This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3019795, IEEE Access

Digital Object Identifier

Trusted Orchestration for Smart Decision-Making in Internet of Vehicles

GEETANJALI RATHEE[1], SAHIL GARG[2], (Member, IEEE), GEORGES KADDOUM[2], (Member, IEEE), BONG JUN CHOI[3], (Senior Member, IEEE), AND M. SHAMIM HOSSAIN.[4], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat-173234, H.P., India (e-mail: geetanjali.rathee123@gmail.com)
[2]Electrical Engineering Department, École de technologie supérieure, Université du Québec, Montréal, QC H3C 1K3, Canada (e-mail: sahil.garg@ieee.org and georges.Kaddoum@etsmtl.ca)
[3]School of Computer Science and Engineering, Soongsil University, Seoul 06978, South Korea (e-mail: davidchoi@soongsil.ac.kr)
[4]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mshossain@ksu.edu.sa)

Corresponding authors: M. Shamim Hossain (e-mail: mshossain@ksu.edu.sa) and Bong Jun Choi (e-mail: davidchoi@soongsil.ac.kr)

This research was supported under the National Research Foundation (NRF), Korea (2019R1C1C1007277) funded by the Ministry of Science and ICT (MSIT), Korea, and the Researchers Supporting Project number (RSP-2020/32), King Saud University, Riyadh, Saudi Arabia.

ABSTRACT Decision-making is of critical significance in Internet-of-Vehicles (IoV), where vehicles need to quickly make decisions in real-time when sharing or transferring the information. In addition, it is necessary to identify the significant factors of an entity while measuring its legitimacy or to record the real-time data generated by it. Traditional automated schemes in IoV are confronted by the issues related to real-time processing and the manner they respond, such as traffic congestion information, fastest route selection, and road accidental information. The exchange of accurate information among vehicles is critical, but the decision-making for IoV has still not been fully investigated in the literature. Further, the involvement of malicious devices in the network may disgrace the network performance by consuming network resources. In this paper, we propose a hybrid decision-making scheme in vehicular informatics for data transferring and processing through VIKOR and analytic hierarchy process (AHP) methods. The proposed model is scrutinized and verified rigorously through several sensing and decision-making metrics against a conventional solution. The simulation results depict that the proposed model leads to 93 percent competence in terms of decision-making, identification of legitimate sensors, and data alteration process when sharing the information through various sensors in IoV.

INDEX TERMS Internet of Vehicles, Decision-making Framework, VIKOR, Analytic hierarchy process, Trusted scheme, Data Sharing

I. INTRODUCTION

THE internet-of-things (IoT) is an umbrella term for recent wireless applications or technologies that comprise processing, sensing, managing, and controlling of a huge amount of information for service-based or application-based developments [1]. In IoT applications, such as smart industrial manufacturing, smart homes, intelligent transportation system (ITS), and Internet-of-Vehicles (IoV), controlling, sharing, managing, and transferring of entities is done through smart devices to provide scalable and updated information to meet application needs [2]–[4]. The exponential growth in today's vehicular technologies has led to the combination of several techniques like IoV, VANETs, and cloud, forming an IoV computing environment to deal with various problems that may occur on roads due to congestion and other traffic issues in real-time [5]. The increased number of vehicles has led IoV to become the most prolonged technological motivation in today's world. The IoV technology enables the vehicle to perform advanced activities by incorporating various smart sensors and processors inside the vehicle for accessing the various information for safe driving, e.g., driving skills, cameras, and sensors to predict the emotional and physical situation of the driver, etc. [6]–[9]. The IoV uses the communication network and computational intelligence of the vehicles for monitoring surroundings and communicating with other vehicles in real-time to learn about

the environment. Despite the rapid development of IoV for traffic management, condition sensing, and congestion control, real-time decision-making is still a challenging issue, especially in urban regions [10], [11].

A. RESEARCH OBJECTIVE AND MOTIVATION

With the rapid expansion of cities and the continuous growth of the urban population, automated (cognitive) networks are quickly becoming norms of our lives where devices are autonomously handled and controlled via IoT devices. Recently, connected and automated vehicles are becoming an increasingly important topic in IoV to improve transportation mechanisms. Along with the various benefits of IoV technology, the development of these automated intelligent devices has led to various security issues, especially when sharing/transferring data and making real-time decisions [12], [13]. With the exploit of intelligent devices, the applications may be compromised by the attackers to inject a huge amount of information into the network to make the network resource unavailable for others. Though some studies have proposed security techniques/frameworks for IoV, very few of them have focused on real-time decision-making, node monitoring, and sharing/transferring of information through smart devices [14]–[16]. Decision-making is considered to be an essential aspect of IoV, where entities need to quickly make decisions on some real-time activities while sharing or transferring the information. In addition, it is necessary to identify the significant factors of an entity that are used to measure its legitimacy or to record its real-time data. Therefore, the objective of this research is to provide a secure communication procedure in IoV by proposing an intelligent decision making and identification system.

B. PAPER CONTRIBUTION

We propose an intelligent decision-making framework that can secure the information shared among vehicles in the IoV network using VIKOR and analytic hierarchy process (AHP) methods [17], [18]. VIKOR is a multi-process selection criteria method that assigns trust values to the nodes by analyzing various measuring attributes, including travel time, response time, energy consumption, interaction effects, etc. It also ensures that any change while sharing or transmitting the sensing reports from devices is immediately reflected in the centralized authority (CM). In addition, an AHP method is integrated with VIKOR to improve real-time communication among the vehicles. The integration of AHP leads to the filtering out of ill-structured information from the generated reports while measuring their legitimacy. In the proposed framework, a trust manager, VIKOR, computes the legitimacy of IoV or IoT devices, providing real-time information to the vehicular devices by recognizing the various services offered by them using decision-making strategies. The integration of AHP in IoV has concerned the attention of scientists and developers since of its decentralized, anonymous, and trusted intelligent ecosystem. Further, the integration of AHP with VIKOR may improve the decision and identification of legitimate and malicious nodes/devices (vehicles) while ensuring the communication process among each other. Although researchers have proposed several trusted and secure decision-making schemes such as trust-based schemes, TOPSIS, and AHP, these models have not sufficiently recognized the issues of data falsification, record alteration in IoV, and decision-making through trusted nodes [19].

