electronics

MDPI

Review

Trust Evaluation Techniques for 6G Networks: A Comprehensive Survey with Fuzzy Algorithm Approach

Elmira Saeedi Taleghani, Ronald Iván Maldonado Valencia, Ana Lucila Sandoval Orozco and Luis Javier García Villalba *

Group of Analysis, Security, and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), Faculty of Computer Science and Engineering, Office 431, Universidad Complutense de Madrid (UCM), Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid, Spain; elmirasa@ucm.es (E.S.T.); ronaldim@ucm.es (R.I.M.V.); asandov@ucm.es (A.L.S.O.)
* Correspondence: javierv@ucm.es; Tel.: +34-91-394-7638

Abstract: Sixth-generation (6G) networks are poised to support an array of advanced technologies and promising high-quality and secure services. However, ensuring robust security, privacy protection, operational efficiency, and superior service delivery poses significant challenges. In this context, trust emerges as a foundational element that is critical for addressing the multifaceted challenges inherent in 6G networks. This review article comprehensively examines trust concepts, methodologies, and techniques that are vital for establishing and maintaining a secure and reliable 6G ecosystem. Beginning with an overview of the trust problem in 6G networks, this study underscores their pivotal role in navigating the network's complexities. It proceeds to explore the conceptual frameworks underpinning trust and discuss various trust models tailored to the unique demands of 6G networks. Moreover, this article surveys a range of scholarly works presenting diverse techniques for evaluating trust by using the fuzzy logic algorithm, which is essential for ensuring the integrity and resilience of 6G networks. Through a meticulous analysis of these techniques, this study elucidates their technical nuances, advantages, and limitations. By offering a comprehensive assessment of trust evaluation methodologies, this review facilitates informed decision making in the design and implementation of secure and trustworthy 6G networks.

Keywords: 6G; trust; security; privacy; evaluations methods; networks

Citation: Saeedi Taleghani, E.; Maldonado Valencia, R.I.; Sandoval Orozco, A.L.; García Villalba, L.J. Trust Evaluation Techniques for 6G Networks: A Comprehensive Survey with Fuzzy Algorithm Approach. *Electronics* **2024**, *13*, 3013. https://doi.org/10.3390/electronics13153013

Academic Editors: Sye Loong Keoh and Minghui Li

Received: 1 May 2024
Revised: 11 July 2024
Accepted: 25 July 2024
Published: 31 July 2024

1. Introduction

The foundation of 6G technology lies in integrating spatial, aerial, terrestrial, and maritime devices within an architecture powered by artificial intelligence (AI). The objective is to provide a high quality of service (QoS) universally, characterized by unprecedented data traffic densities and extensive mobile user connections. This results in increased heterogeneity and diversity among the connected entities.

However, the proliferation of interconnected devices introduces new challenges related to security, privacy, and trust [1,2]. Network services are particularly vulnerable to threats, such as distributed denial-of-service (DDoS) attacks, which can congest critical routing links and disrupt global communication. Other significant threats include SIP flooding attacks and mobile data network attacks using IP spoofing, which waste server resources and deny services to authorized users [3,4]. Conventional security measures such as encryption may prove inadequate against emerging threats.

Trust establishment in 6G networks relies on information sharing among participating entities, both directly and indirectly, to calculate trust levels. However, malevolent nodes may manipulate information prior to dissemination, leading to various forms of attacks, such as badmouthing, aimed at undermining the credibility of other nodes [1]. Additionally, the dynamic and heterogeneous nature of 6G networks renders distinguishing between

malicious attacks and inevitable device faults and link failures challenging. Therefore, assessing trust levels becomes paramount given the critical applications supported by these networks, ranging from autonomous vehicles to smart cities [1].

Robust trust assessment mechanisms enhance the security posture of 6G networks by identifying and mitigating vulnerabilities, as well as safeguarding data confidentiality, integrity, and availability. Furthermore, continuous evaluation of trustworthiness enhances network reliability and resilience, crucial for meeting the stringent requirements of latency-sensitive applications. Trust management in 6G networks necessitates efficient collection, processing, and distribution of evidence while adhering to regulatory frameworks such as the General Data Protection Regulation (GDPR) [5,6]. Reputation management, utilizing interaction data, aids in determining participants' trustworthiness, with blockchain technology offering enhanced security and reliability [7]. Additionally, trust management systems leverage reputation and trustworthiness to facilitate interactions among network entities, addressing the challenge of information asymmetry. Smart contracts serve as third-tier entities, enforcing policies and managing security, privacy, and resilience violations [1,8].

This study provides a comprehensive comparison of trust models using fuzzy algorithms. The key research contributions are:

- Comprehensive analysis of trust concepts;
- Systematic examination of trust assessment algorithms;
- Evaluation of fuzzy logic approaches.

This paper is structured as follows: Section 2 delves into the foundational concepts of trust, offering a detailed exploration of how trust is defined and perceived in a network environment. The methodology employed in this research is detailed in Section 3, outlining the systematic approach taken to gather, analyze, and synthesize relevant literature and data. Section 4 presents a thorough examination of the prevalent algorithms for trust assessment, providing insights into various existing methodologies and their applications. Section 5 is dedicated to fuzzy logic approaches to trust management, exploring the application of fuzzy logic algorithms in trust assessment across diverse network environments and offering a rigorous evaluation framework through effective metrics and comparative analysis of methods. The simulation environment used to validate these methods is also discussed. Sections 6 and 7 address open issues and outline future research directions, followed by a conclusion.

2. Trust Concepts

In the realm of 6G networks, trust represents the belief or conception held by entities, such as mobile devices (MDs), regarding the reliability and integrity of the network environment. It extends to encompass the networkwide perception of an entity's trustworthiness, termed as reputation [1]. Within the context of information technology, trust denotes the confidence placed in a dependable source, which is crucial for maintaining the integrity and security of the system. The existence of trust hinges upon the participation of entities and both quantifiable and non-measurable factors [8,9].

Trust serves as a foundational concept for the development and operation of 6G networks, which are envisaged to prioritize human-centric interactions over machine-centric processes [10]. Consequently, trust assumes paramount importance in fostering acceptance and reliance on network automation. The transition to 6G underscores the need for a holistic approach to trust establishment, integrating trust as an integral component of the network architecture [11]. Moreover, the identified security, privacy, and trust challenges within 6G networks underscore the critical role of trust in ensuring network reliability and integrity [12].

The importance of trust in the 6G ecosystem is underscored by the critical need for security and reliability, which are essential for realizing the full potential and benefits of 6G networks [13]. This emphasis on trust is further highlighted by the integration of blockchain technology, which facilitates efficient resource sharing, secure data interactions, and privacy protection [14]. Furthermore, the adoption of a software-defined zero-trust

architecture underscores the need for trust in establishing a secure and scalable security framework [15]. Early specifications of 6G concepts prioritized trust, security, and privacy, highlighting the foundational role of trust in the development of 6G networks [16].

In conclusion, trust is integral to the reliability, security, and privacy of 6G networks. Integrating trust-building mechanisms, robust security frameworks, and privacy-aware technologies is essential for the successful deployment and operation of 6G networks.

2.1. Trust Management Model

As 6G networks are anticipated to underpin a diverse array of applications, including artificial intelligence, mobile, Internet of Things (IoT), and wireless sensor networks, the necessity for a robust trust management model becomes increasingly evident [17]. Such a model is designed to facilitate, reinforce, and perpetuate trust within the network ecosystem. The foundational step in establishing a secure relationship lies in fostering trust between a trustor and a trustee. Subsequently, trust monitoring constitutes the second stage, wherein pertinent and efficacious data on trust are gathered. These data may encompass evidence derived from trustee monitoring, the compilation of the trustor's relationship history and behaviors, solicitation of recommendations from neighboring nodes of the trustee (in the absence of direct communication), or feedback obtained from other monitoring systems such as Service Level Agreements (SLAs). The third stage involves the evaluation of trust, a process that may vary based on service type and employ diverse methodologies, culminating in decision-making outcomes. The final stage encompasses the control and maintenance of trust, highlighting the dynamic nature of trust relationships. The trust model is depicted in Figure 1.

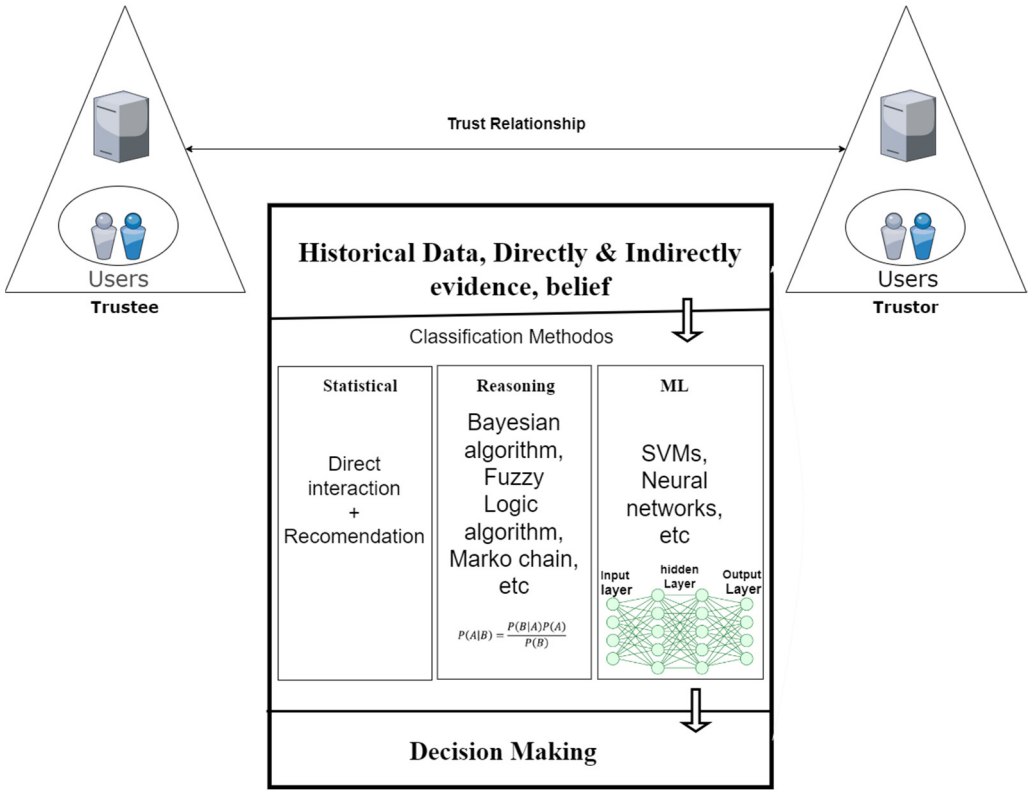

Figure 1. Trust management model.

2.2. Level of Trust Assessment

The level of trust in 6G networks encompasses the confidence and reliability attributed by users, businesses, and stakeholders to the network architecture, services, and ecosystem [12,18]. This multidimensional concept encompasses reliability, security, privacy,

ethical considerations, and the trustworthiness of ecosystem participants [8,19]. Assessing trust in 6G networks involves evaluating the network's ability to deliver reliable connectivity; safeguard data; ensure privacy; address biases; clarify algorithms; and assess the honesty and dedication of network operators, service providers, and device manufacturers [13,20,21]. The level of trust directly influences technology adoption, user confidence, and the realization of 6G networks' potential across various sectors.

Objectives

The objectives of trust evaluation in 6G networks are diverse and pivotal for ensuring the network's success and widespread acceptance. The primary objective of reliability assessment is to ensure uninterrupted connectivity, efficient management of large data traffic volumes, and continuous service availability, even in challenging scenarios [17]. Achieving this objective is critical for identifying vulnerabilities and establishing resilient network structures to enhance reliability [22].

Additionally, the security objective revolves around evaluating the effectiveness of security protocols such as encryption, authentication, and intrusion detection in mitigating cyber threats and unauthorized access [22]. Through security evaluation, stakeholders can identify and address vulnerabilities, implement robust security measures, and safeguard confidential information transmitted across the network [23].

Privacy objectives aim to assess privacy policies, data management procedures, and user consent mechanisms to protect user privacy and ensure compliance with regulations [24]. By evaluating trust in privacy protocols, stakeholders can effectively manage personal data securely and transparently, bolstering trust in the network's privacy measures.

Furthermore, ensuring ethical technology usage aims to evaluate the fairness, transparency, and accountability of AI algorithms and data analytics to mitigate biases and unethical conduct [25]. Trust evaluation fosters ethical technology deployment within the network, promoting responsible use of technologies.

Moreover, evaluating the trustworthiness of stakeholders involves assessing the adherence of network operators, service providers, and device manufacturers to established security guidelines and regulatory compliance [26]. This evaluation cultivates confidence and trust in the broader 6G ecosystem.

The overarching goal is to foster user confidence and promote adoption to establish a trustworthy network environment that meets user expectations [12]. Trust evaluation, encompassing reliability, security, privacy, ethical considerations, and stakeholder trustworthiness, plays a pivotal role in instilling user confidence, driving adoption, and unlocking the full potential of 6G networks [27].

In summary, the objectives of trust assessment in 6G networks include ensuring reliability, mitigating threats, preserving privacy, addressing ethical concerns, evaluating stakeholder trustworthiness, and instilling user confidence. Achieving these objectives is essential for developing a trustworthy network architecture that fosters user trust, encourages adoption, and facilitates successful implementation across diverse domains.

3. Methodology

To conduct this comprehensive survey on trust evaluation techniques for 6G networks with a focus on fuzzy algorithm approaches, a systematic methodology was employed to ensure thoroughness and rigor. The methodology comprises several key phases: literature review, categorization, analysis, and synthesis. Each phase was meticulously designed to build upon the previous one, resulting in a cohesive and comprehensive understanding of the current state and future direction of trust evaluation in 6G networks. The literature review phase involved defining the scope of the survey and establishing selection criteria for the literature, using keywords such as "6G networks", "trust evaluation", "fuzzy logic", "security", "privacy", and "trust" to guide the search across major academic databases, including IEEE Xplore, ACM Digital Library, SpringerLink, and Google Scholar. Only peer-reviewed articles, conference papers, and high-impact journal articles from the last

decade were included to ensure relevance and quality. Articles not directly related to trust evaluation in 6G networks, or those not involving fuzzy logic, were excluded, resulting in a curated list of significant publications.

