IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 10, 2020, accepted December 22, 2020, date of publication December 29, 2020,
date of current version January 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3048077

A Trusted Social Network Using Hypothetical Mathematical Model and Decision-Based Scheme

GEETANJALI RATHEE[1], SAHIL GARG[2,3], (Member, IEEE), GEORGES KADDOUM[2], (Member, IEEE), DUSHANTHA NALIN K. JAYAKODY[3,7], (Senior Member, IEEE), MD. JALIL PIRAN[4], (Senior Member, IEEE), AND GHULAM MUHAMMAD[5,6], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat 173234, India
[2]Electrical Engineering Department, École de Technologie Supérieure, Université du Québec, Montreal, QC H3C 1K3, Canada
[3]School of Computer Science and Robotics, National Research Tomsk Polytechnic University (TPU), 634034 Tomsk, Russia
[4]Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea
[5]Chair of Pervasive and Mobile Computing, King Saud University, Riyadh 11543, Saudi Arabia
[6]Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[7]Centre for Telecommunication Research, School of Engineering, Sri Lanka Technological Campus, Padukka 11500, Sri Lanka

Corresponding authors: Ghulam Muhammad (ghulam@ksu.edu.sa) and Md. Jalil Piran (piran@sejong.ac.kr)

This work was supported in part by the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Pervasive and Mobile Computing; in part by the Tomsk Polytechnic University, Russia, through the Competitive Enhancement Program, under Grant VIU-ISHITR-180/2020; and in part by the Sri Lanka Technological Campus, Sri Lanka, Seed Grant RRSG/20/A7.

ABSTRACT Online social networking is expanding gradually in our professional as well as personal life in a variety of natures, beliefs, attitudes, and personalities. During communicating through the networks, the trust plays a very significant role while undertaking the communication process. This article proposes a secure trusted hypothetical mathematical model for ensuring secure communication among devices by computing the individual trust of each node. In addition, a decision making model is integrated with the hypothetical model for further speeding up the real time communication decision within the network. The proposed phenomenon is validated against variety of security threats by considering both ideal and adversarial models. Furthermore, the proposed framework is compared to a baseline approach against various security threats such as system accuracy, DDoS attack, data falsification threat,and number of processed requests. The proposed scheme is verified by simulating over synthesized data-set.

INDEX TERMS Social networking, trusted networks, hypothetical modelling, TOPSIS, and mathematical model.

I. INTRODUCTION

In conventional human societies, individuals apprehend to interact among each other in order to meet their needs and demands. Smart devices such as phones, laptops, and tabs communicate with each other in public or working places by accessing the internet at anytime and from anywhere. The MANETS has emerged as a significant prospective platform for instant online social societies. In addition, communities' people may interact with each other through various social networking sites for improving their networking. Nowadays, Twitter, Instagram and Facebook are the only major online social networking sites where variety of individuals and enterprises both government and private desire to connect to socialize or deliver their services [1], [2]. Further, Online Social Networking (OSN) [3] has become an informative decimate by entering into nearly each part of our daily life, be it enterprise, commercials or entertainment. Consequently, the ubiquitous OSN has become a significant architecture of our contemporary society [4]–[6].

Though, OSN are becoming huge platforms for data generation among users through rating, discussion or reviews, but the tremendous information can be unreliable, irreverent, non-trusted and very different to filter. In such scenarios,

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Zakirul Alam Bhuiyan.

trust may help the individuals to dissect the reliable and relevant information by addressing credibility and overloaded information [7]–[9]. There exist a variety of OSN applications such as fake news detectors, crowdsensing, social spammers, recommender systems [10]–[12] and re tweet behaviour detection to analyze the trust of an individual. The trust evaluation can be elaborated as the process of analyzing a new trust relation among a pair of individuals that are interacting among each other.

A. OBJECTIVE OF THE RESEARCH

Trust may facilitate individuals to obtain high recommendations and quality opinions with which they may be unacquainted. With the growing popularity and population on OSN, trust has become a very sensitive and significant feature to enable the contact and interaction on the web. Although various trust based approaches have been evaluated by authors/scientists, such as Machine learning, deep learning, regression or prediction based strategies in order to improve/analyze the trust on OSN [13], [14]. But these methods/processes may face variety of issues or challenges such as context-awareness, scarcity of trust relations and change in the trust rate with change in time in cyber-physical environment [15], [16]. Trust of the existing techniques is evaluated using transitive trust propagation i.e. if user 'A' relies on user 'B' which is a friendly to user 'C', then automatically user 'A' trusts user 'C'. Using this chain of trust paths or links, a level/trust rate is analyzed that may vary with time. However, in case of larger transitive trust relations, the individuals may suffer from lack of accuracy where the robustness keeps on decreasing and may leads to severe consequences [17], [18]. Therefore, the OSN is a predictable desire in the future due to the following rationales.

- OSN perceives the online environment and provides on-demand requests to the clients through intelligent communication systems.
- The devices equipped with trust based devices can achieve flawless connectivity and determine the issue of unreliability for online data communication.

Therefore, it is very much needed to compute a direct trust evaluation technique among individuals that may not only reduce the risk of above discussed issues, but also reduce the computational complexity and overhead of transitive chain trust methods [19], [20].