The generated data from the smart devices (IoV) in the proposed framework has been analyzed to make an efficient communication process. Also, the illegal activities carried out by various malicious objects have been discussed against several security measures in terms of the percentage of secure communication data in the presence of compromised IoV devices. In sum, the proposed framework is ensuring IoV security at two different levels.

1) Security using the decision-making model: VIKOR is used to check the legitimacy of the nodes so that a CM can identify the accurate sensing report by managing the transferring and sharing of records over the internet.
2) AHP integration with VIKOR: AHP is used to filter out the ill-structured data and fasten up the decision-making process during real-time sharing/transferring of records.
3) Comprehensive analysis of the proposed framework: The performance analysis is done using several measuring parameters such as message alteration, falsification attack, identification of trusted devices, and decentralized denial-of-Service (DDoS) attacks.

C. OUTLINE

The remaining structure of the paper is illustrated as follows. The related work of IoV and the need for security are discussed in Section II. The hybrid decision-making through VIKOR and AHP is defined in Section III. The performance analysis of the proposed model is presented in Section IV. Finally, section V concludes the paper and provides the future directions of the paper.

II. RELATED WORK

IoV stands for a dynamic and reorganized way of sharing the information among intelligent vehicles that are equipped with communication adapters, control units, and embedded sensors. The smart decision-making model for sharing the records ensures reliable and efficient communication in IoV. This section illustrates the need for a secure communication system in IoV with or without the involvement of decision-making schemes [20]–[23]. A comparative study of existing work on decision-making schemes is further summarized in Table 1.

Bagga et al. [24] surveyed various security requirements and threats to the IoV surroundings. The authors gave a nomenclature of several security schemes and frameworks to provide data privacy by focusing on mutual authentication protocols. In addition, the authors provided an exhaustive comparative scrutiny of authentication protocols with some

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3019795, IEEE Access

TABLE 1. Comparison of existing decision-making schemes

Authors	Contribution	Method	Limitation
Bagga et al. [24]	Reviews security aspects and threats	Provides a detailed comparison on implementation and designing	Does not discuss real-time data sharing and message transmission
Rawat et al. . [25]	Provides identification of data falsification attack using hashes	Reduces end to end delay	Message alteration by malicious nodes
Quian et al. [26]	0-1 programming technique	Secure strategies during switching the vehicles	Increases the key management, communication, and storage overheads
Bui et al. [27]	Dynamic decision-making strategy	Manages the records of sharing traffic information	Increases, communication, and storage overheads
Wanget et al. [28]	Vertical handoff algorithm	Identifies miss alarm to quantify errors	Long delay in data analysis.
Liu et al. [29]	Incentive mechanism	Improves the scalability and participation of SV	Leads to increases in the communication overhead and computational complexity.
Nie et al. [30]	Decentralized decision-making scheme	Allows the independent decisions making by vehicles	Leads to increases in the risk of data alteration and trust identification among nodes.
Guo et al. [31]	Mutual Authentication	Provides confidentiality and distributed storage	Possibility of data alteration.
Kamal et al. [32]	Data provenance using Received Signal Strength Indicator (RSSI)	Secure data transfer using a high value of correlation coefficient	may increase the security risk upon the involvement of adversarial nodes.
Bird et al. [33]	Kryptonight lightweight authentication mechanism	Provided a low functioning networking mechanism for system management and resource usage	Increase the communication overhead during message transmission among each other.
Merchang et al. [34]	Light weight trusted intrusion detection mechanism	Establishes the trusted routes among data transferring	Leads to communication and storage overhead.

testbed descriptions for their designing and implementation process in the IoV surroundings. Quian et al. [26] formulated a deployment of secure strategies for switching on core networks where the selection of path switches that is modeled through 0-1 programming. In addition, the authors converted the 0-1 programming issue to a convex optimization using a log-dot heuristic method to meet security desires with the lowest delay. However, the proposed security strategy was not able to significantly identify IoV security threats, such as a DoS attack. Yin et al. [27] investigated the integration of intelligence into vehicles by providing them with a decision-making process for traversing into specific areas. They proposed a next-generation intelligent system by focusing on the dynamic decision-making of vehicles using a swarm intelligence algorithm. Also, they presented a common framework among vehicles for sharing traffic information. The effectiveness of the proposed scheme is analyzed by constructing a simulated framework with different transportation scenarios. However, the proposed framework leads to an increase in the delay of data sharing/transferring.

Wang et al. [28] presented an analytical framework to analyze vehicular accuracy using a vertical handoff algorithm. The authors considered a missed alarm to quantify the errors. Further, they projected a Kalman filtering based algorithm to analyze the accuracy of the resulting parameters. Also, they proposed a vigorous vertical handoff based on the decision tree to improve the accuracy of the decision-making process. The simulated results validated the improvement of handoff performance in a heterogeneous environment via the proposed solution. However, the involvement of various algorithms leads to an increase in a delay during the data analysis phase. Liu et al. [29] proposed an incentive scheme, called reverse auction that analyzed the economic behaviour based on its communication effect. In addition, the authors changed initial allocation involvement compensation for improving the participation rate of Spare Vehicles (SVs). The simulated results validated the average utility with an increase in vehicles and participation rate by 6.8 percent and 2 percent.

Further, Nie et al. [30] projected a decision-making model that is decentralized and composed of three different modules for making independent decisions to change the lane in the road. They employed a cooperative car-following framework to analyze the future state and incentive model to generate the driver's decision. The framework is numerically analyzed to identify the efficiency, stability, and homogeneity in traffic dynamics. However, the proposed framework leads to high complexity during the elaboration of the driver's decisions. Also, Guo et al. [31] proposed a security scheme of gathering the information collected from various sensors in large scale IoV. The scheme starts by registering the vehicles into the network and associating via a single sign-on and mutual authentication algorithm. They proposed two different security schemes to provide confidentiality and business data collection via distributed storage. Although various authors [35] have proposed several secure decision-making and inference schemes, very few of them have focused on data alteration, message transmission, and sharing of records through legitimate devices. Further, researchers have proposed some lightweight cryptographic algorithms to further improve the security in IoV systems. Kamal et al. [32] have projected a security mechanism for improving the data provenance using high-value correlation coefficients. However, the proposed framework leads to an increase in the security risk upon the involvement of the intruder model. Further, Brid et al. [33] have proposed a kryptoknight lightweight scheme for

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3019795, IEEE Access

managing resource availability. Further, Merchang et al. [34] have defined a lightweight trusted intruder mechanism that established a secure route among data transferring mechanisms. The proposed work further leads to storage and communication overhead issues.

