Management Module. Based on the generated trust model, stakeholders entering into partnerships are considered trustee partners. It is essential to assess how trust information is exchanged among these partners, which occurs in several phases known as trust lifecycle management (TLM). This process involves managing the trust relationships among stakeholders participating in the trust model, including the phases of trust establishment, evaluation, maintenance, and revocation, as detailed in Section 6.3.

4. The Trust Decision-Making Module. In trust relationships, reward and punishment mechanisms are used to monitor stakeholders' behaviors in real-time. Trust scores are recalculated after new events, such as security threats, policy changes, service-level agreement (SLA) violations, service execution failures, and time decay. Negative events decrease previous trust scores, helping to identify more reliable stakeholders, while positive events contribute to increased trust scores. Implementing effective internal policies can help maintain trust in established relationships.

5 INTEGRATION THE 5G-TMA IN 5G ARCHITECTURE

The Business Support System (BSS) is a crucial component of a telecommunications network owned by the Network Operator. It manages customer business operations. Additionally, the BSS oversees Radio Access Network (RAN) applications (referred to as rApps) to enhance operational capabilities and improve network efficiency. The Control Plane Network Function (NF) is responsible for managing network

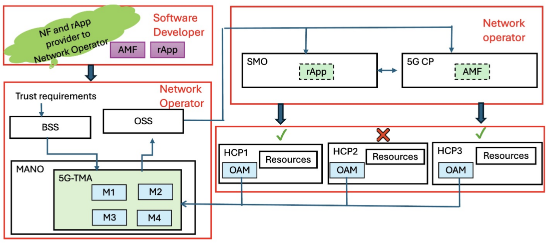


Figure 3: Integration of 5G-TMA in 5G Architecture.

operations and data flow, while the Access and Mobility Management Function (AMF) focuses on user mobility and session management. The BSS initiates workflows to deploy necessary network functions, with the Management and Orchestration (MANO) system handling the orchestration of this deployment process. The BSS establishes a well-coordinated workflow to meet specific service requirements, with the MANO system coordinating these requests for optimal performance. The Network Operator oversees the BSS, Operations Support System (OSS), and MANO, implementing a strategic plan to deploy rApps within the SMO and NF in the Control Plane (CP). The 5G-TMA is designed to collect and process information from the Operations, Administration, and Management (OAM) entities distributed across various HCPs. This data collection takes place when the 5G-TMA modules (M1, M2, M3, and M4 as shown in Figure 2) perform their specific functions within the proposed 5G-TMA architecture. M2 is particularly important in this process, as it determines which HCP(s) should be selected based on the current requirements and conditions. Once M2 has made the selection, it communicates with the OSS to instruct it to deploy and instantiate the relevant applications, known as rApps, along with the AMF. This deployment occurs within the selected HCPs, ensuring that the necessary resources and functionalities are available to support optimal network performance and service delivery.

6 5G-TMA INSTANTIATION

This example demonstrates how to instantiate our architecture in 5G networks, adapting it to the appropriate methodologies and techniques for each use case's unique requirements and challenges.

6.1 Instantiate Trustworthiness Assessment Module

Trustworthiness is often evaluated using qualitative and ambiguous metrics like reliability and reputation, which are challenging to measure with traditional logic systems. Conventional probabilistic methods, such as Bayesian inference (Wong, 2019) or Markov models, struggle to accurately quantify trust relationships (Nefti et al., 2005). The fuzzy logic system effectively addresses uncertainty and imprecise information, which are the challenges of trustworthiness. It allows for evaluating trust metrics that are not strictly binary (such as low, medium, and high), offering a more nuanced and continuous output. Inputs like reputation, reliability, historical behavior, and security metrics are assessed using fuzzy rules to generate a trust score. These rules mimic human reasoning by skillfully handling vague and incomplete data (Ampririt et al., 2021).

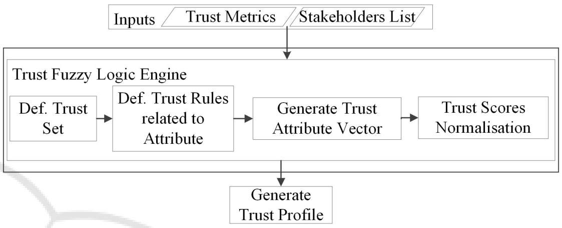


Figure 4: Module I: Trustworthiness Assessment based on Fuzzy Logic.

