information

MDPI

Review

Review of the D2D Trusted Cooperative Mechanism in Mobile Edge Computing

Jie Yuan [1,*], Erxia Li [2], Chaoqun Kang [2], Fangyuan Chang [2] and Xiaoyong Li [1,*]

[1] Key Laboratory of Trustworthy Distributed Computing and Service (Beijing University of Posts and Telecommunications), Ministry of Education, Haidian District, Beijing 100876, China
[2] China Electric Power Research Institute, Haidian District, Beijing 100192, China
* Correspondence: yuanjie@bupt.edu.cn (J.Y.); lixiaoyong@bupt.edu.cn (X.L.)

Received: 22 June 2019; Accepted: 12 August 2019; Published: 15 August 2019

Abstract: Mobile edge computing (MEC) effectively integrates wireless network and Internet technologies and adds computing, storage, and processing functions to the edge of cellular networks. This new network architecture model can deliver services directly from the cloud to the very edge of the network while providing the best efficiency in mobile networks. However, due to the dynamic, open, and collaborative nature of MEC network environments, network security issues have become increasingly complex. Devices cannot easily ensure obtaining satisfactory and safe services because of the numerous, dynamic, and collaborative character of MEC devices and the lack of trust between devices. The trusted cooperative mechanism can help solve this problem. In this paper, we analyze the MEC network structure and device-to-device (D2D) trusted cooperative mechanism and their challenging issues and then discuss and compare different ways to establish the D2D trusted cooperative relationship in MEC, such as social trust, reputation, authentication techniques, and intrusion detection. All these ways focus on enhancing the efficiency, stability, and security of MEC services in presenting trustworthy services.

Keywords: mobile edge computing; trusted cooperative mechanism; D2D; social trust; reputation; authentication techniques

1. Introduction

Mobile edge computing (MEC) is a new computing model for service providers challenged to meet large-scale user demands for improved service speed [1–4]. Especially in the 5G era, MEC can provide users with fast and real-time services [5–8]. From the perspective of the network architecture, MEC enables some of the cloud computing tasks to be undertaken by edge computing devices. The main idea behind the new architecture is to reduce network latency and improve applications by performing related processing tasks close to the end devices [9–12].

MEC is deployed as a supplement and extension of cloud computing for the mobility and efficiency needs of network entities [13,14]. Mobile devices usually receive services from cloud centers, which result in high latency and mobility-related issues [15,16]. MEC can solve these issues by bringing the processing to the edge of the network leveraging mobile base stations (BSs). The European Telecommunications Standards Institute has introduced the concept of Mobile Edge computing where mobile users can utilize the computing services from the BS [17]. Many research works are based on the opinion that some edge users are willing to share a portion of the computational capabilities of their mobile devices and exchange information as a result of different incentives ranging from their willingness to share resources to direct financial gains [18–22]. With the development of terminal devices, mobile edge devices have more and more powerful computing and storage capabilities. In the MEC environment, mobile edge devices can not only be users of services, but also providers of services and information.

Compared with other network computing modes, the MEC environment has more serious and complex security problems [23–28]. In large-scale MEC environments, the network ecological environment comprises different building blocks, such as cloud data centers, MEC platforms, service providers, and edge devices with diverse, dynamic, mobile, and cooperative behavior. The importance and complexity of the security problem lie not only in protecting the security of the edge computing system itself, but also in reducing the security risk caused by the cooperation of unfamiliar nodes, thus improving the security of the whole cooperative computing environment. Meanwhile, the existence of mobile devices, which utilize edge services anytime and anywhere, should be fully considered [29].

The trusted cooperative mechanism provides capabilities for dynamic behavior perception for service provision and can take precautionary measures against malicious service behaviors from authenticated service providers [30,31]. As a complementary technology with traditional network security, the trusted cooperative mechanism provides the corresponding access control by judging the quality of service (QoS), and it makes traditional security services highly reliable by ensuring that all communicating devices are trustworthy during service cooperation [32]. The trusted cooperative mechanism can help solve the problems associated with the above technological configurations [30–32].

Security solutions and the trusted cooperative mechanism in other network environments such as cloud computing and D2D are not completely suitable for edge computing. In the large-scale MEC environment, the network ecological environment is large-scale, complex, and dynamic. At the same time, the behavior of a large number of edge devices is diverse, dynamic, mobile, and cooperative. Compared with other network computing modes, the security problem in MEC is more complex, and large-scale use of mobile devices will bring new security challenges and threats to the deployment of edge cloud servers. Because of the strong mobility of edge devices, new devices in an MEC cluster may never interact with edge service providers or any other devices before getting edge computing services. The D2D trusted cooperative mechanism can help the system evaluate the reliability of such devices, thus ensuring that the system has good dynamic scalability.

The trust cooperative mechanism has become the most important issue for constraining the large-scale deployment and usage of MEC [21,33–36]. Compared with traditional technologies, the MEC architecture has many unique features, such as edge computing resources belonging to each edge user and such resources being completely distributed, heterogeneous, and offset; moreover, these features indicate that unmodified traditional security mechanisms no longer can be used in the MEC architecture [34]. The issue of trusted MEC is a paramount concern of most enterprises. A lack of trust between edge users and providers has hindered the universal acceptance of MEC as an outsourced computing model. Trust is the estimation of the competence of a service provider to complete a task based on reliability, security, and availability in the context of a distributed environment. Trust also enables users to select the most trustworthy resources according to their service requirements. Thus, the development of a dynamically-trusted cooperative technology for MEC has become a key and urgent research direction [21,30–36]. The open MEC collaborative environment involves a large number of terminal devices, and trust is one of the most complex concepts from the perspective of the interaction between terminal devices; many decision factors, such as assumptions, expectations, and behavior, are also involved. Thus, quantifying and forecasting trusted cooperative relationship accurately is extremely difficult [37–41]. Providing highly trustworthy resources necessitates an accurate method for measuring and predicting the usage patterns of MEC resources, whose patterns dynamically change over time. As a result, the degree of trust in service providers should be objectively evaluated based on the real-time service behavior of MEC devices. At the same time, trust itself is a comprehensive index for guaranteeing security, and it needs to identify several trust targets of a service provider, i.e., security, availability, and reliability [35,36]. Each target can be reflected by some measured value, such as security, which refers to the prevention of unauthorized access to a system.

Unauthorized access can be detected according to the number of illegal connections and scanning of important ports [42–46]. Reliability refers to the provision of a trusted service for a given duration and can be evaluated by average response time and average task success ratio. Availability refers to the probability of readiness of the trust and can be evaluated by the CPU frequency, memory size, hard disk capacity, and transmission rate of networking devices.