To resolve these problems, we represent a multi-decision framework based on VIKOR and AHP that can resolve these security problems, manage the information, and efficiently store communication activities in the network. The proposed framework can efficiently predict the behavior of every IoT device by classifying them into malicious and legitimate devices.

III. PROPOSED DECISION-MAKING FRAMEWORK

The proposed framework is based on smart sensors that can sense and manage their surroundings according to the information shared and received from other vehicles via efficient decision-making. The principle of the proposed framework is that instead of homogeneous task distribution, a conventional transportation system is composed of various smart devices or entities with different tasks. The coordination, management, and information sharing among these devices is not only labor-intensive but also significantly time-consuming. Besides, collections of several smart nodes are set-up across IoV for information sharing and intelligent decision-making, thus making management much more cost-effective and improved. This section aims to provide an accurate and intelligent decision-making framework for trusted devices on how to react effectively to a situation, an object, a scenario, and an event.

The proposed hybrid decision-making for IoV is illustrated with the integration of VIKOR and AHP methods. The combination of VIKOR and AHP for intelligent decision-making in IoV results in better sensing, generating, sharing, and transferring of sensitive information by the smart devices. The nodes are also required to submit their generated data to the centralized manager (CM). The CM is defined as a centralized model that demeanor's an independent estimation of devices' recital by analyzing their shared and transmitted reports. The CM is equipped with smart devices that evaluate or analyze the reports offered by every entity in terms of their response time, where IoT enabled nodes to collect and generate the information using various decision-making parameters. The proposed model uses VIKOR combined with AHP to analyze the services of each device. Table 2 and Figure 1 illustrate the major components of the proposed framework in the trusted IoV model, where the framework records the communication and transfers the data through trusted devices in real-time. The CM engages VIKOR and AHP for analyzing and filtering out the service metrics. In this section, we first explain the adversary model and the metrics used for trust evaluation and performance monitoring. Then, we present the trust evaluation process of the CM and the details of the VIKOR and AHP methods. Table 3 presents the list of terminologies used in the paper.

TABLE 2. Number of entities used in the proposed framework.

Entity	Description
CM	Collects generated data from various IoT/IoV devices and identifies malicious/legitimate device suing VIKOR and AHP methods.
VIKOR	VIKOR is a multi-decision processing method to effectively analyze, process and store the records.
AHP	AHP is integrated with VIKOR to speed up the decision process by filtering out the unnecessary data.
IoT device	Provides real-time data transmission.

TABLE 3. List of terminologies and symbols.

Symbol	Description
CI	Consistency Index
fij	Normalized value of i-th alternative and j-th attribute
f_j^*	Best value (+ve ideal)
f_j^-	Worst value (-ve ideal)
L_{pj}	L_p metric
m	number of alternatives
n	number of attributes
NS	Normalized Service
OA	Optimal Alternative
Q_i	Majority of -ve attitude
R_i	Distance rate of i-th alternative corresponding to +ve ideal solution
RNS	Relative Normalized Service
S	Server parameter
Sc_i	Score of i-th alternative
S_i	Distance rate of i-th alternative corresponding to -ve ideal solution
S_{ij}	Relative importance of alternative i-th regarding j-th attribute
W_i	Service weights
x_i	Rating of i-th attributes
x_j	Rating of j-th attributes

A. ADVERSARY MODEL

We consider a malevolent architecture where attackers try to alter the communication process and record information during sharing and transferring of information. Conventionally, to launch the adversary model, the legitimate nodes are selected based on a credit-based voting mechanism. The node having the highest credit value is recorded as the most trustworthy node. Some nodes are selected as semi-trusted and still vulnerable to attacks. The types of attacks are presented below:

- *Data/Message Alteration:* An attacker intercepts and alters information while it is being transmitted.
- *Identification of Trusted Nodes:* Only the legitimate or trusted devices are allowed to transmit or share the information.
- *DDoS Attack:* A group of attackers colludes to make devices temporarily occupied with the intent of disrupting data communication in a real-time environment.
- *Data Falsification Attack (DFA)* An attacker tries to compromise various devices for false reports about data sharing and transferring of information. The level is DFA is calculated as

$$DFA = \sum_{x=1}^{m} \frac{\text{Altered reports}}{\text{Total generated reports}}. \quad (1)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3019795, IEEE Access

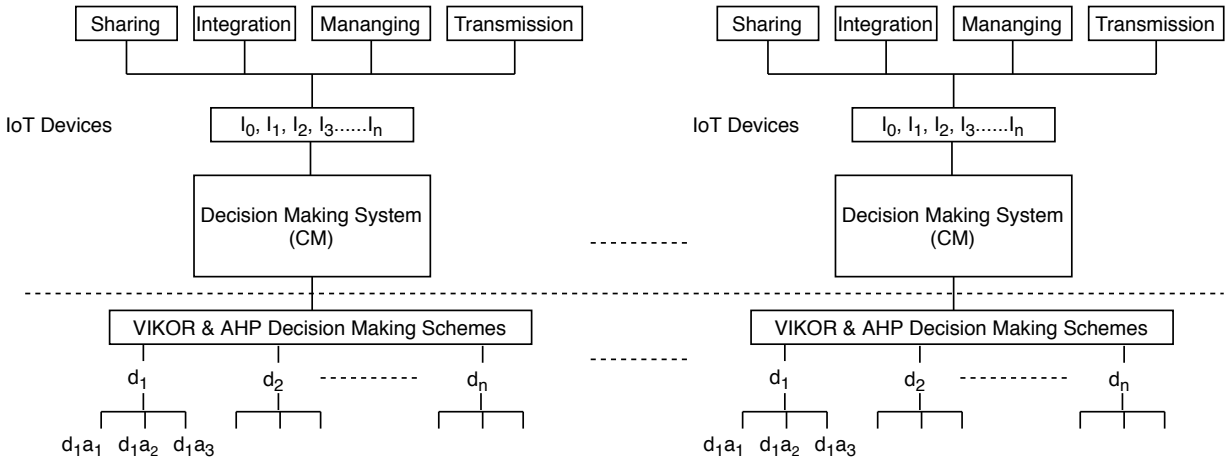

FIGURE 1. Hierarchical model of IoV security framework.