B. PAPER CONTRIBUTION

The paper introduces the need of robust security in networking while also discussing a number of threats that may be posed by various intruders while identifying or recognizing communicating nodes [21], [22]. In order to achieve this, the authors have computed a trust-based hypothetical scheme based on a mathematical model which divides the devices into various categories by identifying their internal behaviour through computed trust rates. In addition, a centralized authority (CA) is put in place that keeps track of each device in the network after a specific interval of time by analysing each individual device. In addition, a decision making model defined as Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) scheme is used to allow the CA to take real time decisions by integrating the hypothetical scheme to speed up the communication mechanism over real time environment in the network. The potential contribution of the paper is structured as follows:

- A trust based hypothetical scheme based on a mathematical model is determined to recognize the legitimacy of devices in social networking.
- Error generation and false authentication detection is recognized to establish the legitimacy or identify the malicious behaviour of the nodes.
- In addition, a decision making scheme known as TOPSIS is used to elaborate the ideal and non-ideal solutions corresponding to each node's legitimate or malicious nature.
- The proposed phenomenon is simulated through MATLAB simulator against two baseline schemes to establish the legitimacy of trust based security in the social network over various security metrics.

C. OUTLINE

The remaining organization of the paper is as follows: section 2 elaborates the literature survey of trust based schemes in social networking by explaining the pros and cons of each scheme. The proposed hypothetical modelling along with TOPSIS is discussed with an algorithm in section 3. Further, section 4 discusses the numerically simulated results against various networking metrics over both ideal and adversarial natures. Finally, the conclusion along with future directions is presented in section 5.

II. RELATED WORK

The association of smart networking systems provides a reliable communication wherever and whenever needed leads to significant utilization of the networks. This section discusses the need for trust based schemes in social media networking [6], [11], [23]. Jiang *et al.* [24] have proposed a trusted evaluation scheme by analyzing the flow and trust propagation similarity in the network. The authors have proposed a trusted GF scheme to identify the path dependence and a model known as trust decay among each node. The proposed mechanism is analyzed experimentally with the data sets of Advagato and Epinions by predicting the higher accuracy. Yan and Wang [25] have proposed a two stage trust level in order to control the data accessing by analyzing through pervasive networking or trusted servers. They have used an encryption scheme using attribute based methods in a heterogeneous environment. The authors have proved the proposed secured scheme by analyzing its computation and communication complexity. The authors claimed that the performance analysis is implemented efficiently and ensured security under relevant models.

Liu *et al.* [26] have surveyed an overview of state-of-art scientists in machine learning and predicted trusted schemes for online social networking. The authors have presented an overflow of predicted trust through machine learning by summarizing the related data sets, metrics and classifiers for evaluating their trusts. In addition, the authors have reviewed, contrasted and compared the related work for exploring the current issues and future directions in the field of trust based online social networking. He *et al.* [27] have proposed a trusted scheme by exploring the internal behaviour of social networks through relationship among each others. The authors have specifically considered a mobile edge computing for device-to-device or in-network communications. They have applied a deep learning scheme for making the automatic decision by allocating the resources. The final decision about the legitimacy of a device is made optimally by observing their states and conditions. The authors have used a Tensor Flow for implementing the Q-learning scheme among various networking metrics to show their effectiveness. Song *et al.* [28] have generalized the social network from two-state to multi-stage social levels. They have modelled an asymmetric multiparty and multi trust social systems by proposing a probabilistic multi-valued decision flow for evaluating their sensitivity [29] and trust analysis. The proposed mechanism is evaluated by demonstrating the numerical results over proposed methodology.

Chen *et al.* [30] have proposed a trusted framework using machine learning technique to facilitate the decision making of multi users based on their various criteria's and features. The authors have initially separated the features based on certain groups according to their empirical studies including behaviour-based, link-based, profile-based and feedback-based criteria's. They have designed a lightweight selection scheme for effective evaluation of single feature through online records. The authors have compared the analyzed machine learning based features with others through real world datasets. The proposed scheme is experimented through overall performance metrics against traditional and existing approaches.

Ghafari *et al.* [31] have analyzed the state-of-art researchers for pair-wise trust predicting schemes. The authors have classified various trust evaluation classifications on various factors by identifying their open issues and future directions. They have elaborated the trust based prediction for analyzing the in-between trust and security among various users [32]. In order to resolve the issues of distrust and trust among users, Nasir and Kim [33] have proposed an estimation continuation trust among disconnected users. The proposed method is based upon transpose and co-citation trust propagation for analyzing the trust among various users. They have estimated weighted average of four partial and complete trust values from trustor to trustee. In addition, the authors have proposed a framework having maximum robustness, accuracy and coverage on real datasets. The proposed scheme is experimented with some recent existing works in terms of robustness and accuracy through similar datasets.

Though, authors have projected various security mechanisms based on various cryptographic methods in social networks. Though, there are still some key issues that needs to be addressed:

- During multi-hop communication mechanism, it is required to ensure the trust of each intermediate node in order to maintain the security in the network.
- Number of schemes are based upon encryption schemes that leads to various computation issues due to heterogeneous environments of the network.
- The trust of each intermediate node needs to be sensed through a reliable device.

In the proposed section, we have shown how a hypothetical mathematical model and decision based schemes cooperation can solve the above-mentioned issues.

III. PROPOSED SOLUTION

A. SYSTEM MODEL

The system model of the proposed phenomenon is represented through a graph $G(V, E)$ where V symbolizes the set of vertices (number of nodes/devices) and E depicts the set of edges (the wireless linking among devices) in the network N. Each edge E from a vertex V_i to another vertex V_j is denoted with a sequence number that depicts the frequency/occurrence of interaction of individual i with individual j. In order to analyze the trust of each node (device), the proposed mechanism uses a mathematical model based on a hypothetical mechanism where the network devices are categorized in certain categories in order to identify the trust/legitimacy of each communicating node. In addition, to speed up the fast decision making while selecting the communicating path or alteration of route upon link damage, the proposed phenomenon used a TOPSIS mechanism that analyzes the behaviour of each communicating device depending upon certain parameters. The TOPSIS scheme provides the ability to make an immediate decision about node alteration/deletion based upon the computed trust values. The depicted Figure 1 represents a four layer architecture of the proposed phenomenon where the bottom layer consists of number of users/smart devices connected through a network for transmitting information via nodes (internal architecture of the nodes) through which data is transferred to the requested users. The security to the users is provided via securing the internal architecture of the social network by computing the trust values. The secured approaches such as the proposed hypothetical scheme, mathematical model and TOPSIS are integrated to secure the architecture. Finally, the top layer consists of online storage such as senor cloud or green cloud, and database servers to store the entire records/information [34], [35].