The trusted cooperative mechanism is based on the concept of the frequent interaction between edge devices and edge servers and the frequent interaction between edge devices. It evaluates the behavior and service reliability of collaborative entities by dynamically acquiring service behavior, thus to solve the corresponding access control problems and ensure the security of all edge nodes during authentication, authorization, and service collaboration. In this manner, the whole system becomes highly secure and trustworthy. The trusted cooperative mechanism can be divided into three main stages: trusted cooperative relationship modeling, trusted cooperative relationship calculation and confirmation, and trusted cooperative relationship evolution.

The trusted cooperative mechanism is more than trusted management. Trusted management usually means a trusted management platform supported by hardware security modules, which is widely used in computing and communication systems to improve security. It is an important part of the trusted cooperative mechanism and provides one of the methods to confirm the trusted cooperative relationship by trusted authentication.

The D2D trusted management and cooperative mechanism in MEC is now a frontier and important research area with a few research results. At present, the trust cooperative mechanism developed for MEC is in the initial stage of development. D2D can work together with MEC and plays an important role in MEC. Some researchers assume that some edge users are willing to share a portion of the computational capabilities of their mobile devices and exchange information because of different incentives ranging from their willingness to share resources to direct financial gains. Some studies in MEC are based on the interaction between mobile edge devices in the MEC system architecture, application pattern, security mechanisms, and the trusted management and cooperative mechanism. In this paper, we present a review of the D2D trusted cooperative mechanism developed for MEC. The sections are organized as follows: Section 2 introduces the MEC structure and the trusted cooperative mechanism and their challenging issues. Section 3 reviews various trusted cooperative relation models. Section 4 concludes the research and presents directions for improvements.

2. Concept and Architecture of the MEC Trusted Cooperative Mechanism

2.1. Mobile Edge Computing Architecture and Applications

The rapid development of the Internet of Things (IoT) and 5G network communication technology makes the era of intelligent communication of the number of mobile communication nodes and the amount of data generated increase exponentially, and the mobile communication environment has become increasingly complex [47]. New applications have put forward higher requirements on mobility, timeliness, reliability, and other aspects, which the centralized data model of cloud computing services can hardly meet, and MEC has consequently emerged as a solution to solve these problems [29].

MEC networks present another type of mechanism of scheduling and utilizing computing and service resources compared with cloud computing. As shown in Figure 1, MEC assigns computing tasks originally performed by cloud servers to network edge devices with computing and analysis capabilities; in this manner, the system can reduce the pressure of network bandwidth, improve computing efficiency and timeliness, reduce the pressure of the cloud computing center, and improve security and reliability, thereby perfectly solving the issues caused by mobile IoT and its services [13,15,16]. Typical applications of MEC include computing, caching, and communications [48]. Despite the advantages of MEC, such as low latency and high energy efficiency, the computing resources of edge networks are still limited. In exploiting the merits of both the edge networks and the cloud platforms at the core network, the cooperation between them is valuable [48]. At the same time, the collaboration between terminal devices is also one of the important applications of MEC. For example, applications, such as crowdsensing, information sharing, and social community construction, can be implemented between two edge devices in a device-to-device (D2D) manner.

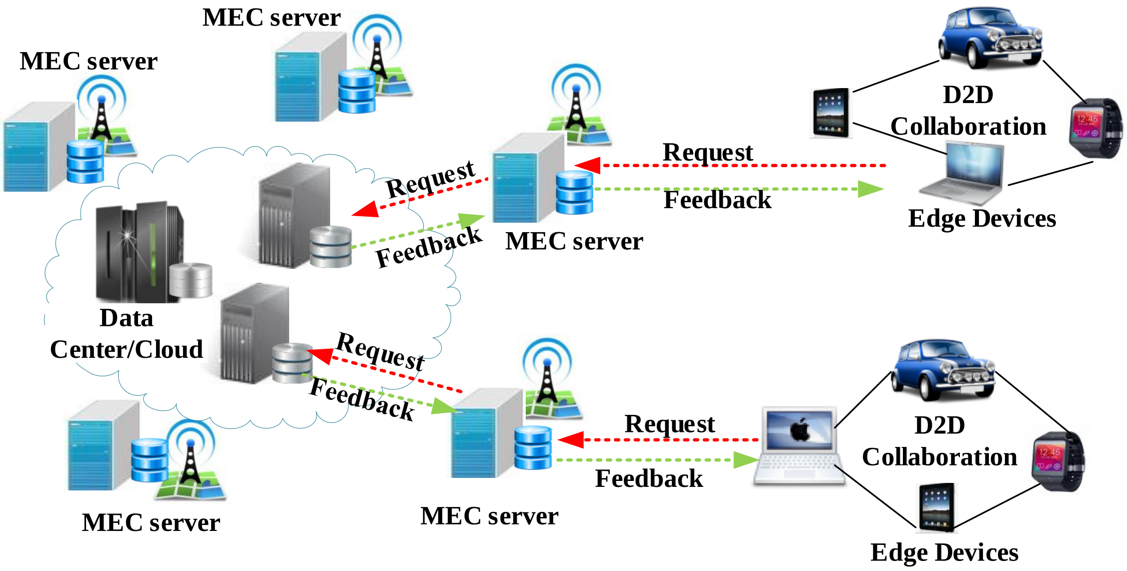

Figure 1. Mobile edge computing architecture.

MEC provides a convenient and reliable service model for operators, equipment providers, IT platform providers, and system integrators. In addition to reducing the congestion of mobile core networks, MEC delivers low latency. Moreover, edge computing provides a way to collect and process information at local edge devices instead of the data center/cloud. MEC can also provide near real-time analysis of data, and it can cut expenses anchored to operations and data management [49].

Many MEC application cases are already being realized in the industrial field. For example, augmented reality network services need an application to analyze data from a user's edge camera to construct a digital representation of the world layered with information, such as images or text. In particular, the application needs to know the user's location information and actions. Supporting an augmented reality service on an MEC platform over the cloud is beneficial because the data relevant to the point of interest are highly localized. In this case, the MEC platform instead of the centralized server handles the user's whereabouts quickly and with low latency.

In the past few years, a large number of connected cars have flooded the automotive industry. As the data collected by connected cars increase, much lower latency is required. In storing and processing data, MEC can extend the connected car cloud to the mobile BS in which the data can be stored and processed near the car quickly. Besides, this technology allows the driver to receive alerts from other vehicles in real time.