The proposed framework is validated against several security metrics like the detection of trusted IoT devices, message alteration, Data Falsification attack, and DDoS threat in the network.

B. SIGNIFICANT METRICS FOR TRUST EVALUATION AND PERFORMANCE MONITORING

This subsection provides significant metrics used for trust evaluation and performance monitoring of sensing records by smart devices. A number of service and computation metrics/parameters are considered in the studies for monitoring the performance of the network and the devices. The following interaction parameters for vehicles are considered: Interaction Frequency (IF), Transmission Time (TT) to transmit/share the data among each other, Energy Consumption (EC), which is the sum of energy consumed by each device, and Interaction Effect (IE). Their description is presented below:

- *Energy consumption (EC):* Illustrated as the sum of energy released/consumed by the devices (d_x, d_y) during data transmission and sharing. It can be used to show the overall effort made by the device.
- *Interaction frequency (IF):* Defined as the ratio of the number of frequencies a device interrelate with a specific device to average number of frequencies it interrelates with all the remaining nodes calculated as

$$IF_{d_{x,y}} = \frac{d_{x,y}}{\overline{d_i}}. \tag{2}$$

  It can be used to show the activeness of the device.
- *Transmission Time (TT):* Illustrated as the amount of period needed to respond to an inquiry from a user. It can be used to show the responsiveness of the device.

The CM uses these metrics for predicting the trust value of each communicating node by applying VIKOR and AHP methods. These parameters are checked multiple periods during a given interval of time.

C. PROCEDURE OF CM TRUST COMPUTATION

The process of recognizing the security and trust events can be put together as a decision-making framework. The security framework is structured hierarchically, as illustrated in Figure 1. The hierarchical model includes VIKOR and AHP methods. VIKOR scheme is used to analyze the deeds of each device, either legitimate or malicious, by determining some computational steps. AHP scheme is used to filter out the ill-structured features while analyzing their trust by effectively checking the consistency of computed measures and alternatives.

The CM uses VIKOR for the trust formulation of the entities. The benefit of using VIKOR over other Multi-Attribute Decision-making (MADM) techniques, known as Simple Additive Weighting (SAW) and Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS), is that it can determine a compromised solution that reflects most decision-making attitudes in various dimensions to judge related elements and variability in real-time. Initially, the VIKOR method generates a L_p metric to formulate or measure the ranking probability of the nodes during the communication process corresponding to ideal (F^*) and feasible (F^c) solution that is defined as [36]

$$L_{pj} = \left\{ \sum_{i=1}^{n} [w_i (f_i)^* - f_{ij})/(f_i^* - f_i)]^p \right\}^{1/p}. \tag{3}$$

D. VIKOR METHOD

The procedure carried out by the CM for analyzing the legitimacy of each device using the VIKOR method is detailed in steps, as shown below.

Step 1: Compute the normalized value: There are n attributes and m alternatives, where several I alternatives are defined as x_i and the rating of j-th aspect for x_j alternative is defined as x_{ij}. In addition, the normalized value process of

x_{ij} having i-th options and j-th dimension is defined as [36]

$$f_{ij} = \frac{x_{ij}}{\sqrt{\sum_{j=1}^{n} x_{ij}^2}}, \tag{4}$$

where, $i = \{1, 2, 3, \ldots, m\}$ and $j = \{1, 2, 3, \ldots, n\}$.

Step 2: Analyze the best and worst values: The worst and best cases are computer to filter out the features for analyzing the behaviour of each devices. The best case is denoted as f_j^*, and the worst case is denoted as f_j^-. They are used for all attribute functions. For the attribute $j = 1-n$, the max and min values of the best and worst cases are defined as:

$$f_j^* = \arg\max fij, \quad i = \{1, 2, \ldots, m\}, \tag{5}$$

$$f_j^- = \arg\min fij, \quad i = \{1, 2, \ldots, m\}, \tag{6}$$

where f_j^* is the +ve ideal solution for j-th criteria and f_j^- is the -ve ideal solution for j-th feature/criteria.

Step 3: Determine the weight attributes: To express the relative importance of +ve and -ve ideal solution, calculate the attribute weights of each device.

Step 4: Compute the alternative's distance to ideal solution: It is used to compute the distance from every alternative to +ve ideal solution and then obtain the sum to attain the final result calculated as below:

$$S_i = \sum_{j=1}^{n} [w_j (f_j)^* - f_j^-)/(f_j^* - f_j^-)], \tag{7}$$

$$R_i = \arg\max_j [w_j (f_j)^* - f_{ij}^-)/(f_j^* - f_j^-)], \tag{8}$$

where S_- represents the distance rate of i-th alternative to +ve ideal solution called best alternative and R_i represents the distance rate of i-th alternative to -ve ideal solution and shows the worst combination. The S_i and R_i are defined as the best and worst rankings, respectively.

Step 5: Compute the VIKOR values S_i for $i = \{1, 2, \ldots, m\}$: Let S^* denote the min S_i, S^- denote the max S_i, R^* denote the min R_i, R^- denote the max R_i, and v denote the strategic weight of majority of criteria. Further, $[(s_i - s^*)/(s^- - s^*)]$ symbolizes the rate of distance from +ve ideal solution to i-th alternatives attainments and $[(R_i - R^*)/(R^- - R^*)]$ represents rate of distance ideal solution to i-th alternative. In case $v > 0.5$, Q_i, the index tends to majority agreement. Otherwise, the index tends to majority negative agreement.