In the classification stage, the selected articles were thematically grouped into the following primary categories: trust evaluation models, trust evaluation methods using fuzzy algorithms, categorization based on different types of networks (considering the unique criteria and challenges faced in each), and critical metrics. A comparative framework was established to systematically compare and contrast different techniques based on parameters such as scalability, privacy, dynamicity, integrity, availability, and context awareness. The analysis phase involved a critical evaluation of each article to understand the strengths, weaknesses, and unique contributions of the proposed techniques. Key methodologies, results, and conclusions were extracted, and different techniques were compared with established parameters. Through this analysis, common trends and emerging patterns in trust evaluation techniques were identified, along with gaps in current research that require further investigation. The final synthesis phase involved integrating the findings into a coherent narrative; summarizing key insights; highlighting innovative approaches, particularly those involving fuzzy logic; and proposing potential areas for future research based on the identified gaps and trends. The survey was structured to present the information logically and coherently, starting with an introduction to 6G networks and the importance of trust evaluation, followed by detailed sections on each identified category and concluding with a discussion on future research directions. Figure 2 provides a simplified overview of the study's structure.

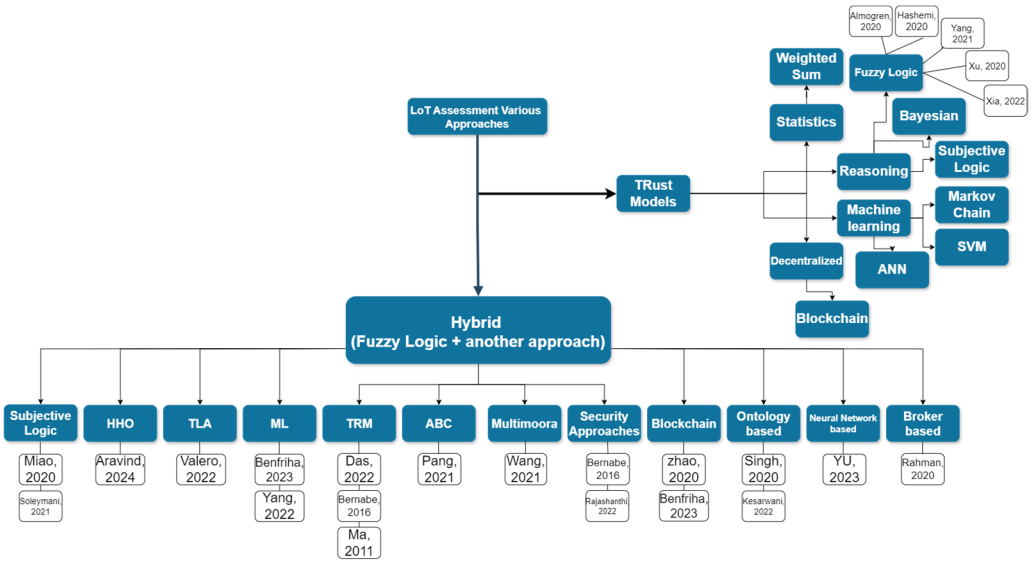

Figure 2. Outline of the study [28–49].

4. Trust Assessment Using Various Approaches

Various trust models are employed to assess the trustworthiness of 6G networks. The models encompass statistical models, reasoning models, machine learning models, decentralized models, and hybrid models. Each category provides unique benefits and factors to examine, enabling stakeholders to select the most appropriate solution depending on the resources, data, and specific requirements of the trust evaluation process.

Trust models used to assess the trust level of 6G networks go beyond the methodologies stated before. These models include reasoning models, statistical models, machine learning models, decentralized models, and hybrid models. Reasoning-based trust models employ deductive reasoning utilizing rule-based systems or knowledge graphs to determine trust relationships. These models have the capability to manage intricate interconnections, but they require manual input of domain knowledge and rule specifications. Statistical trust models employ methods such as regression analysis or Bayesian networks

to quantitatively estimate trust levels based on historical data. However, these models require a significant amount of data in order to achieve accurate results. Trust models based on machine learning utilize methods like supervised learning to automatically detect trust indications and adjust to changing conditions, necessitating sufficient training data and careful model selection.

Decentralized trust models distribute trust evaluations throughout a network, utilizing technologies such as blockchain to provide transparency and consensus, hence decreasing dependence on centralized authorities while introducing complexities [19,50]. Hybrid trust models combine logic, statistical analysis, machine learning, and decentralized features to thoroughly assess trust in 6G networks. These models use several approaches to capture different aspects of trust, resulting in a comprehensive evaluation [51]. Stakeholders have the option to select the most appropriate method by taking into account the resources, data, and specific trust evaluation requirements at hand while examining the benefits and considerations associated with each trust model category.

The trust models have played an essential role in enhancing trust in 6G networks by providing various methods to accurately assess trust levels. By using reasoning, statistics, artificial intelligence, decentralization, and hybrid methodologies, stakeholders can make well-informed choices to guarantee the reliability and security of 6G networks in a progressively interconnected and technologically advanced environment.

4.1. Statistical Methods: Weighted Sum

Weighted sum methods play a pivotal role in assessing the level of trust in 6G networks, offering several advantages in trust evaluation. These methods aggregate diverse trust parameters, such as reliability, honesty, and context-awareness, enabling a more adaptive and context-specific trust evaluation process [52]. By incorporating subjective opinions and uncertainty, weighted sum models enhance the flexibility and robustness of trust assessment in dynamic 6G network environments [53]. Moreover, these models can be tailored to specific application domains, allowing for the customization of trust evaluation criteria based on the unique requirements of 6G networks [54]. However, weighted sum methods also present challenges, such as difficulty in determining appropriate weights for trust parameters, which may introduce bias and inconsistency. Additionally, the interpretability of the weighted sum approach may be limited, as the rationale behind assigned weights may not be transparent, potentially hindering trust establishment [55,56].

4.2. Machine Learning Methods

Evaluating the level of trust in 5G or 6G networks using machine learning (ML) methods involves leveraging ML algorithms to analyze network data, model trust relationships, and enhance security mechanisms. ML methods can detect anomalies, predict security threats, and improve the network performance [57]. They can also be incorporated into federated learning frameworks to support various applications [58]. However, challenges are associated with the use of ML for trust evaluation in advanced networks. Interpretability can be a challenge, making it difficult to understand the decisions made by ML models [59]. Extensive data preprocessing, feature selection, and model training can be time-consuming and resource-intensive, affecting the scalability of ML-based trust evaluation methods [60]. Ensuring the privacy and explainability of ML models in federated learning settings requires a balance between privacy protection and model transparency [61]. In conclusion, while ML methods have significant advantages in enhancing trust and security in 5G and 6G networks, challenges such as interpretability, data preprocessing, and privacy considerations must be addressed to fully leverage the potential of ML in network trust evaluation.

Markov Chain Algorithms: Markov chain algorithm methods have been proposed for trust evaluation in 6G networks, offering versatile applications across various scenarios. Markov chain Monte Carlo (MCMC) techniques have been utilized for trust inference in peer-to-peer networks, while Markov chain-based trust management schemes have been developed for wireless sensor networks [58,62]. These methods leverage Markov chains'

capabilities to predict system parameters and analyze influence graphs, thereby ensuring the reliability and security of 6G networks [63,64]. Moreover, Markov chains have been instrumental in predicting vehicular speed changes in 6G-enabled cooperative autonomous driving scenarios, highlighting their adaptability and efficacy [65].

Support Vector Machines (SVMs): SVMs have emerged as powerful tools for trust evaluation in 6G networks, showcasing their effectiveness in classification tasks and diverse applications. In various 6G network contexts, SVMs have demonstrated superior learning accuracy, faster convergence, and improved energy consumption compared to traditional methods [66]. These models have been successfully applied in federated learning, trust evaluation in mobile ad-hoc networks, and security challenges in 6G technologies [67,68]. Moreover, SVMs have found utility in trust evaluation frameworks for online social networks, vehicular networks, and quantum machine learning algorithms, underscoring their versatility across different network domains [69,70]. Integrated into zero-trust architectures for 6G networks, SVMs contribute significantly to establishing robust security regimes [15].

Artificial Neural Networks (ANNs): ANNs are increasingly employed in evaluating trust in 6G networks due to their capacity to handle complex, non-linear relationships and learn from large datasets. ANNs excel in capturing intricate patterns and relationships within trust-related data, facilitating accurate and adaptive trust assessments [6]. Their ability to handle high-dimensional and noisy data makes them suitable for modeling the dynamic nature of trust in 6G networks [71]. ANNs can be deployed at different network layers, such as edge and cloud computing devices, for distributed trust evaluation, enhancing scalability and efficiency [71]. Nevertheless, ANNs pose challenges in terms of interpretability and computational demands, which require careful consideration in resource-constrained environments [72,73].

4.3. Reasoning Methods

Subjective Logic: Subjective logic offers a mathematical framework for evaluating trust in 6G networks, enabling the modeling and fusion of uncertain and subjective opinions [74,75]. This approach facilitates a nuanced and context-aware evaluation by incorporating subjective assessments from various sources, including network nodes, devices, and users [76]. By considering qualitative and uncertain factors such as user experiences, environmental conditions, and dynamic network behaviors, subjective logic provides a comprehensive understanding of trust levels within the network [77]. Moreover, subjective logic allows for the adaptation and learning of trust evaluations over time, enabling dynamic adjustments based on evolving subjective assessments [78].

However, the utilization of subjective logic for trust evaluation in 6G networks presents certain challenges. These include difficulties in interpreting and processing subjective assessments, the necessity to establish standardized frameworks for capturing and integrating subjective opinions, and the dynamic nature of subjective assessments [76,78]. Therefore, careful consideration of its implementation, interpretation, and processing is crucial to harness its full potential in enhancing trust and security in 6G communication systems.

Bayesian Methods: Bayesian algorithms offer another approach to evaluating trust levels in 6G networks, leveraging Bayesian networks (Bnets) to model the integration of communications, navigation, sensors, and services [79]. Through Bayesian networks, complex relationships within the network, including entity relationships, can be mathematically and graphically represented [80]. This methodology is particularly suitable for assessing trust in complex 6G networks, as it aids in mitigating malicious behavior, enhancing security measures, and establishing reliable communication channels [81].

The Bayesian approach facilitates indirect trust calculation based on the uncertainty of direct trust, effectively excluding malicious feedback and providing a robust foundation for trust evaluation in 6G networks [80,81]. By incorporating probabilistic reasoning, Bayesian methods offer a systematic and principled framework for trust assessment, contributing to the overall reliability and security of 6G communication systems.

4.4. Decentralized: Blockchain

Blockchain technology, characterized by its distributed ledger system where information is stored across multiple nodes, each possessing an identical copy of the ledger, offers a secure, traceable, decentralized, and immutable data storage solution [26]. Leveraging these properties, blockchain technology has the potential to enhance trust within network environments by ensuring the legitimacy of trust-related data. For instance, in the proposed B-RAN framework [14], which utilizes blockchain, trust relationships in wireless networks are established through an identity-based consensus mechanism. Smart contracts facilitate swift actions on the blockchain, while a hash puzzle-solving requirement for device access helps mitigate resource abuse, latency issues, and unauthorized network access. By enforcing adherence to predefined rules, this hash access scheme fosters trust between clients and network resources. Similarly, in addressing dynamic spectrum access for IoT systems, a trust evaluation mechanism proposed in [82] leverages blockchain technology to ensure privacy, information transparency, decentralized spectrum access, automatic spectrum management, and flexibility through parameterized smart contracts. Trust-related information stored in the blockchain evolves based on the consistency of cooperative measurements in IoT networks, enhancing trustworthiness.

Blockchain technology has been shown to enhances trust in 5G and 6G networks by mitigating vulnerabilities, enhancing privacy, and providing distributed trust models. Several studies have offered valuable insights to assess the level of trust in 5G and 6G networks using blockchain technology. Rahman et al. highlighted the potential of blockchain in mitigating hazards and vulnerabilities in 5G networks and enhancing privacy, trustworthiness, and dependability. Similarly, they emphasized that blockchains in 5G networks provide distributed trust models that bolster security and safeguards against breaches [83]. In 6G networks, Wang et al. introduced the SIX-Trust framework, which includes sustainable trust, infrastructure trust, and xenogenesis trust layers to ensure a secure and trustworthy network [2]. Al-Ansi et al. discussed the integration of blockchain technology in service migration to 6G networks, underlining its role in offering a secure and decentralized platform for managing migration processes [84]. Gao et al. stressed the significance of blockchain in meeting the communication and security requirements of 5G networks, such as reliability, low latency, and secure transmission [85].

The integration of blockchain technology into 6G networks presents opportunities to improve trust relationships by guaranteeing the authenticity and reliability of trust-related data [26,86]. Blockchain's inherent features of traceability, immutability, and transparency hold promise for enhancing trustworthiness and resolving data-sharing challenges within 6G networks [14]. However, challenges such as computational overheads, energy-intensive operations, scalability limitations, and potential security vulnerabilities, including threats from quantum computing, may hinder the widespread adoption and long-term dependability of blockchain-based trust assessment in 6G networks [12,86]. Additionally, regulatory and interoperability issues may need to be addressed for seamless integration [14].

In conclusion, while blockchain technology offers significant potential to enhance trust and security in 6G communication networks, a thorough evaluation of its limitations and potential challenges is essential to realize its full benefits. Despite its promise to ensure security and transparency, addressing concerns such as computational demands and security vulnerabilities will be crucial for maximizing its effectiveness in bolstering trust within 6G networks.

4.5. Comparative Analysis of Trust Assessment Methods

Various methodologies have been employed to evaluate trust levels within 6G networks, encompassing Bayesian, weighted sum, subjective logic, Markov chains, SVM, neural networks, and blockchain. Each approach presents distinct advantages and disadvantages, necessitating careful consideration for selection. Bayesian methods offer a versatile probabilistic approach to confidence assessment by integrating prior knowledge and evidence. However, they may struggle with uncertainty and rely heavily on certain

assumptions. Weighted sum techniques effectively manage uncertainty and subjective opinions, providing flexibility and customization. Nonetheless, challenges arise in determining the appropriate weights and achieving limited interpretability. Subjective logic excels in handling uncertainty and contextualized evaluation, but demands significant computational resources and encounters difficulties in defining operators. Markov chain models are beneficial for dynamic systems, but may falter in complex scenarios. Support vector machines are suitable for high-dimensional data, but require extensive tuning and lack explainability. Artificial neural networks process complex relationships, but face challenges in terms of interpretability and high computational demands. Blockchain offers decentralization and immutability, but at the expense of high resource consumption and regulatory hurdles. To select the most suitable approach for enhancing trust, security, and privacy within the 6G network ecosystem, it is imperative to weigh these strengths and limitations. Table 1 provides an overview of the advantages and disadvantages of the common trust assessment methods.