2.2. D2D Trusted Cooperative Mechanism in MEC

Orchestrating diverse security mechanisms in large-scale MEC environments is an important and complex issue. In large-scale MEC environments, the network ecological environment is particularly complex and dynamic. This type of network comprises different building blocks, such as cloud data centers, MEC platforms, service providers, and service users. Moreover, a large number of edge devices whose behavior is diverse, dynamic, mobile, and cooperative need to cooperate efficiently with one another and edge data centers anytime and anywhere [29,48]. Compared with other network computing modes, the security problem between devices in the MEC environment is more complex.

Numerous security threats are the key factors that restrict MEC development and popularization. Without strong guaranteed security and the trusted cooperative mechanism, the advantages of MEC will be concealed by malicious attacks, cooperative deception, and other security threats. The consequences will be extremely serious if the computing capabilities are brought to the edge without an effective security mechanism. The importance and complexity of the security problem lie not only in protecting the security of the edge computing system itself, but also in reducing the security risk brought by cooperating with unfamiliar nodes; in this manner, the security of the whole cooperative computing environment can be improved. Meanwhile, the existence of mobile devices, which utilize edge services anytime and anywhere, should be considered [29].

In [34], the author proposed a trustworthy D2D cooperative mechanism in the MEC architecture with a cloud platform (Figure 2). Edge computing pushes part of the calculation task from cloud data centers to proxy servers at the edge of the network during data processing, and this configuration can bring several potential advantages as follows: dealing with applications at the edge, which reduces network latency and produces much faster responses to the service requests of users; adding edge servers close to device clusters, which is likely a much cheaper way of achieving scalability than fortifying the servers in the cloud data center, which can also increase the network bandwidth for users; and removing the single point of failure in the infrastructure by lowering the dependency on the cloud data center, which can reduce the susceptibility to denial of service attacks and improve service availability. As shown in Figure 2, the trustworthy edge computing architecture based on the multi-source feedback trust calculation mechanism comprises three layers: a network layer, a broker layer, and device a layer [34].

- The network layer is supported by the traditional cloud computing platform. The central server that hosts the master database is located within a professionally-managed cloud data center. Cloud computing promises more power, safer data, and easier access to the information and tools needed for successful implementation in any industry or organization compared with the alternatives. In this condition, we can assume that the cloud data center is reliable and always available, while attacks and other risks to the central server are beyond the scope of this work.
- The broker layer is used to monitor the service behavior of devices and aggregate the feedback from these devices. In an open edge computing environment, a large number of undependable (or malicious) devices and feedback from these undependable devices may yield incorrect evaluation results. However, the limited work at present mainly focuses on a reliable feedback mechanism for an edge computing environment. Hence, we extend traditional feedback mechanisms such that feedback can come not only from devices, but also from brokers, thus effectively reducing networking risk and improving system reliability. More importantly, different from traditional feedback aggregation mechanisms, the trust aggregate calculation based on feedback information is entirely derived from brokers. This approach can reduce the energy costs of devices and render the proposed trust mechanism a lightweight scheme from the perspective of client energy cost.
- The device layer consists of various edge devices. In the process of service coordination, multiple participating devices communicate with the brokers through the Internet via WiFi or cellular access points. The devices are divided into different domains based on their location, and each domain is managed by a broker. In the area of wireless computer networking, the broker is derived from the BS. A radio receiver/transmitter serves as the hub of the local wireless network, and it may also serve as the gateway between a wired network and the wireless network. The device layer typically consists of a low-power transmitter and wireless router. After completing a service collaboration, both devices will submit mutual evaluation information to the broker. Before the collaborative service of the two devices, a device will send a request message to its broker to ensure the trustworthiness of the collaborator.

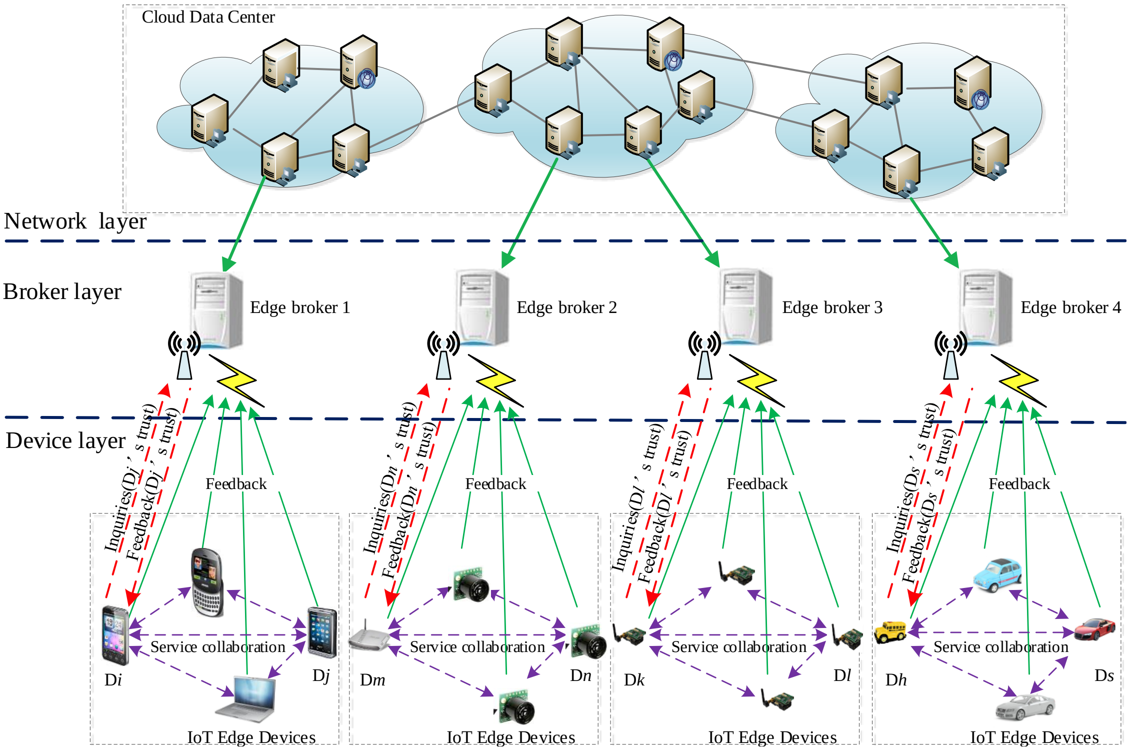

Figure 2. Trustworthy D2D cooperative mechanism in the mobile edge computing (MEC) architecture with the cloud platform.

