

Received May 4, 2020, accepted May 18, 2020, date of publication June 24, 2020, date of current version July 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004738

Off-Street Vehicular Fog for Catering Applications in 5G/B5G: A Trust-Based Task Mapping Solution and Open Research Issues

FATIN HAMADAH RAHMAN¹, S. H. SHAH NEWAZ^{1,2}, (Senior Member, IEEE),
THIEN WAN AU¹, (Member, IEEE), WIDA SUSANTY SUHAILI¹, AND
GYU MYOUNG LEE³, (Senior Member, IEEE)

¹School of Computing and Informatics, Universiti Teknologi Brunei, Jalan Tungku Link, Gadong BE1410, Brunei Darussalam

²KAIST Institute for Information Technology Convergence, Daejeon 34141, South Korea

³Department of Computer Science, Faculty of Engineering and Technology, Liverpool John Moores University, Liverpool L3 3AF, U.K.

Corresponding author: S. H. Shah Newaz (shah.newaz@utb.edu.bn)


This work was supported by Universiti Teknologi Brunei (UTB), Brunei Darussalam.

ABSTRACT One of the key enablers in serving the applications requiring stringent latency in 5G networks is fog computing as it is situated closer to the end users. With the technological advancement of vehicles' on-board units, their computing capabilities are becoming robust, and considering the underutilization of the off-street vehicles, we envision that the off-street vehicles can be an enormously useful computational source for the fog computing. Additionally, clustering the vehicles would be advantageous in order to improve the service availability. As the vehicles become highly connected, trust is needed especially in distributed environments. However, vehicles are made from different manufacturers, and have different platforms, security mechanisms, and varying parking duration. These lead to the unpredictable behavior of the vehicles where quantifying trust value of vehicles would be difficult. A trust-based solution is necessary for task mapping as a task has a set of properties including expected time to complete, and trust requirements that need to be met. However, the existing metrics used for trust evaluation in the vehicular fog computing such as velocity and direction are not applicable in the off-street vehicle fog environments. In this paper, we propose a framework for quantifying the trust value of off-street vehicle fog computing facilities in 5G networks and forming logical clusters of vehicles based on the trust values. This allows tasks to be shared with multiple vehicles in the same cluster that meets the tasks' trust requirements. Further, we propose a novel task mapping algorithm to increase the vehicle resource utilization and meet the desired trust requirements while maintaining imposed latency requirements of 5G applications. Results obtained using iFogSim simulator demonstrate that the proposed solution increases vehicle resource utilization and reduces task drop noticeably. This paper presents open research issues pertaining to the study to lead the way for future research directions.

INDEX TERMS Vehicular fog, trust, task mapping, 5G/B5G, fog computing.

I. INTRODUCTION

As emerging applications require stringent latency, this will eventually force the cellular networks to advance to 5G and beyond 5G (5G/B5G), where 5G/B5G have to serve a wide range of applications in diversified scenarios [1]. One key enabler that can assist 5G/B5G in meeting the stringent latency requirement is fog computing as it is situated closer

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

to the end users. Fog computing contributes in reducing the latency which is crucial for the emerging applications with time-sensitive requirements such as virtual reality and haptics and robotics, as they may not be accomplished through cloud computing as observed in Table 1. Apart from serving the applications with the stringent latency requirement, fog computing is also able to reduce the burden from the back-haul network and increase the traffic throughput. In addition, distributed security mechanisms are needed in facilitating new applications and services in 5G/B5G. This needs to be

TABLE 1. Overview of latency requirement of latency-stringent applications.

Applications	Latency Requirement	Remarks
Virtual reality	10 - 20 ms [15]	Long latency in Virtual Reality (VR) could result in motion sickness.
Smart traffic control	10 ms [16]	Strict end-to-end latency is needed by automated collision avoidance system in ensuring vehicle safety.
Haptics and robotics	1 ms [15]	Remote control and real-time feedback collection require strict end-to-end latency requirement.
Online gaming	30 - 50 ms [16]	High latency than required would deteriorate gaming experience.
High precision drone control	20 ms [17]	Drone flying with real time control needs strict end-to-end latency requirement.
Education and Culture	5 - 10 ms [16]	Real time online interaction between trainer and learner would require very low latency.

properly addressed as a pervasive use of artificial intelligence for huge data exchange would pose a challenge in terms of security, privacy, and trust [2]. Moreover, a trust-based solution is required in order to meet the Service Level Agreement (SLA) of applications that can only be served by the fog computing facilities (e.g. augmented reality and smart traffic control). Therefore, one can foresee the importance of trust in fog computing in order to cater the applications in 5G/B5G.

Additional computation and storage capacities that can be found around the network access segment are particularly seen in vehicles whether they are mobile such as for social Internet of Vehicles [3], or off-street (parked) vehicles in the fog computing field [4], [5]. Considering that off-street vehicles are abundantly available (vehicles remain parked 96% of the time [6]), using the parked vehicles as part of fog computing facilities can reduce the investment in deploying dedicated fog computing infrastructures for the end users. Furthermore, as 5G cells are relatively small, taking the moving vehicles into consideration in Vehicular Fog Computing (VFC) can result in frequent handover, incur additional processing overheads, and degrade the service. This has convinced us to only consider off-street vehicles as part of fog and in the subsequent sections of the paper, we refer a vehicle that becomes part of fog computing as a v-fog.

Despite the promising prospects of off-street v-fogs, they are of different nature to the conventional fog computing devices and hence they may face dissimilar challenges that are unique to off-street v-fog itself. Although the vehicles might provide availability from the capabilities (i.e. processing, networking, and storage), availability of the vehicles can also be observed in terms of its parking duration. Different vehicles have different parking durations with different spatio-temporal conditions, hence their availability for being part of the fog infrastructure also varies. One of the alternatives to solve this problem is using the clustering concept, as clustering the v-fogs can increase service availability through multiple replications and caching [7]–[9]. Other advantages of clustering include having a cluster head to ease management, apart from minimizing collisions in the communication channel to reduce the communication overhead [7]–[9].

On the other hand, being heterogeneous and distributed in nature imply that the off-street v-fogs are unpredictable

because they are temporary and dynamic. Undoubtedly, as vehicle capabilities are advancing with various storage mechanisms [10] and computational power, security threats consequently are becoming even more and more sophisticated. Compromised v-fog components such as Electric Control Unit (ECU) can lead to undesired events [11] and inaccurate sensors may inevitably send false information back to a legitimate enquirer, rendering the v-fog as malicious and vulnerable to various attacks. For instance, vehicles such as Tesla Model X and Jeep Cherokee were previously hacked to perform unauthorized actions and car safety features can even be shutdown [12]–[14]. Although hard security can simply be achieved with appropriate measures such as access control, authentication, and authorization, they are insufficient in safeguarding the entire operations. Even encryption techniques used for secure communication of the v-fog components come at the cost of extra processing time. Moreover, security mechanisms vary across different manufacturers and platforms. Hence, using security metric alone is insufficient in achieving an efficient and dependable v-fog based edge computing.

In moving vehicles, trust-based solutions as seen in [7], [8], [18]–[20] are used to address the shortcomings and challenges of the current solutions that depend on only security, e.g. heterogeneity and additional processing delay. Additionally, using trust-based solutions allow us to incorporate a combination of multiple diverse metrics for performance measurement. It is worth noting that the trust assessment of these existing works is focusing on data trust and communication trust. Yet, when a v-fog itself is not trusted, it can relay false data and the trust of the data will be tampered. Meanwhile, the trust of the communication emphasizes more on vehicle proximity while neglecting other factors that are equally important in assessing trust of a v-fog. Furthermore, the metrics used for trust evaluation as observed in [20] in moving vehicles such as velocity, speed and direction are not applicable to off-street v-fog environments as they are stationary.

As the applications that demand fog support in 5G would require the trust-based service, the v-fog can have a pivotal role in offering large source of computational and storage power. Thus, we think that it is increasingly important to develop a framework that can quantify trust value of a v-fog

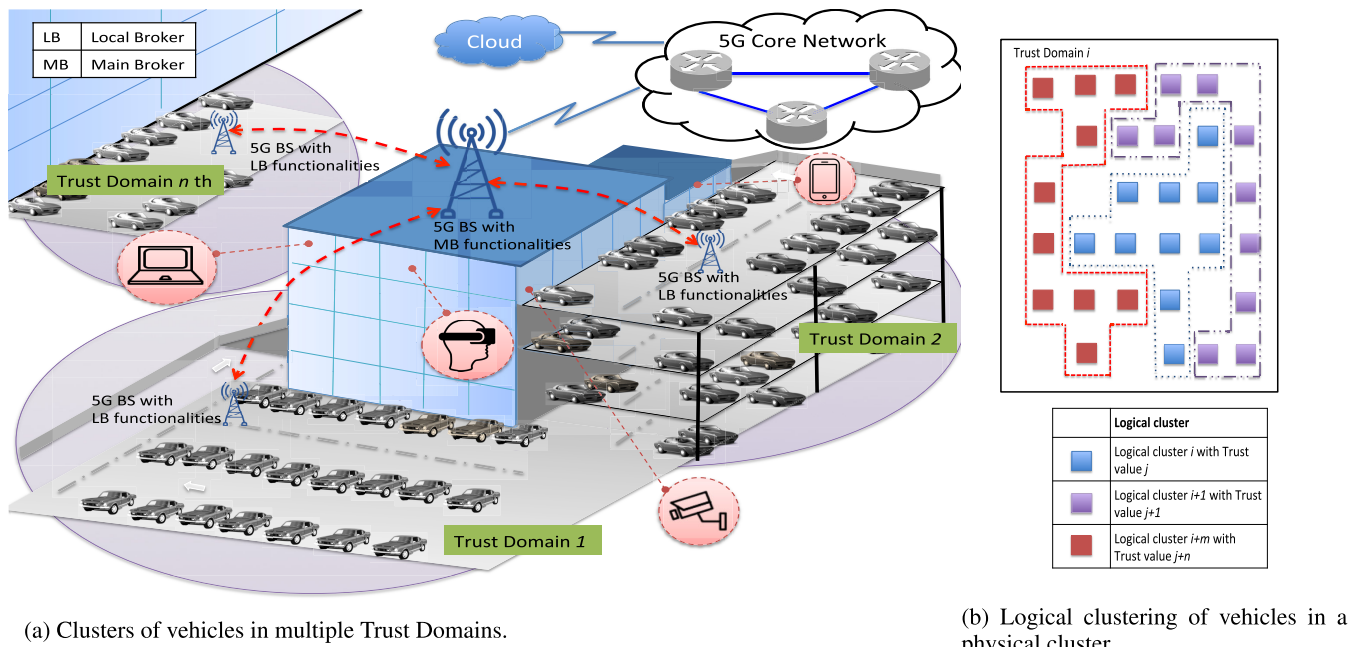


FIGURE 1. Parked v-fogs in different Trust Domains and logical clusters.

in the 5G environment. To the best of our knowledge, this is the first study that proposes a framework for measuring the trust value of off-street v-fogs and clustering the v-fogs according to their trust values. Unlike the aforementioned studies focusing on data trust and communication trust, our trust is entity-based and the meaning of trust in our context is referred as the expectation that a v-fog will behave in an intended manner, similar to the trust definition in [21]. The framework in this paper is illustrated as a scenario of physical clusters of v-fogs shown in Fig. 1a. The physical cluster which is referred in [21] as a Trust Domain¹ is adopted in this study. Figure 1a shows a physical cluster of v-fogs that are connected to a Base Station (BS) where the BS communication range determines a Trust Domain's coverage. Furthermore, v-fogs that are in the same physical space may not belong in the same Trust Domain as there is a possibility of having multiple Trust Domains overlapping in a single physical space and different Trust Domain might be operated using different service operator standards.

Motivated by the above observations, we address the need of trust-based solutions in the off-street v-fog environments to support the applications in 5G and make the following contributions in this paper:

- We devise a solution that aims at catering the latency requirement of the applications in 5G, reducing the task

¹ITU-T in [21] has defined Trust Domain as a set of information and associated resources consisting of users, networks, data repositories, and applications (or services) that manipulate the data in those data repositories. Different trust domains may share the same social-cyber-physical components, and a single trust domain may employ various levels of trust.

drop and seemingly paving the way for increasing the overall satisfaction of the clients.