B. HYPOTHETICAL MATHEMATICAL MODELLING

The hypothetical mathematical modelling is validated on two types of networks i.e. ideal and malicious. In the case where intruders try to compromise or forge the legitimate devices

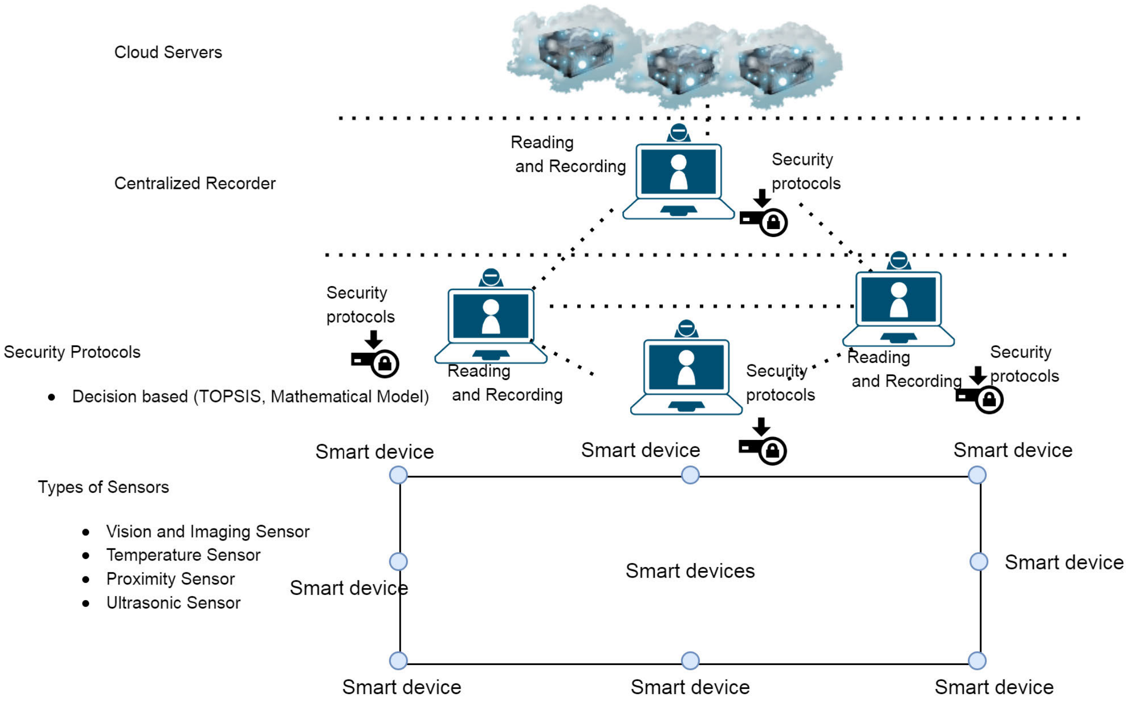

FIGURE 1. A trusted social network using hypothetical decision making model.

or undertake an illegal activity by generating huge number of false requests/messages, the attacker may pose passive or active threats such as network congestion, address forging, masquerade threat, DoS or data falsification attack and so on. The threats generated by intruders lead to less trust rate that may further degrade the network performance adversely. The new devices/nodes further added to extend the network might be malicious and may try to act/behave like legitimate nodes by forging their address upon entrance of a malicious node in the network; the compromised nodes may increase the congestion by sending huge amount of fake messages in the network. Further, the nodes may attract their neighbouring nodes by showing the shortest path towards destination for routing the messages. The trust of each communicating node is identified through various internal behaviours such as energy consumption (E_{Con}), packet to be forwarded (pkt_{frd}), packet to be received (pkt_{rcv}) and activeness of device avt characteristics as shown in the equation below 1.

$$Trust = E_{Con} + pkt_{frd} + pkt_{rcv} + avt \tag{1}$$

Now, there exist four different scenarios for both the network scenarios in order to analyze the hypothetical structural behaviour of each node.

- H_{a0} is the first hypothesis which states that none of the nodes including legitimate and malicious nodes are able to prove their authenticity to the Centralized Authority (CA).
- H_{a1} is the second hypothesis where Legitimate IoT Device (LID) needs the CA approval to get entry inside the network.
- H_{a2} is the third hypothetical scenario where malicious nodes try to replicate the legitimate nodes by forging their addresses.
- H_{a3} is the last hypothetical condition where both legitimate and malicious nodes try to prove their legitimacy inside the network.

The number of generated equations according to the above mentioned scenarios is defined in equation 2 as:

$$\begin{aligned} &H_{a0} = \text{neither LID nor MD,,} \quad H_{a1} = \text{LID only,} \\ &H_{a2} = \text{MD only,,} \quad H_{a3} = \text{LID and MD both.} \end{aligned} \tag{2}$$

Now, the absence and presence of malicious nodes is indicated through MD_{off} and MD_{on} where the hypothetical property 'H_{μ_k} is represented through γ_k as defined in the equation 3:

$$\begin{aligned} \gamma_0 &= P(H_{a0}) = P(H_0), \quad MD^{off} = P(MD^{off}/H_0)P_{H0,} \\ \gamma_1 &= P(H_{a1}) = P(H_1), \quad MD^{off} = P(MD^{off}/H_1)P_{H1,} \\ \gamma_2 &= P(H_{a2}) = P(H_0), \quad MD^{on} = P(MD^{on}/H_0)P_{H0,} \\ \gamma_3 &= P(H_{a3}) = P(H_1), \quad MD^{on} = P(MD^{on}/H_1)P_{H1} \end{aligned} \tag{3}$$

In addition, the respective attacking strategies of the proposed hypothetical model upon presence or absence of malicious devices through attacking metrics δ and θ are defined as: δ = P(MD^{on}/H_1) and θ = P(MD^{on}/H_0). The above stated equations, according to the previously defined equations may be rewritten as in the equation 4:

$$\begin{aligned} \gamma_0 &= (1-\theta)P(H_0), \\ \gamma_1 &= (1-\delta)P(H_1), \end{aligned}$$

TABLE 1. Proposed entities of the framework.