The D2D trustworthy cooperative mechanism as a complementary technology to the traditional network security mechanism can provide a basis for reliable decision making for entity interaction in the MEC network environment. It evaluates the behavior and service reliability of collaborative nodes by dynamically acquiring service behavior, thus to solve the corresponding access control problems and ensure the security of all edge nodes during authentication, authorization, and service collaboration. In this manner, the whole system becomes highly secure and trustworthy.

The D2D trusted cooperative mechanism in large-scale MEC environments may be one of the most important, but difficult issues in the security mechanisms. Billions of mobile edge devices that also provide computation services can cooperate anytime and anywhere with one another among edge data centers. These devices and centers initially need to know if other mobile edge devices or edge data centers are safe or trusted in identity, capability, performance, stability, and efficiency; otherwise, they will encounter unsatisfactory services and even affect the information disclosure or cause privacy issues, virus problems, and malicious attacks.

2.3. Classification of the Trusted Cooperative Mechanism

In distributed network environments, the trusted cooperative mechanism gauges the device according to its trustworthiness in identity, honesty, performance, ability, and stability. The trusted cooperative mechanism can be classified in many ways.

Classification according to different substances: The trusted cooperative mechanism can be classified on the basis of QoS or social trust. Trust based on QoS considers energy, unselfishness, competence, cooperativeness, reliability, and task completion capability. Social trust considers intimacy, honesty, privacy, centrality, and connectivity [50].

Classification according to different angles of performance: The trusted cooperative mechanism can be classified on the basis of behavioral trust or identity trust. Identity trust is mainly concerned with verifying the authenticity of the identity of entities in the network to determine whether they are authorized to access entities. Behavioral trust is concerned with trust in a broader sense. Users can adjust and update their trust relationship in a dynamic and timely manner according to their past experience of contact with one another.

Classification according to different sources of trust: The trusted cooperative mechanism can be classified on the basis of direct trust, indirect trust, or overall trust. Direct trust describes the experience of direct interaction between two entities. Indirect trust represents trust between two entities through indirect feedback from third parties. Overall trust is the combination of direct trust and indirect trust.

In large-scale MEC environments and on the basis of participation at different network levels, the trusted cooperative mechanism can be classified on the basis of the centralized model, the distributed model, or the semi-centralized model. In the centralized trusted cooperative mechanism, cloud servers are responsible for information collection, computing, and feedback. This first mechanism has the advantage of memory usage and calculation, but it is limited in terms of reliability, stability, high communication overhead, scalability, efficiency, and adaptability. In the distributed trusted cooperative mechanism, the edge device itself performs all the collection, computing, and decision making without considering the participation of cloud servers or edge servers. This second mechanism has the advantage of reliability, scalability, stability, and low bandwidth pressure, but it is limited in terms of calculation ability, efficiency, and adaptability. In the semi-centralized trusted cooperative mechanism, edge devices perform under the control of BSs or edge servers, which can respond to the information collection, computing, and feedback without the participation of cloud servers. This third mechanism has the advantage of reliability, scalability, stability, efficiency, adaptability, and low bandwidth pressure.

2.4. Trusted Edge Computing Network Control Structure

The trusted cooperative mechanism can be generally divided into three parts: the confirmation of the trusted cooperative relation model, the establishment of the trusted factor indication system, and the calculation and evaluation of the trusted value.

The trusted cooperative relation model is the foundation of the trusted cooperative mechanism. The confirmation of the trusted cooperative relationship in large-scale MEC environments may be one of the most important but difficult issues in security mechanisms and the trusted cooperative mechanism. A trusted cooperative relation can be established in many ways, such as trusted cooperative relations based on social trust, authentication techniques, and intrusion detection.

The trusted MEC network control structure mainly includes three aspects: a cloud service layer, a service control layer, and an edge termination layer. As shown in Figure 3, the integrated trusted indicators of the trusted network coordination mechanism for edge computing include four aspects: identity credibility assessment, behavior credibility assessment, capability credibility assessment, and security credibility assessment.

- Trust of identity: This indicator is mainly used to confirm the uniqueness of an entity and decide whether the entity can be authorized. The main considerations are identity authentication, access control, common technologies for authentication, authorization, encryption, data hiding, digital signature, public-key certificate, and access control policy.
- Trust of behavior: The entity's historical behavior record and current behavior characteristics are used to judge the entity's trust and behavioral expectation dynamically, and the access and service authority are given according to the trust of the entity, which is undeniable and authoritative. In different network environments, the trust evaluation model of an entity's behavior is extremely extensive. Obtaining the trust value of the entity through direct evaluation and indirect evaluation and performing an aggregation algorithm calculation are therefore proposed.
- The capability of trust: This indicator refers to the ability and reliability of the entity's response time, available bandwidth, storage space, computing power, and mission execution success rate. In the field of trusted computing, previous types of trusted computer systems were based entirely on the assumption that hardware devices and network communications were secure and reliable. However, in actual large-scale edge computing network environments, hardware

devices or network communications are highly likely to be unstable and unreliable during the interaction process. The trust of the edge devices is perceived and monitored in a trusted computer system. Moreover, dynamic measurement is a necessary indicator.

- Security of MEC: This indicator comprehensively considers the security credibility of entities from the aspects of privacy protection, data security, and sharing security. In large-scale MEC network environments, users do not want their privacy, personal data, personal behavior characteristics, and other information to be mastered by the server or the cloud. After processing the user information, the mobile edge device extracts the necessary information and uploads the result to the cloud server, which greatly enhances the privacy protection of the user, ensures data security, and guarantees shared security. Therefore, the trust evaluation of the security of the edge devices in terms of privacy protection, data security, and sharing security is also an important indicator.