Table 1. Comparison of trust assessment techniques.

Category	Techniques	Advantages	Disadvantages
Statistics	Weighted sum	• Effective handling of uncertainty and subjective opinions • Flexibility, customization, and robustness	• Difficulty in determining weights • Limited interpretability
Reasoning	Bayesian	• Offer a versatile and probabilistic approach to trust assessment	• Cannot deal with the uncertainty of trust • Prior knowledge is hard to obtain
	Subjective logic	• Handle uncertainty and subjective opinions effectively	• Difficult to define operators • Require significant computational resources
Machine learning	Markov chain	• Useful for modeling dynamic systems	• Challenges with complex and large state spaces
	Support Vector Machines	• Applicable to high-dimensional and nonlinear data • Good generalization ability	• Poor explainability • Require extensive tuning and optimization
	Artificial Neural Networks	• Adept at processing complex, non-linear relationships • Can be deployed at different network layers	• Interpretability challenges • Computational demands
Decentralized	Blockchain	• Decentralization and consistency • Immutability and traceability	• High resource consumption: to reach a consensus • Low consensus efficiency results in low scalability

5. Fuzzy Logic Approaches in Trust Management

Fuzzy logic presents a versatile and adaptable approach to trust assessment, offering a means to quantify uncertainty within different contexts. Rooted in human decision-making processes, fuzzy logic introduces a truth concept that accommodates inaccuracies and uncertainties, enhancing the flexibility of reasoning.

The components of a fuzzy logic system (see Figure 3) comprise:

- **Fuzzification:** This initial step involves defining input and output variables, such as reliability and behavior, with linguistic terms (e.g., high, medium, low). This linguistic approach captures the inherent vagueness and imprecision in trust-related data.
- **Rule Base Construction:** Building a rule base entails formulating linguistic rules that connect input variables to output, expressing relationships between trust factors (e.g., if reliability is high and behavior is consistent, then trust is high).
- **Fuzzy Inference:** By applying these rules and fuzzy logic operators (e.g., AND, OR), the system computes a degree of trust based on inputs, considering their linguistic terms and associated rules. This process enables nuanced and flexible evaluations.
- **Defuzzification:** Converting the fuzzy output into a crisp value (e.g., low, medium, high trust) facilitates practical use or decision making, ensuring that the final trust level is comprehensible and actionable.

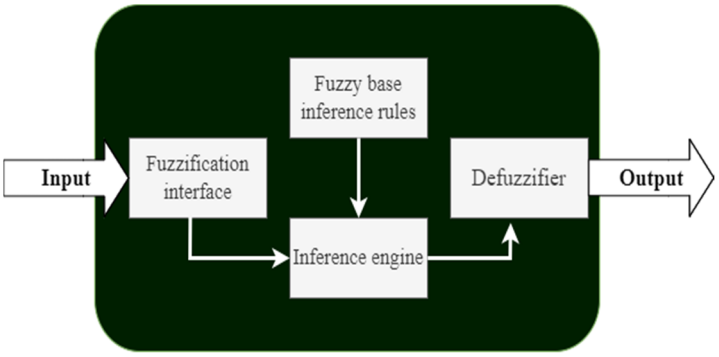

Figure 3. Fuzzy logic system (Mamdani model).

The fuzzy logic system adeptly manages the inherent uncertainty and imprecision in trust evaluation, providing an adaptive and nuanced approach to determining trust levels, particularly in complex systems like 6G networks. Evaluation of node trust in the fuzzy logic model can be achieved using various input parameters.

In the previous sections, we discussed the advantages and disadvantages of the various methods. Now, we apply the same analysis to fuzzy logic algorithms. Fuzzy logic algorithms possess distinct advantages and disadvantages inherent to this method. However, these characteristics can vary significantly when fuzzy logic is combined with other methods:

- **Advantages of Fuzzy Logic:** Fuzzy logic methodology offers several advantages for assessing trust in 6G networks. It enables trust evaluation based on experience, plausibility, and location accuracy, crucial components in trust assessment. Moreover, fuzzy logic systems have found extensive applications in various fields like web services, cloud computing, and social networks, showcasing their adaptability and utility. Additionally, fuzzy logic facilitates the development of classification criteria for assessing trust, resulting in a structured approach to trust evaluation and enhanced detection capabilities.
- **Disadvantages of Fuzzy Logic:** Despite its utility in other network applications, employing fuzzy logic for trust assessment in 6G networks presents certain drawbacks. Challenges arise in precisely characterizing and interpreting language variables and fuzzy rules, potentially leading to uncertainty and imprecision in trust assessment. Furthermore, fuzzy logic may introduce computing overhead and complexity, impacting the real-time decision-making capabilities crucial for 6G networks. Careful consideration is necessary to address these challenges and ensure reliable and robust trust management in 6G networks, particularly when incorporating fuzzy algorithms into IoT trust management techniques.

5.1. Exploring the Application of Fuzzy Logic Algorithms in Trust Assessment across Diverse Network Environments

5.1.1. IoT

Bernabe et al. proposed fuzzy logic algorithms to infer trust values for IoT devices based on multiple dimensions. The system consists of a fuzzy control system (FCS) that analyzes analog input values and generates trust values. This model enhances security by considering security evidence inferred from transactions. The system uses fuzzy logic to handle the vagueness and uncertainty of information in IoT environments and includes a lightweight and flexible access control mechanism based on Distributed Capability-Based Access Control (DCapBAC). The system's performance is evaluated in terms of trust expectations, reward requests, fuzzy trust quantification, authentication, token validation, and full trust processing [28].

This study uses a multidimensional trust model to assess trust in IoT environments, including fuzzy logic algorithms and other technologies. It considers reputation systems, which assess the reliability and historical behavior of IoT devices, and security mechanisms, which quantify the trust values. These factors help to evaluate the security posture of IoT devices and ensure secure interactions within the ecosystem. The multidimensional trust model provides a holistic assessment of trust values for IoT devices by considering factors such as reputation, QoS, security, and social relationships [28].

Hashemi et al. proposed the multi-fuzzy, dynamic, and hierarchical trust model (FDTM-IoT) as a dynamic, comprehensive, and hierarchical trust model designed to enhance routing security in IoT networks. It calculates trustworthiness in multiple dimensions, including quality of service, quality of peer-to-peer communication, and contextual information. The model is designed to be flexible and adaptable to changing environmental conditions. Fuzzy logic is used to handle uncertainty, making trust decisions more robust. The model is integrated into the Routing Protocol for Low power and Lossy Networks (RPL) protocol, enhancing security and network performance. Performance evaluations show the model's effectiveness in enhancing routing security in dynamic IoT environments [29]. This study utilizes a multistep fuzzy model to evaluate the level of trust among IoT devices.

Yu et al. introduce a fuzzy attribute trust algorithm as a supplementary approach to address trust evaluation challenges in Artificial Intelligence of Things (AIoT) networks. The fuzzy algorithm addresses the lack of interaction records and uncertainty in AIoT environments, allowing for a more accurate evaluation of smart terminals' trust values. It also mitigates mismatches between trust values and the real-time state of smart terminals. The fuzzy algorithm is scalable and adaptable, allowing for the addition of new fuzzy factors to accommodate different application scenarios. The model's performance is competitive with existing approaches, demonstrating its effectiveness in addressing trust evaluation challenges in AIoT networks. The model's performance, adaptability, and scalability contribute to its potential for enhancing the trustworthiness of smart terminals in AIoT environments [30].

In addition to the fuzzy logic algorithm, this study utilized a neural network-based trust evaluation algorithm to assess the level of trust in smart terminals within AIoT networks. A neural network, consisting of four layers, was deployed at the terminal layer of the cloud-edge-terminal collaborative AIoT trust model (CET-AoTM). It complements the fuzzy logic algorithm by evaluating trust based on historical interactions and experience attributes. This approach enhances the CET-AoTM model's trust evaluation capabilities, addressing challenges in dynamic AIoT environments and the lack of historical interaction records for new smart terminals. The neural network algorithm contributes to the overall effectiveness and accuracy of the trust evaluation, providing a comprehensive assessment of smart terminals in AIoT networks [30].

Almogren et al. presented a fuzzy-based trust management mechanism for Internet of Medical Networks (IoMT) devices. The mechanism evaluates the trustworthiness of IoMT nodes through fuzzy logic processing, identifying compromised or Sybil nodes. This

approach ensures only trustworthy nodes participate in the network, reducing the risk of Sybil attacks and enhancing overall security [31].

Aravind et al. proposed a fuzzy algorithm to assess trust levels in geographical data routing in IoT applications. The fuzzy algorithm accommodates uncertainties and imprecisions inherent in trust assessment, allowing for a more nuanced and flexible evaluation. This approach can effectively handle the dynamic and diverse nature of IoT networks, where nodes may exhibit varying levels of trustworthiness based on their behaviors and interactions. The use of fuzzy logic optimization for route selection, considering factors like QoS, trust, energy, distance, delay, and overhead, led to improved efficiency in geographical data routing in IoT applications [32].

In addition to the fuzzy logic algorithm, the paper also integrates Harris Hawk's Optimization (HHO) for optimization purposes, demonstrating its superiority in terms of energy efficiency, network lifespan, and overall effectiveness. Comparative analysis and statistical analysis demonstrate the robustness and reliability of the proposed fuzzy logic-based routing protocol. The deployment of the higher convergent HHO model for fine-tuning the membership function resulted in improved convergence and scalability, making the proposed approach suitable for long data communication networks and bulky IoT device networks. The combination improves trust evaluation and routing protocol performance by considering factors like trust, energy, distance, delay, overhead, and QoS [32].

5.1.2. Cloud Network

Kesarwani et al. proposed fuzzy logic to calculate the trust values of cloud users and service providers. The study proposes two trust-based access control models: user-based and cloud service providers-based. These models identify trusted resources for users and authorize access based on trust values. The models combine elasticity and performance evaluations to determine trust values, controlling access permissions for cloud resources. The paper also introduces subjective trust models based on user and service provider behavior, improving the accuracy and reliability of trust evaluations in cloud computing environments. The results demonstrate the effectiveness of the proposed trust-based access control models in enhancing security, resource allocation, and access control in cloud computing environments [33].

The article uses an ontology-based approach and fuzzy logic to evaluate trust in cloud computing environments. It effectively captures and represents contextual information, enhancing the accuracy and reliability of trust assessments. The study aims to develop comprehensive trust-based access control models considering various factors and parameters to evaluate the trustworthiness of users and service providers in cloud computing settings [33].

Rahman et al. presented a fuzzy-based trust evaluation framework for fog computing. Fuzzy logic is used to evaluate trust based on multiple parameters, such as performance, reliability, security, price, and reputation. The framework employs a fuzzy-based filtering algorithm to select fogs based on trust evaluation criteria such as availability, quality of service, security, user feedback, and cost. The article also highlights the importance of continuous improvement in trust evaluation mechanisms [34].

Soleymani et al. proposed a new trust management framework for multi-cloud environments by integrating fuzzy logic principles for trust calculation and a combination of subjective and objective trust evaluation. The model handles ambiguity in trust-related parameters and feedback data, allowing for a more flexible approach. The study's simulation validation confirms the effectiveness of the components, highlighting the importance of feedback evaluation and trust negotiation in improving trust values and security in multi-cloud environments [35].

Xia et al. proposed a fuzzy logic algorithm to evaluate the trust value of edge devices in a Cloud–edge–end Collaboration (CEEC) environment. The model includes four fuzzy trust factors, an incentive mechanism, trust weight allocation, and edge intelligence management. The fuzzy logic algorithm outputs the trust evaluation value (TEV), which is categorized

into Untrust, Trust-3, Trust-2, and Trust-1. The incentive score mechanism ensures the quality of collaborative evaluations and recruits high-quality edge devices for cooperation. The model's ability to detect malicious behavior, reduce error rates, and incentivize positive participation contributes to the advancement of trust management mechanisms in complex edge computing environments [36].

This study assesses trust in edge devices using the fuzzy logic algorithm in addition to a CEEC computing power architecture and the MATLAB Fuzzy Logic Library. This increases the assessment of trust, encourages collaboration, and strengthens security and dependability in networks for cloud–edge–end collaboration. Defuzzification procedures, fuzzy sets, and rules are used in the construction of the fuzzy logic algorithm [36].

5.1.3. Ad Hoc Networks

Rajashanthi et al. proposed fuzzy logic for trust evaluation in Mobile Ad Hoc Networks (MANETs). The fuzzy algorithm considers multiple network performance and security criteria, generates IF-THEN rules based on expert knowledge, and uses membership functions to map input variables to linguistic variables representing trust levels. The study evaluates the fuzzy logic approach's effectiveness in enhancing trust-based decision making for secure multipath routing, aiming to improve reliability and security in MANETs. The fuzzy algorithm's performance is evaluated in terms of its ability to enhance QoS, security, and trustworthiness in data communication [37].

This study uses a combination of fuzzy logic and secure trust mechanisms to assess trust in MANETs. Secure trust mechanisms such as cryptographic techniques, digital signatures, and secure communication protocols are used to establish trust relationships among nodes. To enhance security, encryption protocols, authentication mechanisms, and access control policies have been implemented. Machine learning techniques are also used to analyze trust-related data and patterns, thereby enhancing the accuracy and efficiency of trust evaluation processes in MANETs. The integration of these technologies and methods with the fuzzy logic algorithm aims to create a robust trust evaluation system for secure multipath routing in MANETs, thereby enhancing the reliability and effectiveness of trust assessment in dynamic wireless network environments [37].