- Propose a framework that encompasses both physical and logical clustering concept, where physical clustering of v-fogs is based on the v-fog's Trust Domain, and logical clustering of v-fog is based on the v-fog's trust value as shown in Fig. 1b. The combination of both can provide more stability in processing any incoming tasks.
- We propose the Vehicle Cluster Formation (VCF) algorithm for logical clustering of v-fogs, where a logical cluster refers to a group of v-fogs with trust values that fall within the cluster's trust value range. V-fogs that are in the same Trust Domain might belong to a different logical cluster as illustrated in Fig. 1b. As a v-fog's trust value changes over time, this algorithm allows the v-fog to be logically assigned from one cluster to another well-suited cluster.
- We propose the Task Mapping (TM) algorithm with the objective of trust based task mapping effectively in order to reduce task drop.

The performance evaluation of the proposed work is conducted using iFogSim simulator. Our results demonstrate that the proposed work outperforms the existing solution in terms of higher cluster utilization and lower percentage of task drop.

The rest of the paper is arranged as follows: Section II presents the existing studies on task mapping and trust in vehicular environments. Section III elaborates more on the workflow of the proposed work, the VCF algorithm and the TM algorithm. The performance evaluation and open research issues are presented in Section IV and Section V respectively, followed by the conclusions in Section VI.

II. BACKGROUND STUDY

Section II-A first discusses the existing studies on task mapping, and the works on trust evaluation in the vehicular networks are elaborated Section II-B.

A. TASK MAPPING

The capability of the computational and storage resources of vehicles has increasingly gained attention in the recent years [22]–[26], where several studies have uncovered the potential of idle vehicle resources for the purpose of content distribution [9], [27]–[33]. Realizing the promising future of smart vehicles, various vehicle clustering algorithms have been proposed to harness its potential in the areas of vehicular routing or vehicle resources. Nonetheless, the existing research efforts focus on creating stable clusters of mobile vehicles [7], [34]–[38]. The authors in [27] propose the idea of ParkCast that leverages roadside parking to distribute contents in urban Vehicular Ad-hoc Networks (VANETs). With wireless devices and rechargeable batteries, parked vehicles can communicate with any vehicles driving through them. Parked vehicles at each roadside are grouped into a line cluster as far as possible, which is locally coordinated for node selection and data transmission. Meanwhile, the authors in [39] have exploited parked vehicles to provide a virtual network infrastructure to facilitate data exchange and to extend the vehicular network for improved connectivity. A cluster of parked vehicles constitutes a single virtual network node which is formed based on a virtual routing protocol that also features Distributed Hash Table functionality.

There are numerous studies that have looked into resource allocation [40]–[42] and task allocation [43]–[45] in vehicles. In [43], the authors propose a two-sided matching scheme and a deep reinforcement learning approach to schedule offloading requests and allocate network resources in vehicular edge computing. Vehicles upload tasks to RSUs where RSUs obtain global information of vehicular offloading tasks through the relay station. Authors in [44] propose a meta-heuristic approach, called Hybrid Adaptive Particle Swarm Optimization for task scheduling and resource allocation in v-fog. The authors consider a three-layer v-fog architecture where the bottom layer represents the On-Board Unit (OBU) vehicle resources, the middle layer consisting of roadside fogs and the top layer consisting of the centralized fog of high-end servers. The mobile vehicle resources are leveraged to various services requested by other vehicles and individuals on the road. Unlike the work in [44], the authors in [45] propose a learning-based distributed task offloading framework based on the multi-armed bandit theory. It enables vehicles that perform task-offloading to learn the performance of vehicles that provide the service, thus to make task offloading decisions individually and minimize the average offloading delay.

B. TRUST IN VEHICULAR ENVIRONMENTS

Despite the potentials of v-fogs mentioned previously, trust is identified as an issue in vehicular networks [46]–[50] and various works have tried to address the issue. The authors in [51] propose a trust and reputation management framework for VANETs based on similarities between messages and similarities between vehicles. Similarities and reputations of recommenders are used as weightage for computing comprehensive reputation for the message producer. The framework is applied to help the drivers to decide whether or not they should believe the received messages. The study in [52] has built a data-centric trust model and emphasized on the distance, time and relations between node types and data types for a reliable data acquisition in VANETs. Their model focused on four factors, namely data reporter's trustworthiness, the correlative trustworthiness of the event and its reporter, the proximity in geographic location, and the proximity in time. In an effort to reduce intrusion detection in VANETs, the work in [53] proposes a secure clustering algorithm where the authors introduce a social behavior parameter to assure more connectivity within a cluster and elect a more stable and trusted vehicle as the cluster head.

In [54], the authors propose a secure and stable vehicular clustering algorithm based on hybrid mobility similarities and the trust management scheme. However, the existing vehicle clustering algorithms are not suited in the off-street vehicle context in our paper. Meanwhile, authors in [20] propose a trust model that assesses the accuracy and integrity of a sender of an event message of a vehicle. By using fuzzy logic, it evaluates the trust value based on experience, plausibility, and accuracy level of location, where experience and plausibility are dependent upon past direct interaction and location verification using distance and time, respectively. Although their concept and methodology are almost similar to our study in this paper, some of the metrics such as velocity and speed cannot be adopted in our off-street vehicle scenario. Therefore, the solution in [20] cannot be applied for parking VFC based computing.

In order to meet the trust requirements of tasks, a Simple Matching solution is presented in our previous study [55] where tasks are migrated from one fog to other fogs of similar trust value. Although the trust requirements of the tasks are met throughout their completion, the frequent migration implies an increase in processing delay. Moreover, no simulations are conducted to experiment on its performance. The closest work that resembles our proposed work is observed in [56]. The authors propose a trust-aware brokering scheme to match cloud resources to the end user requests. Since the cloud is stationary, availability is not considered as part of their evaluation criteria for cloud. This is also observed in [57] that proposes a trust model for the cloud. However, availability plays an important factor in mobile-based resources in the VFC. It is apparent from the aforementioned studies that their focuses are more inclined towards communication

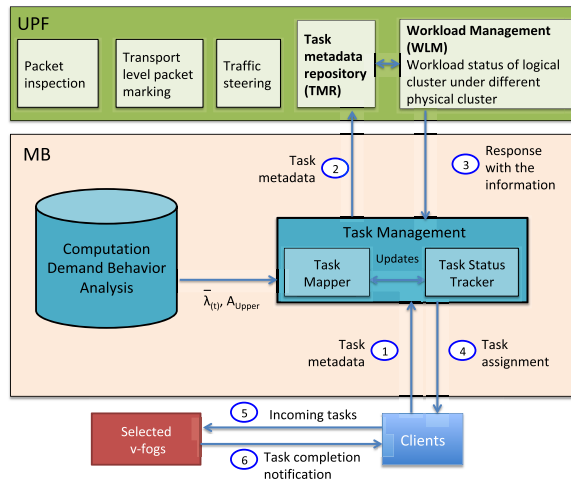
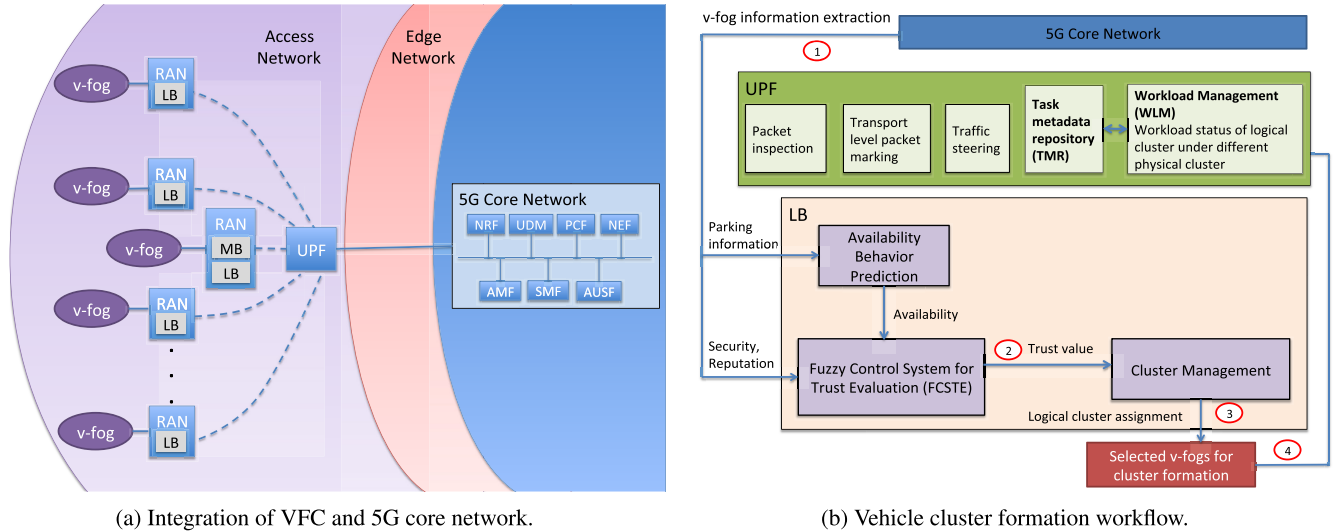


FIGURE 2. The integration of VFC with the 5G core network and functional block diagrams of MB and LB in the proposed solution.

trust or data trust. Nevertheless, studies looking into how the off-street vehicle trust can affect task mapping are currently overlooked.

III. PROPOSED WORK

The objectives of our study are to provide a trust-based service using v-fog for the applications in 5G and maximize the utilization of v-fog resources. In order to facilitate this, we derive a framework that comprises of two algorithms namely the Vehicle Cluster Formation (VCF) algorithm and the Task Mapping (TM) algorithm. Section III-A elaborates the system model, Section III-B describes the workflow of our proposed solution and the proposed algorithms are presented in Section III-C.

A. SYSTEM MODEL

With the global increase of vehicle charging stations [58], we can surmise that power will not be an issue when we consider that the parking lots are equipped with power charging

ports. Although it is common in various places globally to impose parking time restrictions, there are no time restrictions for vehicles to park for the sake of simplicity of this study.

Our study focuses on Vehicle-to-Infrastructure (V2I) communication where the v-fogs communicate with their respective BS. As depicted in Fig. 2a, in our solution, several functional entities of the 5G core network are used in order to integrate with the VFC. We assume that the VFC ecosystem is integrated with the User Plane Function (UPF) of the 5G core network similar to [59] and the UPF is placed in the access network to reduce the latency as proposed in [60]. The UPF can be seen as a distributed and configurable data plane which is controlled by the Session Management Function (SMF) of the 5G network. It is also in charge of traffic steering of the user plane towards the desired applications or network functions. Although this particular capability is not in the scope of our study, we make the following assumptions that the UPF has a global knowledge including the traffic forwarding latency from one point to another point. It uses this

knowledge for efficient traffic forwarding in 5G. Therefore, in our solution, it can play an increasingly important role in the decision-making process where tasks are assigned to the VFC computational facilities.

In the 5G core network, the list of network functions and the services they produce are handled by the Network Resource Function (NRF), and the Policy Control Function (PCF) handles the rules and regulations of the 5G system. For the PCF function, we assume that the VFC operator may impose relevant policies relating to the v-fogs in our solution. The Unified Data Management (UDM) function is responsible for the 5G services related to users and their subscriptions. We assume that other VFC-related procedures such as IP address allocation management of the v-fogs and DHCP services are done in the SMF. On the other hand, the Access and Mobility Management Function (AMF) handles mobility related procedures, in which the capability is useful in our solution in tracking the v-fog parking behavior and the average sojourn parking time of a v-fog. Meanwhile, the information of v-fog is uploaded to the Network Exposure Function (NEF) of the 5G core network as it plays a role in authorizing all access requests originating from outside of the system. Whereas the authentication procedures of a v-fog can be done in the Authentication Server Function (AUSF).