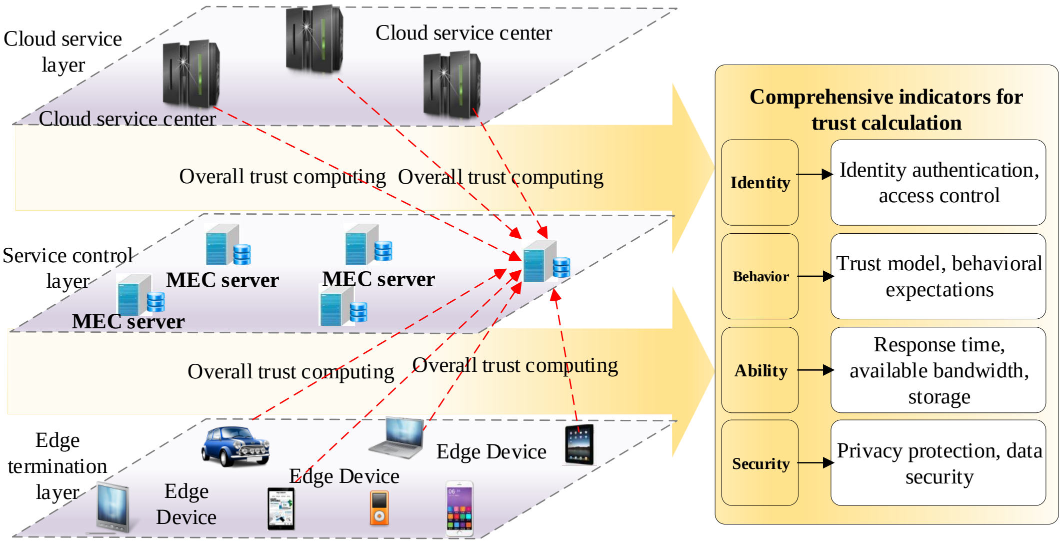

Figure 3. Trusted edge computing network control structure.

3. Existing Trusted Cooperative Relation Models

The trusted cooperative mechanism of MEC can effectively provide a basis for decision making about the interaction of network entities, and it is the foundation for the survival and development of MEC. This approach can efficiently solve the security problems of MEC, particularly by using the trusted cooperative mechanism. In large-scale MEC environments, the confirmation of the trusted cooperative relationship is the foundation of the trusted cooperative mechanism. Current studies have focused on the following aspects.

3.1. Trusted Cooperative Relation Model Based on Social Trust

Ying et al. [20] presented a social trust relation scheme to enhance the security of mobile social networks by using uncertain reasoning to derive trust values due to the uncertainty in trust evaluation. Trust evaluation from direct observations and indirect observations was derived from the Bayesian inference approach and Dempster–Shafer theory, respectively. By combining these two trust values, a more accurately estimated trust value of a mobile user can be obtained for social trust evaluation, which is one of the factors that should be considered comprehensively. Meanwhile, a deep Q-learning algorithm was exploited to solve the formulated optimization problem by considering dynamic scenarios. Extensive simulation results showed the effectiveness of the proposed scheme.

Habak et al. [18] proposed the femtocloud system that provides a dynamic, self-configuring, and multi-device mobile cloud from a cluster of mobile devices, which build trust based on in-person and social relationships. The mobile devices must be willing to share a portion of their computational capabilities as a result of different incentives, which range from their willingness to share resources to their willingness to share direct financial gains. A femtocloud controller was responsible for deciding which mobile devices will be added to the compute cluster in the current environment according to their preferences and behavior in different scenarios, after which it assigned tasks to available devices to maximize the metric of interest. The evaluation demonstrated the potential of femtocloud clustering to provide meaningful computational resources at the edge.

In [34], the authors proposed a reliable and lightweight trust computing mechanism for IoT Edge devices, after which it rapidity, real-timeliness, effectiveness, and accuracy were comprehensively considered, which enabled users to focus on issues related to trust calculation in IoT edge computing. The global trust degree of devices was used as a measure of the provider's competence to provide the required service, which comprised three parts: direct trust (based on direct interaction records between two devices), feedback trust from other edge devices, and feedback trust from service brokers. Processing the trust calculation at the edge of the network without the participation of the central network was much more efficient. Furthermore, a feedback information fusion algorithm based on objective information entropy theory was adopted to enhance adaptability and reliability.

Huang et al. [28] proposed the adoption of a reputation management mechanism based on familiarity, similarity, and timeliness, which should be applied to the reputation calculation of edge devices close to mobile vehicles in the edge computing environment of vehicle networks. A distributed reputation management system for mobile vehicles to perform local reputation management services was proposed. The system collected, weighed, and aggregated all vehicle reputation in the region to form a letter. The reputation knowledge base used multiple weighted subjective logic to calculate and update the reputation value, and it designed and used a resource optimization allocation algorithm based on the reputation value to compute unloading scenarios. This scheme can enhance security protection, improve overall performance, and help service providers optimize resource allocation during unloading.

3.2. Trusted Cooperative Relation Model Based on Authentication Techniques

Echeverria et al. [51] presented a solution to establish trusted identities in disconnected environments based on secure key generation and exchange in the field without a trusted third party. A threat model for disconnected environments was identified, and the solution to establish trust was implemented in the context of a client/server tactical cloudlets systems, which consisted of four subprocesses: bootstrapping, pairing, WiFi authentication, and API requests. The first two processes performed the actual trust establishment; the other two processes authenticated a paired device requesting access at the WiFi and network level, respectively. Then, new components and four different communication protocols were added. The solution can be applied to any form of trusted communication between two or more computing nodes. The implementation was evaluated against the threat model and by performing vulnerability analysis. The results about the resilient solution could address most of the threats and characteristics of disconnected environments if combined with proper application-, OS-, network-, and site-level controls.

Cui et al. [52] proposed an efficient message authentication scheme based on the edge computing of vehicular ad hoc networks (VANETs) that included trusted authority, roadside units (RSU), and any vehicle equipped with an onboard unit, in which the vehicle participating in the message authentication was called an edge computing vehicle (ECV). The RSU acted as the cloud of the vehicle, and a part of the vehicle acted as an edge-computing node to assist the RSU with the message authentication task. A number of ECVs were elected to assist the RSU in authenticating the message signature sent by nearby vehicles. Then, the results of the RSU were based on the available computation power of the vehicle. The RSU verified the results sent from the ECVs, determined the legitimacy of these messages, and finally, broadcast the information regarding the legitimacy to the vehicle through a cuckoo filter. Consequently, the vehicle needed to only query the filter to determine whether the message was valid, and it did not need to verify the received messages independently in most cases. The security analytical results showed that the proposed scheme could meet the basic security requirements of VANETs and improve the efficiency of message authentication.

Goh et al. [53] studied the architecture of trusted data dissemination in edge computing. User requirements, equipment requirements, security factors, and resource configuration were determined according to different application requirements. Three architecture schemes were proposed to verify the authenticity and accuracy of the query results generated by the edge servers. The first trusted mechanism did not need a security guarantee from the edge service providers and instead adopted the solution based on the Merkle hash tree. The second trusted mechanism recognized that although the edge service providers themselves were not sufficiently secure, they could trust a minimum number of edge servers to process queries and then collectively verify the results. The trusted data forwarding mechanism proposed by Goh et al. was based on edge servers that ran different operating systems and used different security products to protect them, which made it more difficult for attackers to endanger all edge servers without being detected at the same time. The third trusted mechanism combined the first two schemes, i.e., a single edge server generated query results and forwarded them to a set of validators for verification.