The fuzzy system as illustrated in Figure 4 consists of four main components: System Inputs, Fuzzification, Fuzzy Inference Engine, and Defuzzification. System Inputs are variables analyzed to make decisions in uncertain scenarios concerning trust metrics. Fuzzification determines the degree of membership for each input within various trust sets. The Fuzzy Inference Engine processes fuzzy inputs based on defined trust rules, producing trust membership degrees. Defuzzification converts these outputs into a deterministic format called a trust profile. Fuzzy trust sets represent varying levels of trust among 5G stakeholders, with their corresponding membership functions. A trust profile structure is used to evaluate a stakeholder's trustworthiness, including stakeholder identification, overall trust score, trust metrics, contextual details, recommendations, and a timestamp. The context highlights strengths and areas for improvement, while the recommendations offer strategic enhanced trustworthiness and mitigate risks.

6.2 Instantiate Trust Assessment

Trust in network systems often relies on rational expectations and cooperation from trusted entities; incomplete information can complicate the confirmation process. We propose a framework that combines GT and RL to address these trust issues. GT analyzes strategic decision-making interactions that can lead to conflicting outcomes, while RL helps agents understand the consequences of their actions and enhances their decision-making abilities. Trust-based RL optimizes interactions by adjusting trust levels based on the actions and decisions of others. Deep Reinforcement Learning (DRL) (Xiong et al., 2019) and GT together can tackle complex problems in dynamic environments characterized by high stakeholder mobility. We propose a dynamic trust model specifically designed for 5G stakeholders. This model is tailored to various use cases and effectively addresses the complexities of trust relationships in advanced 5G networks. It allows stakeholders to adjust their strategies in real-time, fostering trust and cooperation that are essential for the successful deployment and operation of 5G networks. As illustrated in Figure 5, the trust assessment module evaluates the trust levels among various 5G stakeholders and their relationships within a partnership. Its primary goal is to identify effective strategies for successfully deploying 5G services. This module creates a dynamic trust model by employing predictive GT and adaptive RL. It utilizes trust profiles, network metrics, and global data to identify stakeholders involved in a trust-based partnership. Furthermore, it assesses their trust relationships to develop a comprehensive trust model for collaboration.

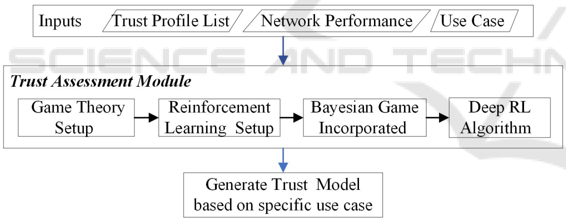


Figure 5: Module II: Trust Assessment Based on GT & RL.

Step 1- Setup of Bayesian Game. Bayesian game theory predicts trust strategies among 5G stakeholders aligned with partnership objectives, considering their private information and beliefs to optimize utility and foster trusting relationships.

- The 5G ecosystem comprises stakeholders denoted as $P = \{p_1, p_2, \ldots, p_n\}$, including network operators and HCPs, each characterized by a type θ_i, encompassing their capabilities, strategic preferences, and trust profile. Each stakeholder P_i has a trust strategy set, S_i, based on quantitative measures for decision-making, with the distribution function $F_i(\theta_i)$ representing initial assumptions about other stakeholders' private information in space $\mathcal{S}$.
- Each stakeholder has a payoff function, represented by $u_i : S_1 \times S_2 \times ... \times S_n \to \mathbb{R}$, which maps a combination of trust strategies to a real number representing the payoff to the stakeholder, denoted as player p_i. This function considers the individual stakeholder and others' strategies, considering trust-related aspects.

Step 2: Setup the DRL. The State Space $\mathcal{S}$ represents all possible trust states observed by RL agents within 5G stakeholders, including public perceptions of different trust types and conditions. Each state $s \in \mathcal{S}$ represents a vector of trust-related variables $s = \{v_1, v_2, ..., v_n\}$, and the Reward Function $R(s,a)$ offers immediate rewards for actions a and states s, combining economic benefits and trust-related outcomes.

Step 4: DRL Algorithm. DRL is a machine learning technique that enables agents to make optimal decisions without prior knowledge of the system or environment. It aims to maximize long-term rewards by learning from past experiences. A trust model is developed by integrating RL to optimize dynamic trust strategies, reacting to current situations, and anticipating future states based on stakeholder trust behaviours. GT provides structured insights into effective trust strategies, enhancing the learning process within the RL process.