In order to allocate the tasks to a v-fog, an intermediate node namely a broker is considered in our proposal. We assume that there are two hierarchies of brokers referred to as Main Broker (MB) and Local Broker (LB), where the v-fog drivers are willing to share the required information to these brokers and participate in the v-fog enrollment in VFC. The MB and LB are deployed in the 5G BSs as depicted in Fig. 1a. Here, the 5G BS serves as a Trust Domain, and each Trust Domain contains multiple logical clusters. As discussed in Section I, with the possibility of having multiple Trust Domains overlapping in a single physical space and different Trust Domain might operate using different operator standards, v-fogs that are in the same physical space may not belong in the same Trust Domain. Prior to determining which 5G BS that the MB should be deployed in, factors such as network connectivity and the average distance between the respective 5G BS are considered beforehand. The selected 5G BS with MB functionality becomes the top hierarchy that manages a group of LBs. Additionally, both the MB and LB are connected to the UPF, as illustrated by their functional block diagrams in Fig. 2b and 2c. These three entities are further elaborated below:

1) MB

The MB functions as a load balancer that is running the TM algorithm (that will be discussed further in Section III-C). In order to run the TM algorithm, the MB requires the help of UPF in gathering the list of qualified logical clusters to process the incoming tasks from the clients. The functions of the components in the MB block diagram are explained below:

- **Task Management:** The metadata of the tasks forwarded from the clients are processed in this component before the tasks are assigned to and processed by the selected v-fogs. This metadata includes information such as the task's response time and trust requirements. The Task Management component contains two sub-components namely Task Mapper and Task Status Tracker where the TM algorithm is running. The Task Mapper processes the task metadata using the TM algorithm and the MB forwards it to the UPF. This algorithm will be further discussed in Section III-C2. At this stage, it is worth highlighting that the final decision on the most appropriate v-fog is made in the MB; however, the initial screening of the candidate v-fogs is made at the UPF using the supplied metadata obtained from the clients.
- **Computation Demand Behavior Analysis (CDBA):** This component stores the arrived timeseries task arrival history that is used to predict the behavior of future incoming tasks. As the task arrival rate of a logical cluster may vary, there is a level of uncertainty where its variance might be > 0 . In particular, in our solution, this timeseries data is used to obtain information namely the average number of task arrival for a logical cluster at a given time, denoted by $\bar{\lambda}_l$, and the upper limit of task arrival variance for the logical cluster, denoted by A_{upper} . These metrics are then stored in the UPF.

2) LB

The main functions of the LB include evaluating and managing the trust of v-fogs as well as keeping track of the available v-fog resources. The latest update of the workload status of the logical clusters that it is governing is periodically updated to the UPF. The functions of the components in the LB block diagram are explained below:

- **Availability Behavior Prediction:** Whenever a v-fog parks and is attached to a BS, its attachment information is stored in the AMF entity of the 5G core network. This information can be used to understand the parking behavior pattern (e.g. average availability duration at particular parking space) of a particular v-fog. Such information can be part of the metrics to be used by the LB in order to quantify the trust of the v-fog.
- **Fuzzy Control System for Trust Evaluation (FCSTE):** This component performs the trust evaluation process of the v-fogs based on three input metrics i.e. security, reputation, and availability. These metrics are chosen in this study as they have been considered previously in several studies [61], [62]. The availability information is obtained from the Availability Behavior Prediction component of the LB, and the security and reputation information of the v-fog are obtained from the UPF. The output of the FCSTE component is the v-fog's trust value where the maximum trust value is 1.
- **Cluster Management:** This component is responsible in assigning the v-fogs to their respective logical clusters

based on the v-fogs' trust value. The VCF algorithm, that creates the logical clustering, is running in this component in which we will further discuss later in Section III-C1. The response time of a server is highly affected by its utilization [63]. Thus, we assume that the VFC operator can set the utilization threshold of each of the v-fog based on the application latency requirement that the logical clusters need to comply, similar to [64], [65].

In order to meet the the application latency requirement (R_{alr}), we need to find the maximum utilization for a given service rate (μ) for i th v-fog ($\rho_{max}^{(i)}$). This is calculated using (1) which is based on the M/M/1 queueing model. The i th v-fog's utilization threshold is denoted by $\rho_t^{(i)}$, where the *current utilization* $\leq \rho_t^{(i)} \leq \rho_{max}^{(i)}$.

$$\rho_{max}^{(i)} = 1 - \frac{1}{\mu R_{alr}}. \quad (1)$$

Once the $\rho_{max}^{(i)}$ is obtained, we can get the maximum arrival rate that the v-fog can accept ($\lambda_{max}^{(i)}$) as follows,

$$\lambda_{max}^i = \rho_{max}^{(i)} \mu_i, \quad (2)$$

where $\bar{\mu}_i$ is the average service rate of i th v-fog. In order to calculate the total number of the maximum tasks (arrival) that the entire logical cluster comprised of m number of v-fogs can serve, it is quantified using (3).

$$\lambda_{max} = \sum_{i=1}^m \rho_{max}^{(i)} \mu_i. \quad (3)$$

As each of the LBs needs to quantify the remaining capacity of reassigned tasks that each of its logical clusters can accommodate at a given time, denoted by λ_f , this component uses the $\bar{\lambda}_l$ and A_{upper} metrics obtained from the UPF to calculate λ_f for each of the logical clusters. At this point, the λ_{max} is already obtained from (3) and it is assumed that the value for task arrival that are meant to be processed by a logical cluster at time t , denoted as $\lambda_l(t)$ is known. Finally, the λ_f for each of the logical clusters of a LB can be quantified using (4), and it is updated into the UPF.

$$\lambda_f = \lambda_{max} - \lambda_l(t) - (A_{upper} - \bar{\lambda}_l). \quad (4)$$

Therefore, one can see how the value of the predefined R_{alr} can dynamically affect the ρ_{max} , which in turn influences and controls the λ_{max} . In other words, the λ_{max} that a logical cluster can accept while meeting the R_{alr} will vary. The relationship between these parameters and how they affect the logical clusters' performance in terms of utilization, percentage of task drop, and λ_f can be observed in the results in Section IV-C.

²The research findings in [66] impart that there is an optimal point of server utilization at which a server reaches its maximum energy efficiency. One of the criteria in deciding the ρ_t can be the energy consumption.

3) UPF

The UPF contains multiple functional components in the 5G network. Apart from having the existing functions such as packet inspection, transport level packet marking, and traffic steering, here it comprises of two other presumed functions i.e. the Workload Management (WLM) and Task Metadata Repository (TMR). Upon receiving a request from a client, the MB will inform the TMR of the UPF about the request and the TMR forwards the information to the WLM. The WLM can have two alternative ways in gathering the latest workload status of the logical clusters to serve the request from the group of LBs, namely a polling method or a trap-based method.

It is worth mentioning that before assigning a task to a logical cluster, the MB needs to have the current average task processing response time (R_c) and λ_f of each of the logical clusters at a given time. Additionally, the MB needs to take into account the total delay, denoted as T_d (which is quantified in (7)) from the task's originating source (client) to each candidate logical cluster. We assume that the UPF is capable of measuring T_d as it is in charge of traffic steering in 5G. Having these statistics i.e latest workload status of the logical clusters and the aforementioned additional metrics readily available in the WLM allows the UPF to respond to the MB upon request.

B. WORKFLOW OF PROPOSED SOLUTION

When a v-fog reaches a Trust Domain, the LB of the Trust Domain quantifies the trust value of the v-fog and assigns the v-fog into a logical cluster of that LB using the VCF algorithm. The LB feeds the logical cluster information (comprising of R_c , λ_f and T_d) into the UPF periodically as mentioned in Section III-A3. Upon request, the UPF will forward this logical cluster information to the MB to map the tasks with the respective logical clusters using the TM algorithm. Prior to discussing the workflow of how the MB finds the most appropriate logical cluster in accomplishing the tasks, we first need to elaborate on how each LB clusters the v-fogs into multiple logical clusters.

Figure 2b shows that upon being parked and attached to a 5G BS, the LB in the BS extracts the details of the v-fog from the 5G core network ①. The 5G core network then forwards the v-fog's parking information to the Availability Behavior Prediction component of the LB to estimate the v-fog's availability, and it directly forwards v-fog's security and reputation information to the FCSTE component of the LB. These three metrics i.e. availability, security and reputation are then used by the FCSTE component for trust evaluation of the v-fog. Since the values of these metrics are always changing, their values have to be collected in a timely interval by the LB from the 5G core network. These metrics are further elaborated below:

- **Security:** Security is chosen as part of the trust evaluation metrics as it holds high importance and is closely intertwined in the establishment of trust [67]–[69].

Hence, before any task is going to be processed by a vehicle, it is necessary to evaluate the security level of the vehicle. However, security solutions for fog system developers and designers are lacking [70]. Assigning a value to a vehicle’s security would be difficult as this information is usually not disclosed unless specified. Our security calculation follows the method used in the real world where the value of security is the summation of multiple security-related metrics [71].

- **Reputation:** Trust and reputation are highly coupled and related in a distributed system. Reputation of a vehicle plays a part in the trust evaluation as it is also one of the most commonly metrics used [72]. Although reputation calculation might face issues of unfair ratings or dishonest feedback from users [73], here the reputation of the v-fog is given by the LB. The vehicles’ reputation would increase over time as the tasks assigned to them are completed.
- **Availability:** Availability of a v-fog is measured in terms of its parking duration. The LB would be able to estimate the v-fog’s parking duration from the Availability Behavior Prediction component in the LB. Unlike reputation, the availability of a v-fog will decrease over time.

Fuzzy Control System (FCS) poses the ability to mimic the human mind to effectively employ modes of approximate reasoning rather than exact [74]. Motivated by the wide use of FCS in trust evaluation [55], [61], [75], we have adopted the FCS for trust evaluation in the FCSTE component in this study. The three metrics described previously form the set $X = \{security, availability, reputation\}$ that are treated as the inputs of the FCS where each input is further characterized by a linguistic variable set, $L = \{poor, average, excellent\}$. Meanwhile, trust is the output represented by the linguistic variable set $P = \{poor, bad, average, good, excellent\}$ where their membership functions are shown in Fig. 3. To map the scalar input vector data into a scalar output, fuzzy rules are used. Based on (5), the number of rules i is equivalent to 27 to ensure all possible occurrences are covered in the FCS. These rules are defined in Table 2.

$$i = |X|^{|L|} \tag{5}$$

The Mamdani-based fuzzy inference system is applied where the “AND” operator for three antecedents and one consequent are used for the rules that follow the form “ $R_i = \text{if (security is } l \text{ AND availability is } l \text{ AND reputation is } l \text{) then (trust is } t \text{)}$ ”, where $l \in L$ and the trust value for each rule is represented by $t \in [0, 1]$. The trust output for every rule is derived based on heuristic reasoning and the final v-fog trust value is $v_t \in [0, 1]$.

Once the trust evaluation of the v-fog is done, the FCSTE component forwards the v-fog’s trust value to the Cluster Management component of the LB where the VCF algorithm is running ②. When the v-fog’s trust value falls in the trust value range of a logical cluster, it will be assigned to that logical cluster (c_i) which belongs in the set

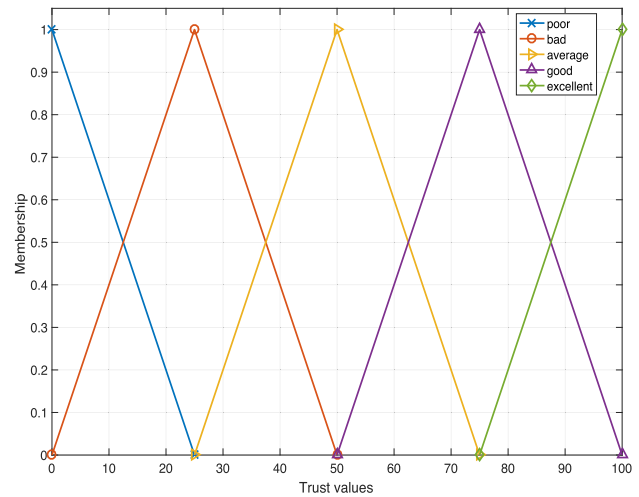


FIGURE 3. Fuzzy membership values for trust evaluation.

TABLE 2. Fuzzy-based rules to determine trust value of vehicles.