Entity	Details
CA	The CA is responsible to analyse the authenticity of each device by collecting their TV's
IoT Device	Used to gather/record the information from the environment
TOPSIS	Computes the trust value of each communicating device
Hypothetical Mathematical Model	Categorize the devices into four various categories

$$\gamma_2 = \theta P(H_0),$$
$$\gamma_3 = \delta P(H_1). \tag{4}$$

Further, let α_m and α_f depict the false probability and non-identification probabilities at CA respectively. The α_f and α_m with respect to MD absence and presence can rewritten as $\alpha_m = P(D_{off}/MD^{on})$ $\alpha_a = P(D_{on}/MD^{off})$, where D_{on} and D_{off} where the D_{off} and D_{on} represent the absence and presence of an MD in the online social network.

C. SYSTEM ERROR

In order to examine the validity of each communicating device, a system error state is computed that identifies the failure of CA to validate the accurate solution/decision about presence or absence of MD in the network. The system error S_e that represents this behaviour is redefined as in the equation 5:

$$\begin{aligned}\alpha_e &= P(MD^{on}, D^{off}) + P(MD^{off}, D^{on})\\ &= P(\frac{D^{off}}{MD^{on}}) + P(\frac{D^{on}}{MD^{off}})P(MD^{off})\\ &= \alpha_m P(MD^{on}) + \alpha_{fa} P(MD^{off}.) \end{aligned} \tag{5}$$

In addition, the Signal to Noise Ratio (SNR) of both ideal and malicious nodes is computed during the user's mobility from one place to another as SNR_{LN} and SNR_{MD} for recognizing their attack strength metric as $\mu = SNR_{MD}/(1 + SNR_{LID})$. Further, the compromised nodes are considered while computing the SNR ratio through hypothesis H_{a1} and H_{a3} by confirming the presence and probability of γ_1 and γ_3 of new node. The SNR of compromised node and the SNR of compromised node network (CNN) can be defined as in the below equation 6:

$$C_{NN} = \gamma_1.log_2(1 + SNR_{LID} + \gamma_3.log_2(1 + \frac{SNR_{LID}}{1 + SNR_{MD}}) \tag{6}$$

D. TOPSIS FOR SECURED DECISION

After categorizing the communicating nodes into various hypothetical models, the proposed approach is integrated with TOPSIS for further identifying a trust based decision while online communicating over social networks. The TOPSIS scheme is integrated with hypothetical modelling to speed up the decision making process during immediate action by CA. Table 1 represents the major components of the proposed solution required for elaborating the secured model framework. The CA is used for monitoring or sensing the communication process of the entire network. The performance recordings are analyzed regularly at a certain interval of time. In addition, an automatic alarm generation process is there that is triggered upon analyzing the malicious and legitimate behaviour by defining them into certain varieties such as uncertain, non-trusted and trusted.

1) METRICS FOR EVALUATING AND MONITORING THE TRUST OF SENSING RECORDS

The proposed framework considered the following metrics and computational scenarios for analyzing the performance.

- *Energy consumption (EC):* It is denoted as the amount of energy consumed and released by each device while receiving or forwarding any information.

$$EC_{node} = pkt_{rcv} + pkt_{frd} \tag{7}$$

- *Interaction (Itr) frequency:* Detects the active behaviour of any node in the network for identifying of its malicious behaviour.

$$Itrd_{x,y} = \frac{d_{x,y}}{\sum N_z} \tag{8}$$

where z=1,2,. . . n

- *Receiving/transmitting time:* The amount of time required by each device for receiving the incoming packets from preceding nodes and forwarding all the packets to its succeeding node.

The above mentioned metrics are used by TOPSIS mechanism for analyzing the trust evaluation of each node. Let us consider $EMV_{m_i}^{t-1}$ as an entire measured value of metric m_i at time $t-1$, then EMV of m_i at time 't' as $EMV_{p_i}^t$ can be evaluated by the equation 9:

$$EMV_{p_i}^t = \frac{EMV_{p_i}^{t-1} + CMV_{p_i}^t}{n_{p_i}^{t-1} + 1}, \tag{9}$$

During performance analysis, the above mentioned service and computation metrics are considered where $EMV_{m_i}^t$ are the values recognized for metrics m_i up to time $t-1$ and $EMV_{m_i}^t$ is Emerged measured value of metric m_i at time t.

The main practice of decision scheme called TOPSIS that is employed by CA is elaborated as follows:

1) The construction of an evaluation metric having $M_{N_{x,y}}$ with x sensing metrics and y trust rates corresponding to each metric, where $N_{x,y}$ denotes the intersection between each metric and criteria where $x = 1 \ldots n$ and $y = 1, 2, \ldots m$. The $N_1, N_2, \ldots N_n$ are the n sensing

metrics while $N_1, N_2 \dots N_m$ are the trust rates of m metrics.

2) The matrix $N_{(n\times m)}$ is further normalized to form a normalized metric as $NN_{(n\times m)}$. The range of trust rates is varying from $0-1$ where 0 is the least trusted device and 1 is the most trusted device.