6.3 Instantiate TLM

The Trust Life Cycle Management (TLM) in Figure 6 facilitates collaboration among partners by establishing trust agreements for data exchange and interaction among 5G stakeholders. The MNO identifies potential HCPs like AWS, Google Cloud, and Microsoft Azure, establishes trust requirements based on regulatory standards, business needs, and security policies, issues digital certificates, manages credentials, implements access control policies, and conducts continuous checks to ensure only authorized HCPs can access the network and sensitive data.

Maintaining trust requires continuously monitoring and analyzing behavior, collecting feedback, and enforcing strict access controls. We assess risks to identify potential threats and vulnerabilities associated with each HCP, using quantitative trust metrics to evaluate their trustworthiness. Additionally, we conduct compliance checks to ensure that HCPs adhere to defined trust policies and regulatory standards. We also respect ZTA to verify every access request. Trust evaluation involves updating policies based on trust assessments, adjusting reputation scores, and considering thresholds. If an HCP is found to be non-compliant or poses a security risk, their credentials and access rights will immediately be revoked. Inci-

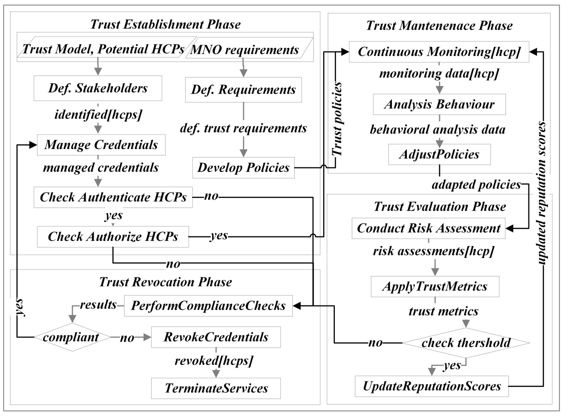


Figure 6: Trust Life Cycle Management Phases.

dent response procedures will be activated to address any breaches of trust and mitigate potential impacts on the network and services. Revoking trust means terminating the services provided by HCPs that are no longer trusted or needed and ensuring that all data is handled securely. Specific procedures are in place to ensure that HCPs leave the system without compromising network security or data integrity.

7 5G-TMA ANIMATION

The 5G-TMA is animated to adapt to various scenarios and demonstrate its real-world applicability. It offers context-specific trust establishment, monitoring, evaluation, and enforcement methodologies in response to 5G stakeholder changes, specifically supporting trust relationships between CSPs, MNOs, and HCPs.

1. Animate Trustworthiness Assessment Process. Data collection in O-RAN and 5G architectures involves multiple stakeholders, each responsible for specific data types. Efficient data collection and analysis are crucial for optimizing network performance, ensuring security, and delivering high-quality services. In O-RAN architecture, the Radio Intelligent Controller (RIC), including both Near-Real-Time (Near-RT) and Non-Real-Time (Non-RT) components, along with interfaces such as E2 and O1, play vital roles in data collection (Bonati et al., 2022). In contrast, traditional 5G architectures rely on Operations, Administration, and Maintenance (OAM) systems, Network Management Systems (NMS), and various network interfaces (F1, N2, N3, S1) for data collection and management (Lei et al., 2021; 3GPP, 2020; Sharma et al., 2021). These components and interfaces are designed to gather data efficiently, supporting the optimization of network performance, the maintenance of quality of service, and the facilitation of advanced network management capabilities. Trust-based fuzzy logic measures trustworthiness among partners by adjusting trust attributes and normalization processes based on specific requirements. This results in a trust profile for each partner, generated using trust contribution rules from trust metrics, as shown in Figure 7. The fuzzy set $F_R = \{L_S, M_S, H_S\}$ categorizes trust metric scores into low L_S, medium M_S, and high H_S, with membership functions 1, 2, and 3 representing the minimum l, medium m, and maximum h trust metric scores for each category.

$$L_S(x) = \begin{cases} 1 & , \quad (x <= l) \\ \frac{h-x}{h-l} & , \quad (l < x < h) \\ 0 & , \quad (x >= l) \end{cases} \tag{1}$$

$$M_S(x) = \begin{cases} 0 & , \quad (x <= l) or (x >= h) \\ \frac{x-l}{m-l} & , \quad (l < x < m) \\ \frac{h-x}{h-m} & , \quad (m < x < h)) \end{cases} \tag{2}$$