Singh et al. proposed fuzzy classification and optimization techniques to evaluate the trustworthiness of nodes in Flying Ad Hoc Networks (FANETs). The Trust-Based Clustering Scheme (TBCS) model demonstrated improved trust evaluation, enhanced performance, and scalability. It outperformed existing models like Community of Interest dynamic Hierarchical Trust management (COI-HiTrust) and AFStrust (fuzzy logic rules prediction method), as well as a model proposed by Pushpita et al. in terms of accuracy, performance, and adaptability in FANETs. The model also outperformed cluster-based models in terms of the packet drop ratio, outperforming the AFStrust and COI-HiTrust trust models. The results and improvements in the article demonstrate the effectiveness of the TBCS model in enhancing trust, security, and performance in FANETs [38].

Benfriha et al. proposed fuzzy logic to assess drone trustworthiness in complex environments. The Fuzzy-based Unmanned Aerial Vehicles behavior analytics for trust management in FANETs (FUBA) model improves trust management in FANETs, particularly under challenging conditions like bad weather and poor signal strength. It also shows a lower error ratio. The FUBA model's scalability and practicality are addressed [39].

Miao et al. proposed a fuzzy comprehensive strategy, mutual authentication, and incentive mechanisms to ensure reliable communication, prevent malicious access, and encourage credible behaviors. It addresses security and performance aspects, enhancing privacy protection and message integrity. The scheme also introduces an incentive mechanism to encourage credible behaviors and uses lazy updates and dynamic storage structures to support On Board Unit mobility [40].

This study discusses the use of an entropy method in trustworthiness evaluation, which corrects the original weight by integrating subjective and objective factors. This approach overcomes subjectivity and ensures a more reasonable result in trust evaluation.

Combining the entropy method with fuzzy logic enhances the accuracy and reliability of trustworthiness assessment in Vehicular Ad Hoc Networks, improving the overall trustworthiness assessment process [40].

5.1.4. Wireless Sensor Networks

Pang et al. utilized a fuzzy trust model (FTM) in conjunction with the Artificial Bee Colony (ABC) algorithm to detect malicious nodes in wireless sensor networks. The FTM was used to calculate indirect trust between nodes by integrating communication attributes, data attributes, and physical attributes to address multi-attribute decision problems. The ABC algorithm was then employed to optimize the FTM for detecting dishonest recommendation attacks by considering fitness functions such as recommended deviation and interaction index deviation. By combining the FTM and ABC algorithms, the strategy aimed to enhance the security performance of the network by effectively identifying and isolating malicious nodes [41].

This study utilizes the ABC algorithm to optimize the trust model for detecting dishonest recommendation attacks. The ABC algorithm is employed to enhance the effectiveness of the trust evaluation process by optimizing the fuzzy trust model and considering fitness functions, such as the recommended deviation and interaction index deviation. Combining the fuzzy trust model with the ABC algorithm aims to improve the accuracy and efficiency of malicious node detection in wireless sensor networks (WSN) [41].

Das et al. presented a fuzzy-based approach to trust management in wireless sensor networks. The scheme uses real-time past experience, credit-based calculations, peer recommendations, and past reputations to evaluate sensor node trustworthiness. The scheme focuses on reducing communication overhead, computational time, and memory utilization by emphasizing decision making over data comparison. It also aims to establish secure communication by combining direct trust and beta reputation, ensuring only trusted nodes participate in routine activities. The paper presents simulation results to demonstrate the effectiveness of the scheme in handling malicious nodes; reducing communication and memory overhead; focusing on decision making rather than data comparison; and protecting against various attacks, such as self-promoting attacks and bad-mouthing attacks [42].

This study introduces a trust evaluation method for wireless sensors that combines fuzzy logic with reputation calculations and peer recommendations. This method considers the past behaviors and interactions of sensor nodes to assess their trustworthiness. This approach enhances the accuracy and effectiveness of trust assessments, allowing for better differentiation between trustworthy and untrustworthy nodes in a network. The combination of these methods provides a comprehensive approach to trust management in wireless sensor networks [42].

Yang et al. proposed a fuzzy logic to estimate trust levels among nodes based on past interactions, QoS metrics, and recommendations from other nodes. This approach addresses uncertainty and imprecision in trust evaluation in Industrial Wireless Sensor Networks (IWSNs), providing a more flexible and adaptive approach. Fuzzy logic also offers a smoother control surface, ensuring stable and reliable trust assessment outcomes in dynamic network environments. It also allows for adaptive trust thresholds based on varying trust levels and environmental conditions, ensuring network security. This holistic approach to trust evaluation leads to more informed decision making in cluster head selection and secure routing. The results show enhanced security, adaptive trust thresholds, energy efficiency, performance evaluation, and robust trust evaluation [43].

5.1.5. Mobile Network

Ma et al. introduced a fuzzy comprehensive evaluation method to quantify trust in dynamic trust management scenarios. The authors proposed a trust quantification algorithm that considers fuzziness and uncertainty in trust relationships, enhancing its robustness and applicability in dynamic and open network environments. The algorithm's

effectiveness is demonstrated through simulation results, indicating alignment with entity behavior. The fuzzy comprehensive evaluation method contributes to trust management by providing a systematic and effective approach to quantifying trust values, making it valuable for decision-making processes in various industries and organizations. The paper emphasizes the importance of considering fuzziness and uncertainty in trust quantification and its contribution to trust management practices [44].

The article discusses the use of credit and reputation mechanisms in trust quantification, which are integral components of the process. Credit mechanisms evaluate an entity's trustworthiness based on behavior information and interactions with other entities. They represent the evaluation result of the owner of an object on a subject after certain interactions. The reputation mechanism considers the degree of trust of an object on a subject based on multiple credit values over time. It is calculated by combining credit values from different interactions with appropriate weights. The article provides a comprehensive approach to trust quantification that considers both qualitative aspects captured by fuzzy logic and quantitative aspects represented by credit and reputation evaluations. This multi-faceted evaluation process enhances the robustness and accuracy of trust assessment in dynamic network environments [44].

Wang et al. incorporate probabilistic linguistic term sets (PLTS) to improve trust scaling by providing a more accurate and flexible way to express trust evaluations. PLTS allows decision makers to depict evaluation information using multiple linguistic terms with corresponding probabilities, capturing uncertainty and hesitancy in trust assessments. This approach contrasts with hesitant fuzzy linguistic term sets (HFLTS), which may lead to inaccuracies in reflecting expert views. PLTS also distinguishes the opinions of different recommenders more clearly, avoiding suboptimal solutions. The fuzzy algorithm used in the model handles uncertainty and vagueness in decision-making processes, allowing decision makers to express their opinions using linguistic terms representing degrees of trust or trustworthiness. The fuzzy logic helps to quantify and process subjective information, resulting in more accurate trust evaluations. The model also adopts the Multi-Objective Optimization by Ratio Analysis (MULTIMOORA) method for decision making, addresses context-dependent trust modeling, handles vagueness and uncertainty, and constructs a structural trust evaluation by decomposing trust into multiple building blocks. This comprehensive approach to trust modeling addresses the complexities and challenges associated with trust assessment in various application scenarios [45].

This study, in addition to the fuzzy logic algorithm, uses the Multi-Objective Optimization by Ratio Analysis (MULTIMOORA) method to evaluate trust levels. This robust decision-making technique combines three subordinate orders to rank the alternatives. The integration of the MULTIMOORA method with the fuzzy logic algorithm provides a comprehensive and structured approach for trust evaluation. The fuzzy logic algorithm handles uncertainty and vagueness, whereas the MULTIMOORA method fuses multiple criteria to derive a final ranking based on the trustworthiness of the alternatives. This research aims to create a robust trust evaluation model that considers various trust-related characteristics, leading to more accurate and context-aware assessments in multi-agent systems and networked environments [45].

Zhao et al. proposed a fuzzy comprehensive evaluation to assess trust among nodes in software-defined networks (SDNs). This method uses fuzzy logic to handle the complexity of node behavior, allowing for a more nuanced evaluation of trust attributes. TrustBlock also improves trust calculation by calculating trust values from direct, indirect, and historical perspectives. It uses the entropy method for objectivity and resilience to periodic attacks [46].

This study uses blockchain technology to evaluate trust levels in SDN nodes, thus enhancing the integrity and controllability of trust evaluation. The double-layer blockchain architecture is used for identity authentication, trust-value storage, consensus mechanisms, and trust-value tracking. Blockchain ensures data authenticity, irreparability, and openness, whereas the consensus mechanism filters malicious recommendation nodes and prevents

colluding attacks. The immutability of blockchains allows for the tracking of historical trust data and prevents rapid fluctuations. This robust and secure framework addresses both the reliability and security aspects of trust assessments in dynamic network environments. The TrustBlock model achieves high detection rates of up to 98.89%, an accuracy rate of 98%, and enhanced security and reliability by utilizing a double-layer blockchain architecture [46].

Xu et al. proposed a fuzzy trust mechanism that calculates trust values based on similarity, correlation, and user interaction. The mechanism uses a fuzzy comprehensive evaluation algorithm to compute fuzzy trust, considering multi-dimensional features and trust levels. The mechanism achieves personalized privacy without compromising the usability of mobile social applications. The paper also includes theoretical analysis and simulation experiments to demonstrate its effectiveness in addressing privacy concerns and providing users with control over their sensitive information [47].

Valero et al. proposed a fuzzy-based trust management system to address security and trust challenges in 5G networks. The system evaluates device trustworthiness using factors like behavior, reputation, and context. This approach handles uncertainty and imprecision in data, improving the system's accuracy and effectiveness in preventing Sybil attacks [48]. The framework successfully established trust between OpenFlow controllers and network management apps, identified malicious feedback, and introduced a dynamic trust model for Internet of Things scenarios with 89–95 percent success rates.

Yang et al. proposed a combination of fuzzy logic theory and generative adversarial learning to develop an intelligent trust management framework for 6G wireless networks. The methodology involved fuzzification to convert input trust attributes into type-2 fuzzy sets, followed by inference type reduction and defuzzification to obtain the final trust value. A dataset was prepared to train the GAN-based autoencoder, which used feature extraction, data labeling, and trust vector creation. The outcomes and enhancements demonstrated, which incorporated AI-based methods and cutting-edge trust assessment mechanisms, can increase security, resilience, and trust management in 6G wireless networks [49].

In addition to the fuzzy logic algorithm, this study uses Generative Adversarial Networks (GANs) for trust evaluation in 6G networks. GANs are a deep learning framework with two neural networks, the generator and the discriminator, trained simultaneously. The method enhances trust decision making by training autoencoders on trust-related data and synthesizing additional samples. This approach provides a comprehensive and adaptive approach to trust management in dynamic networks [49].

5.2. Effective Metrics and Comparative Analysis of Methods Based on These Metrics

In this section, we present an exhaustive analysis of trust level evaluation methodologies, with a specific emphasis on the fuzzy algorithm. Our review centers on key metrics including scalability, privacy, dynamics, integrity, availability, and context awareness, as delineated in Table 2. We aim to elucidate the efficacy and applicability of fuzzy algorithms in addressing these critical facets of trust assessment within diverse network environments. Initially, we provide brief definitions of these criteria, followed by a discussion of how each criterion is addressed in the reviewed literature.

Scalability is paramount in evaluating trust within 6G networks. Given the burgeoning demands for data rates, low latency, and reliability, scalability becomes indispensable. As 6G networks are envisioned to accommodate a vast array of connected devices and handle high data rates, an adaptable network infrastructure is imperative [87]. Furthermore, the scalability enhancements expected in 6G vis-à-vis current technologies underscore the need for scalable solutions capable of accommodating the anticipated surge in connected devices.

Integrity assumes a pivotal role in trust evaluation within 6G networks, ensuring their reliability and security. It encompasses the trustworthiness of the system, data, and entities involved, pivotal for upholding the authenticity and consistency of information within 6G networks [88]. Maintaining network integrity is fundamental for fostering trust among connected devices and facilitating the secure exchange of information, and is pivotal for the success of 6G networks.

Table 2. Comparison of trust evaluation in 6G networks by using fuzzy logic.

Category	Type	Technology	Ref.	Scalability	Integrity	Availability	Privacy	Dynamicity	Context Awareness
IoT Networks	AIoT [1]	FL and Neural Network	[30]	yes	yes	yes	-	yes	yes
	IoT [7]	FL and TRM and Security	[44]	yes	yes	yes	-	yes	Some degree
	IoT	FL	[29]	yes	yes	yes	-	yes	yes
	IoMT [6]	FL	[31]	-	yes	yes	-	yes	-
	IoT	FL and HHO	[32]	yes	yes	yes	-	yes	yes
Ad-Hoc Networks	MANETs [9]	FL and Security	[37]	-	yes	-	-	yes	-
	FANETs [5]	FL and ontology	[38]	definitely yes	yes	-	Some degree	yes	-
	FANETs	FL and ML and BC	[39]	yes	yes	-	-	yes	yes
	VANETs [10]	FL and Subjective	[40]	yes	yes	yes	yes	yes	-
Mobile Networks	SDN	FL and BC	[46]	yes	yes	yes	yes	-	-
	5G	FL	[47]	-	yes	yes	yes	yes	-
	5G	FL and TRM	[28]	-	yes	-	-	yes	-
	6GWN [12]	FL and GAN	[49]	-	yes	yes	-	yes	yes
	5G	FL and TLA	[48]	yes	yes	yes	yes	yes	yes
	5G	FL and Multimoora	[45]	yes	yes	-	-	yes	yes
Wireless Sensor Networks	IWSN [8]	FL	[43]	-	yes	yes	-	yes	yes
	WSN [11]	FL and TRM	[42]	-	yes	-	-	yes	Some degree
	WSN	FL and ABC	[41]	-	yes	-	-	yes	-
Cloud Networks	CN [3]	FL and ontology	[33]	yes	yes	yes	-	yes	-
	CN	FL and Subjective	[35]	yes	yes	yes	-	yes	yes
	CEEC [2]	FL	[36]	yes	yes	yes	-	yes	yes
	FCN [4]	FL and broker-based	[34]	-	yes	yes	yes	yes	-

[1] AIoT: Artificial Intelligence of Things, [2] CEEC: Cloud–Edge–End Collaboration, [3] CN: Cloud Networks, [4] FCN: Fog Computing Networks, [5] FANETs: Flying Ad-Hoc Networks, [6] IoMT: Internet of Medical Networks, [7] IoT: Internet of Things, [8] IWSN: Industrial Wireless Sensor Networks, [9] MANETs: Mobile Ad Hoc Networks, [10] VANETs: Vehicular Ad Hoc Networks, [11] WSN: Wireless Sensor Networks, [12] WN: Wireless Network.