Step 6: Rank alternatives by Q_i value: The ranking is needed to make the ideal, malicious, and trustworthy decision of each node according to computed Q_i values in Step 4. To speed up the data sharing and transferring process among the devices, it is necessary to filter out the non-required/ill-structured characteristics or features while analyzing their trusts. For this purpose, we integrate the VIKOR method with AHP to speed up the decision process by deciding the relative significance of measuring parameters systematically.

E. AHP METHOD

The steps for computing the AHP scheme weights are detailed in steps, as shown below.

Step 1: Generate a pair-wise comparison matrix through relative consequence of service metrics. As there are S number of service parameters, the pair-wise evaluation of the i-th alternative with j-th criteria acquiesces a square matrix $S_{n\times n}$ as

$$\mathbf{S}_{n\times n} = \begin{array}{c} \\ S_1 \\ S_2 \\ \vdots \\ S_n \end{array} \begin{array}{c} \begin{array}{cccccc} S_1 & S_{12} & \ldots & \ldots & S_{1n} \end{array} \\ \begin{bmatrix} 1 & S_{12} & \ldots & \ldots & S_{1n} \\ S_{21} & 1 & \ldots & \ldots & S_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ S_{n1} & S_{n2} & \ldots & \ldots & 1 \end{bmatrix} \end{array} \tag{9}$$

where S_{ij} denotes the relative consequence of alternative i concerning the j-th criteria.

Step 2: Calculate service weights (W_i) are obtained by calculating the systematic mean of i-th row and the normalized statistical mean of the rows in the assessment matrix.

Step 3: Validate W_i of every service metrics from Step 2 and calculate normalized service (NS) matrix as $NS_{n\times 1} = S_{n\times n} \times W_{n\times 1}$. **Step 4:** Calculate the relative normalized service (RNS) matrix defined as $RNS_{n\times 1} = NS_{n\times 1}/W_{n\times 1}$.

Step 5: Calculate the maximum eigenvalue $E_{\max}$ by taking the average of $RNS_{n\times 1}$ matrix. Also calculate Consistency Index (CI) as $(E_{\max} - n)/(n-1)$.

Step 6: Acquire the random index (RI) for the number of attributes and calculate the consistency ratio defined as RI/CI.

Step 7: Computer the score of the i-th alternative as

$$Sc_i = \sum_{j=1}^{n} V_{ij}, \quad i = \{1, 2, 3, \ldots, n\}. \tag{10}$$

Step 8: Select the Optimal Alternative (OA) is by calculating $\text{OA}_{\text{SAW}} = \sum_{i=1}^{n} S_i$, where S_i is the matrix score from the set of alternatives i.

The procedure outlined above determines the final ideal service by defining various factors. The metrics mentioned above, such as EC, IF, and TT, are worn in the calculation of the trust matrix of every device based upon several measuring metrics by the CM using VIKOR and AHP.

IV. PERFORMANCE ANALYSIS

A. SIMULATION SETUP

We analyze the performance of the proposed hybrid framework in comparison with a baseline scheme in terms of trusted device identification, resistance to data falsification attack, and prevention to DDoS attack. The smart/IoV devices are uniformly dispersed in a simulation area of 700 $\times$ 700 m^2. The evaluation is done for several numbers of IoV devices between 100 and 900. The smart devices are initially classified into several types according to their communication behavior such as malicious, ideal, hyperactive, excessive energy consumption, and so on. In addition, to validate the security of the proposed work, the compromised number of nodes are inserted during the communication process in the network at the rate of 20 to 70 percent. Further, the running time of the network is considered at 60 seconds

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3019795, IEEE Access

TABLE 4. Simulation parameters.

Parameter	Value
Area of simulation	700×700 m^2
Initial number of IoV devices	100
Parameters of weight	25, 35
Number of IoV devices	100-900
Ratio of compromised devices	20, 70 percent
Device mobility	0-25 m/s
Running time	60 s

at a single interval. The proposed framework is simulated using MATLAB to depict the management and efficiency of message transmission in IoV. Simulation metrics are detailed in Table 4.

B. BASELINE SCHEME

To validate the proposed framework, we have taken two traditional approaches as baseline scheme 1 and baseline scheme 2. First, to address secure information transferring/sharing through trusted devices, Guo et al. [31] (baseline scheme 1) proposed a security method for gathering the information collected from various sensors in a large scale IoV. It starts by registering the vehicles into the network via a single sign-on and mutual authentication algorithm. They proposed two different security schemes to provide confidentiality and secure data collection via distributed storage. Their numerical simulation using MATLAB confirms the effectiveness and security of their data sharing scheme in IoV. Second, Buaban et al. [37] (baseline scheme 2) proposed a condition-based decision-making model that used several fuzzy logic and context-sensitive schemes to identify the legitimacy of the communicating nodes. The decision method chosen to identify the legitimate nodes was TOPSIS that validated the results using MATLAB.

Our proposed framework is compared with the baseline scheme1 and baseline scheme 2. In comparison, instead of ensuring security using a mutual authentication algorithm, the trusted devices are selected by the CM using VIKOR and AHP methods for data sharing and a trusted decision-making model. The validity of the projected framework is confirmed over several security metrics such as message alteration, DDoS attack, data falsification attack, and trusted node identification.

C. RESULTS AND DISCUSSIONS

The impact of the proposed hybrid security framework using VIKOR and AHP methods on the IoV is illustrated in this section. Figure 2 shows the automation and recording of information provided by various devices. The involvement of multiple criterion schemes in the decision-making model of the node's legitimacy by the proposed hybrid framework performs better in comparison with other schemes. As depicted in Figure 2, the proposed framework can effectively identify the number of malicious devices as the number of devices in the network increases. The number of malicious nodes increases with the increase in the network size. Still,

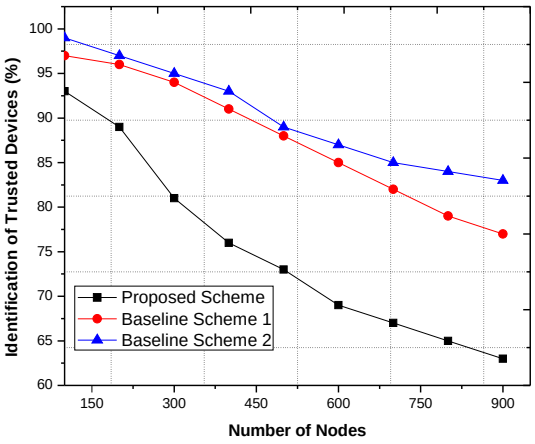

FIGURE 2. Identification rate of trusted devices.