3) Further a set of weights W_x where $x = 1\dots n$ are identified for sensing the metrics for measuring their identity for sensing the metrics for measuring their internal behaviours through interaction frequency, receiving/transmitting rates and energy consumption metrics.

$$M_{n\times m} = \begin{array}{c} Parameter \\ M_1 \\ M_2 \\ \vdots \\ M_n \end{array} \begin{bmatrix} M_1 & M_2 & \dots & \dots & M_n \\ 1 & M_{12} & \dots & \dots & M_{1n} \\ M_{21} & 1 & \dots & \dots & M_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ M_{n1} & M_{n2} & \dots & \dots & 1 \end{bmatrix} \tag{10}$$

4) Further, the normalized decision weights are computed for each node corresponding to each metrics as.

$$T = (t_{n\times m}) = (w_j NNWP_{x,y})_{n\times m} \tag{11}$$

where $x = 1, 2, \dots$ n, $y = 1, 2, \dots$ m and $NNWP_{(x,y)}$ is normalized NN weighted which is obtained after various calculated parameters.

5) Analyze the Ideal Alternate (AI) A_I and Non-ideal Alternate (AN)) alternative A_N for every metrics in step 4 and capture the weighted normalized decision metrics considering perspective weight MW_y as:

$$T = (t_{n*m}) = (MW_j NN_{x,y})_{n*m}, \tag{12}$$

where x=1,2,... n and y=1,2,... m and NN is (Normalized Networking Parameters)

6) Determine A_I and A_N for each device communication perspective as:

$$\begin{aligned} A_I &= \left\{ \begin{matrix} \langle min(t_{xy}|x = 1, 2, \dots, m)|j \in y_-\rangle \\ \langle max(t_{xy}|x = 1, 2, \dots, m)|y \in J_+\rangle \end{matrix} \right\} \\ &\equiv \left\{ t_{xy} = 1, 2, \dots, n \right\} \end{aligned} \tag{13}$$

$$\begin{aligned} A_N &= \left\{ \begin{matrix} \langle max(t_{xy}|x = 1, 2, \dots, m)|y \in J_-\rangle \\ \langle min(t_{xy}|x = 1, 2, \dots, m)|y \in J_+\rangle \end{matrix} \right\} \\ &\equiv \left\{ t_{Ny} = 1, 2, \dots, n \right\} \end{aligned} \tag{14}$$

where

$$Y_+ = \left\{ y = i = 1, 2, \dots, n| \right\}$$

where, j associated with the criteria having a positive impact and

$$Y_- = \left\{ y = i = 1, 2, \dots, n| \right\}$$

where, y associated with the criteria having a negative impact

7) Further identify the various metrics of each A_i from ideal are through the Euclidean distance as:

$$S_{i+} = \left\{ \sum_{y=1}^{n} (t_{xy} - t_{Xy})^2 \right\}^{0.5} \tag{15}$$

$$S_{i-} = \left\{ \sum_{y=1}^{n} (t_{xy} - t_{Ny})^2 \right\}^{0.5} \tag{16}$$

In above equations, x=1,2,... n and y=1,2,... m

8) In addition, the relative closeness of A_I is denoted through RC_x that is expressed as:

$$RC_x = \frac{S_{x-}}{(S_{x+} + S_{x-})} \tag{17}$$

where x = 1,2,...,m. From RC_x, Relative Fairness (RF_x) is derived as $RF_x = 1 - RC_x$.

9) Analyze the NSM_{xy} variance for each $NM_x = 1, 2, \dots, n$ $NM_x = 1\dots n$ using $V_{xy} = var(NSP_x y)$ where y=1... m

10) Analyze the final rates of trusted T_x, untrusted UT_x and uncertain UC_x from SP_x from RC_x, RF_x and V_x as:

$$T_x = \frac{RC_x}{RC_x + RF_x + V_x} \tag{18}$$

$$UT_x = \frac{RF_x}{RC_x + RF_x + V_x} \tag{19}$$

$$UC_x = \frac{V_x}{RC_x + RF_x + V_x} \tag{20}$$

11) Finally, rank the alternatives through T_x where T_x determine the height trusted rate of device N.

The procedure to compute device's trust through mathematical modelling and TOPSIS method is described through an algorithm as shown below:

The proposed mechanism is simulated and validated over both ideal and adversarial models.

E. IDEAL

An ideal case is the one where all the devices act as authentic and cooperate with each other. All the nodes have significant threshold values and take part in the communication process for transmitting/forwarding the data in the network. Each node has ideal trust rate for analysis, sensing, monitoring and responding the users request in the network. It means according to proposed mathematical model, all the nodes lie under H_{a0} where all the nodes act as legitimate. In addition, an ideal solution is there to take immediate decisions making during real time communication through TOPSIS. However, an ideal network can't exist in the environment where number of intruders constantly try to invade the network to do some malicious activity. Therefore, the validity of the proposed phenomenon is analyzed over an adversarial model.

F. ADVERSARY

An adversarial model is the one where number of legitimate nodes inside the network turn into malicious with an increasing rate. The adversarial nodes are added into the network in two scenarios.