Availability: The availability of 6G networks is indispensable for ensuring the reliability and accessibility of services, particularly in applications like augmented reality (AR) and virtual reality (VR) in remote healthcare settings. Moreover, it facilitates efficient and distributed intelligence through federated learning of explainable AI models, underscoring its significance in trust evaluation [89].

Privacy assumes paramount importance in the assessment of trust within 6G networks due to the sensitivity and confidentiality of the data being processed and transferred [90]. Robust privacy-aware technologies are imperative, as 6G networks are poised to handle increasingly sensitive user data, thereby elevating the risk of privacy breaches.

Dynamicity: The dynamic nature of network settings and interactions necessitates consideration when evaluating trust within 6G networks. Dynamic trust evaluation models are indispensable for effectively estimating trust levels in real time while accommodating the evolving behavior of entities and the network environment [91].

Context Awareness emerges as a crucial factor in trust evaluation within 6G networks, enhancing adaptability and intelligence. It enables systems to dynamically adjust behavior based on environmental and situational cues, thereby facilitating more intelligent and energy-efficient operations [92]. Context-aware trust models are pivotal for addressing context-based attacks targeted at IoT systems.

5.2.1. Comparative Analysis Based on Metrics

To provide a comprehensive comparison, we analyzed the different methods using the aforementioned metrics. Each method has strengths and weaknesses that can be highlighted through comparative analysis.

In [30], the authors demonstrated several aspects that align with the criteria of scalability, integrity, availability, dynamicity, and context awareness in trust evaluation:

- **Scalability**: The CET-AoTM model exhibited scalability in trust evaluation by leveraging a cloud-edge-terminal collaborative architecture. This architecture allows for the distribution of trust evaluation tasks among different layers, enabling the system to scale efficiently as the number of smart terminals and interactions increases.
- **Integrity**: The trust evaluation algorithm in the CET-AoTM model focuses on maintaining the integrity of trust values by considering factors such as historical interactions, cumulative experience attributes, and fuzzy-logic-based trust attributes. This approach helps to ensure the reliability and integrity of trust evaluations for smart terminals in AIoT networks.
- **Availability**: The demand-driven cloud–edge–terminal collaboration mechanism in the CET-AoTM model enhances availability by adapting a trust evaluation based on specific computing service requirements. This mechanism ensures that trust evaluations are available when required for different types of tasks, balancing availability with the demands of AIoT services.
- **Dynamicity**: The CET-AoTM model acknowledges the dynamic nature of AIoT environments by utilizing a fuzzy attribute trust algorithm to address uncertainty and adapt to changing conditions. This dynamic approach allows the trust evaluation system to adjust to the evolving trust requirements and environmental dynamics in AIoT networks.
- Context Awareness: The demand-driven collaboration mechanism in the CET-AoTM model demonstrates context awareness in trust evaluation by considering the specific requirements of computing tasks in the AIoT. By adapting trust evaluation based on task demands, the model exhibits awareness of the context in which trust assessments are made, enhancing the relevance and effectiveness of trust evaluations.

The study [44] addressed the criteria of scalability, integrity, and dynamicity in trust evaluation:

- Scalability: Although the scalability of the proposed method is not explicitly discussed in the provided excerpts, the use of a fuzzy comprehensive evaluation method suggests a systematic approach that could potentially be scalable to larger networks or systems.

- Integrity: By considering credit and reputation in trust quantification, this approach appears to address the integrity of trust assessments by incorporating past interactions and evaluations.
- Dynamicity: The authors discuss the dynamism of trust, credit, and reputation, indicating that the proposed method accounts for changes in trust relationships over time, aligning with the dynamic nature of trust management.

The article [29] addressed several important criteria related to the security and efficiency of routing in IoT networks. Here, we analyze the alignment of the proposed FDTM-IoT model with the criteria of scalability, integrity, availability, privacy, dynamicity, and context awareness.

- Scalability: The FDTM-IoT model demonstrates scalability by applying it to various network sizes, from small- to large-scale IoT environments. The dynamic and hierarchical structure of the model allows for the addition or removal of dimensions and sub-dimensions, making it adaptable to different network scales.
- Integrity: The trust calculations and fuzzy logic used in the FDTM-IoT model contribute to maintaining data integrity within the IoT network. By considering multiple dimensions, such as quality of service and contextual information, the model ensures that trust evaluations are comprehensive and reliable, enhancing overall data integrity.
- Availability: The FDTM-IoT model is integrated into the RPL routing protocol as FDTM-RPL aims to improve network availability by enhancing security mechanisms and performance. The model's resistance to attacks such as BLACK-HOLE, SYBIL, and RANK attacks contributes to maintaining network availability under challenging conditions.
- Privacy: While this article primarily focuses on trust-based routing security, the FDTM-IoT model's consideration of contextual information and the quality of peer-to-peer communication can indirectly contribute to privacy protection within IoT networks.
- Dynamicity: The FDTM-IoT model is designed to be dynamic, allowing for real-time monitoring of the behavior of IoT and continuous trust evaluation. The adaptability of the model to changing environmental conditions and behaviors enhances its dynamicity, making it suitable for dynamic IoT environments.
- Context Awareness: The FDTM-IoT model incorporates contextual information as a key dimension of trust evaluation. By considering contextual factors such as the mobility of things, security capabilities, and device intelligence capacity, the model demonstrates context awareness in assessing trustworthiness among IoT entities.

The research [31] addressed several important aspects of trust evaluation, including scalability, integrity, availability, privacy, dynamicity, and context awareness.

- Scalability: While this article primarily focuses on trust evaluation within this specific context, it provides a foundation for scalability by addressing the trustworthiness of interconnected IoMT devices. However, the scalability of the mechanism to larger IoMT networks or different deployment scenarios requires further investigation.
- Integrity: The trust evaluation process in the FTM-IoMT includes assessing the integrity of nodes as one of the trust attributes. By considering integrity as a key factor in trust assessment, the mechanism aims to ensure the integrity of communication and interaction within the IoMT network.
- Availability: By evaluating trust attributes and identifying compromised or Sybil nodes, the mechanism contributes to maintaining the availability of trustworthy services in the IoMT environment.
- Dynamicity: The fuzzy-based trust management mechanism in the FTM-IoMT utilizes fuzzy logic processing to dynamically assess the trustworthiness of nodes based on attributes such as receptivity and compatibility. This dynamic evaluation contributes to adapting to changes in the IoMT network and addressing potential threats.

The study in [32] addressed several important aspects of trust evaluation, including scalability, integrity, availability, dynamicity, and context awareness:

- Scalability: The use of fuzzy logic and the Harmony Search Algorithm (HHO) in the routing protocol allows for scalable trust evaluation by considering multiple factors such as energy, distance, delay, overhead, QoS, and trust. This approach enables the system to handle a large number of nodes and effectively adapt to changing network conditions.
- Integrity: By incorporating trust as one of the evaluation criteria in the routing protocol, the article ensures that data integrity is maintained during the routing process. Trust evaluation helps identify trustworthy nodes for data transmission, thereby enhancing the overall integrity of the network.
- Availability: The trust evaluation mechanism based on fuzzy logic and the HHO algorithm ensures the availability of reliable routes for data transmission in IoT networks. By selecting optimal routes that consider trust levels, the system enhances the availability of communication paths within the network.
- Dynamicity: The use of fuzzy logic and optimization algorithms allows for a dynamic trust evaluation in response to changing network conditions and node behaviors. The system can adapt to dynamic environments and adjust the trust levels based on real-time data and feedback.
- Context Awareness: The trust evaluation process considers various contextual factors, such as energy consumption, distance, delay, QoS requirements, and the trustworthiness of nodes. By incorporating these contextual parameters into the evaluation criteria, the system demonstrates the level of context awareness in trust evaluation.

In [37], the authors addressed several important aspects, including scalability, integrity, and dynamicity:

- Scalability: This study proposes a secure trust-based multipath routing system that can potentially scale large MANETs by incorporating optimal fuzzy logic for route selection. However, specific scalability aspects, such as the ability to handle a large number of nodes or network size, are not explicitly discussed in the provided excerpts.
- Integrity: The use of secure trust mechanisms and fuzzy logic for route selection indicates a focus on maintaining the data integrity within the network. By evaluating trust values based on various criteria, the system aims to ensure the integrity of the data transmission and routing decisions.
- Dynamicity: The dynamic nature of MANETs, characterized by node mobility and changing network conditions, was considered in this study. The use of fuzzy logic for trust evaluation and multipath routing suggests an adaptive approach to handling dynamic network environments.

Several crucial requirements of scalability, integrity, privacy, and dynamicity were covered in the paper [38]:

- Scalability: The detection accuracy of the model increases with network size, indicating that the scheme can effectively handle larger FANETs while maintaining trust and security.
- Integrity: The TBCS model focuses on evaluating the trustworthiness of nodes based on their behavior, which contributes to maintaining the integrity of the network. By segregating malicious nodes and selecting secure Cluster Heads, the model enhances the overall integrity of communication in FANETs.
- Privacy: This article emphasizes the importance of trust in segregating noncooperative and malicious nodes, which indirectly contributes to enhancing privacy in communication within FANETs. By identifying and isolating malicious nodes, the TBCS model helps to protect the privacy of legitimate network participants.
- Dynamicity: The scheme's performance is highlighted as better than that of existing models when dealing with high-speed nodes and an increasing number of malicious nodes, demonstrating its adaptability to dynamic network conditions.

The paper in [39] included a number of crucial factors in assessing trust, such as context awareness, scalability, integrity, and dynamicity:

- Scalability: This article discusses the scalability of the FUBA model by having each drone evaluate the trustworthiness of adjacent drones and relay this information to a ground control station. This approach efficiently restricts the dissemination of trust data and evenly distributes the computational load, thereby enabling the deployment of scalable FUBA.
- Integrity: The FUBA model aims to differentiate between legitimate and malicious drone actions, enhancing the integrity of the network by effectively evaluating and understanding node behaviors in FANETs.
- Dynamicity: The FUBA model leverages fuzzy logic to handle uncertain and dynamic data related to UAV behavior in FANETs. This approach allows for adaptability and responsiveness to evolving tactics used by malicious drones, indicating a level of dynamicity in the trust evaluation process.
- Context awareness: The FUBA model incorporates contextual information, such as weather conditions, signal strength, and historical data, to make more accurate decisions about the legitimacy of a drone's presence. This demonstrates the level of context awareness in the trust evaluation process, enabling the model to adapt to diverse operating environments and scenarios.

The research study in [40] examined various factors crucial to evaluating trust, such as availability, privacy, scalability, integrity, and dynamicity:

- Scalability: The scheme incorporates a lazy update and dynamic storage structures to support the mobility of on-board units (OBUs), which can enhance scalability by reducing the computational overhead for road-side units (RSUs).
- Integrity: By utilizing fuzzy theory and behavioral big data for trust evaluation, the scheme aims to ensure the integrity of the trustworthiness assessment in VANETs, enhancing the reliability of communication and message authenticity.
- Availability: The mutual authentication process and incentive mechanisms in the scheme contribute to ensuring the availability of trust evaluation services in VANETs and promoting continuous and reliable communication among participants.
- Privacy: The scheme provides mutual authentication with conditional anonymity between the RSU and OBU, protecting the privacy of participants while maintaining traceability in the case of disputes, thus addressing privacy concerns in trust evaluation.
- Dynamicity: The scheme considers the mobility of vehicles in VANETs and incorporates mechanisms such as lazy updates and dynamic storage structures to adapt to the dynamic nature of the network, enhancing the system's ability to handle changes and updates efficiently.

Several important variables in assessing trust were covered in the article in [46], including context awareness, scalability, integrity, availability, privacy, and dynamicity.

- Scalability: TrustBlock's use of a double-layer blockchain architecture and adaptive historical trust weight demonstrates considerations for scalability by providing a framework for managing trust values at the network scale.
- Integrity: The use of blockchain technology in TrustBlock ensures the integrity of the trust data, providing tamper-proof and irrefutable storage of trust values, which contributes to maintaining the integrity of the trust evaluation process.
- Availability: TrustBlock's approach to trust evaluation, utilizing blockchain for secure and effective trust value storage and sharing, contributes to ensuring the availability of trust-related information in SDN.
- Privacy: While this article primarily focuses on trust evaluation and security aspects, the use of blockchain technology in TrustBlock can potentially contribute to privacy preservation through secure and authenticated data storage and sharing.
- Dynamicity: TrustBlock's adaptive historical trust weight and comprehensive evaluation model reflect considerations for dynamic trust assessment, allowing for the adjustment of trust values over time based on node behavior and interactions.

- Context Awareness: The trust evaluation model in TrustBlock considers the context of node interactions and behaviors, incorporating direct, indirect, and historical trust perspectives to provide a comprehensive assessment of node trustworthiness within the context of SDN networks.

Scalability, integrity, availability, privacy, and dynamicity are critical factors in evaluating trust and were included in the study [47]:

- Scalability: Although the scalability aspect is not explicitly mentioned in the provided excerpts, the use of fuzzy trust calculations and the consideration of online and offline information suggest a scalable approach to managing trust and privacy in a network with a large number of users.
- Integrity: The Trust2Privacy mechanism focuses on preserving the integrity of users' information by allowing them to set privacy levels and encrypt sensitive data according to their preferences. This approach ensures that users have control over the integrity of their personal information even after it is shared on social platforms.
- Availability: Using cryptographic tools to protect different levels of sensitive information, the mechanism aims to balance privacy preservation with the availability of information for users.
- Privacy: Privacy preservation is a central aspect of the Trust2Privacy mechanism. By establishing a relationship between trust and privacy based on users' privacy policies and using cryptographic tools for information protection, the mechanism aims to provide users with control over their privacy settings and to ensure the confidentiality of their data.
- Dynamicity: By updating trust values based on interactions and considering changes in user relationships over time, the Trust2Privacy mechanism demonstrates a level of dynamicity in managing trust and privacy in a mobile social context.