3.3. Trusted Cooperative Relation Model Based on Intrusion Detection

Mtibaa et al. [22] proposed HoneyBot, a defense technique for D2D malicious communication to detect and isolate malicious nodes in MEC platforms. This technique consisted of selecting a set of mobile devices/machines called HoneyBot nodes (or HoneyBots). These nodes aimed to detect any malicious activity or insider attacks and coordinate with other neighboring nodes to track the malicious node or botmaster for isolation. Detection and tracking algorithms were proposed and investigated to leverage insecure D2D-infected communication channels, thus accurately and efficiently identifying suspected malicious nodes and isolating them. The data-driven evaluation and analysis, based on three real-world mobility traces, showed that the number and placement of HoneyBot nodes in the network could considerably affect tracking delay and detection accuracy.

Kozik et al. [54] proposed an attack detection approach based on distributed extreme learning machine (ELM) technology, which leveraged HPC cluster resources for time-consuming and computationally-expensive classifier training. The design and properties of the ELM classifier enabled the efficient computation and analysis of the collected data in the edge computing environment. The proposed approach analyzed and classified online the aggregated traffic captured by NetFlows on specific edge nodes located in the proximity of the data sources to be protected. The ELM classifier training process could be decoupled and shifted to the edge cloud to benefit only the edge computing capabilities required to perform traffic classification effectively based on much more sophisticated pre-built models. Moreover, the effectiveness of the proposed detection scheme was proven by using a variety of experiments on real-world attack datasets.

3.4. Comparison of Trusted Cooperative Relation Models for MEC

Current studies showed that the trusted cooperative relationship in MEC could be confirmed in many ways, and they all focused on enhancing the efficiency, accuracy, stability, and scalability of MEC services. In addition, these schemes could be improved in certain aspects. Table 1 shows the comparison of current MEC trusted cooperative relation models based on different trusted cooperative bases, network latency, calculation efficiency, reliability, scalability, and memory usage.

The trusted cooperative architecture can be centralized, semi-centralized, or hybrid with clusters/groups and distributed edge devices. In the centralized trusted cooperative architecture, the trusted cooperative relationship is calculated and fed back by central servers with excellent calculation efficiency and memory usage, but network latency, such as trusted central DBMS [53], which is above the edge servers. In the semi-centralized trusted cooperative architecture, edge servers/clouds/brokers are responsible for trusted information collection and trusted cooperative relationship calculation with less network latency and satisfactory calculation efficiency and memory usage. The hybrid trusted cooperative architecture is a combination of the distributed and semi-centralized structure where both edge servers/clouds/brokers and edge devices are involved in the trusted cooperative relationship calculation with satisfactory performance in all respects.

The trusted calculation methods of the trusted cooperative mechanism include methods based on social trust, reputation, authentication, and intrusion detection. The edge service provider can be edge servers/clouds/brokers or both edge servers/clouds/brokers and edge devices. Meanwhile, the trusted cooperative relationship calculation can be processed and stored in edge servers/clouds/brokers or the trusted central DBMS.

Table 2 shows the comparison of current MEC trusted cooperative relation models based on different trust calculation executors, edge service providers, and the trusted cooperative architecture.

Table 1. Comparison of trusted cooperative relation models for MEC I.

Trusted Cooperative Relation Model	Basics	Network Latency	Calculation Efficiency
Ying et al. [20]	Social Trust	Medium	Low
Habak et al. [18]	Social Trust	Low	Medium
Yuan et al. [34]	Social Trust	Low	High
Huang et al. [28]	Reputation	Low	Medium
Echeverria et al. [51]	Authentication	Medium	High
Cui et al. [52]	Authentication	Low	Medium
Goh et al. [53]	Authentication	Medium	High
Mtibaa et al. [22]	Intrusion Detection	Low	Medium
Kozik et al. [54]	Intrusion Detection	High	Low
Trusted Cooperative Relation Model	**Reliability**	**Scalability**	**Memory Usage**
Ying et al. [20]	High	High	High
Habak et al. [18]	Medium	Medium	Medium
Yuan et al. [34]	High	High	High
Huang et al. [28]	Medium	Medium	Medium
Echeverria et al. [51]	High	High	High
Cui et al. [52]	Medium	Medium	Medium
Goh et al. [53]	High	High	High
Mtibaa et al. [22]	Medium	Medium	Medium
Kozik et al. [54]	High	High	High

Table 2. Comparison of trusted cooperative relation models for MEC II.

Trusted Cooperative Relation Model	Basics	Trust Calculation Executor
Ying et al. [20]	Social Trust	BSs
Habak et al. [18]	Social Trust	Edge Servers
Yuan et al. [34]	Social Trust	Edge Brokers
Huang et al. [28]	Reputation	Edge Servers
Echeverria et al. [51]	Authentication	Edge Servers
Cui et al. [52]	Authentication	Edge Servers
Goh et al. [53]	Authentication	Trusted Central DBMS
Mtibaa et al. [22]	Intrusion Detection	Edge Servers
Kozik et al. [54]	Intrusion Detection	Edge Clouds
Trusted Cooperative Relation Model	**Edge Service Provider**	**Architecture**
Ying et al. [20]	BSs and Edge Devices	Hybrid
Habak et al. [18]	Edge Servers	Hybrid
Yuan et al. [34]	Edge Brokers and Edge Devices	Hybrid
Huang et al. [28]	Edge Servers	Semi-centralized
Echeverria et al. [51]	Edge Servers	Semi-centralized
Cui et al. [52]	Edge Servers	Semi-Centralized
Goh et al. [53]	Edge Servers	Centralized
Mtibaa et al. [22]	Edge Servers and Edge Devices	Hybrid
Kozik et al. [54]	Edge Clouds	Semi-centralized

4. Conclusions and Future Directions

The D2D trusted cooperative mechanism in MEC was discussed and analyzed in this paper. MEC is a distributed network that assigns computing tasks originally performed by cloud servers to network edge devices with computing and analysis capabilities, where edge devices can not only enjoy edge services, but also provide edge services. The D2D trusted cooperative mechanism can help edge entities establish trusted cooperative relationships and achieve satisfactory and safe services. Then, the different schemes to establish the trusted cooperative relationship in MEC, such as social trust, reputation, authentication techniques, and intrusion detection, were determined and compared. All these schemes focused on enhancing the efficiency, accuracy, stability, and scalability for MEC services and had different performances in MEC environments. Future research on the trusted cooperative mechanism of MEC should adequately consider the following: the features of MEC, such as the function of edge servers or BS; the numerous, dynamic, and collaborative characteristic of MEC edge devices; and the MEC server requirement of stability, security, real-timeliness, and many other factors.