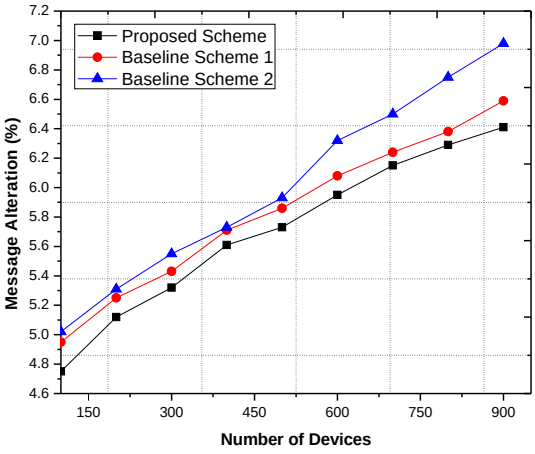

FIGURE 3. Percentage of message alteration.

since our proposed framework can identify more malicious nodes, the percentage of identified trusted devices decreases as the number of nodes increases. However, both baseline scheme 1 and baseline scheme 2 are not able to correctly identify the trusted devices. The significant improvement of the proposed framework is due to VIKOR and AHP methods that efficiently analyze the record of each smart device using several metrics and make accurate decisions to block or process records. In contrast, the baseline scheme performs worse because the efficiency of stored information decreases as the interconnection and complexity among smart devices increases.

Figure 3 shows the message alteration process measured by several smart devices. We can observe that messages cannot be altered much. This is because the involvement of multiple criteria attributes by the VIKOR sterns the process of node identification as compared to the baseline scheme.

Figure 4 shows the percentage of data falsification attacks where attackers try to analyze the communication pattern and alter the trusted devices into malicious nodes. The process of data falsification in the case of the proposed model is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3019795, IEEE Access

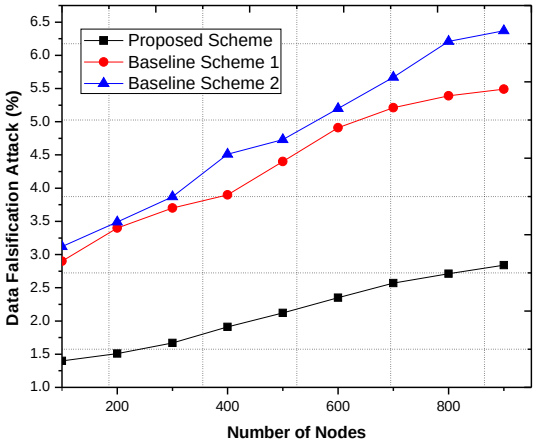

FIGURE 4. Percentage of data falsification attack.

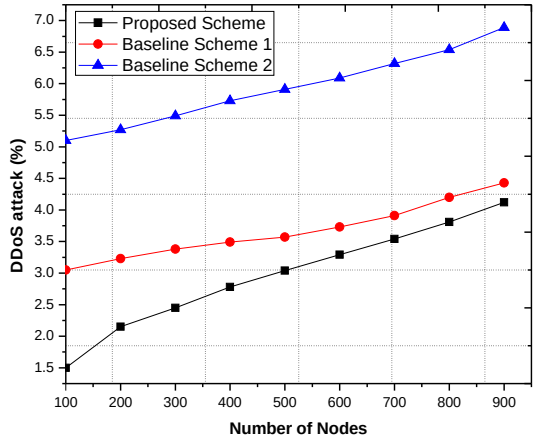

FIGURE 5. Percentage of DDoS attack.

significantly low in comparison with the baseline scheme. The reason is that the baseline scheme relies on a mutual authentication process that may increase the chances of a man-in-middle attack where intruders may successfully clone the legitimate nodes and start acting maliciously in the network.

Figure 5 shows the percentage of DDoS threats in the network. The proposed framework significantly performs better as compared to the existing scheme because of the two-stage security process conducted by the CM using VIKOR and AHP using several measuring parameters. However, in the case of the conventional scheme, the content management and handling of records can be transferred or altered due to the smaller number of considered metrics.

D. IMPACT OF DECISION-MAKING FRAMEWORK IN IOV

So far, the proposed and conventional schemes were simulated up to 900 devices. Upon increasing the scalability of records, the measuring parameters in the proposed framework, such as execution time, message alteration, and record accuracy, show better results as compared to the conventional scheme. The use of a multi-criterion decision-making process that does not cause network congestion or performance degradation because VIKOR and AHP methods filter out the non-required features when identifying the trust and behavior of communicating nodes. The proposed framework may increase the complexity among the devices while sharing the information among each other as we are integrating AHP and VIKOR to analyze the legitimacy of each node in the network.

V. CONCLUSION

In this paper, we have commenced an efficient hybrid decision-making framework to provide secure sharing/transferring of information among various vehicles with sensors. The proposed framework classifies the vital parameters using VIKOR, where sensors efficiently manage the sharing and transferring of information. Moreover, the AHP technique is integrated with VIKOR to simplify the non-beneficial issues by hierarchically arranging decision-making features. Thus, the proposed hybrid framework can efficiently speed up and accurately sense the shared information through the VIKOR and AHP methods. The proposed framework is verified rigorously using several trusted evaluation parameters such as shared record accuracy, legitimate sensor nodes, data transmission time, and message alteration record. Our simulation results exhibit that the proposed framework achieves 93 percent in the success rate as compared to the conventional scheme. As future work, the accuracy of the proposed hybrid decision-making framework will be enhanced by considering other security-sensitive issues, such as falsification attack, false record generation, and pattern observation, using VIKOR and AHP methods.