Scalability, integrity, availability, dynamicity, and context awareness are the five key criteria addressed in this article [28]:

- Scalability: The TACIoT system is designed to be implemented on both constrained and nonconstrained IoT devices. The Trust Manager component can be deployed on devices with varying hardware capabilities, indicating the level of scalability of the system.
- Integrity: By incorporating pieces of evidence and security-related mechanisms into trust calculations, the system enhances the integrity of access control decisions and the interactions between IoT devices.
- Availability: The implementation and testing of TACIoT on real devices in a testbed environment demonstrates the feasibility of the system for practical use.
- Dynamicity: The flexibility and adaptability of the access control mechanism in TACIoT, along with the customization options for fuzzy rules and weights, suggest a level of dynamicity in the system. IoT devices can dynamically adjust their access control decisions based on changes in trust values and environmental conditions.
- Context Awareness: The trust model in TACIoT considers multiple dimensions such as reputation, quality of service, security aspects, and social relationships. By considering these contextual factors, the system demonstrates the degree of context awareness when evaluating the trust values for IoT devices.

The study [49] included a number of crucial integrity, availability, dynamism, and context awareness requirements, including:

- Integrity: The methodology aims to enhance the integrity of trust management in 6G networks by employing GAN-based autoencoders for trust decision making and incorporating synergetic detection schemes. The system can detect and respond to potential threats or integrity breaches, thereby ensuring the reliability of the trust evaluations.
- Availability: By leveraging AI techniques and fuzzy logic for trust evaluation, this methodology aims to maintain the availability of network services and data delivery.

- Dynamicity: The dynamic nature of 6G wireless networks is considered using GAN-based autoencoders that can adapt to evolving trust scenarios. The ability of the methodology to learn and analyze trust information in real time enhances its capability to address dynamic changes in network behavior and trustworthiness.
- Context Awareness: The integration of fuzzy logic for trust evaluation and adversarial learning for decision making enables the methodology to be context-aware in assessing trust levels based on specific network contexts and behaviors. Context awareness enhances the accuracy and relevance of trust evaluations in diverse network environments.

In evaluating trust, ref. [48] satisfied the following requirements: scalability, integrity, availability, privacy, dynamicity, and context awareness:

- Scalability: The proposed framework was designed to be scalable, allowing it to handle large-scale 5G networks with multiple domains and tenants.
- Integrity: The framework includes a trust management module that monitors, evaluates, and updates the trust chain generated among different network entities, thereby ensuring the integrity of the network.
- Availability: This framework includes an intra-domain module that monitors the domain network for potential threats or ongoing attacks, mitigating them if needed and if possible, and ensuring the availability of the network.
- Privacy: The framework includes a trust management module that ensures the privacy of sensitive data by monitoring and evaluating the trustworthiness of network entities.
- Dynamicity: The framework is designed to address the dynamicity of 5G infrastructure threats and multitenancy security risks, providing solutions to ensure secure and trustworthy communication in multitenant environments.
- Context awareness: The framework includes an intra-domain module that uses dynamic traffic analysis to identify attacks and vulnerabilities within the 5G infrastructure, as well as in a multi-tenant/multi-domain environment, demonstrating context awareness in trust evaluation.

Several significant scalability, integrity, dynamicity, and context awareness criteria were covered in [45]:

- Scalability: This approach allows for a scalable framework in which decision makers can customize the trust evaluation criteria based on specific application contexts, thereby enhancing the scalability of the model.
- Integrity: By incorporating probabilistic linguistic term sets and the MULTIMOORA method, the model aims to provide accurate and reliable trust assessments, thereby upholding integrity in the decision-making processes.
- Dynamicity: This model accounts for the dynamic reliability of opinions provided by recommenders and the evolving nature of trust assessments in different contexts. By incorporating dynamic trustworthiness criteria and adapting them to changing trust-related attributes, the model demonstrates the level of dynamicity in trust evaluation.
- Context awareness: By allowing the trustor to define trustworthiness criteria based on specific application scenarios, the model exhibits context awareness and tailors trust assessments according to the unique requirements of different contexts.

Several crucial factors for assessing trust were covered in the article in [43], including context awareness, scalability, integrity, availability, privacy, and dynamicity:

- Scalability: By utilizing fuzzy trust evaluation and outlier detection mechanisms, the protocol can scale effectively to accommodate a large number of sensor nodes while maintaining efficient cluster formation and secure communication.
- Integrity: By incorporating fuzzy logic, transmission overhearing, and outlier detection, the protocol enhances the integrity of the network by ensuring that trustworthy nodes are assigned leadership roles within the clusters, thereby maintaining data integrity and security.

- Availability: By balancing energy savings and security assurance in cluster head selection, the protocol optimizes resource utilization and prolongs the network's lifetime, enhancing overall availability.
- Dynamicity: The adaptive trust thresholds, outlier detection, and fuzzy-based trust evaluation methods of the protocol enable dynamic adjustments to trust levels based on changing network conditions and node behaviors. This dynamicity allows the protocol to adapt to evolving threats and uncertainties in the network environment, thereby enhancing its responsiveness and effectiveness.
- Context Awareness: The fuzzy trust evaluation method considers multiple factors and parameters, such as past interactions, QoS metrics, and energy levels, to assess the trust levels among nodes. By incorporating contextual information into the trust evaluation process, the protocol demonstrated a level of context awareness that enhanced the accuracy and relevance of trust assessments in diverse network scenarios.

In [42], the authors addressed several important criteria in trust evaluation, including scalability, integrity, availability, privacy, dynamicity, and context awareness:

- Integrity: The scheme focuses on maintaining the integrity of trust management processes by utilizing fuzzy logic for accurate decision making and by considering both direct and indirect trust factors. This ensured that the trustworthiness of the sensor nodes was evaluated in terms of integrity and precision.
- Dynamicity: The scheme's utilization of real-time past experience, credit-based calculations, and peer recommendations for trust evaluation reflects a dynamic approach to trust management, allowing for adaptation to changing network conditions and the dynamic behavior of sensor nodes.
- Context awareness: The hierarchical trust evaluation approach and the use of fuzzy logic in the scheme demonstrate a level of context awareness by considering the feedback from cluster heads of different clusters and the past reputation of cluster heads given by others. This context-aware approach contributes to a more informed trust assessment.

The study in [41] addressed several important criteria in trust evaluation, including integrity and dynamicity.

- Integrity: This method focuses on detecting dishonest recommendation attacks and ensuring the integrity of trust values exchanged between nodes. Using the FTM and ABC algorithms, the approach aims to maintain the integrity of trust evaluations and identify malicious nodes that may compromise network integrity.
- Dynamicity: This methodology accounts for the dynamic nature of sensor networks by considering factors such as node mobility, environmental changes, and node behavior variations.

The study in [33] covered a number of significant factors, such as context awareness, scalability, availability, integrity, privacy, and dynamicity:

- Scalability: This is defined as the ability of a cloud system to function well when changes occur in the volume or size to satisfy user needs. By incorporating scalability as a factor in trust evaluation, the models aim to ensure that cloud resources can be scaled effectively to accommodate varying workloads.
- Integrity: By evaluating factors such as security, performance, and user feedback, the models contribute to maintaining the integrity of cloud resources and access control mechanisms.
- Availability: In the context of cloud computing, users can access resources in the correct format and location. By assessing availability as a parameter, the models aim to ensure that cloud services are accessible and reliable for users.
- Dynamicity: By incorporating dynamic trust evaluation mechanisms, the models adapt to changing conditions and user interactions, thereby enhancing the responsiveness and adaptability of access control in cloud environments.

The study in [35] satisfied the trust evaluation criteria of scalability, integrity, availability, and dynamicity:

- Scalability: This model is designed to handle large-scale computing problems in multi-cloud environments, making it scalable.
- Integrity: The inclusion of a feedback evaluation component in the framework helps identify and rectify fake feedback, enhancing the integrity of trust values.
- Availability: The trust negotiation component of the framework facilitates the generation of service level agreements (SLAs) based on trust values, thereby enhancing the availability of cloud computing services.
- Dynamicity: This model incorporates fuzzy logic principles to handle the dynamic and uncertain nature of trust-related parameters and feedback data in multi-cloud environments, making it dynamic.

Several crucial factors in assessing trust were covered in the article [36], including context awareness, scalability, availability, integrity, and dynamicity:

- Scalability: By utilizing fuzzy logic and incentive mechanisms, the model can be scaled to accommodate varying numbers of edge devices and adapt to changes in the network environment, making it suitable for scalable trust evaluation in CEEC networks.
- Integrity: By incorporating an incentive mechanism and a negative decay mechanism, the model promotes honest and cooperative behavior among edge devices, thereby contributing to the integrity of trust evaluations in the CEEC environment.
- Availability: The model encourages continuous engagement through rewards and penalties, ensuring that trust evaluations are consistently updated and available for decision making in real-time scenarios, thus improving the availability of trust data in the CEEC network.
- Dynamicity: The fuzzy-based trust evaluation model is designed to adapt to the dynamic nature of edge-computing environments. By incorporating fuzzy logic to handle uncertainty and variability in trust factors as well as the incentive negative decay mechanism to address intermittent selfish behavior, the model can effectively respond to changes in trust dynamics and promote continuous cooperation among edge devices, demonstrating dynamicity in trust evaluation.
- Context awareness: By incorporating context-specific trust factors and incentives tailored to the CEEC network model, the model demonstrates awareness of the unique characteristics and requirements of trust evaluation in edge computing contexts, thereby enhancing context awareness in trust assessment.

Scalability, integration, availability, dynamicity, and context awareness are just a few of the critical requirements addressed in the study cited in [34]:

- Scalability: By utilizing algorithms that consider user preferences and criteria, the framework can be scaled to handle diverse user requirements and fog service offerings.
- Integrity: By ensuring confidentiality and authentication in fog services, the framework contributes to maintaining the integrity of the data and transactions within the fog computing environment.
- Availability: The framework aims to provide reliable and available fog services to users by monitoring factors such as the transmission rate, response time, and usability.
- Dynamicity: This framework can dynamically match users with trustworthy fog services by adapting to changing user requirements and fog service conditions.
- Context awareness: By tailoring fog service selection based on user-specific criteria and priorities, the framework provides an understanding of the context in which fog services are utilized.

5.2.2. Simulation Environment

Simulation and evaluation software stand as indispensable tools in the articles under review, enabling researchers to model, analyze, and validate their hypotheses, experiments, and findings. These tools serve as conduits for simulating intricate scenarios, testing pa-

rameters, and assessing the efficacy of proposed solutions within a controlled environment. Researchers typically provide detailed descriptions of the software employed, elucidating specific packages, algorithms, and models utilized in their studies. In the peer-reviewed articles surveyed in this study, sections dedicated to simulation applications and parameters are frequently included, offering insights into the methodologies employed, as illustrated succinctly in Figure 4. Such comprehensive utilization of simulation and evaluation software not only facilitates rigorous scientific inquiry, but also enhances the reproducibility and robustness of research outcomes in the field.

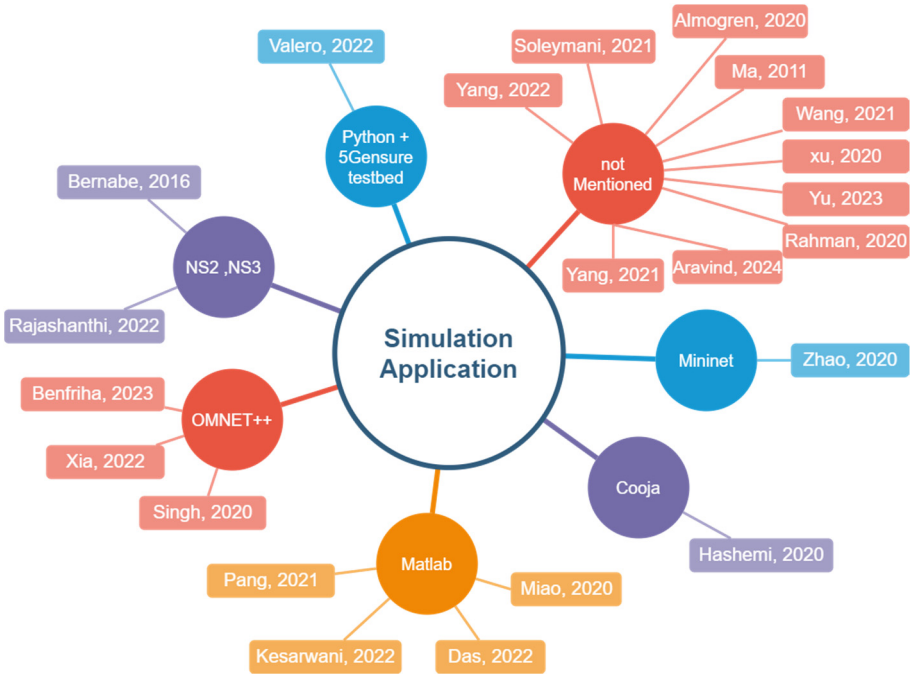

Figure 4. Simulation environments [28–49].

In the following section, we discuss the results obtained from the simulation tools referenced in the articles, specifying the names of the simulation software utilized.

In [28], Network Simulator 3 was used to simulate the implementation and testing of a trust-aware access control mechanism on constrained and non-constrained devices. The simulation results evaluate the trust model, which considers reputation, QoS, security aspects, and social relationships for computing trust values. Performance metrics such as response times, trust computation times, access control decisions, and overall system efficiency provide insights into a system's operational efficiency and effectiveness in managing trust and access control in IoT environments.

A study [29] conducted using the Cooja simulator on the Contiki 3.0 operating system revealed significant findings. This research employed performance metrics such as the average number of parent changes, packet loss ratio, and end-to-end delay to evaluate the efficiency and reliability of the proposed FDTM-RPL protocol. The FDTM-RPL protocol proved effective in mitigating major attacks on IoT networks, including SYBIL, RANK, and BLACKHOLE attacks, thereby enhancing the network performance and security. In addition, when compared to standard protocols, the FDTM-RPL protocol exhibited substantial improvements in performance across various attack scenarios and network sizes. This enhanced performance is attributed to the protocol's trust-aware routing mechanism and fuzzy-based trust evaluation, both of which collectively contribute to its robustness against common IoT attacks.

MATLAB software was used for the simulations in [33]. It used fuzzy c-means clustering to categorize users based on their trust values and behavioral parameters. Surface view diagrams were generated to visualize the trust models for both users and providers.