MEC is a revolutionary architecture of wireless mobile networks. The system has many new features compared with the existing 3G/4G/5G cellular systems, and it has better QoE/QoS performance and flexibility. Therefore, a wide variety of research challenges and opportunities should be considered in future research [21,33–35,48].

- Trusted MEC application and deployment: We can combine trust management with incentive mechanisms to encourage collaboration across devices. Implementing and evaluating our proposed trust calculation mechanism on various edge computing systems, such as distributed file sharing, is an important direction of future research.
- Overall trust adaptive computing: We should fully consider the weight distribution issue in the fused computation of direct trust and feedback trust. The implementation of convergence and the accurate, rapid, objective, and dynamic computing of overall trust evaluation and prediction are also important directions of future research.
- Trusted data acquisition and storage: The main tasks of trusted data collection include identity data, behavior data, security data, and capability data. The efficient data collection mechanism for calculating direct trust and feedback is a basic task for deploying trusted MEC applications.
- Trust analysis and calculation: Trust analysis and calculation include three core tasks: direct trust calculation, feedback trust calculation, and overall trust fusion calculation. By adopting an effective adaptive machine learning algorithm, we can accurately calculate and predict direct trust, feedback trust, and overall trust. According to the result of the trust calculation, the related mobile node can perform access control authorization.
- Seamless integration of trusted collaboration mechanisms with existing mobile IoT systems: The mobility of the mobile IoT environment and the characteristics of nodes belonging to different management domains can be combined. In this manner, a high-trust network collaborative management framework based on identity trust and behavior trust can be achieved by the domain. Moreover, the trustworthy behavior between domains can be fed back and monitored, and complex management is established. The network environment and the various external interferences can then achieve stability and adaptive reliability in the MEC network.

Funding: This work was supported by in part by the project "Research on Security Architecture for Next Generation Distribution Automation System of State Grid Corporation of China".

Acknowledgments: The authors would like to convey their heartfelt gratitude to the reviewers and the Editor for the valuable suggestions and important comments, which greatly helped them to improve the presentation of this manuscript.

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

References

1. Mach, P.; Becvar, Z. Mobile edge computing: A survey on architecture and computation offloading. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1628–1656. [CrossRef]
2. Mao, Y.; Zhang, J.; Letaief, K.B. Dynamic computation offloading for mobile-edge computing with energy harvesting devices. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 3590–3605. [CrossRef]
3. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile edge computing: A survey. *IEEE Internet Things J.* **2017**, *5*, 450–465. [CrossRef]
4. Tran, T.X.; Hajisami, A.; Pandey, P.; Pompili, D. Collaborative mobile edge computing in 5G networks: New paradigms, scenarios, and challenges. *arXiv* **2016**, arXiv:1612.03184.
5. Hu, Y.C.; Patel, M.; Sabella, D.; Sprecher, N.; Young, V. Mobile edge computing—A key technology towards 5G. *ETSI White Pap.* **2015**, *11*, 1–16.
6. Rimal, B.P.; Van, D.P.; Maier, M. Mobile edge computing empowered fiber-wireless access networks in the 5G era. *IEEE Commun. Mag.* **2017**, *55*, 192–200. [CrossRef]
7. Yu, Y. Mobile edge computing towards 5G: Vision, recent progress, and open challenges. *China Commun.* **2016**, *13*, 89–99. [CrossRef]
8. Fajardo, J.O.; Liberal, F.; Giannoulakis, I.; Kafetzakis, E.; Pii, V.; Trajkovska, I.; Bohnert, T.M.; Goratti, L.; Riggio, R.; Lloreda, J.O. Introducing mobile edge computing capabilities through distributed 5G cloud enabled small cells. *Mob. Netw. Appl.* **2016**, *21*, 564–574. [CrossRef]
9. Wang, S.; Zhao, Y.; Xu, J.; Yuan, J.; Hsu, C.H. Edge server placement in mobile edge computing. *J. Parallel Distrib. Comput.* **2019**, *127*, 160–168. [CrossRef]
10. Bellavista, P.; Belli, D.; Chessa, S.; Foschini, L. A Social-Driven Edge Computing Architecture for Mobile Crowd Sensing Management. *IEEE Commun. Mag.* **2019**, *57*, 68–73. [CrossRef]
11. Cui, Q.; Gong, Z.; Ni, W.; Hou, Y.; Chen, X.; Tao, X.; Zhang, P. Stochastic Online Learning for Mobile Edge Computing: Learning from Changes. *IEEE Commun. Mag.* **2019**, *57*, 63–69. [CrossRef]
12. Zhang, F.; Liu, G.; Zhao, B.; Fu, X.; Yahyapour, R. Reducing the network overhead of user mobility–induced virtual machine migration in mobile edge computing. *Softw. Pract. Exp.* **2019**, *49*, 673–693. [CrossRef]
13. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
14. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K.B. A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2322–2358. [CrossRef]
15. Ahmed, E.; Akhunzada, A.; Whaiduzzaman, M.; Gani, A.; Ab Hamid, S.H.; Buyya, R. Network-centric performance analysis of runtime application migration in mobile cloud computing. *Simul. Model. Pract. Theory* **2015**, *50*, 42–56. [CrossRef]
16. Pace, P.; Aloi, G.; Gravina, R.; Caliciuri, G.; Fortino, G.; Liotta, A. An Edge-based Architecture to Support Efficient Applications for Healthcare Industry 4.0. *IEEE Trans. Ind. Inform.* **2018**, *15*, 481–489. [CrossRef]
17. Wazir, Z.; Ejaz, A.; Saqib, H.; Ibrar, Y.; Arif, A. Edge computing: A survey. *Future Gener. Comput. Syst.* **2019**, *97*, 219–235.
18. Habak, K.; Zegura, E.W.; Ammar, M.; Harras, K.A. Workload management for dynamic mobile device clusters in edge femtoclouds. In Proceedings of the Second ACM/IEEE Symposium on Edge Computing, San Jose/Fremont, CA, USA, 12–14 October 2017; pp. 1–14.
19. Habak, K.; Ammar, M.; Harras, K.A.; Zegura, E. Femto Clouds: Leveraging Mobile Devices to Provide Cloud Service at the Edge. In Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, USA, 27 June–2 July 2015.
20. He, Y.; Yu, F.R.; Zhao, N.; Yin, H. Secure Social Networks in 5G Systems with Mobile Edge Computing, Caching, and Device-to-Device Communications. *IEEE Wirel. Commun.* **2018**, *25*, 103–109. [CrossRef]
21. Yuan, J.; Li, X. A multi-source feedback based trust calculation mechanism for edge computing. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018; pp. 819–824.
22. Mtibaa, A.; Harras, K.; Alnuweiri, H. Friend or Foe Detecting and Isolating Malicious Nodes in Mobile Edge Computing Platforms. In Proceedings of the IEEE 7th International Conference on Cloud Computing Technology & Science, Vancouver, BC, Canada, 30 November–3 December 2015.