REFERENCES

[1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[2] S. Mumtaz, A. Bo, A. Al-Dulaimi, and K.-F. Tsang, "Guest editorial 5g and beyond mobile technologies and applications for industrial iot (iiot)," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2588–2591, 2018.

[3] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 924–935, 2019.

[4] S. Garg, K. Kaur, N. Kumar, and J. J. Rodrigues, "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in sdn: A social multimedia perspective," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 566–578, 2019.

[5] S. Garg, K. Kaur, S. H. Ahmed, A. Bradai, G. Kaddoum, and M. Atiquzzaman, "Mobqos: Mobility-aware and qos-driven sdn framework for autonomous vehicles," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 12–20, 2019.

[6] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2017.

[7] M. S. Hossain, G. Muhammad, B. Song, M. M. Hassan, A. Alelaiwi, and A. Alamri, "Audio–visual emotion-aware cloud gaming framework," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 12, pp. 2105–2118, 2015.

[8] M. I. Ashraf, M. Bennis, C. Perfecto, and W. Saad, "Dynamic proximity-aware resource allocation in vehicle-to-vehicle (v2v) communications," in *2016 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2016, pp. 1–6.

[9] M. S. Hossain and G. Muhammad, "Cloud-based collaborative media service framework for healthcare," *International Journal of Distributed Sensor Networks*, vol. 10, no. 3, p. 858712, 2014.

[10] P. Mishra, A. Biswal, S. Garg, R. Lu, M. Tiwary, and D. Puthal, "Software defined internet of things security: Properties, state of the art, and future research," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 10–16, 2020.

[11] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "Sdn-based secure and privacy-preserving scheme for vehicular networks: A 5g perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8421–8434, 2019.

[12] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Robust session key generation protocol for social internet of vehicles with enhanced security provision," *The Journal of Supercomputing*, pp. 1–34, 2020.

[13] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019.

[14] M. F. Alhamid, M. Rawashdeh, H. Al Osman, M. S. Hossain, and A. El Saddik, "Towards context-sensitive collaborative media recommender system," *Multimedia Tools and Applications*, vol. 74, no. 24, pp. 11 399–11 428, 2015.

[15] H.-C. Liu, M. Yang, M. Zhou, and G. Tian, "An integrated multi-criteria decision making approach to location planning of electric vehicle charging stations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 362–373, 2018.

[16] A. R. Domingues, P. Marques, R. Garcia, F. Freire, and L. C. Dias, "Applying multi-criteria decision analysis to the life-cycle assessment of vehicles," *Journal of cleaner production*, vol. 107, pp. 749–759, 2015.

[17] M. Yavuz, B. Oztaysi, S. C. Onar, and C. Kahraman, "Multi-criteria evaluation of alternative-fuel vehicles via a hierarchical hesitant fuzzy linguistic model," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2835–2848, 2015.

[18] H. Liao, Z. Xu, and X.-J. Zeng, "Hesitant fuzzy linguistic vikor method and its application in qualitative multiple criteria decision making," *IEEE Transactions on Fuzzy Systems*, vol. 23, no. 5, pp. 1343–1355, 2014.

[19] M. Dağdeviren and İ. Yüksel, "Developing a fuzzy analytic hierarchy process (ahp) model for behavior-based safety management," *Information sciences*, vol. 178, no. 6, pp. 1717–1733, 2008.

[20] M. Velasquez and P. T. Hester, "An analysis of multi-criteria decision making methods," *International journal of operations research*, vol. 10, no. 2, pp. 56–66, 2013.

[21] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[22] A. Hammoud, H. Sami, A. Mourad, H. Otrok, R. Mizouni, and J. Bentahar, "Ai, blockchain, and vehicular edge computing for smart and secure iov: Challenges and directions," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 68–73, 2020.

[23] S. Liu, Y. Yu, W. Hu, Y. Peng, and X. Yang, "Intelligent vulnerability analysis for connectivity and critical-area integrity in iov," *IEEE Access*, vol. 8, pp. 114 239–114 248, 2020.

[24] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54 314–54 344, 2020.

[25] D. B. Rawat, M. Garuba, L. Chen, and Q. Yang, "On the security of information dissemination in the internet-of-vehicles," *Tsinghua science and technology*, vol. 22, no. 4, pp. 437–445, 2017.

[26] Y. Qian, M. Chen, J. Chen, M. S. Hossain, and A. Alamri, "Secure enforcement in cognitive internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1242–1250, 2018.

[27] Y. Zhang, R. Wang, M. S. Hossain, M. F. Alhamid, and M. Guizani, "Heterogeneous information network-based content caching in the internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 10 216–10 226, 2019.

[28] B. Ma, D. Wang, S. Cheng, and X. Xie, "Modeling and analysis for vertical handoff based on the decision tree in a heterogeneous vehicle network," *IEEE Access*, vol. 5, pp. 8812–8824, 2017.

[29] J. Liu, W. Wang, D. Li, S. Wan, and H. Liu, "Role of gifts in decision making: an endowment effect incentive mechanism for offloading in the iov," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6933–6951, 2019.

[30] J. Nie, J. Zhang, W. Ding, X. Wan, X. Chen, and B. Ran, "Decentralized cooperative lane-changing decision-making for connected autonomous vehicles," *IEEE Access*, vol. 4, pp. 9413–9420, 2016.

[31] L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale internet of vehicle," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 601–610, 2017.

[32] M. Kamal *et al.*, "Light-weight security and data provenance for multi-hop internet of things," *IEEE Access*, vol. 6, pp. 34 439–34 448, 2018.

[33] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, "The kryptoknight family of light-weight protocols for authentication and key distribution," *IEEE/ACM transactions on networking*, vol. 3, no. 1, pp. 31–41, 1995.

[34] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," *IET information security*, vol. 6, no. 2, pp. 77–83, 2012.