Trust evaluation results are presented based on performance, elasticity, security, and user feedback to determine access permissions and resource allocation in cloud environments. MATLAB software was instrumental in conducting simulations of trust-based access control models using fuzzy logic.

The study in [36] used the OMNET++ 5.6.2 simulation platform. The results showed a 19.11% improvement in the detection rate of malicious edge devices and a 16.20% reduction in the error detection rate. The Lightweight Fuzzy Collaborative Trust Evaluation Model (LFCTEM) also reduced error reporting, indicating its effectiveness in enhancing trustworthiness in CEEC networks. Comparative analysis with existing algorithms, such as the Dynamic Trust Evaluation Model (DTEM) and Fuzzy Lightweight Trust Evaluation and Evaluation Value (FLTEEV), confirmed the effectiveness of the scheme in detecting malicious behavior and improving trust assessments.

The study [37] used Network Simulator Version 2 (NS2) to simulate 250 nodes in a 1000 m $\times$ 1000 m network area. The simulation parameters included Media Access Control (MAC) type, propagation, antenna type, interference range, transmission range, simulation time, traffic source, packet size, and rate. The results showed that the proposed secure trust-based multipath routing system with optimal fuzzy logic outperformed existing techniques in terms of energy efficiency and network lifetime.

OMNET++ simulation software was used to evaluate the packet delivery ratio (PDR) performance and transmission delay under different network scenarios [38]. The results show that the PDR increases with network speed, which is attributed to frequent connection breakages. The simulation also assessed the transmission delay, analyzed how the model minimized delays, and ensured efficient communication in the FANETs. Omnet++ simulations were used to gather empirical data on the TBCS model's performance in realistic FANET scenarios, providing insights into its effectiveness in enhancing trust, security, and communication reliability in dynamic and challenging network environments.

The study in [39] was tested using the Omnet++ simulation software. The simulation involved ten Unmanned Aerial Vehicles (UAVs) and a ground control station that shared a wireless communication medium. The performance of the model was evaluated by increasing the number of UAVs in the simulation from 10 to 200. The recording module in Omnet++ tracked the end-to-end delay, providing insights into network characteristics. The model's performance was compared to established models, such as Flying Named Data Networking (FNDN) and UNION (a trust model distinguishing intentional and UNIntentional misbehavior in inter-UAV communication), to assess its effectiveness and efficiency in FANETs.

The study in [40] was tested using MATLAB 2015Ra on a laptop with Intel Core i7-8550 processors. The results showed the scheme's efficiency and effectiveness in terms of security and performance, outperforming the existing schemes in the authentication phase. The scheme achieved anonymity and traceability while minimizing the computational and time costs for each participant.

In [41], MATLAB2016a simulation software was used to evaluate the performance of a method for detecting malicious nodes in wireless sensor networks. The simulation environment was a 200 m $\times$ 200 m square area with 100 nodes divided into four clusters. The performance of the model was assessed using the recognition rate and false-positive rate metrics. The results show that the FTM-ABC strategy maintained a high recognition rate and low false-positive rate, even with a 50% number of dishonest nodes, indicating its robustness and reliability in detecting malicious nodes.

In [42], MATLAB was used to simulate a 50 min hierarchical trust management scheme in wireless sensor networks. The simulations evaluated its impact on network behavior, trust levels, and overall performance, validating its effectiveness in enhancing the security and reliability of wireless sensor networks.

In [46], which used a double-layer blockchain architecture for trust evaluation in SDNs, a detection rate of up to 98.89% was achieved in simulations using Mininet and the POX controller. This high detection rate demonstrates the ability of the model to identify and

mitigate potential security threats, thereby enhancing the overall robustness and reliability of SDN systems.

The study in [48] used the 5GENSURE testbed to evaluate the security properties of data flows in 5G and beyond networks. The results provide insights into the effectiveness of the proposed framework in addressing the security challenges in network slices in multi-domain scenarios. The analysis of security properties helped to assess the framework's performance in dynamic network environments, demonstrating its practical applicability and effectiveness in 5G multi-domain scenarios.

6. Open Issues

As we envision the future of trust management in 6G networks, several promising avenues for further research and development emerge. One such direction involves exploring hybrid trust evaluation models that amalgamate fuzzy logic algorithms with machine learning techniques. This integration holds the potential to bolster the accuracy and efficiency of trust assessment processes significantly. Additionally, investigating the incorporation of emerging technologies like artificial intelligence and blockchain into trust management frameworks could yield innovative solutions for fortifying the security and dependability of 6G networks.

Scalability and dynamicity: Future research endeavors should focus on devising trust assessment systems capable of accommodating the scalability and dynamic nature of evolving network architectures. By adapting to fluctuating network conditions and escalating complexities, research efforts can ensure the continued effectiveness of trust management systems.

Privacy-aware technologies: Addressing the paramount concern of safeguarding sensitive user data and mitigating the risk of privacy breaches necessitates the development of advanced encryption techniques, secure data-sharing protocols, and privacy-preserving mechanisms. Despite its critical importance, this area remains relatively underexplored and warrants dedicated research efforts to enhance the confidentiality and integrity of user information in 6G networks.

Context-aware trust models: Dynamic adjustments in behavior based on environmental and situational cues are imperative for enhancing the adaptability, intelligence, and energy efficiency of 6G networks. Future research endeavors should explore the seamless integration of context-awareness into trust evaluation frameworks, thereby facilitating real-time decision making and augmenting the trustworthiness of network interactions.

Newcomer nodes solution: Another critical aspect that demands attention is the evaluation of trust for newcomer nodes. As newcomers join the network, determining their initial trust value becomes challenging due to the lack of availability of relevant information. Future work should address this challenge by devising methodologies to evaluate trust for new nodes effectively.

Overall, the future trajectory of trust management for 6G networks hinges on leveraging cutting-edge technologies, enhancing the robustness of trust evaluation models, and confronting the evolving challenges posed by next-generation network environments. By pursuing these avenues of research, we can pave the way for the realization of secure, reliable, and resilient 6G networks.

7. Conclusions

The exploration of trust and security in 6G networks underscores the pivotal role of trust management in safeguarding security, ensuring reliability, and upholding privacy. The study sheds light on the potential vulnerabilities introduced by malevolent nodes and the dynamic, heterogeneous nature of 6G networks, underscoring the need for adaptive and resilient trust evaluation methodologies. Thus, this review not only provides a nuanced understanding of trust evaluation techniques using the fuzzy logic algorithm, but also offers valuable insights for informed decision making in designing and implementing secure and trustworthy 6G networks. Through comprehensive research, various approaches have been

investigated, with particular attention paid to the fusion of the fuzzy algorithm with other evaluation methodologies. Synergizing the fuzzy algorithm with complementary methods holds the potential to yield more robust solutions. Moving forward, strategic utilization of fuzzy logic algorithms alongside the integration of AI and blockchain technologies is advocated to cultivate a secure and efficient 6G ecosystem, thereby paving the way for a future characterized by heightened trust and resilience in communication networks.

Author Contributions: Conceptualization, E.S.T., R.I.M.V., A.L.S.O. and L.J.G.V.; methodology, E.S.T., R.I.M.V., A.L.S.O. and L.J.G.V.; validation, E.S.T., R.I.M.V., A.L.S.O. and L.J.G.V.; investigation, E.S.T., R.I.M.V., A.L.S.O. and L.J.G.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the EU Horizon Europe programme PRIVATEER under Grant Agreement No. 101096110. This work was also funding by the Ministry of Economic Affairs and Digital Transformation and the European Union—NextGenerationEU under UNICO R&D Advanced 5G and 6G Program (Grants TSI-063000-2021-49, TSI-063000-2021-50 and TSI-063000-2021-76).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ahmad, I.; Yau, K.-L.A.; Ling, M.H.; Keoh, S.L. Trust and reputation management for securing collaboration in 5g access networks: The road ahead. *IEEE Access* **2020**, *8*, 62542–62560. [CrossRef]
2. Wang, Y.; Kang, X.; Li, T.; Wang, H.; Chu, C.-K.; Lei, Z.; Cheng, C. SIX-Trust for 6G: Towards a Secure and Trustworthy Future Network. *IEEE Access* **2023**, *11*, 107657–107668. [CrossRef]
3. Li, H.; Zhu, J.; Qiu, H.; Wang, Q.; Zhou, T.; Li, H. The new threat to internet: DNP attack with the attacking flows strategizing technology. *Int. J. Commun. Syst.* **2015**, *28*, 1126–1139. [CrossRef]
4. Kang, D.W.; Oh, J.H.; Im, C.T.; Yi, W.S.; Won, Y.J. A practical attack on mobile data network using IP spoofing. *Appl. Math. Inf. Sci.* **2013**, *7*, 2345–2353. [CrossRef]
5. Li, W.; Meng, W. BCTrustFrame: Enhancing trust management via blockchain and IPFS in 6G era. *IEEE Netw.* **2022**, *36*, 120–125. [CrossRef]
6. Ylianttila, M.; Kantola, R.; Gurtov, A.; Mucchi, L.; Oppermann, I.; Yan, Z.; Nguyen, T.H.; Liu, F.; Hewa, T.; Liyanage, M.; et al. 6G white paper: Research challenges for trust, security and privacy. *arXiv* **2020**, arXiv:2004.11665.
7. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Toward blockchain-based trust and reputation management for trust-worthy 6G networks. *IEEE Netw.* **2022**, *36*, 112–119. [CrossRef]
8. Huawei 6G Research Team; Liu, F.; Sun, R.; Wang, D.; Javali, C.; Liu, P. 6G Native Trustworthiness. 2022. Available online: https://www.huawei.com/en/huaweitech/future-technologies/6g-native-trustworthiness (accessed on 24 July 2024).
9. Shafi, M.; Jha, R.K.; Jain, S. Intelligent Trust Ranking Security Preserving Model for B5G/6G. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 3549–3561. [CrossRef]
10. Ayoub, O.; Troia, S.; Andreoletti, D.; Bianco, A.; Tornatore, M.; Giordano, S.; Rottondi, C. Towards explainable artificial intelligence in optical networks: The use case of lightpath QoT estimation. *J. Opt. Commun. Netw.* **2022**, *15*, A26–A38. [CrossRef]
11. Veith, B.; Krummacker, D.; Schotten, H.D. The road to trustworthy 6G: A survey on trust anchor technologies. *IEEE Open J. Commun. Soc.* **2023**, *4*, 581–595. [CrossRef]
12. Hakeem, S.A.A.; Hussein, H.H.; Kim, H. Security requirements and challenges of 6G technologies and applications. *Sensors* **2022**, *22*, 1969. [CrossRef] [PubMed]
13. Sharma, V. Functional Security and Trust in Ultra-Connected 6G Ecosystem. *EAI Endorsed Trans. Ind. Netw. Intell. Syst.* **2022**, *9*, e5. [CrossRef]
14. Wang, J.; Ling, X.; Le, Y.; Huang, Y.; You, X. Blockchain-enabled wireless communications: A new paradigm towards 6G. *Natl. Sci. Rev.* **2021**, *8*, nwab069. [CrossRef] [PubMed]
15. Chen, X.; Feng, W.; Ge, N.; Zhang, Y. Zero trust architecture for 6G security. *IEEE Netw.* **2023**, *38*, 224–232. [CrossRef]
16. Yan, Z.; Yang, L.T.; Li, T.; Miche, Y.; Yu, S.; Yau, S.S. Guest Editorial: Trust, Security and Privacy of 6G. *IEEE Netw.* **2022**, *36*, 100–102. [CrossRef]
17. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.-J.A. The roadmap to 6G: AI empowered wireless networks. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [CrossRef]
18. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The roadmap to 6G security and privacy. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1094–1122. [CrossRef]
19. Shala, B.; Trick, U.; Lehmann, A.; Ghita, B.; Shiaeles, S. Blockchain and trust for secure, end-user-based and decentralized IoT service provision. *IEEE Access* **2020**, *8*, 119961–119979. [CrossRef]