Execution of TOPSIS and Hypothetical Mathematical Model

```
Input: A network 'N' consist of n number of devices.
Output: The devices are categorized as legitimate/malicious.
Step 1: A random trust value TV is distributed to the entire devices n.
Step 2: The TV is changed by identifying their internal behaviour through CA.
Step 3: An immediate decision making is done through TOPSIS where each device $n_i$ is categorized into $A_I$ and $A_N$.
```

$$A_I = \left\{ \begin{array}{l} \langle min(t_{xy}|x = 1, 2, \ldots, n)|j \in y_{-}\rangle \\ \langle max(t_{xy}|x = 1, 2, \ldots, n)|y \in J_{+}\rangle \end{array} \right\} \equiv \left\{ t_{xy} = 1, 2, \ldots, n \right\} \tag{21}$$

$$A_N = \left\{ \begin{array}{l} \langle max(t_{xy}|x = 1, 2, \ldots, m)|y \in J_{-}\rangle \\ \langle min(t_{xy}|x = 1, 2, \ldots, m)|y \in J_{+}\rangle \end{array} \right\} \equiv \left\{ t_{Ny} = 1, 2, \ldots, n \right\} \tag{22}$$

```
Step 4: Each node $n_i$ is categorized among 4 different categories through mathematical model.
i=1 to n
If $(TV_I) \geq 0.5$ then
Device $n_i$ is malicious
Device can be unknown
$(TV_I > 0.5$ && $TV_j < 0.7)$ Device $n_i$ is legitimate/malicious
Device $n_i$ is malicious
```

- Where number of existing legitimate nodes are turned via intruders into malicious devices.
- Where new devices as malicious are trying to enter inside the network by forging the ID of legitimate devices.

In both the scenarios, the number of compromised nodes are increasing at the rate of 5% upon increasing the network scalability where adversarial model is verified by the proposed mechanism to validate whether AHP and mathematical model are able to identify the adversarial nodes in the network or not. The proposed mechanism is validated upon adversarial and ideal models where compromised devices are increasing at the rate of 0-5%, also number of nodes are moving from one place to another for controlling the network environment.

IV. IMPLEMENTATION SETUP

The proposed phenomenon is simulated over a social environment consisting of 900 IoT devices interacting among each other. Each IoT device has sufficient energy to receive and forward the information to their neighbouring nodes. The approach is validated over synthesized data generated from mathematical modelling through four various hypothetical categories during the manual generation of synthesized data; each node interacts with every other node for transmitting/communicating, recording or sensing the user's data. Each node maintains a matrix of routing information that is updated after a specific interval of time. The CA routes the path through highly trusted path for communicating from source to destination. Upon simulation, each device is categorized into number of categories along with various metrics. The simulation parameters are depicted in Table 2.

TABLE 2. Simulation parameters.

Terms	Meaning
Total Devices	900
Trust values	0-1
Types of devices	Legitimate and Malicious
Device's Mobility	0-5 m/s
Device's Bandwidth	20 MHz
Trust evaluation method	TOPSIS
Device Analysis	Hypothetical

A. BASELINE METHOD

The proposed phenomenon is simulated and verified against Liu *et al.* [26] and Chen *et al.* [30]. The Liu *et al.* [26] have presented an overflow of predicted trust through machine learning by summarizing the related data sets, metrics and classifiers for evaluating their trusts, while Chen *et al.* [30] have initially separated the features based on certain groups according to their empirical studies including behaviour-based, link-based, profile-based and feedback-based criteria. However, the proposed phenomenon enhances the network security by TOPSIS and hypothetical mathematical modelling by regularly analyzing the categories the nodes are placed into. The three approaches are simulated and computed against number of graphs over ideal and adversarial scenarios against variety of metrics.

B. PERFORMANCE ANALYSIS

The proposed phenomenon is evaluated over 4000 virtual machines in order to evaluate their trust models that are equally distributed in the network. The synthesized data is generated via normalized distributed pattern where fewer malicious nodes try to enter as new device (ND) in the network during mobility. The network is considered during handoff process where users are mobile in nature and moving from one place to another and connected via various devices in their communication.

All the three security scenarios are processed request, DDoS threat, data alteration, distribution of devices in various categories and system accuracy. Initially, 100 devices are deployed in the network that are added upon every minute in the network. In addition, malicious devices are adding at a rate of 5% upon adding network devices. Several network metrics are elaborated based upon created test bed environment. The represented Figure 2 analyzes the system accuracy for identifying the malicious number of nodes from the network. The proposed framework leads to approximately 88% of predicted accuracy as compared to other traditional security mechanisms.

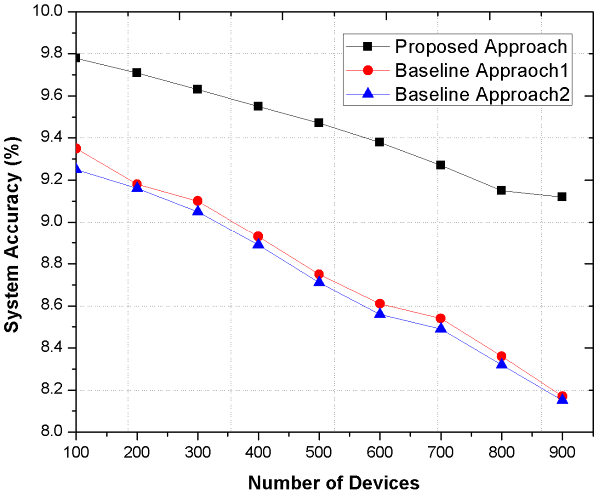

FIGURE 2. System accuracy.

Further, the proposed approach analyses the DDoS attacks as depicted in Figure 3 where traditional approaches lead to complex computational mechanisms and show high network congestion inside the network.

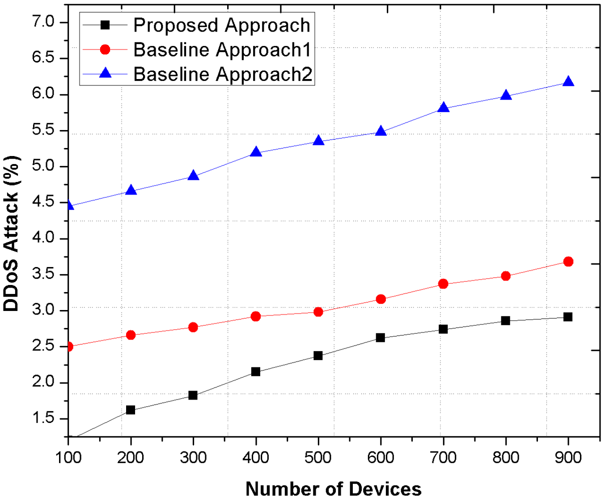

FIGURE 3. DDoS threat.