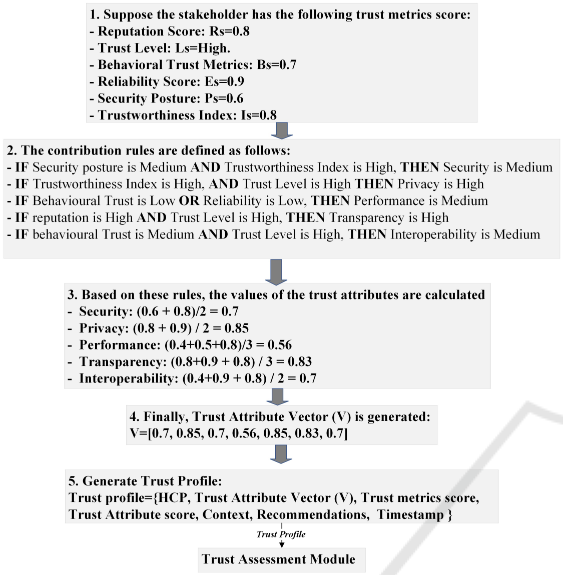
$$H_S(x) = \begin{cases} 0 & , \quad (x <= m) \\ \frac{x-m}{h-m} & , \quad (m < x < h) \\ 1 & , \quad (m < x <= h)) \end{cases} \tag{3}$$

To effectively deploy 5G services in HCPs, it is essential to consider several trust attributes: security, privacy, reliability, performance, compliance, transparency, and interoperability. Security guarantees the confidentiality of data, while privacy safeguards user information. Reliability ensures uninterrupted service. Transparency involves clear data handling policies, and interoperability allows for seamless integration with existing systems and vendor equipment. The rules determine how trust metrics such as reputation scores R_s, trust levels L_s, behavioral trust B_s, reliability scores E_s, security posture P_s, and trustworthiness index I_s contribute to trust attributes by considering expert knowledge, domain-specific requirements, and trust metric characteristics, for instance, ***If*** R_s is high ***AND*** L_s is high, ***Then*** Transparency is high. Attribute values are calculated based on their corresponding trust metrics, which are aggregated, normalized, or weighted to create a trust attribute vector for each stakeholder. This vector compiles with other information into a structure called a trust profile, as shown in Figure 7. Additionally, We proposed Table 1 to illustrate the contribution of trust metrics in trust attributes for defining rules related to them.

2. Animate Trust Assessment Process. The trust model, generated by GT and RL, considers stakeholder OAM roles as DRL agents, enabling MNOs to select HCPs for service deployment based on trust metrics like reliability and data security.

Table 1: Trust Metrics involved in the Trust Attribute.

	Trust Metrics					
Trust Attributes	R_s	L_s	B_s	E_s	P_s	I_s
Security					✓	✓
Privacy		✓				✓
Performance			✓	✓		✓
Transparency	✓	✓				✓
Interoperability		✓	✓			✓



1. Suppose the stakeholder has the following trust metrics score:
- Reputation Score: Rs=0.8
- Trust Level: Ls=High.
- Behavioral Trust Metrics: Bs=0.7
- Reliability Score: Es=0.9
- Security Posture: Ps=0.6
- Trustworthiness Index: Is=0.8

2. The contribution rules are defined as follows:
- **IF** Security posture is Medium **AND** Trustworthiness Index is High, **THEN** Security is Medium
- **IF** Trustworthiness Index is High, **AND** Trust Level is High **THEN** Privacy is High
- **IF** Behavioural Trust is Low **OR** Reliability is Low, **THEN** Performance is Medium
- **IF** reputation is High **AND** Trust Level is High, **THEN** Transparency is High
- **IF** behavioural Trust is Medium **AND** Trust Level is High, **THEN** Interoperability is Medium

3. Based on these rules, the values of the trust attributes are calculated
- Security: (0.6 + 0.8)/2 = 0.7
- Privacy: (0.8 + 0.9) / 2 = 0.85
- Performance: (0.4+0.5+0.8)/3 = 0.56
- Transparency: (0.8+0.9 + 0.8) / 3 = 0.83
- Interoperability: (0.4+0.9 + 0.8) / 2 = 0.7

4. Finally, Trust Attribute Vector (V) is generated:
V=[0.7, 0.85, 0.7, 0.56, 0.85, 0.83, 0.7]

5. Generate Trust Profile:
Trust profile={HCP, Trust Attribute Vector (V), Trust metrics score, Trust Attribute score, Context, Recommendations, Timestamp }

Trust Assessment Module

Figure 7: Generate a Trust Profile using Fuzzy Logic.