Rule	Security	Reputation	Availability	Trust
1	Excellent	Excellent	Excellent	Excellent
2	Excellent	Excellent	Average	Excellent
3	Excellent	Excellent	Poor	Good
4	Excellent	Average	Excellent	Excellent
5	Excellent	Average	Average	Good
6	Excellent	Average	Poor	Average
7	Excellent	Poor	Excellent	Good
8	Excellent	Poor	Average	Average
9	Excellent	Poor	Poor	Bad
10	Average	Excellent	Excellent	Excellent
11	Average	Excellent	Average	Good
12	Average	Excellent	Poor	Average
13	Average	Average	Excellent	Good
14	Average	Average	Average	Average
15	Average	Average	Poor	Bad
16	Average	Poor	Excellent	Average
17	Average	Poor	Average	Bad
18	Average	Poor	Poor	Bad
19	Poor	Excellent	Excellent	Good
20	Poor	Excellent	Average	Average
21	Poor	Excellent	Poor	Bad
22	Poor	Average	Excellent	Average
23	Poor	Average	Average	Bad
24	Poor	Average	Poor	Bad
25	Poor	Poor	Excellent	Bad
26	Poor	Poor	Average	Poor
27	Poor	Poor	Poor	Poor

$C = \{c_{i+1}, c_{i+2}, \dots, c_m\}$, where $i = 0$ and c_i represents the i th logical cluster in the set C ③. Over time, when a v-fog’s trust value changes due to its changing metric values, it will be moved to a logical cluster that accommodates the v-fog’s trust value. This vehicle clustering process is described later on in Algorithm 1 in Section III-C1. Moreover, the v-fogs that move away from the Trust Domain are no longer participating in the cluster. The current status of the logical clusters i.e. the workload status of the logical clusters of a LB are updated at the UPF ④. The UPF will use this information when it is needed by the MB. After elaborating on how the LB clusters

the v-fogs in its Trust Domain into multiple logical clusters, next we explain how the MB finds the most appropriate logical cluster in accomplishing the tasks.

Figure 2c shows that a client first sends a task request to the MB in the form of task metadata consisting of the trust requirement denoted as Tr ①. Upon receiving the task metadata, the Task Management component forwards the task metadata to the TMR component in the UPF where the TMR forwards it to the WLM in order to process the request ②. Having the workload status of logical clusters that are collected from the LB earlier, including the additional metrics mentioned in Section III-A i.e. R_c , T_d , and λ_f readily available in the WLM, the UPF forwards these statistics to the MB's Task Management component ③ to help the MB in the decision-making process. The logical clusters that meet the Tr are first selected. Then, based on T_d the Task Management component might find more than one of the selected logical clusters belonging in different Trust Domains that meet the R_{alr} (previously defined in Section III-A2). To ensure optimal performance and minimal latency, the Task Management component selects the logical cluster with the lowest value of T_d to process the task and notify the client ④. This is described further in Section III-C2. Once the client receives the cue, the client can send the task to the v-fogs of the logical cluster ⑤. After the task is completed, the v-fogs will notify the client ⑥.

C. PROPOSED ALGORITHMS

This part of the section elaborates on both the VCF and TM algorithms that are mentioned previously as follows:

1) VEHICLE CLUSTER FORMATION (VCF) ALGORITHM

Algorithm 1 shows that as a v-fog reaches a Trust Domain, the v-fog's trust value (v_t) is evaluated using FCS as explained in Section III-B where the three metrics i.e. security, reputation, and availability are considered. Depending on the number of clusters, each cluster has its own trust range predefined by an upper bound, T_{max} , and a lower bound T_{min} . After the v_t of a v-fog is evaluated and if the v-fog's v_t falls into a logical cluster's trust range, the v-fog is assigned to the logical cluster. The v-fog's v_t will change over time and the v-fog will be assigned to another logical cluster where its v_t fits into the logical cluster's trust range. However, when the v-fog moves away from the Trust Domain, it no longer participates in the cluster formation.

2) TASK MAPPING (TM) ALGORITHM

Algorithm 2 mainly aims at improving the resource utilization of the logical clusters. Clients with tasks to be processed pass their task metadata to the MB. After defining the number of logical clusters in a Trust Domain as well as the ρ_t (utilization threshold) of the v-fogs, the algorithm first acknowledges the client's Tr and R_{alr} requirements obtained from the metadata. Next, the algorithm creates a set LC_T with the logical clusters (c) that meet the Tr . From LC_T , the MB then identifies the c that meets the R_{alr} . They form the set LC_{RT} ,

Algorithm 1: Vehicle Cluster Formation (VCF) Algorithm

Data: security, availability, reputation values
Result: trust value, membership of a v-fog in a logical cluster

```

1 initialization;
2 v-fog joins a Trust Domain;
3 Set trust range upper bound and lower bound for each
  cluster as  $T_{max}$  and  $T_{min}$ ;
4 if v-fog is still in Trust Domain respectively then
5   LB obtains values from v-fog for X =
     {security, availability, reputation};
6   Evaluate  $v_t$  using FCS;
7   if  $T_{max} > v_t \geq T_{min}$  then
8     Assign v-fog to  $c_j$ ;
     /*  $j$  represents the  $j$ th logical
       cluster */
9
10 else
11   v-fog leaves cluster participation;
12 end

```

where $LC_{RT} \subseteq LC_T$. To ensure optimal performance and minimal latency, c with the lowest value of T_d is chosen to process the task.

If an incoming task is meant to be processed by c_{j+1} , it is referred to as a local task to c_{j+1} . In cases where the c_{j+1} is not present (i.e. no v-fog belong to c_{j+1}) or its $\bar{\rho}_t^{j+1}$, defined in (6), has exceeded the threshold, the task can only be processed by c_{j+2} if c_{j+2} has not exceeded its $\bar{\rho}_t^{j+2}$ and can still accommodate space to process. This task is known as a reassigned task to the c_{j+2} that is processing it. However, when c_{j+2} is unavailable, the MB will proceed to look at the rest of the logical clusters in an ascending manner until it finds one that can process the task. This implies that a logical cluster can not only process local tasks assigned to it, but it can also process reassigned tasks simultaneously as illustrated in Fig. 4. When none of the logical clusters are available, the task will then be dropped.

$$\bar{\rho}_T^j = \frac{\sum_{i=1}^m \rho_t^{(i)}}{m}, \quad (6)$$

where m represents the total number of v-fogs in a logical cluster.

The computation complexity of the VCF algorithm is $O(N)$, where N is the number of logical clusters. On the other hand for the TM algorithm, when a task is assigned to the logical cluster that meets the requirements it has a constant computation complexity of $O(N)$. However, when a task is a reassigned task, the computation complexity to execute the code block is proportional to the number of logical clusters, N . In this case, the computation complexity to run the second part of the TM algorithm will increase

Algorithm 2: Task Mapping (TM) Algorithm

Data: incoming tasks
Result: task assignment
Init:
 Set $j = 1$;
 Set $counter = 1$;
 Utilization threshold, th ;
 Logical cluster, c ;
 Number of logical cluster in a Trust Domain, m ;

```

1  $Task_{req} = \{Tr, R_{alr}\};$ 
  /* Client's task request */
2 while  $c$  is present do
3   if  $c$ 's trust satisfy  $Tr$  then
4      $c \in LC_T$ ;
5 end
6 for  $c \in LC_T$  do
7   /* Identify clusters that meet  $R_{alr}$  */
8   if  $R_{alr} \leq T_d^{(j,k)}$  then
9      $c \in LC_{RT}$ ;
10    if  $x \leq \min \{ T_d^{(j,k)} \}$  then
11       $c$  is picked.
12 end
13 if  $j \neq n$  then
14   if  $c_j$  size  $\neq 0$  and  $\rho < th$  then
15     Assign tasks to  $c_j$ ;
16 else
17   while  $counter \leq m$  do
18     if  $(counter + j) \neq m$  then
19       if  $c_j$  size  $\neq 0$  and  $\rho < th$  then
20         Assign tasks to  $c_{counter+j}$ ;
21       else if  $(counter + j) = m$  then
22         if  $c_m$  size  $\neq 0$  and  $\rho < th$  then
23           Assign tasks to  $c_m$ ;
24         else
25           Drop tasks;
26         end
27        $counter \leftarrow counter + 1$ ;
28 end
29 end
    
```

proportionately as N increases. Hence, the overall computation complexity of the TM algorithm is $O(N)$.

D. PROBLEM FORMULATION FOR MEASURING LATENCY

Prior to assigning a task to a logical cluster, T_d is needed to identify the logical clusters that can meet the client's R_{alr} . Figure 5 shows a sequence of events to help us to understand the incurring T_d throughout the process that can affect the performance of a logical cluster which is calculated as follows (7):

$$\bar{T}_d = \bar{T}_R + 2(\bar{T}_{MB} + \bar{T}_{UPF} + \bar{T}_{C,F}) + \bar{T}_{LB} + R_{c_i}, \quad (7)$$

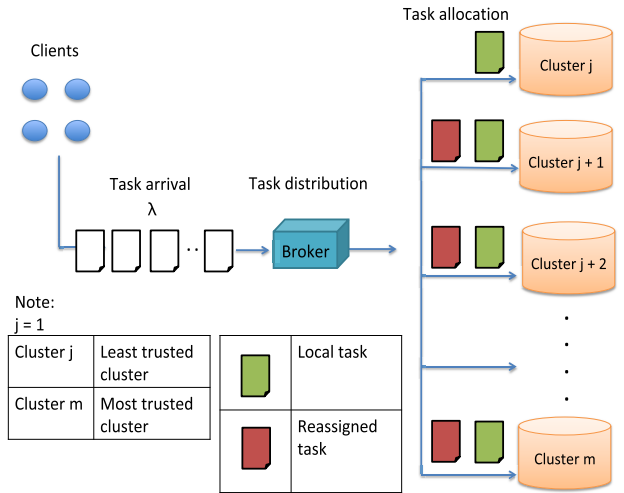


FIGURE 4. Arrival, distribution and allocation of local and reassigned tasks among logical clusters.

where T_R is the time taken for a client to send or receive a task associated request/response message. The time taken for the MB, UPF, and LB to process the message are denoted by T_{MB} , T_{UPF} , and T_{LB} respectively. $T_{C,F}$ is the time taken for the client to send the message to a logical cluster and back after the client receives the information on the selected logical cluster. Meanwhile, R_{c_i} is the response time of the i th logical cluster.

In our T_d calculation, we exclude the event of how the v-fogs are assigned to a logical cluster. As depicted in Fig. 5, at each node (e.g. UPF), a message experiences delay which is composed of mainly transmission (T_{trans}), propagation (T_{prop}) and processing delay (T_{proc}). Then, following the procedures stated in [76], we quantify the average delay a message experience at each node along with the propagation delay to reach that node as follows:

$$T_{node} = T_{trans} + T_{prop} + T_{proc}. \quad (8)$$

T_{trans} is the time required to transmit the message through the transmission channel given by (9).

$$T_{trans} = \frac{\text{length of message (bits)}}{\text{transmission rate of a node (kbps)}}. \quad (9)$$

T_{prop} is the time required for the message to propagate from one node to another that is calculated using (10).

$$T_{prop} = \frac{\text{distance of one node to another (m)}}{\text{transmission speed (m/s)}}. \quad (10)$$

Meanwhile T_{proc} refers to the time taken by the nodes to process the message which is calculated using (11) where μ_n is the service rate of a node. This processing may include activities in the node such as receiving message error detection and correction and processing it, checking for bit-level errors in the message that has occurred during transmission or deciding the message's next destination.

$$T_{proc} = \frac{1}{1 - \frac{\mu_n}{\lambda_l(t)}}. \quad (11)$$

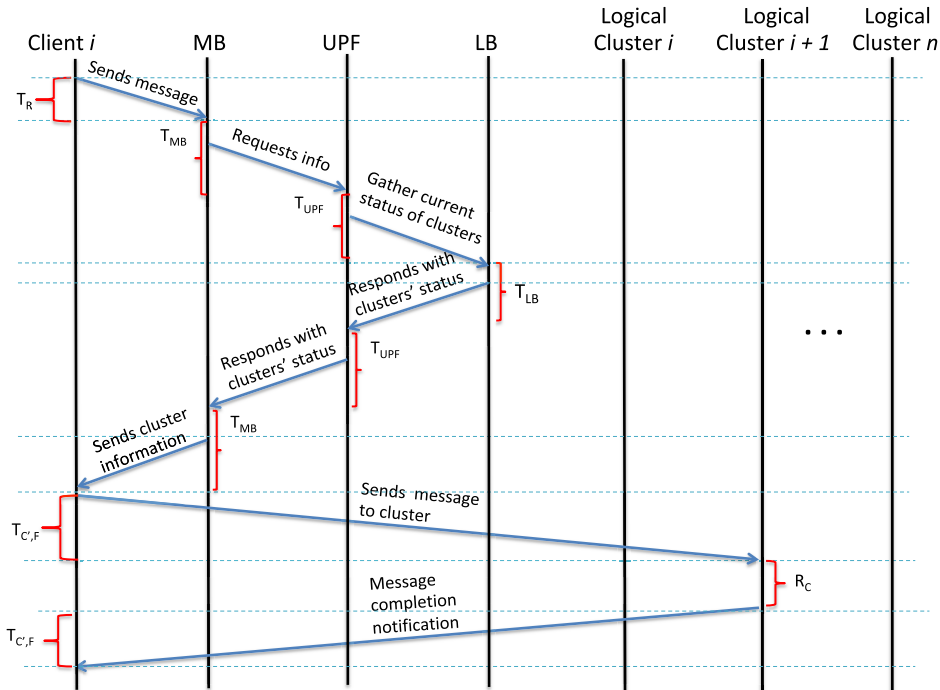


FIGURE 5. Event sequence from the point where a client sends a message for task processing to the MB to the point where the client receives the message with task completion notification from the logical cluster in the proposed solution with delay information under each node.