Moreover, Figure 4 shows data falsification threat where number of devices are altered by the intruders and proposed mechanism is effectively able to identify those devices. The proposed mechanism significantly identifies altered records by malicious devices because of their trust rate and decision making model criteria as compared to existing scheme.

Finally, Figure 5 depicts processed requests by the intermediate devices between source and destination. The proposed scheme involves maximum legitimate number of devices for data transmission/communication as compared to baseline schemes.

C. DISCUSSION OF RESULTS

The proposed scheme is effectively analyzed with calculated simulation results along with the hypothetical mathematical model and decision making scheme against a variety of

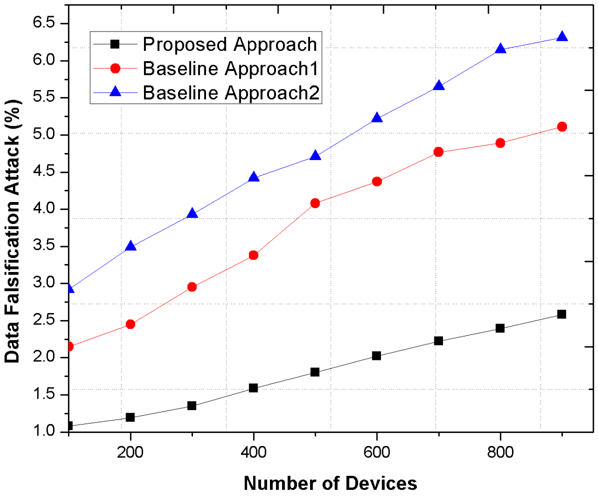

FIGURE 4. Data falsification threat.

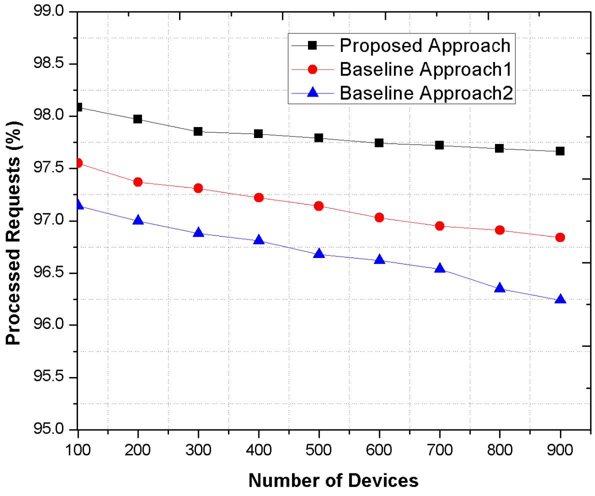

FIGURE 5. Processed request.

traditional security schemes. The evaluated results successfully measure variety of security threats like data alteration and DoS attacks with their implementation details. The evaluated results lead to approximately 88% of network accuracy as compared to both baseline mechanisms in both the networking scenarios, ideal as well as adversarial. The overall proposed phenomenon achieves significant and improved results over various networking metrics with various devices in the network.

V. CONCLUSION

The proposed phenomenon elaborates a hypothetical mathematical modelling and decision making scheme in order to ensure a trust based social networking environment. The proposed scheme determines a mathematical scheme to categorize the devices into various categorizes by computing their individual trust rates. In addition, a TOPSIS decision making scheme is integrated with the hypothetical model to further analyze the system accuracy and for immediate decision making as compared to baseline schemes. The proposed scheme is simulated over number of security threats with an approximation of 88% accuracy as compared to baseline mechanisms. Further, the amount of time required to compute/analyze the trust of individual and combined devices along with their communication and computational mechanisms can be reported in future works.

The future enhancement in the current procedure will be considered as the identification of random possibility of threat detection by recognizing the dynamic patterns of malicious nodes. In addition, the number of dynamic threats that can be encountered while communicating the message in the network.

REFERENCES

[1] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The Internet of Things: Review and theoretical framework," *Expert Syst. Appl.*, vol. 133, pp. 97–108, Nov. 2019.

[2] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.

[3] M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Collaborative analysis model for trending images on social networks," *Future Gener. Comput. Syst.*, vol. 86, pp. 855–862, Sep. 2018.

[4] S. Shelke and V. Attar, "Source detection of rumor in social network—A review," *Online Social Netw. Media*, vol. 9, pp. 30–42, Jan. 2019.

[5] Z. Zhang, Y. Gao, and Z. Li, "Consensus reaching for social network group decision making by considering leadership and bounded confidence," *Knowl.-Based Syst.*, vol. 204, Sep. 2020, Art. no. 106240.

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

[7] Y. Yin, J. Xia, Y. Li, W. Xu, and L. Yu, "Group-wise itinerary planning in temporary mobile social network," *IEEE Access*, vol. 7, pp. 83682–83693, 2019.

[8] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. M. M. Rahman, and M. S. Hossain, "Sybil defense techniques in online social networks: A survey," *IEEE Access*, vol. 5, pp. 1200–1219, 2017.

[9] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "FCSS: Fog-computing-based content-aware filtering for security services in information-centric social networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 4, pp. 553–564, Oct. 2019.

[10] W. Min, B.-K. Bao, C. Xu, and M. S. Hossain, "Cross-platform multi-modal topic modeling for personalized inter-platform recommendation," *IEEE Trans. Multimedia*, vol. 17, no. 10, pp. 1787–1801, Oct. 2015.