Step 1: Initial Setup. The process involves defining trust requirements, establishing an initial trust level, and forming initial beliefs based on historical performance or previous interactions. The initial beliefs of the MNO regarding the trustworthiness of each HCP range from 0 to 1, as follows:

- HCP1: Security: 0.7, Performance: 0.6, Interoperability: 0.8
- HCP2: Security: 0.5, Performance: 0.5, Interoperability: 0.7
- HCP3: Security: 0.9, Performance: 0.85, Interoperability: 0.9

Step 2: GT Model. MNOs and HCPs use GT to enhance their decision-making processes, with an emphasis on security, performance, and interoperability. MNOs focus on prioritizing robust security protocols, ensuring low latency, maintaining high reliability, and achieving seamless integration with existing systems. On the other hand, HCPs aim to improve interoperability, realize cost savings, and allocate resources effectively to boost security and performance, while also ensuring strong interoperability.

Step 3: Define Strategies. The MNO and HCP are strategizing to maximize their utility functions based on trust levels. The MNO chooses HCPs with high trust ratings. HCP1 invests in advanced interoperability standards, which moderately improve security. In contrast, HCP2 focuses on maintaining baseline performance and cost-effectiveness without significant investments. Meanwhile, HCP3 implements advanced security solutions.

Table 2: Generate trust model based final trust levels.

Cloud Provider	Security	Performance	Interoperability	Selected
HCP1	0.72	0.65	0.85	YES
HCP2	0.52	0.55	0.73	NO
HCP3	0.93	0.88	0.92	YES

Step 4: Run RL. In Trust Relationships, RL involves three components: state space, action space, and a reward function. The initial state considers security, performance, and interoperability levels. MNOs select HCPs based on trust levels, adjust investments, and reward high-score HCPs.

- HCP1: Security increases to 0.72, Performance rises to 0.65, Interoperability improves to 0.85.
- HCP2: It remains stable, with Security at 0.52, Performance at 0.55, and Interoperability at 0.73.
- HCP3: Security increases to 0.93, Performance rises to 0.88, Interoperability improves to 0.92.

The MNO's rewards are determined by the trust levels assigned to each HCPs. HCP1 receives a moderate reward for improving interoperability, HCP2 is given a lower reward due to minimal enhancements, and HCP3 is awarded the highest reward for making substantial investments across all areas.

Step 5: Final Decision. Table 2 shows that the model integrates GT and RL to dynamically adjust trust levels. This capability allows MNOs to make informed decisions, ensuring reliable service deployment for HCP1 and HCP3.

8 FUTURE DIRECTIONS

The novelty of this work is unlike existing trust evaluation mechanisms that operate in silos; it is the first to construct a comprehensive 5G trust management architecture. Our 5G-TMA integrates trust across the RAN, Core Network, and Orchestration/Management layers, ensuring end-to-end trust. The initiative aims to foster trust among various 5G stakeholders, including CSPs, service providers like HCPs, mobile network operators, and end-users. It is designed for compatibility with heterogeneous hardware, diverse vendors, and global standards (e.g., 3GPP, O-RAN). It also incorporates dynamic and context-aware trust assessment using AI/ML models that adapt to evolving network behaviors, user activities, and threat landscapes.

Trustworthiness is crucial for 5G and future 6G telecommunication services, encompassing factors like security, reliability, and safety. However, evaluating trust in a 5G environment is complex, influenced by factors like device reliability, communication behavior, and past interactions (Yang et al., 2021). Future research should explore new parameters and methods to manage trust among parties, ensuring high-trust components in telecommunication services. Development of comprehensive trust evaluation metrics and the use of machine learning and artificial intelligence are expected to improve adaptive and accurate trust evidence collection. Interoperability between 3GPP standards and O-RAN architectures can be challenging, especially when incorporating Zero Trust principles. Future research should focus on establishing standardized protocols and interfaces for trust management, including uniformly applying trust metrics and security policies across network components (Sun et al., 2022). Our plan aims to enhance the trust life cycle management in 5G and 6G networks by integrating detailed trust metrics, AI, blockchain technologies, and privacy-preserving techniques. This integration will improve trust assessments, interoperability, security, and compliance with international standards. Furthermore, we plan to establish a test bed to evaluate the framework's security, trust management, and network slice establishment performance.