20. Mitra, P.; Bhattacharjee, R.; Chatterjee, T.; De, S.; Karmakar, R.; Ghosh, A.; Adhikari, T. Towards 6G communications: Architecture, 926 challenges, and future directions. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 6–8 July 2021; pp. 1–7.
21. Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wirel. Commun.* **2020**, *27*, 126–132. [CrossRef]
22. Yang, Y.; Ma, M.; Wu, H.; Yu, Q.; Zhang, P.; You, X.; Wu, J.; Peng, C.; Yum, T.-S.P.; Shen, S.; et al. 6G network AI architecture for everyone-centric customized services. *IEEE Netw.* **2022**, *37*, 71–80. [CrossRef]
23. Letaief, K.B.; Shi, Y.; Lu, J.; Lu, J. Edge artificial intelligence for 6G: Vision, enabling technologies, and applications. *IEEE J. Sel. Areas Commun.* **2021**, *40*, 5–36. [CrossRef]
24. Kamath, H.S.; Bhandari, A.; Shekhar, S.; Ghosh, S. A Survey on Enabling Technologies and Recent Advancements in 6G Communication. *Proc. J. Phys. Conf. Ser.* **2023**, *2466*, 012005. [CrossRef]
25. Ziegler, V.; Schneider, P.; Viswanathan, H.; Montag, M.; Kanugovi, S.; Rezaki, A. Security and Trust in the 6G Era. *IEEE Access* **2021**, *9*, 142314–142327. [CrossRef]
26. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open J. Commun. Soc.* **2020**, *1*, 957–975. [CrossRef]
27. Tu, Z.; Zhou, H.; Li, K.; Song, H.; Quan, W. Blockchain-based differentiated authentication mechanism for 6G heterogeneous networks. *Peer-to-Peer Netw. Appl.* **2023**, *16*, 727–748. [CrossRef]
28. Bernabe, J.B.; Ramos, J.L.H.; Gomez, A.F.S. TACIoT: Multidimensional trust-aware access control system for the Internet of Things. *Soft Comput.* **2016**, *20*, 1763–1779. [CrossRef]
29. Hashemi, S.Y.; Aliee, F.S. Fuzzy, dynamic and trust based routing protocol for IoT. *J. Netw. Syst. Manag.* **2020**, *28*, 1248–1278. [CrossRef]
30. Yu, C.; Xia, G.; Song, L.; Peng, W.; Chen, J.; Zhang, D.; Li, H. CET-AoTM: Cloud-Edge-Terminal Collaborative Trust Evaluation Scheme for AIoT Networks. In *International Conference on Service-Oriented Computing*; Springer: Cham, Switzerland, 2023; pp. 143–158.
31. Almogren, A.; Mohiuddin, I.; Din, I.U.; Almajed, H.; Guizani, N. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *IEEE Internet Things J.* **2020**, *8*, 4485–4497. [CrossRef]
32. Aravind, K.; Maddikunta, P.K.R. Optimized Fuzzy Logic based Energy-Efficient Geographical Data Routing in Internet of Things. *IEEE Access* **2024**, *12*, 18913–18930. [CrossRef]
33. Kesarwani, A.; Khilar, P.M. Development of trust based access control models using fuzzy logic in cloud computing. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 1958–1967. [CrossRef]
34. Rahman, F.H.; Au, T.-W.; Newaz, S.S.; Suhaili, W.S.; Lee, G.M. Find my trustworthy fogs: A fuzzy-based trust evaluation framework. *Futur. Gener. Comput. Syst.* **2020**, *109*, 562–572. [CrossRef]
35. Soleymani, M.; Abapour, N.; Taghizadeh, E.; Siadat, S.; Karkehabadi, R. Fuzzy rule-based trust management model for the security of cloud computing. *Math. Probl. Eng.* **2021**, *2021*, 6629449. [CrossRef]
36. Xia, G.; Yu, C.; Chen, J. A Fuzzy-Based Co-Incentive Trust Evaluation Scheme for Edge Computing in CEEC Environment. *Appl. Sci.* **2022**, *12*, 12453. [CrossRef]
37. Rajashanthi, M.; Valarmathi, K. A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs. *Wirel. Pers. Commun.* **2020**, *112*, 75–90. [CrossRef]
38. Singh, K.; Verma, A.K. TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks. *Wirel. Pers. Commun.* **2020**, *114*, 3173–3196. [CrossRef]
39. Benfriha, S.; Labraoui, N.; Bensaid, R.; Salameh, H.B.; Saidi, H. FUBA: A fuzzy-based unmanned aerial vehicle behaviour analytics for trust management in flying ad-hoc networks. *IET Netw.* **2023**, *13*, 208–220. [CrossRef]
40. Miao, T.; Shen, J.; Lai, C.F.; Ji, S.; Wang, H. Fuzzy-based trustworthiness evaluation scheme for privilege management in vehicular ad hoc networks. *IEEE Trans. Fuzzy Syst.* **2020**, *29*, 137–147. [CrossRef]
41. Pang, B.; Teng, Z.; Sun, H.; Du, C.; Li, M.; Zhu, W. A malicious node detection strategy based on fuzzy trust model and the abc algorithm in wireless sensor network. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1613–1617. [CrossRef]
42. Das, R.; Dash, D.; Sarkar, M.K. HTMS: Fuzzy based hierarchical trust management scheme in WSN. *Wirel. Pers. Commun.* **2020**, *112*, 1079–1112. [CrossRef]
43. Yang, L.; Lu, Y.Z.; Yang, S.X.; Guo, T.; Liang, Z.F. A Secure Clustering Protocol with Fuzzy Trust Evaluation and Outlier Detection for Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 4837–4847. [CrossRef]
44. Ma, S.; He, J.; Shuai, X. Application of fuzzy comprehensive evaluation method in trust quantification. *Int. J. Comput. Intell. Syst.* **2011**, *4*, 768–776.
45. Wang, Y.; Tian, L.; Wu, Z. Trust modeling based on probabilistic linguistic term sets and the MULTIMOORA method. *Expert Syst. Appl.* **2021**, *165*, 113817. [CrossRef]
46. Zhao, B.; Liu, Y.; Li, X.; Li, J.; Zou, J. TrustBlock: An adaptive trust evaluation of SDN network nodes based on double-layer blockchain. *PLoS ONE* **2020**, *15*, e0228844. [CrossRef] [PubMed]
47. Xu, G.; Liu, B.; Jiao, L.; Li, X.; Feng, M.; Liang, K.; Ma, L.; Zheng, X. Trust2Privacy: A novel fuzzy trust-to-privacy mechanism for mobile social networks. *IEEE Wirel. Commun.* **2020**, *27*, 72–78. [CrossRef]

48. Valero, J.M.J.; Sánchez, P.M.S.; Lekidis, A.; Hidalgo, J.F.; Gil Pérez, M.; Siddiqui, M.S.; Celdrán, A.H.; Pérez, G.M. Design of a security and trust framework for 5G multi-domain scenarios. *J. Netw. Syst. Manag.* **2022**, *30*, 7. [CrossRef]
49. Yang, L.; Li, Y.; Yang, S.X.; Lu, Y.; Guo, T.; Yu, K. Generative adversarial learning for intelligent trust management in 6G wireless networks. *IEEE Netw.* **2022**, *36*, 134–140. [CrossRef]
50. Yin, Y.; Fang, H. A Novel Multiple Role Evaluation Fusion-Based Trust Management Framework in Blockchain-Enabled 6G Network. *Sensors* **2023**, *23*, 6751. [CrossRef] [PubMed]
51. Sedjelmaci, H.; Ansari, N. Zero trust architecture empowered attack detection framework to secure 6G edge computing. *IEEE Netw.* **2023**, *38*, 196–202. [CrossRef]
52. Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. Trust in vehicles: Toward context-aware trust and attack resistance for the internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 9546–9560. [CrossRef]
53. Feng, X.; Yuan, Z. A novel trust evaluation mechanism for edge device access of the Internet of things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3015206. [CrossRef]
54. Sagar, S.; Mahmood, A.; Sheng, M.; Zaib, M.; Zhang, W. Towards a machine learning-driven trust evaluation model for social Internet of Things: A time-aware approach. In Proceedings of the MobiQuitous 2020—17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Darmstadt, Germany, 7–9 December 2020; pp. 283–290.
55. Gao, Y.; Li, X.; Li, J.; Gao, Y.; Philip, S.Y. Info-trust: A multi-criteria and adaptive trustworthiness calculation mechanism for information sources. *IEEE Access* **2019**, *7*, 13999–14012. [CrossRef]
56. Nasir, S.U.; Kim, T.-H. Trust computation in online social networks using co-citation and transpose trust propagation. *IEEE Access* **2020**, *8*, 41362–41371. [CrossRef]
57. Puspita, R.H.; Ali, J.; Roh, B.h. An Intelligent Admission Control Scheme for Dynamic Slice Handover Policy in 5G Network Slicing. *Comput. Mater. Contin. CMC* **2023**, *75*, 4612–4631.
58. Li, X.; Feng, D. Markov chain based trust management scheme for wireless sensor networks. *J. Netw.* **2014**, *9*, 3263. [CrossRef]
59. Bahaa, A.; Shehata, M.; Gasser, S.M.; El-Mahallawy, M.S. Call failure prediction in ip multimedia subsystem (ims) networks. *Appl. Sci.* **2022**, *12*, 8378. [CrossRef]
60. Zhu, Y.; Liu, C.; Zhang, Y.; You, W. Research on 5G Core Network Trust Model Based on NF Interaction Behavior. *KSII Trans. Internet Inf. Syst.* **2022**, *16*, 3333–3354.
61. Morocho-Cayamcela, M.E.; Lee, H.; Lim, W. Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions. *IEEE Access* **2019**, *7*, 137184–137206. [CrossRef]
62. Yang, G.; Zhang, L.; Tan, Z.; Yu, H.; Li, S. A new method of trust inference based on Markov model for peer-to-peer network. In Proceedings of the 2012 IEEE 12th International Conference on Computer and Information Technology, Chengdu, China, 27–29 October 2012; pp. 349–354.
63. Dutta, U. Sampling Random Graphs with Specified Degree Sequences. Ph.D. Thesis, University of Colorado at Boulder, Boulder, CO, USA, 2022.
64. Berkhout, J.; Heidergott, B.F. Analysis of Markov influence graphs. *Oper. Res.* **2019**, *67*, 892–904. [CrossRef]
65. Chen, X.; Leng, S.; He, J.; Zhou, L. Deep-learning-based intelligent intervehicle distance control for 6G-enabled cooperative autonomous driving. *IEEE Internet Things J.* **2020**, *8*, 15180–15190. [CrossRef]
66. Zhou, X.; Liang, W.; She, J.; Yan, Z.; Wang, K.I.-K. Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5308–5317. [CrossRef]
67. Patel, N.J.; Jhaveri, R.H. Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A 832 survey. In Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, 2–3 January 2015; pp. 468–472.
68. Fantacci, R.; Picano, B. A D2D-Aided Federated Learning Scheme with Incentive Mechanism in 6G Networks. *IEEE Access* **2022**, *11*, 107–117. [CrossRef]
69. Zhao, K.; Pan, L. A machine learning based trust evaluation framework for online social networks. In Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, China, 24–26 September 2014; pp. 69–74.
70. Yi, B.; Cao, H.; Song, X.; Wang, J.; Guo, W.; Huang, Z. Measurement and Real-Time Recognition of Driver Trust in Conditionally Automated Vehicles: Using Multimodal Feature Fusions Network. *Transp. Res. Rec.* **2023**, *2677*, 311–330. [CrossRef]
71. Singh, K.; Verma, A.K.; Aggarwal, P. Analysis of various trust computation methods: A step toward secure FANETs. In *Computer and Cyber Security*; Auerbach Publications: Boca Raton, FL, USA, 2018; pp. 171–193.
72. Koeppe, A.; Bamer, F.; Selzer, M.; Nestler, B.; Markert, B. Explainable artificial intelligence for mechanics: Physics-informing neural networks for constitutive models. *arXiv* **2021**, arXiv:2104.10683. [CrossRef]
73. Apparaju, A.; Arandjelović, O. Towards new generation, biologically plausible deep neural network learning. *Sci* **2022**, *4*, 46. [CrossRef]
74. Alhadad, N.; Busnel, Y.; Serrano-Alvarado, P.; Lamarre, P. Trust evaluation of a system for an activity with subjective logic. In *International Conference on Trust, Privacy and Security in Digital Business*; Springer: Cham, Switzerland, 2014; pp. 48–59.
75. Alemneh, E.; Senouci, S.M.; Brunet, P.; Tegegne, T. A two-way trust management system for fog computing. *Future Gener. Comput. Syst.* **2020**, *106*, 206–220. [CrossRef]

76. Sohail, M.; Wang, L.; Jiang, S.; Zaineldeen, S.; Ashraf, R.U. Multi-hop interpersonal trust assessment in vehicular ad-hoc networks using three-valued subjective logic. *IET Inf. Secur.* **2019**, *13*, 223–230. [CrossRef]
77. Yuan, J.; Zhou, H.; Chen, H. Subjective logic-based anomaly detection framework in wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2012**, *8*, 482191. [CrossRef]
78. Kurdi, H.; Alfaries, A.; Al-Anazi, A.; Alkharji, S.; Addegaither, M.; Altoaimy, L.; Ahmed, S.H. A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. *J. Supercomput.* **2019**, *75*, 3534–3554. [CrossRef]
79. Henrique, P.S.R.; Prasad, R. Bayesian Neural Networks for 6G CONASENSE Services. In Proceedings of the 2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC), Herning, Denmark, 30 October–2 November 2022; pp. 291–296.
80. Feng, R.; Han, X.; Liu, Q.; Yu, N. A credible Bayesian-based trust management scheme for wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 678926. [CrossRef]
81. Hosseinnezhad, M.; Azgomi, M.A.; Dishabi, M.R.E. A probabilistic trust model for cloud services using Bayesian networks. *Soft Comput.* **2024**, *28*, 509–526. [CrossRef]
82. Ye, J.; Kang, X.; Liang, Y.-C.; Sun, S. A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks. *IEEE Internet Things J.* **2022**, *9*, 13263–13278. [CrossRef]
83. Rahman, A.; Khan, M.S.I.; Montieri, A.; Islam, M.J.; Karim, M.R.; Hasan, M.; Kundu, D.; Nasir, M.K.; Pescapè, A. BlockSD-5GNet: Enhancing security of 5G network through blockchain-SDN with ML-based bandwidth prediction. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e4965. [CrossRef]
84. Al-Ansi, A.; Al-Ansi, A.M.; Muthanna, A.; Koucheryavy, A. Blockchain technology integration in service migration to 6gcommunication networks: A comprehensive review. *Indones. J. Electr. Eng. Comput. Sci* **2024**, *34*, 1654–1664.
85. Gao, F.; Chen, D.L.; Weng, M.H.; Yang, R.Y. Revealing development trends in blockchain-based 5g network technologies through patent analysis. *Sustainability* **2021**, *13*, 2548. [CrossRef]
86. Muntaha, S.T.; Lazaridis, P.I.; Hafeez, M.; Ahmed, Q.Z.; Khan, F.A.; Zaharis, Z.D. Blockchain for Dynamic Spectrum Access and Network Slicing: A Review. *IEEE Access* **2023**, *11*, 17922–17944. [CrossRef]
87. Ranaweera, C.; Lim, C.; Tao, Y.; Edirisinghe, S.; Song, T.; Wosinska, L.; Nirmalathas, A. Design and deployment of optical x-haul for 5G, 6G, and beyond: Progress and challenges. *J. Opt. Commun. Netw.* **2023**, *15*, D56–D66. [CrossRef]
88. Feng, R.; Xu, X.; Zhou, X.; Wan, J. A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. *Sensors* **2011**, *11*, 1345–1360. [CrossRef]
89. Baccour, E.; Allahham, M.S.; Erbad, A.; Mohamed, A.; Hussein, A.R.; Hamdi, M. Zero touch realization of pervasive artificial intelligence as a service in 6G networks. *IEEE Commun. Mag.* **2023**, *61*, 110–116. [CrossRef]
90. Nguyen, T.; Tran, N.; Loven, L.; Partala, J.; Kechadi, M.T.; Pirttikangas, S. Privacy-aware blockchain innovation for 6G: Challenges and opportunities. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
91. Tian, J.; Zhang, J.; Zhang, P.; Ma, X. Dynamic trust model based on extended subjective logic. *KSII Trans. Internet Inf. Syst. (TIIS)* **2018**, *12*, 3926–3945.
92. Lewis, C.; Li, N.; Varadharajan, V. Targeted Context based Attacks on Trust Models in IoT Systems. *Authorea Prepr.* **2023**.