Based on the latency calculation of the M/M/1 queuing model in [76], we use (12) in order to calculate R_{c_i} at a given time, where m is the number of v-fogs, $\lambda_i(t)$ is the arrival rate of tasks and μ_i is the service rate of a v-fog.

$$R_{c_i} = \frac{1}{m\mu_i - \lambda_i(t)}. \quad (12)$$

In order for a logical cluster to be selected to process a task, the expression in (13) has to be met where $T_d^{(i,k)}$ is the delay between c_i and client k .

$$R_{alr} \geq T_d^{(i,k)}. \quad (13)$$

IV. PERFORMANCE EVALUATION

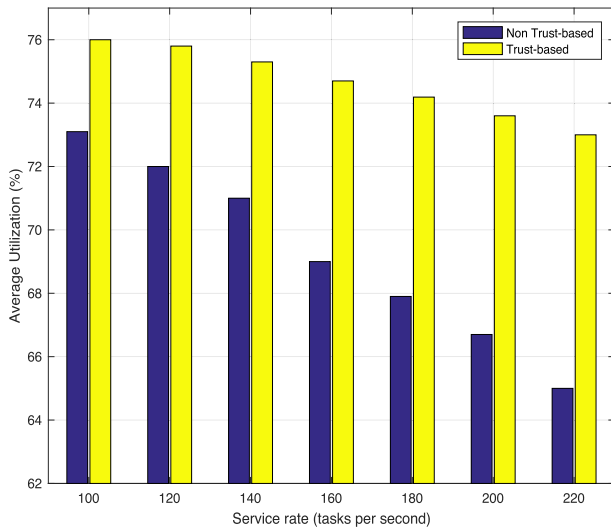
Performance comparisons between the proposed solution and the existing solution [55], herein referred as the Simple Matching solution, are made in this section. Our simulations are carried out using a Java-based simulator called iFogSim [77] where it is further modified to suit our algorithms. Three new classes, namely Tasks, Cluster and FuzzyEvaluation are added to the iFogSim simulator while the existing classes namely, DCNSFog, FogDevice, Controller and Config classes are partially altered. In order to reflect the role of the 5G components mentioned in Section III-A, we assume that some nodes in our simulator perform the role of UPF, MB and LB, where they take part in different activities including the vehicle cluster formation and task allocation. The incoming tasks which are tagged with IDs are of various sizes and have different expected

completion time. Although tasks with different trust requirements are generated randomly, the tasks are generated at a constant rate throughout the simulation. There are 80 v-fogs under each Trust Domain where these values remain constant and we assume that the security value for all v-fogs would be randomly generated and the values will remain constant throughout the simulation. Section IV-A demonstrates the importance of incorporating trust in task mapping in VFC, whereas Section IV-B through Section IV-D show the performance of the proposed work under the influence of varying task service rate, application latency requirement, and task arrival rate.

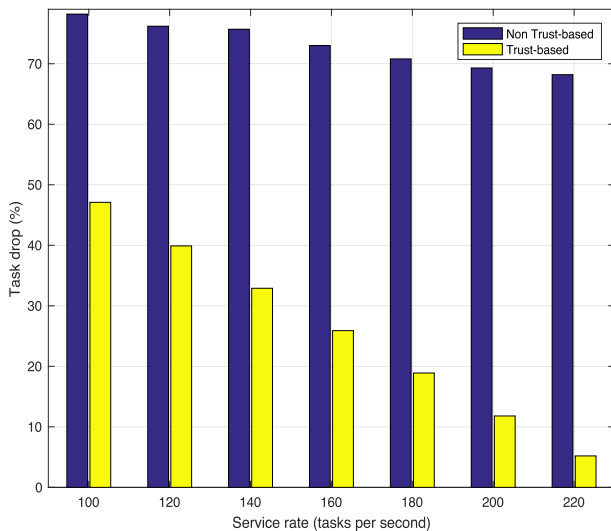
A. IMPORTANCE OF TRUST IN TASK MAPPING

Ensuring trust adds a layer of assurance to the end users and acts as one of the ways to aid a system in decision making. Trust-based task mapping is crucial in improving the VFC's performance. For comparison, we imagine an identical solution to our proposed solution, except that here the tasks are allocated randomly to the logical clusters regardless of the trust requirement of the task that needs to be met. We refer to this identical solution as a non trust-based task mapping in this section. The results are presented in Fig. 6 in order to impart the significance of our trust-based task mapping against the non trust-based task mapping.

Figure 6a shows that as the service rate increases, the average utilization decreases for both solutions. However, the average utilization of the trust-based task mapping outperforms the non trust-based task mapping where the former's



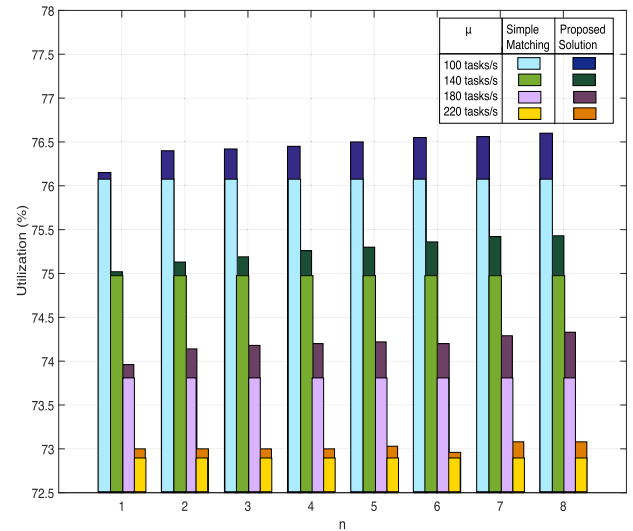
(a) Utilization performance comparison.



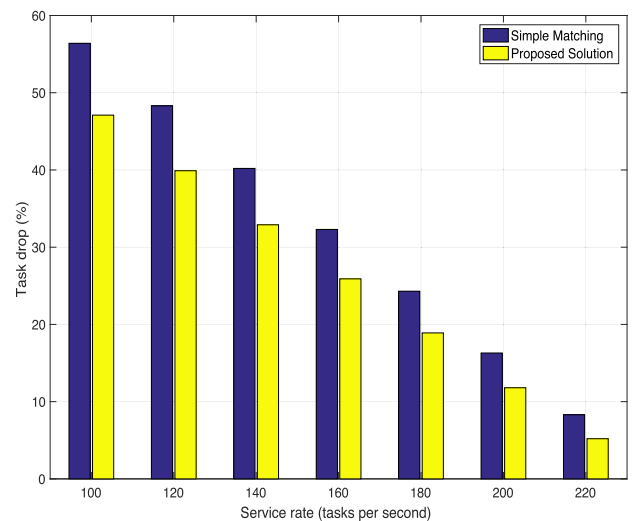
(b) Task drop performance comparison.

FIGURE 6. Performance comparison on utilization and task drop between trust-based task mapping and non trust-based task mapping.

average utilization has a minimum value of 73% and maximum value of 76%, whereas the latter’s average utilization has a minimum value of 65% and maximum value of 73%. Consequently, the decrease of utilization leads to the decrease of task drop as shown in Fig. 6b. Here, the non trust-based task mapping obtains higher percentage of task drop as compared to the trust-based task mapping. One possible reason is because the non trust-based task mapping assigns the tasks to the logical clusters that may not be suitable (it does not match the trust requirement) in serving the tasks, as the v-fogs with low trust value might leave the logical clusters while processing the tasks. Furthermore, it can be observed that as the service rate increases, the non trust-based task mapping only has a slight percentage decrease of task drop, whereas the trust-based task mapping shows a significant reduction of task drop from 46% to only 5%.



(a) Influence of task service rate on utilization.



(b) Influence of task service rate on task drop.

FIGURE 7. Effect of varying task service rate on cluster utilization and task drop.

B. INFLUENCE OF SERVICE RATE OF LOGICAL CLUSTERS

Simply balancing the incoming tasks to a matching logical cluster might be sufficient quality-wise, but not quantity-wise. Providing both quality and quantity is imperative for v-fogs as emphasizing only on quality can result in under-utilization of resources. The results in Fig. 7 show how the proposed solution is able to improve the logical cluster utilization and task drop performance. In this scenario, λ is set to 2 tasks/s and $\bar{\rho}_l$ (average utilization threshold of a logical cluster) is set to 0.8.

Figure 7a shows that as μ increases, the logical cluster utilization subsequently decreases for both Simple Matching and the proposed solution while maintaining same utilization threshold. However, the logical cluster utilization of the Simple Matching solution is almost the same throughout each logical cluster. On the other hand, the proposed solution

shows increasing utilization as the tasks are passed to the next logical cluster. This implies that the proposed solution is able to delegate more tasks towards more trusted logical clusters. Using the proposed solution, when μ increases from 100 tasks/s to 240 tasks/s, there is a noticeable decrease in utilization where the utilization of the logical clusters are becoming uniform. Furthermore, the increase in μ additionally results in declining percentage of task drop in both solutions as shown in Fig. 7b. When μ is 100 tasks/s, the proposed solution and the Simple Matching solution have task drop of 47% and 56% respectively. The task drop lowers to 5% and 8% for the proposed solution and the Simple Matching solution respectively as the μ increases to 220 tasks/s. The proposed solution outperforms the Simple Matching solution as it has demonstrated a lower task drop percentage.

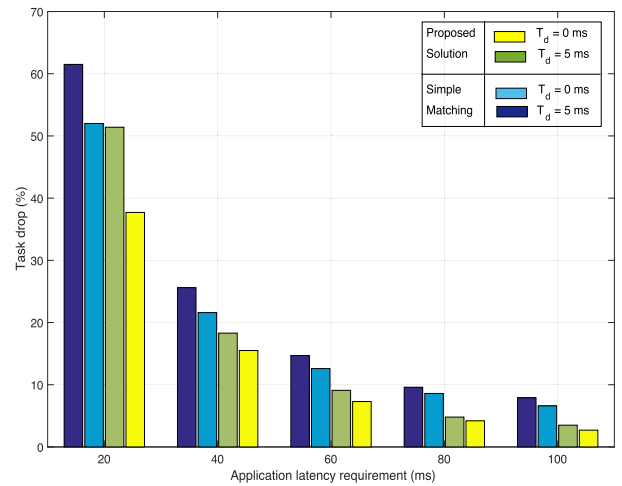
C. INFLUENCE OF APPLICATION LATENCY REQUIREMENT

As mentioned before, when a request first comes to the MB, the MB is responsible in identifying the closest LB to cater to the request. If the MB finds the condition stated in (13) is not met by all the logical clusters, the task will be rejected by the MB. Hence, in order to show how $T_d^{(i,k)}$ (delay between a client and a logical cluster) and R_{c_i} (response time of the i th logical cluster) can influence the performance in our proposed solution, we present the results in Fig. 8. In this scenario, λ is set to 1 tasks/s and μ is set to 100 tasks/s. Influence of the R_{alr} (application latency requirement) with $\bar{T}_d = 0$ ms and $\bar{T}_d = 5$ ms are measured against the percentage of task drop, average utilization, and the λ_f ranging from 20 ms to 100 ms (this includes the time when request is made until the time when the request is served)³.