[35] Q. Fang, J. Sang, C. Xu, and M. S. Hossain, "Relational user attribute inference in social media," *IEEE Transactions on Multimedia*, vol. 17, no. 7, pp. 1031–1044, 2015.

[36] Y. Huang, Y. Yan, and Y. Ji, "Optimization of supply chain partner based on vikor method and g1 method," in *2008 International Seminar on Future BioMedical Information Engineering*. IEEE, 2008, pp. 172–175.

[37] M. Băban, C. F. Băban, and M. D. Şuteu, "Maintenance Decision-Making Support for Textile Machines: A Knowledge-Based Approach using Fuzzy Logic and Vibration Monitoring," *IEEE Access*, vol. 7, pp. 83 504–83 514, 2019.

GEETANJALI RATHEE received her Ph.D. in Computer Science Engineering from Jaypee University of Information Technology (JUIT), Waknaghat, Himachal Pradesh, India in 2017. She is currently working as an Assistant Professor in the Department of Computer Science Engineering and Information Technology with JUIT. Her research interests include handoff security, cognitive networks, blockchain technology, resilience in wireless mesh networking, routing protocols, and networking, and industry 4.0. Until now, she has approximately 25 publications in peer-reviewed journals and more than 15 publications in international and national conferences. She is also a reviewer for various journals such as IEEE Transactions on Vehicular Technology, Wireless Networks, Cluster Computing, Ambience Computing, Transactions on Emerging Telecommunications Engineering, and the International Journal of Communication Systems.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3019795, IEEE Access

SAHIL GARG [S'15, M'18] received his Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018. He is currently a post-doctoral research fellow at École de technologie supérieure, Université du Québec, Montréal, Canada. He has many research contributions in the area of machine learning, big data analytics, security & privacy, internet of things, and cloud computing. He has over 60 publications in high ranked Journals and Conferences, including 40+ top-tier journal papers and 20+ reputed conference articles. He was awarded the IEEE ICC best paper award in 2018 at Kansas City, Missouri. He is currently a Managing Editor of Springer's Human-centric Computing and Information Sciences (HCIS) journal. He is also an Associate Editor of IEEE Network Magazine, IEEE System Journal, Elsevier's Applied Soft Computing, Elsevier's Future Generation Computer Systems (FGCS), and Wiley's International Journal of Communication Systems (IJCS). In addition, he also serves as the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications. He guest-edited a number of special issues in top-cited journals, including IEEE T-ITS, IEEE TII, IEEE IoT Journal, IEEE Network, and Future Generation Computer Systems (Elsevier). Dr. Garg serves/served as the workshop chair/publicity co-chair for several IEEE/ACM conferences, including IEEE Infocom, IEEE Globecom, IEEE ICC, ACM MobiCom, etc. He is a member of ACM.

GEORGES KADDOUM [M'11] received his Bachelor's degree in electrical engineering from the École Nationale Supérieure de Techniques Avancés (ENSTA), France, his M.Sc. degree in telecommunications and signal processing from Telecom Bretagne (ENSTB), Brest, in 2005, and his Ph.D. degree in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), Toulouse, France, in 2009. He is currently an Associate Professor and Tier 2 Canada Research Chair with the École de Technologie Supérieure, University of Quebec, Montréal, Canada. His recent research activities cover wireless communication networks, resource allocations, security and space communications, and navigation. He was awarded the ÉTS Research Chair in physical-layer security for wireless networks in 2014, and the prestigious Tier 2 Canada Research Chair in wireless IoT networks in 2019. He has published over 150+ journal and conference papers and has two pending patents. In addition, he received the research excellence award of the Université du Québec in the year 2018. In the year 2019, he received the research excellence award from the ÉTS in recognition of his outstanding research outcomes.

BONG JUN CHOI [SM'20] is an associate professor at the School of Computer Science Engineering and jointly at the School of Electronic Engineering, Soongsil University, Seoul, Korea. Previously, he was an assistant professor at the Department of Computer Science, State University of New York Korea, Korea, and concurrently a research assistant professor at the Department of Computer Science, Stony Brook University, USA. He received his B.Sc. and M.Sc. degrees from Yonsei University, Korea, both in Electrical and Electronics Engineering, and the Ph.D. degree from the University of Waterloo, Canada, in Electrical and Computer Engineering. His current research focuses on energy-efficient networks, distributed mobile wireless networks, smart grid communications, and network security. He is a member of the IEEE and the ACM.

M. SHAMIM HOSSAIN [Senior Member, IEEE] is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa, Canada. He has authored and coauthored more than 275 publications including refereed journals (200+ SCI/ISI-Indexed papers, 100+ IEEE/ACM Transactions/Journal papers, 10+ ESI highly cited papers, 1 hot paper), conference papers, books, and book chapters. Recently, he co-edited a book on "Connected Health in Smart Cities", published by Springer. He has served as cochair, general chair, workshop chair, publication chair, and TPC for over 12 IEEE and ACM conferences and workshops. Currently, he is the cochair of the 3rd IEEE ICME workshop on Multimedia Services and Tools for smart-health (MUST-SH 2020). He is a recipient of a number of awards, including the Best Conference Paper Award and the 2016 ACM Transactions on Multimedia Computing, Communications and Applications (TOMM) Nicolas D. Georganas Best Paper Award, and the 2019 King Saud University Scientific Excellence Award (Research Quality). He is on the editorial board of the IEEE TRANSACTIONS ON MULTIMEDIA, IEEE NETWORK, the IEEE MULTIMEDIA, the IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, the Journal of Network and Computer Applications (Elsevier), and the International Journal of Multimedia Tools and Applications (Springer). He also presently serves as a lead guest editor of IEEE Network, ACM Transactions on Internet Technology, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) and Multimedia systems Journal. Previously, he served as a guest editor of IEEE Communications Magazine, IEEE Network, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE (currently JBHI), the IEEE TRANSACTIONS ON CLOUD COMPUTING, International Journal of Multimedia Tools and Applications (Springer), Cluster Computing (Springer), Future Generation Computer Systems (Elsevier), Computers and Electrical Engineering (Elsevier), Sensors (MDPI), and International Journal of Distributed Sensor Networks. He is a senior member of the ACM.