23. Vassilakis, V.; Chochliouros, I.P.; Spiliopoulou, A.S.; Sfakianakis, E.; Belesioti, M.; Bompetsis, N.; Wilson, M. Security analysis of mobile edge computing in virtualized small cell networks. In Proceedings of the IFIP International Conference on Artificial Intelligence Applications and Innovations, Thessaloniki, Greece, 16–18 September 2016; Springer: Cham, Switzerland, 2016; pp. 653–665.
24. He, D.; Chan, S.; Guizani, M. Security in the internet of things supported by mobile edge computing. *IEEE Commun. Mag.* **2018**, *56*, 56–61. [CrossRef]
25. Stojmenovic, I.; Wen, S.; Huang, X.; Luan, H. An overview of fog computing and its security issues. *Concurr. Comput. Pract. Exp.* **2016**, *28*, 2991–3005. [CrossRef]
26. Liu, H.; Zhang, Y.; Yang, T. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
27. Mollah, M.B.; Azad, M.A.K.; Vasilakos, A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. *J. Netw. Comput. Appl.* **2017**, *84*, 38–54. [CrossRef]
28. Huang, X.; Yu, R.; Kang, J.; Zhang, Y. Distributed reputation management for secure and efficient vehicular edge computing and networks. *IEEE Access* **2017**, *5*, 25408–25420. [CrossRef]
29. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2016**, *78*, 680–698. [CrossRef]
30. Azzedin, F.; Ridha, A. Feedback behavior and its role in trust assessment for peer-to-peer systems. *Telecommun. Syst.* **2010**, *44*, 253–266. [CrossRef]
31. Li, X.; Ma, H.; Zhou, F.; Gui, X. Service Operator-Aware Trust Scheme for Resource Matchmaking across Multiple Clouds. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 1419–1429. [CrossRef]
32. Li, X.; Ma, H.; Zhou, F.; Gui, X. T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1402–1415.
33. Li, X.; Yuan, J.; Ma, H.; Yao, W. Fast and Parallel Trust Computing Scheme Based on Big Data Analysis for Collaboration Cloud Service. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1917–1931. [CrossRef]
34. Yuan, J.; Li, X. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion. *IEEE Access* **2018**, *6*, 23626–23638. [CrossRef]
35. Yuan, J.; Li, X. A Broker-Guided Trust Calculation Model for Mobile Devices of D2D Communications. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 1–6.
36. Li, J.; Li, X.; Gao, Y.; Yuan, J.; Fang, B. Dynamic Trustworthiness Overlapping Community Discovery in Mobile Internet of Things. *IEEE Access* **2018**, *6*, 74579–74597. [CrossRef]
37. Li, X.; Zhou, F.; Yang, X. A multi-dimensional trust evaluation model for large-scale P2P computing. *J. Parallel Distrib. Comput.* **2011**, *71*, 837–847. [CrossRef]
38. Li, X.Y.; Gui, X.L. Research on dynamic trust model for large scale distributed environment. *J. Softw.* **2007**, *18*, 1510–1521. [CrossRef]
39. Li, X.; Zhou, F.; Yang, X. Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1944–1957. [CrossRef]
40. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
41. Lu, Z.; Qu, G.; Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 760–776. [CrossRef]
42. Tang, J.; Ibrahim, M.; Chakrabarty, K.; Karri, R. *Security and Trust, Secure and Trustworthy Cyberphysical Microfluidic Biochips*; Springer: Cham, Switzerland, 2020; pp. 19–49; Unpublished.
43. Jain, A.K.; Tokekar, V.; Shrivastava, S. Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks. In *Information and Communication Technology*; Springer: Singapore, 2018; pp. 39–47.
44. Paul, A.B.; Biswas, S.; Nandi, S.; Chakraborty, S. MATEM: A unified framework based on trust and MCDM for assuring security, reliability and QoS in DTN routing. *J. Netw. Comput. Appl.* **2018**, *104*, 1–20. [CrossRef]
45. Tewari, A.; Gupta, B.B. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Gener. Comput. Syst.* **2018**, in press. [CrossRef]
46. Peccoud, J.; Gallegos, J.E.; Murch, R.; Buchholz, W.G.; Raman, S. Cyberbiosecurity: From naive trust to risk awareness. *Trends Biotechnol.* **2018**, *36*, 4–7. [CrossRef]

47. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of Things in the 5G Era: Enablers, Architecture and Business Models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
48. Wang, S.; Zhang, X.; Zhang, Y.; Wang, L.; Yang, J.; Wang, W. A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications. *IEEE Access* **2017**, *5*, 6757–6779. [CrossRef]
49. Nathan, C. What Is Multi-access Edge Computing? 2017. Available online: https://www.rcrwireless.com/20170707/wireless/what-is\-mobile-edge-computing-tag27 (accessed on 21 May 2019).
50. Rani, V.U.; Sundaram, K.S. Review of Trust Models in Wireless Sensor Networks. *Int. Sch. Sci. Res. Innov.* **2014**, *8*, 371–377.
51. Echeverra, S.; Klinedinst, D.; Williams, K.; Lewis, G.A. Establishing Trusted Identities in Disconnected edge environment. In Proceedings of the 2016 IEEE/ACM Symposium on Edge Computing (SEC), Washington, DC, USA, 27–28 October 2016.
52. Cui, J.; Wei, L.; Zhang, J.; Xu, Y.; Zhong, H. An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1621–1632. [CrossRef]
53. Goh, S.T.; Pang, H.H.; Deng, R.H.; Bao, F. Three Architectures for Trusted Data Dissemination in Edge Computing. *Data Knowl. Eng.* **2006**, *58*, 381–409. [CrossRef]
54. Kozik, R.; Chora, M.; Ficco, M.; Palmieri, F. A scalable distributed machine learning approach for attack detection in edge computing environments. *J. Parallel Distrib. Comput.* **2018**, *119*, 18–26. [CrossRef]