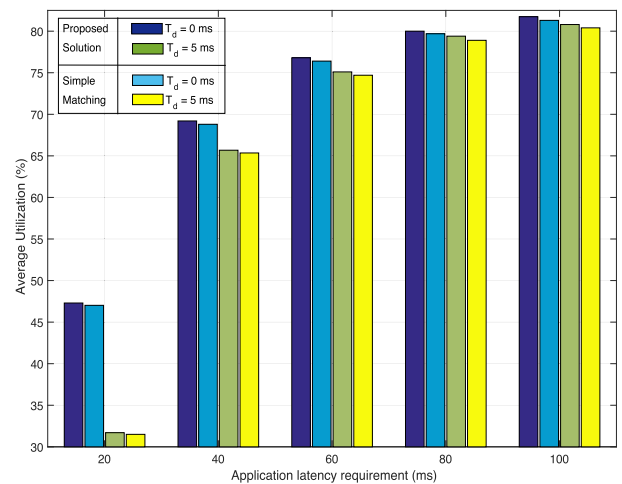
For simplicity of this study, we assume that the predefined R_{alr} is set by the VFC operator to a particular Trust Domain. Result in Fig. 8a shows that as the R_{alr} becomes relaxed, declining percentage of task drop is observed in both Simple Matching and proposed solution. In this figure, the proposed solution also exhibits a lower task drop compared to the Simple Matching solution in both $\bar{T}_d = 0$ ms and $\bar{T}_d = 5$ ms. This is because when the logical clusters have a stringent R_{alr} , the ρ_r (utilization threshold) is set smaller so that the response time remains within the R_{alr} . As the R_{alr} increases from 80 ms onward, the task drop is less than 10% for $\bar{T}_d = 0$ ms and $\bar{T}_d = 5$ ms in both the Simple Matching and proposed solution.

When the R_{alr} becomes lenient, increasing average utilization is observed in Fig. 8b where the proposed solution has a slightly higher average utilization compared to the Simple Matching solution. It can be observed that when $\bar{T}_d = 5$ ms, both the proposed solution and the Simple Matching solution experience lower average utilization compared to when $T_d = 0$ ms throughout the increasing R_{alr} . This indicates that as the \bar{T}_d increases, it can reduce the logical cluster utilization and selecting a logical cluster closer to the client is important

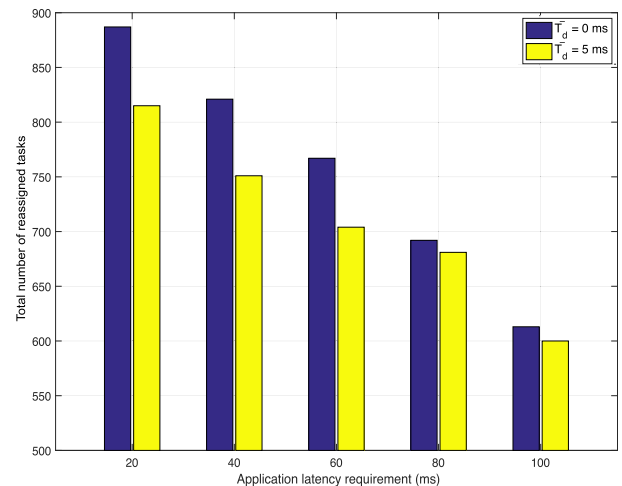
³Table 1 is used as a reference as to what kinds of applications that can be served in our solution.



(a) Influence of application latency requirement on task drop.



(b) Influence of application latency requirement on utilization.



(c) Influence of application latency requirement on total number of reassigned tasks.

FIGURE 8. Effect of application latency requirement on task drop, utilization and total number of reassigned tasks.

to maximize the utilization of the v-fogs. Figure 8c shows the influence of R_{alr} on the total λ_f (reassigned tasks) that is only

applicable to the proposed solution in both $\bar{T}_d = 0$ ms and $\bar{T}_d = 5$ ms. The increase of R_{alr} from 20 ms to 100 ms shows the reduction of the total λ_f from 880 to 630 for $\bar{T}_d = 0$ ms, and from 820 to 600 for $\bar{T}_d = 5$ ms. This is because the logical clusters are able to process the tasks in a relaxed manner and hence the tasks do not have to be processed by the subsequent logical clusters.

D. INFLUENCE OF TASK REQUEST ARRIVAL RATE

Similar to μ , λ can also influence the logical cluster performance. To show how the λ affects both the proposed solution and the Simple Matching solution, results are presented in Fig. 9. For these sets of experiments, A_{upper} and $\bar{\lambda}_l$ parameters are fixed predefined values, and μ is set to 100 tasks/s and $\bar{\rho}_t$ is set to 0.8. The logical cluster utilization increases as λ increases from 1 task/s to 3 tasks/s shown in Fig. 9a for both the proposed solution and the Simple Matching solution. The proposed solution produces a higher utilization compared to the Simple Matching solution, where the highest recorded utilization has reached 77% when λ is 3 tasks/s. In the Simple Matching solution, the average utilization is almost similar in all of the logical clusters, whereas in the proposed solution, increasing average utilization is observed in an ascending manner of the logical clusters (i.e. the higher trust value of the logical cluster, the more it is being utilized). However, as λ increases, the average utilization cannot be beyond $\bar{\rho}_t$ and λ above λ_{max} will not be admitted into the logical cluster.

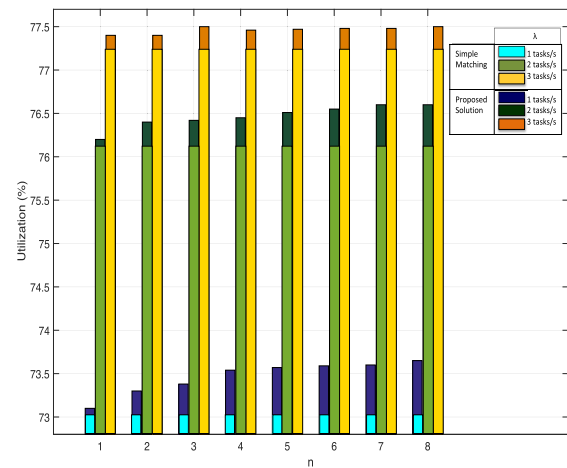
As previously mentioned, the value for λ_f is obtained from (4), and the result in Fig. 9b shows that when λ is doubled from 2 tasks/s to 4 tasks/s, the λ_f that a logical cluster has to process increases. Another important observation from this figure is that the logical cluster with high trust value tends to process more tasks than those with relatively low trust value (i.e. Cluster 1 has no λ_f task to process; whereas Cluster 8 processes the highest amount of tasks).

V. OPEN RESEARCH ISSUES

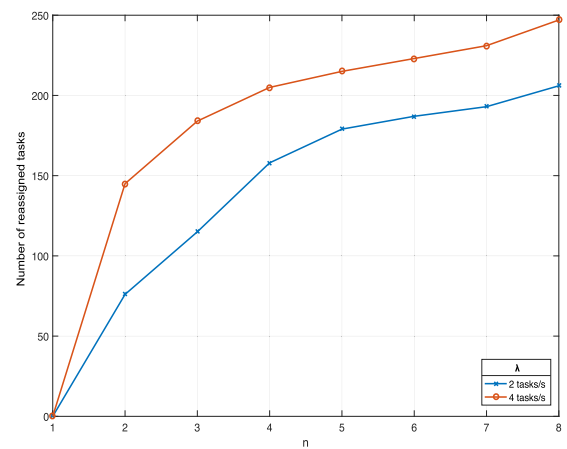
In this section, we discuss how the proposed solution can be further improved and we bring forward some issues that can be further studied in the future. These include defining the application latency requirement, defining optimal operational coverage, trust mapping, driver profiling, factors affecting delay, task migration issues and quantifying security.

A. DEFINING APPLICATION LATENCY REQUIREMENT

As the clients run myriad applications, applying the same R_{alr} for all the logical clusters in the Trust Domain may not be realistic. The stringent value of R_{alr} , the more tasks are being pushed to the logical clusters with high trust value. Ideally, the R_{alr} set by the VFC operator can be imposed to some or all logical clusters when needed. This VFC operator may need to understand the demands of the clients and the type of applications that the clients request prior to setting the percentage of logical clusters that need the R_{alr} . It also requires a dynamic mechanism that enables the R_{alr} to be



(a) Influence of task arrival rate on utilization.



(b) Influence of task arrival rate on the number of reassigned tasks.

FIGURE 9. Effect of varying task arrival rate on cluster utilization and the number of reassigned tasks.

set differently for these logical clusters in order to improve the clients' experience and at the same time increase the utilization of the v-fogs and reduce the task drop.

B. DEFINING OPTIMAL OPERATIONAL COVERAGE

Although, it was not the scope of this paper to decide how many LBs should be connected under one MB, it should be studied in the future as it has an impact on the overall VFC performance. As the management lies in the MB, it is necessary to know the maximum number of LBs that the MB is capable of managing, before it experiences performance degradation. Aside from adding burden to the MB, having LBs beyond that the MB can handle will increase additional delays including queuing delay and service delay while managing the LBs. Similarly, to ensure a logical cluster can perform within the required application latency requirement, it is important to consider the optimal number of clients that can be served under a logical cluster. Logical clusters that are highly dense with clients will encounter bottleneck as these clients communicate to the LB. This in turn will increase the response time and subsequently affect the overall

performance of a logical cluster as we have found in our result in Fig. 8, where it shows that application latency requirement would have significant impact on the utilization. Hence, network traffic needs to be managed efficiently in order to avoid traffic congestion. To achieve that, a potential candidate solution would be using Software-Defined Network (SDN) [78] and Network Function Virtualization (NFV) technologies for intelligent traffic engineering [79].

C. TRUST MAPPING

The use of fuzzy logic in this study has helped to define the grey area of trust where the LB considers trust range of 0 to 1. While it is known to the LB, the clients requesting for certain trust requirements would not know the precise trust value to ask for. For instance, if a client requests for the highly trusted service from the LB, it could mean any value from 0.7 to 1 from the LB's point of view, but in fact the client might only accept trust values of only 0.9 to 1. On the other hand, as various clients have varying trust values, a trust value of 0.5 could be untrustworthy for one client but not for the others. To put it simply, what may be trustworthy from the LB's perspective may not actually be trustworthy for the client and vice versa. The subjective nature of trust in this manner has to be tackled to allow both parties to find a middle ground for a trust unit that both can agree on. To avoid such confusion and mistranslation from both parties, it is crucial to address such problems to improve the quality of experience by the clients.

D. DRIVER PROFILING

This study considers the security, availability and reputation metrics to evaluate trust of a v-fog. Although a v-fog has one unique identification, it may not be driven by the same person every time and various drivers may exhibit different behavior (mobility and sojourn duration behavior). Varying behavior would be observed especially in scenarios where the vehicle is not used for personal purpose and the drivers frequently interchange. This can be observed such as when the v-fog is a commercial vehicle owned by a company, or a vehicle rented by tourists. This can alter the values of the availability metric and make precise future prediction difficult. One solution is to propose a driver profiling mechanism that dynamically adapts to the change of drivers. This is achievable through means such as face recognition capability that is applied at the entrance of the parking lot. Moreover, this can be beneficial if it is applicable in different locations as well since drivers tend to behave differently with respect to the location they are at.

E. FACTORS AFFECTING DELAY

As mentioned in Section III and illustrated in Fig. 5, there are various types of delay that encompass the end-to-end delay, \bar{T}_d . These include delay in sending a request for the broker \bar{T}_R , delay of responding from the LB to the client \bar{T}_{Rep} , delay of sending tasks from the cluster \bar{T}_{Rep} and from the cluster back to the client, $\bar{T}_{C,F}$. From Fig. 8, we have noticed that as the \bar{T}_d value increases, the performance degrades.

This indicates that it is important to devise ways in minimizing the delay to improve the logical cluster utilization and maintain optimal performance. To achieve this, the VFC needs a better operation procedure to help manage the overall network traffic flow. Additionally, an improved traffic steering or load balancing capability that incorporates the NFV may be beneficial.

F. TASK MIGRATION ISSUES

In the event where a v-fog is leaving a logical cluster in the midst of processing the tasks, the uncompleted part of the tasks can be migrated to other v-fogs in the same logical cluster to maintain high availability and assure that the trust requirement is still being met. Alternately, tasks can also be replicated to all v-fogs to ensure high availability where the same task can be processed in parallel in multiple vehicles. Furthermore, the LB can perform interval tracking to see the progress of the tasks being processed. However, if the client only moves from a Trust Domain to a different Trust Domain, the LB in that new Trust Domain can take control of the client and resume the request. This collaborative tracking between all the LBs can thus enhance the Quality of Service (QoS) as packets are being constantly monitored from the moment they are being processed until they are completed.