9 CONCLUSION

This paper presents an intelligent trust management architecture for stakeholders in 5G services, utilizing HCPs as the primary shared infrastructure. It is designed to handle trust constraints, quantify 5G stakeholder trustworthiness, and address trust management issues in new 5G technologies and business environments. It aims to create trustworthy networks with flexibility, reliability, and scalability. We then present a scenario demonstrating our architecture's support for trust relationships between CSPs and HCPs in 5G service deployment. The architecture is extensible, accommodating multiple 5G stakeholders and providing a generic approach to assessing trustworthiness.

REFERENCES

3GPP (2020). 5g system overview. Accessed: 2024-07-02.

Alonso, A., Persson, H. S., and Kassaei, H. (2022). 5g architecture for hybrid and multi-cloud environments. *Ericsson Technology Review*, 2022(3):2–12.

Ampririt, P., Ohara, S., Qafzezi, E., Ikeda, M., Matsuo, K., and Barolli, L. (2021). An integrated fuzzy-based admission control system (ifacs) for 5g wireless networks: Its implementation and performance evaluation. *Internet of Things*, 13:100351.

Bonati, L., Polese, M., D'Oro, S., Basagni, S., and Melodia, T. (2022). Openran gym: An open toolbox for data collection and experimentation with ai in o-ran. In *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 518–523. IEEE.

Lei, W., Soong, A. C., Jianghua, L., Yong, W., Classon, B., Xiao, W., Mazzarese, D., Yang, Z., Saboorian, T., Lei, W., et al. (2021). 5g system architecture. *5G System Design: An End to End Perspective*, pages 297–339.

Maman, M., Calvanese-Strinati, E., Dinh, L. N., Haustein, T., Keusgen, W., Wittig, S., Schmieder, M., Barbarossa, S., Merluzzi, M., Costanzo, F., et al. (2021). Beyond private 5g networks: applications, architectures, operator models and technological enablers. *EURASIP Journal on Wireless Communications and Networking*, 2021:1–46.

Nefti, S., Meziane, F., and Kasiran, K. (2005). A fuzzy trust model for e-commerce. In *Seventh IEEE International Conference on E-Commerce Technology (CEC'05)*, pages 401–404. IEEE.

Scarfone, K. and Hoffman, P. (2007). Guide to secure web services. Technical report, National Institute of Standards and Technology (NIST).

Sharma, P., Jain, S., Gupta, S., and Chamola, V. (2021). Role of machine learning and deep learning in securing 5g-driven industrial iot applications. *Ad Hoc Networks*, 123:102685.

Sun, S., Repeta, M., Healy, M., Nandall, V., Fung, E., and Thomas, C. (2022). Towards 5g zero trusted air interface architecture. *arXiv preprint arXiv:2211.03776*.

Svare, H., Gausdal, A. H., and Möllering, G. (2020). The function of ability, benevolence, and integrity-based trust in innovation networks. *Industry and Innovation*, 27(6):585–604.

Valero, J. M. J., Sánchez, P. M. S., Pérez, M. G., Celdrán, A. H., and Pérez, G. M. (2023). Trust-as-a-service: A reputation-enabled trust framework for 5g network resource provisioning. *Computer Communications*, 211:229–238.

Wary, J.-P., Gaber, C., Lacoste, M., Vilchez, J. S., Chopin, M., de Oca, E. M., UMU, N. P. P., Alemany, P., Vilalta, R., Muñoz, R., et al. (2019). Intelligent security and pervasive trust for 5g and beyond.

Wong, S. (2019). The fifth generation (5g) trust model. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–5. IEEE.

Xiong, Z., Zhang, Y., Niyato, D., Deng, R., Wang, P., and Wang, L.-C. (2019). Deep reinforcement learning for mobile 5g and beyond: Fundamentals, applications, and challenges. *IEEE Vehicular Technology Magazine*, 14(2):44–52.

Yang, L., Yu, K., Yang, S. X., Chakraborty, C., Lu, Y., and Guo, T. (2021). An intelligent trust cloud management method for secure clustering in 5g enabled iomt. *IEEE Transactions on Industrial Informatics*, 18(12):8864–8875.

Zhang, S., Wang, Y., and Zhou, W. (2019). Towards secure 5g networks: A survey. *Computer Networks*, 162:106871.