However, there would be several issues in task migration if the above-mentioned solutions are in place. Firstly, replicating the same task to some of the v-fogs in the logical cluster can ensure high availability but at the cost of high energy consumption in processing as well as adding redundancy that consumes the v-fogs processing capacity. This can impact the v-fogs performance if they are overloaded with tasks. Secondly, the availability of the v-fog can be impacted by the various types of parking restrictions. This will have an impact towards the kinds of tasks that are suitable to be processed by the v-fogs. Thus, an efficient and dynamic task mapping solution is needed to prevent these problems. Thirdly, upon leaving the logical cluster, the v-fog has to discard the work that they have processed to allocate other incoming tasks to be processed. This becomes a security concern if the v-fog still has records of the tasks. The tasks may contain sensitive and confidential information that should not be disclosed to an external party, as they can be exploited by malicious users to perform attacks. To ensure the tasks are discarded properly, the LB can perform a quick series of security checks on v-fogs prior to leaving the logical clusters.

G. QUANTIFYING SECURITY

Another important aspect that needs to be considered in a VFC is security. Quantifying security is a challenge knowing that security itself is an intangible metric. Security is not derived from a single metric as it comprises of myriad factors. In order to assess mobile security, Gartner has conducted various security evaluation towards mobile devices and operating systems where they specifically evaluate Android Enterprise security in two categories, built-in security and corporate-managed security [80]. To date, not many literature

have distinguished methods in evaluating security and the metrics needed in the evaluation. Understandably, this is due to the broad scope of security itself and its applications in various layers. Although ensuring the utmost security is desirable, having rigid security can nonetheless render higher processing and response time. Hence, it is imperative to balance security and QoS to achieve optimal performance, and more studies should be conducted to understand security in order to measure it.

VI. CONCLUSION

The study of vehicles acting as fogs has been rising as of late. However, unlike the conventional fog devices, fog operators may face challenges when the vehicles become part of fog computing. We believe that security alone will not be enough to integrate the vehicles as part of a fog computing infrastructure as a fog (computing device) needs to ensure not only security to its customers, but also its availability. Therefore, evaluating their trust which can be measured through different factors is imperative. This study is the first effort that provides a trust-based edge computing solution for off-street vehicular fog environment. Our work differs from the existing trust evaluation of mobile v-fogs as the metrics they have used such as velocity, speed and direction are not applicable to stationary or parked v-fogs. Hence, we have chosen a set of metrics (i.e. security, availability, and reputation) for trust evaluation that are more relevant and suitable for the scenario of our study. Additionally, this study demonstrates how the v-fogs can be integrated with 5G infrastructure in order to leverage its capacity. We propose a novel architecture and procedures taking into consideration different 5G core network equipment that will come in to play in order make this successful integration. Results from the performance comparison between the Simple Matching solution and the proposed solution show that the proposed solution has performed better based on its increasing utilization and lesser percentage of task drop. This paper also presented several open research issues that should be studied for future research.

REFERENCES

- [1] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul. 2019.
- [2] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 42–50, Sep. 2019.
- [3] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, "A cooperative quality-aware service access system for social Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2506–2517, Aug. 2018.
- [4] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 2, pp. 426–441, Mar. 2020.
- [5] A. M. I. Yura, S. H. S. Newaz, F. H. Rahman, T. W. Au, G. M. Lee, and T.-W. Um, "Evaluating TCP performance of routing protocols for traffic exchange in street-parked vehicles based fog computing infrastructure," *J. Cloud Comput.*, vol. 9, no. 1, pp. 1–20, Dec. 2020.
- [6] *Keeping the Nation Moving: Facts on Parking*, RAC Found., London, U.K., Oct. 2012.
- [7] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyber-physical systems," *Future Gener. Comput. Syst.*, vol. 56, pp. 476–492, Mar. 2016, doi: 10.1016/j.future.2015.09.004.
- [8] A. Lutfi, A. Zouinkhi, and M. S. Bouhlel, "Smart trust management for vehicular networks," *Int. J. Electron. Comput., Energetic, Electron. Commun. Eng.*, vol. 10, no. 8, pp. 1107–1114, 2016.
- [9] H. Gong and L. Yu, "Content downloading with the assistance of roadside cars for vehicular ad hoc networks," *Mobile Inf. Syst.*, vol. 2017, pp. 1–9, Sep. 2017.
- [10] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA J. Autom. Sinica*, vol. 5, no. 1, pp. 19–35, Jan. 2018.
- [11] C. Huang, F. Naghdy, H. Du, and H. Huang, "Shared control of highly automated vehicles using steer-by-wire systems," *IEEE/CAA J. Autom. Sinica*, vol. 6, no. 2, pp. 410–423, Mar. 2019.
- [12] A. Greenberg, "A deep flaw in your car lets hackers shut down safety features," *Wired*, vol. 11, pp. 26–30, Aug. 2017. [Online]. Available: <https://www.wired.com/story/car-hack-shut-down-safety-features/>
- [13] E. Weise. (2017). *Chinese Group Hacks a Tesla for the Second Year in a Row*. [Online]. Available: <https://www.usatoday.com/story/tech/2017/07/28/chinese-group-hacks-tesla-second-year-row/518430001/>
- [14] K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Oct. 2016, pp. 1044–1055. [Online]. Available: <http://dl.acm.org/citation.cfm?doi=2976749.2978302>
- [15] C. C. Byers, "Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for fog-enabled IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 14–20, Aug. 2017.
- [16] ITU-Report. (2014). *The Tactile Internet*. Accessed: Apr. 25, 2019. [Online]. Available: <https://www.itu.int/oth/T2301000023/en>
- [17] G. Yang, X. Lin, Y. Li, H. Cui, M. Xu, D. Wu, H. Rydén, and S. B. Redhwan, "A telecom perspective on the Internet of drones: From LTE-advanced to 5G," pp. 1–8, 2018, *arXiv:1803.11048*. [Online]. Available: <https://arxiv.org/abs/1803.11048>
- [18] J. Zhang, C. Chen, and R. Cohen, "Trust modeling for message relay control and local action decision making in VANETs," *Secur. Commun. Netw.*, vol. 6, no. 1, pp. 1–14, Jan. 2013.
- [19] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 90, pp. 1–13, Jul. 2018, doi: 10.1016/j.adhoc.2018.08.010.
- [20] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.
- [21] H. Oh, T.-W. Um, and J. K. Choi, "Trust provisioning for future ICT infrastructures and services," ITU-T, Geneva, Switzerland, Tech. Rep. TD267, 2016.
- [22] R. Cogill, O. Gallay, W. Griggs, C. Lee, Z. Nabi, R. Ordóñez, M. Ruffli, R. Shorten, T. Tchakian, R. Verago, F. Wirth, and S. Zhuk, "Parked cars as a service delivery platform," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2014, pp. 138–143.
- [23] F. Hagenauer, F. Dressler, O. Altintas, and C. Sommer, *Cars as a Main ICT Resource of Smart Cities*. Amsterdam, The Netherlands: Elsevier, 2016, ch. 7, doi: 10.1016/B978-0-12-803454-5.00007-9.
- [24] S. K. Datta, J. Haerri, C. Bonnet, and R. F. Da Costa "Vehicles as connected resources: Opportunities and challenges for the future," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 26–35, Jun. 2017.
- [25] B. Baron, M. Campista, P. Spathis, L. H. M. K. Costa, M. D. de Amorim, O. C. M. B. Duarte, G. Pujolle, and Y. Viniotis, "Virtualizing vehicular node resources: Feasibility study of virtual machine migration," *Veh. Commun.*, vol. 4, pp. 39–46, Apr. 2016, doi: 10.1016/j.vehcom.2016.04.001.
- [26] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Vehicle as a resource (VaaR)," *IEEE Netw.*, vol. 29, no. 1, pp. 12–17, Jan./Feb. 2015.
- [27] N. Liu, M. Liu, G. Chen, and J. Cao, "The sharing at roadside: Vehicular content distribution using parked vehicles," in *Proc. 31st Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Mar. 2012, pp. 2641–2645.
- [28] S. Abdelhamid, H. S. Hassanein, G. Takahara, and H. Farahat, "Caching-assisted access for vehicular resources," in *Proc. 39th Annu. IEEE Conf. Local Comput. Netw.*, Sep. 2014, pp. 28–36.
- [29] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "On-road caching assistance for ubiquitous vehicle-based information services," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5477–5492, Dec. 2015.
- [30] L. Gu, D. Zeng, S. Guo, and B. Ye, "Leverage parking cars in a two-tier data center," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 4665–4670.

- [31] H. Gong, L. Yu, N. Liu, and X. Zhang, "Mobile content distribution with vehicular cloud in urban VANETs," *China Commun.*, vol. 13, no. 8, pp. 84–96, Aug. 2016.
- [32] U. Shevade, Y.-C. Chen, L. Qiu, Y. Zhang, V. Chandar, M. K. Han, H. H. Song, and Y. Seung, "Enabling high-bandwidth vehicular content distribution," in *Proc. 6th Int. Conf. Co-NEXT*, 2010, p. 1. [Online]. Available: <http://portal.acm.org/citation.cfm?doid=1921168.1921199>
- [33] Z. Su, Q. Xu, Y. Hui, M. Wen, and S. Guo, "A game theoretic approach to parked vehicle assisted content delivery in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6461–6474, Jul. 2017.
- [34] M. Aissa, A. Belghith, and B. Bouhdid, "Cluster connectivity assurance metrics in vehicular ad hoc networks," *Procedia Comput. Sci.*, vol. 52, pp. 294–301, Jan. 2015, doi: [10.1016/j.procs.2015.05.088](https://doi.org/10.1016/j.procs.2015.05.088).
- [35] H. R. Arkian, R. E. Atani, and A. Pourkhalili, "A stable clustering scheme based on adaptive multiple metric in vehicular ad-hoc networks," *J. Inf. Sci. Eng.*, vol. 31, pp. 1–16, Mar. 2013.
- [36] N. Maslekar, M. Boussedjra, J. Mouzna, and H. Labiod, "A stable clustering algorithm for efficiency applications in VANETs," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2011, pp. 1188–1193.
- [37] O. A. Wahab, H. Otrouk, and A. Mourad, "VANET QoS-OLSR: QoS-based clustering protocol for vehicular ad hoc networks," *Comput. Commun.*, vol. 36, no. 13, pp. 1422–1435, Jul. 2013.
- [38] O. A. Wahab, A. Mourad, H. Otrouk, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks," *Expert Syst. Appl.*, vol. 50, pp. 40–54, May 2016.
- [39] F. Hagenauer, C. Sommer, T. Higuchi, O. Altintas, and F. Dressler, "Poster: Using clusters of parked cars as virtual vehicular network infrastructure," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 7–8.
- [40] V. P. Harigovindan, A. V. Babu, and L. Jacob, "Proportional fair resource allocation in vehicle-to-infrastructure networks for drive-thru Internet applications," *Comput. Commun.*, vol. 40, pp. 33–50, Mar. 2014, doi: [10.1016/j.comcom.2013.12.001](https://doi.org/10.1016/j.comcom.2013.12.001).
- [41] M. Nabi, R. Benkoczi, S. Abdelhamid, and H. S. Hassanein, "Resource assignment in vehicular clouds," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
- [42] H. R. Arkian, R. E. Atani, and A. Pourkhalili, "A cluster-based vehicular cloud architecture with learning-based resource management," in *Proc. IEEE 6th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2014, pp. 162–167, doi: [10.1109/CloudCom.2014.157](https://doi.org/10.1109/CloudCom.2014.157).
- [43] Z. Ning, P. Dong, X. Wang, J. J. P. C. Rodrigues, and F. Xia, "Deep reinforcement learning for vehicular edge computing: An intelligent offloading system," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, 2019, Art. no. 60.
- [44] S. Midya, A. Roy, K. Majumder, and S. Phadikar, "Multi-objective optimization technique for resource allocation and task scheduling in vehicular cloud architecture: A hybrid adaptive nature inspired approach," *J. Netw. Comput. Appl.*, vol. 103, pp. 58–84, Feb. 2018, doi: [10.1016/j.jnca.2017.11.016](https://doi.org/10.1016/j.jnca.2017.11.016).
- [45] Y. Sun, X. Guo, S. Zhou, Z. Jiang, X. Liu, and Z. Niu, "Learning-based task offloading for vehicular cloud computing systems," 2018, *arXiv:1804.00785*. [Online]. Available: <http://arxiv.org/abs/1804.00785>
- [46] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.
- [47] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET: A survey," *Procedia Comput. Sci.*, vol. 45, pp. 592–601, Jan. 2015.
- [48] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, no. 1, pp. 325–344, Apr. 2014.
- [49] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. R. Baee, and S. Mandala, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, pp. 1–22, May 2015.
- [50] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Gener. Comput. Syst.*, vol. 88, pp. 16–27, Nov. 2018, doi: [10.1016/j.future.2018.05.008](https://doi.org/10.1016/j.future.2018.05.008).
- [51] N. Yang, "A similarity based trust and reputation management framework for VANETs," *Int. J. Future Gener. Commun. Netw.*, vol. 6, no. 2, pp. 25–34, 2013.
- [52] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017, doi: [10.1016/j.adhoc.2016.10.011](https://doi.org/10.1016/j.adhoc.2016.10.011).
- [53] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Electr. Eng.*, vol. 43, pp. 33–47, Apr. 2015, doi: [10.1016/j.compeleceng.2015.02.018](https://doi.org/10.1016/j.compeleceng.2015.02.018).
- [54] S. Oubabas, R. Aoudjit, J. J. P. C. Rodrigues, and S. Talbi, "Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme," *Veh. Commun.*, vol. 13, pp. 128–138, Jul. 2018, doi: [10.1016/j.vehcom.2018.08.001](https://doi.org/10.1016/j.vehcom.2018.08.001).
- [55] F. H. Rahman, T.-W. Au, S. H. S. Newaz, W. S. Suhaili, and G. M. Lee, "Find my trustworthy fogs: A fuzzy-based trust evaluation framework," *Future Gener. Comput. Syst.*, vol. 109, pp. 562–572, Aug. 2020, doi: [10.1016/j.future.2018.05.061](https://doi.org/10.1016/j.future.2018.05.061).
- [56] X. Li, H. Ma, F. Zhou, and W. Yao, "T-broker: A trust-aware service brokering scheme for multiple clouds collaborative services," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1402–1415, Jul. 2015.
- [57] P. Zhang, Y. Kong, and M. Zhou, "A domain partition-based trust model for unreliable clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2167–2178, Sep. 2018.
- [58] O. Hafez and K. Bhattacharya, "Optimal design of electric vehicle charging stations considering various energy resources," *Renew. Energy*, vol. 107, pp. 576–589, Jul. 2017, doi: [10.1016/j.renene.2017.01.066](https://doi.org/10.1016/j.renene.2017.01.066).
- [59] S. Kekki, W. Featherstone, Y. Fang, P. Kuure, A. Li, A. Ranjan, D. Purkayastha, F. Jiangping, D. Frydman, G. Verin, K.-W. Wen, K. Kim, R. Arora, A. Odgers, L. M. Contreras, and S. Scarpina, "MEC in 5G networks," ETSI, Sophia Antipolis, France, White Paper 28, 2018, pp. 1–28, no. 28.
- [60] I. Leyva-Pupo, A. Santoyo-González, and C. Cervelló-Pastor, "A framework for the joint placement of edge service infrastructure and user plane functions for 5G," *Sensors*, vol. 19, no. 18, p. 3975, Sep. 2019.
- [61] A. Tadjeddine, A. Kayssi, A. Chehab, and H. Artail, "Fuzzy reputation-based trust model," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 345–355, Jan. 2011.
- [62] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting reputation-based trust management for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2016.
- [63] N. T. Thomopoulos, *Fundamentals of Queuing Systems: Statistical Methods for Analyzing Queuing Models*. New York, NY, USA: Springer, 2012.
- [64] S. H. S. Newaz, Á. Cuevas, G. M. Lee, N. Crespi, and J. K. Choi, "Adaptive delay-aware energy efficient TDM-PON," *Comput. Netw.*, vol. 57, no. 7, pp. 1577–1596, May 2013.
- [65] S. H. S. Newaz, M. S. Jang, F. Y. M. Alaelddin, G. M. Lee, and J. K. Choi, "Building an energy-efficient uplink and downlink delay aware TDM-PON system," *Opt. Fiber Technol.*, vol. 29, pp. 34–52, May 2016.
- [66] R. Buyya, A. Beloglazov, and J. Abawajy, "Energy-efficient management of data center resources for cloud computing: A vision, architectural elements, and open challenges," 2010, *arXiv:1006.0308*. [Online]. Available: <http://arxiv.org/abs/1006.0308>
- [67] V. Jain, R. S. Kushwah, and R. S. Tomar, "Named data network using trust function for securing vehicular ad hoc network," in *Soft Computing: Theories and Applications*, vol. 742. Singapore: Springer, 2019, pp. 463–471. [Online]. Available: <http://link.springer.com/10.1007/978-981-13-0589-4>
- [68] X. Wu, R. Zhang, B. Zeng, and S. Zhou, "A trust evaluation model for cloud computing," *Procedia Comput. Sci.*, vol. 17, pp. 1170–1177, Jan. 2013, doi: [10.1016/j.procs.2013.05.149](https://doi.org/10.1016/j.procs.2013.05.149).
- [69] C. D. Jensen, "The importance of trust in computer security," in *Trust Management VIII (IFIP Advances in Information and Communication Technology)*, J. Zhou, N. Gal-Oz, J. Zhang, and E. Gudes, Eds. Berlin, Germany: Springer, 2014, pp. 0–12.
- [70] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, Dec. 2017, Art. no. 19.
- [71] *How Bitsight Calculates Security Ratings*, BitSight, Boston, MA, USA, 2019.
- [72] R. Mühlbauer and J. Kleinschmidt, "Bring your own reputation: A feasible trust system for vehicular ad hoc networks," *J. Sens. Actuator Netw.*, vol. 7, no. 3, p. 37, Sep. 2018.
- [73] Y. Wu, C. Yan, Z. Ding, G. Liu, P. Wang, C. Jiang, and M. Zhou, "A novel method for calculating service reputation," *IEEE Trans. Autom. Sci. Eng.*, vol. 10, no. 3, pp. 634–642, Jul. 2013.
- [74] H. Suzuki, "Fuzzy sets and membership functions," *Fuzzy Sets Syst.*, vol. 58, no. 2, pp. 61–103, Sep. 1993. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/0165011493904895>

- [75] A.-S. Yin and S.-Y. Zhang, "A survey of trusted network trust evaluation methods," in *Security and Privacy in New Computing Environments* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 284, J. Li, Z. Liu, and H. Peng, Eds. Cham, Switzerland: Springer, 2019, pp. 87–95. [Online]. Available: <http://link.springer.com/10.1007/978-3-030-21373-2>
- [76] O. J. Pandey and R. M. Hegde, "Low-latency and energy-balanced data transmission over cognitive small world WSN," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7719–7733, Aug. 2018.
- [77] R. Mahmud and R. Buyya, "Modeling and simulation of fog and edge computing environments using iFogSim toolkit," in *Fog and Edge Computing: Principles and Paradigms*, R. Buyya and S. N. Srirama, Eds. Hoboken, NJ, USA: Wiley, 2019, ch. 17, pp. 433–465.
- [78] X. Wang, C. Wang, J. Zhang, M. Zhou, and C. Jiang, "Improved rule installation for real-time query service in software-defined Internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 2, pp. 225–235, Feb. 2017.
- [79] A. S. D. Alfoudi, S. H. S. Newaz, A. Otebolaku, G. M. Lee, and R. Pereira, "An efficient resource management mechanism for network slicing in a LTE network," *IEEE Access*, vol. 7, pp. 89441–89457, 2019.
- [80] E. Liderman. (2019). *Android Enterprise Security Assessed by Gartner*. [Online]. Available: <https://www.blog.google/products/android-enterprise/android-enterprise-security-assessed-gartner/>



FATIN HAMADAH RAHMAN received the bachelor's degree in computer network and security from Universiti Teknologi Brunei (UTB), Brunei, in 2016. She is currently pursuing the Ph.D. degree in computing and information systems with Universiti Malaya. She has undergone an internship under the Security Research Group, Universiti Malaya, Malaysia. She has published her research in several renowned conferences and journals, such as *Future Generation Computer Systems*, (Elsevier), the *Journal of Cloud Computing* (Springer), and the IEEE ICAC. Her research interests include fog computing, the IoT, trust management, and network security.



S. H. SHAH NEWAZ (Senior Member) received the B.Sc. degree in information and communication engineering from East West University (EWU), Dhaka Bangladesh, and the M.Sc. and Ph.D. degrees from the Korea Advanced Institute of Science and Technology (KAIST), in 2010 and 2013, respectively. During his Ph.D. degree at KAIST, he served as a collaborating Researcher with the Institute Telecom, Telecom SudParis, France. He served as a Postdoctoral Researcher with KAIST, from August 2013 to July 2016. He is currently working as a Lecturer under the School of Computing and Informatics (SCI), Universiti Teknologi Brunei (UTB), Brunei. He is also holding an Adjunct Professor position with KAIST, South Korea. He has written and coauthored in more than 60 prestigious international journals and conferences. His research interests include energy-efficient passive optical networks, network function virtualization, software defined networks, mobility and energy efficiency issue in wireless networks, local cloud/fog computing, smart grid and content delivery networks, all with specific focus, mainly on protocol design and performance aspects. He is a member of ACS.



THIEN WAN AU received the B.Eng. degree in electrical and electronics Engineering from the University of Glasgow, U.K., the M.Sc. degree in data communications systems from Brunel University, U.K., and the Ph.D. degree from the University of Queensland, Australia. He is currently an Assistant Professor and the Dean of the Graduate Studies and Research Office, Universiti Teknologi Brunei (UTB). His research includes disaster management, sensor networks, edge and fog computing, software defined network (SDN), the Internet of Things,

android systems, intelligent agent systems, and eLearning experiential learning. His research works have been published in more than 40 articles in academic journals and conferences. He has also recently completed a few projects, such as Providing an Efficient and Reliable ICT Infrastructure for Smart Grid Data Analytics through Fog Computing, Mathematical Wall, and Development of Software Agent-based Smart Prepaid Wireless Energy Meter. He has also been invited as a Keynote and a Guest Speakers to conferences.



WIDA SUSANTY SUHAILI received the B.Sc. degree in computer science and M.Sc. degree (Hons.) from the University of Strathclyde, Glasgow, U.K., in 2003 and 2004, respectively, and the Ph.D. degree in education technology from the University of Edinburgh, U.K., in 2015. As an Assistant Professor with the School of Computing and Informatics, Universiti Teknologi Brunei (UTB), she has focused on SMART Initiative projects upon obtaining her Ph.D. She is the Project Coordinator of the school where she foresees all the student projects within the School. She is the Thrust Lead of Digital and Creativity research thrust in the University. She has been actively involved in SMART research projects under ASEAN IVO with the theme smart environment, smart agriculture, smart disaster management, and smart Cities. She is also the ASEAN S&T Fellowship 2019/2020, where her focus is on the use of Science Technology and Innovation in the improvement of paddy plantation in Brunei. Her research interests include the Internet of Things (IoT), data communications networking, and cloud computing.



GYU MYOUNG LEE (Senior Member, IEEE) joined the Liverpool John Moores University (LJMU), U.K., in 2014, as a Senior Lecture with the Department of Computer Science and was promoted to a Reader, in 2017. He has been with the KAIST Institute for IT convergence, Daejeon, South Korea, as an Adjunct Professor, since 2012. Before joining the LJMU, he worked with the Institut Mines-Telecom, Telecom SudParis, from 2008. Until 2012, he was invited to work with the Electronics and Telecommunications Research Institute (ETRI), South Korea. He worked as a Research Professor with KAIST, South Korea, and a Guest Researcher with the National Institute of Standards and Technology (NIST), USA, in 2007. He worked as a Visiting Researcher with the University of Melbourne, Australia, in 2002. Furthermore, he also has work experience in industries in South Korea. His research interests include the Internet of Things, Web of Things, computational trust, knowledge centric networking, and services considering all vertical services, smart grid, energy saving networks, cloud-based big data analytics platform, and multimedia networking and services. He has been actively participating in standardization meetings including ITU-T SG 13 (Future Networks and cloud) and SG20 (IoT and smart cities and communities), IETF, and oneM2M, and so on, and currently serves as a Rapporteur of Q16/13 (Knowledge centric trustworthy networking and services) and Q4/20 (e/Smart services, applications and supporting platforms) in ITU-T. He is also the Chair of ITU-T Focus Group on Data Processing and Management (FG-DPM) to support the IoT and smart cities and communities. He has contributed more than 300 proposals for standards and published more than 100 articles in academic journals and conferences. He received several Best Paper Awards in international and domestic conferences and served as a Reviewer of the IEEE journals/conference papers and an Organizer/Member of committee of international conferences.

...