[11] M. F. Alhamid, M. Rawashdeh, H. A. Osman, M. S. Hossain, and A. E. Saddik, "Towards context-sensitive collaborative media recommender system," *Multimedia Tools Appl.*, vol. 74, no. 24, pp. 11399–11428, 2015.

[12] M. A. Rahman and M. S. Hossain, "A location-based mobile crowdsensing framework supporting a massive ad hoc social network environment," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 76–85, Mar. 2017.

[13] D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," *Future Gener. Comput. Syst.*, vol. 87, pp. 803–815, Oct. 2018.

[14] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 56–63, Jul./Aug. 2011.

[15] I. Kayes and A. Iamnitchi, "Privacy and security in online social networks: A survey," *Online Social Netw. Media*, vols. 3–4, pp. 1–21, Oct. 2017.

[16] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," *IEEE Syst. J.*, vol. 11, no. 1, pp. 118–127, Mar. 2017.

[17] F. Hao, S. S. Yau, G. Min, and L. T. Yang, "Detecting k-balanced trusted cliques in signed social networks," *IEEE Internet Comput.*, vol. 18, no. 2, pp. 24–31, Mar. 2014.

[18] L. Guo, C. Zhang, and Y. Fang, "A trust-based privacy-preserving friend recommendation scheme for online social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 4, pp. 413–427, Jul. 2015.

[19] O. Bodriagov and S. Buchegger, "Encryption for Peer-to-Peer social networks," in *Proc. IEEE 3rd Int. Conf. Privacy, Secur., Risk Trust*, Oct. 2011, pp. 47–65.

[20] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3015–3045, 4th Quart., 2017.

[21] F. Raji, A. Miri, and M. D. Jazi, "CP2: Cryptographic privacy protection framework for online social networks," *Comput. Electr. Eng.*, vol. 39, no. 7, pp. 2282–2298, Oct. 2013.

[22] Z. Liu, D. Luo, J. Li, X. Chen, and C. Jia, "N-mobishare: New privacy-preserving location-sharing system for mobile online social networks," *Int. J. Comput. Math.*, vol. 93, no. 2, pp. 384–400, Feb. 2016.

[23] S. Qian, T. Zhang, C. Xu, and M. S. Hossain, "Social event classification via boosted multimodal supervised latent Dirichlet allocation," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 11, no. 2, pp. 1–22, Jan. 2015.

[24] W. Jiang, J. Wu, F. Li, G. Wang, and H. Zheng, "Trust evaluation in online social networks using generalized network flow," *IEEE Trans. Comput.*, vol. 65, no. 3, pp. 952–963, 2015.

[25] Z. Yan and M. Wang, "Protect pervasive social networking based on two-dimensional trust levels," *IEEE Syst. J.*, vol. 11, no. 1, pp. 207–218, Mar. 2017.

[26] S. Liu, L. Zhang, and Z. Yan, "Predict pairwise trust based on machine learning in online social networks: A survey," *IEEE Access*, vol. 6, pp. 51297–51318, 2018.

[27] Y. He, C. Liang, F. R. Yu, and Z. Han, "Trust-based social networks with computing, caching and communications: A deep reinforcement learning approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 66–79, Jan. 2020.

[28] X. Song, X. Jia, and N. Chen, "Sensitivity analysis of multi-state social network system based on mdd method," *IEEE Access*, vol. 7, pp. 167714–167725, 2019.

[29] Y. Zhang, X. Ma, J. Zhang, M. S. Hossain, G. Muhammad, and S. U. Amin, "Edge intelligence in the cognitive Internet of Things: Improving sensitivity and interactivity," *IEEE Netw.*, vol. 33, no. 3, pp. 58–64, May 2019.

[30] X. Chen, Y. Yuan, L. Lu, and J. Yang, "A multidimensional trust evaluation framework for online social networks based on machine learning," *IEEE Access*, vol. 7, pp. 175499–175513, 2019.

[31] S. M. Ghafari, A. Beheshti, A. Joshi, C. Paris, A. Mahmood, S. Yakhchi, and M. A. Orgun, "A survey on trust prediction in online social networks," *IEEE Access*, vol. 8, pp. 144292–144309, 2020.

[32] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.

[33] S. U. Nasir and T.-H. Kim, "Trust computation in online social networks using co-citation and transpose trust propagation," *IEEE Access*, vol. 8, pp. 41362–41371, 2020.

[34] M. S. Hossain and G. Muhammad, "Cloud-based collaborative media service framework for healthcare," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 3, Mar. 2014, Art. no. 858712.

[35] K. Lin, J. Song, J. Luo, W. Ji, M. S. Hossain, and A. Ghoneim, "Green video transmission in the mobile cloud networks," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 1, pp. 159–169, Jan. 2017.

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

SAHIL GARG (Member, IEEE) received the Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018. He is currently a Postdoctoral Research Fellow with the École de Technologie Supérieure, Université du Québec, Montreal, Canada. He has many research contributions in the area of machine learning, big data analytics, security and privacy, the Internet of Things, and cloud computing. He has more than 60 publications in high-ranked journals and conferences, including more than 40 top-tier journal articles and more than 20 reputed conference papers. He is a member of ACM. He was awarded the IEEE ICC Best Paper Award in 2018 at Kansas City, MO. He serves/served as the Workshop Chair/Publicity Co-Chair for several IEEE/ACM conferences, including IEEE Infocom, IEEE Globecom, IEEE ICC, and ACM MobiCom. He is the Managing Editor of *Human-Centric Computing and Information Sciences (HCIS)* (Springer) journal. He is also an Associate Editor of *IEEE Network Magazine*, *Applied Soft Computing* (Elsevier), and *International Journal of Communication Systems (IJCS)* (Wiley). 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 TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, and *Future Generation Computer Systems* (Elsevier).

GEORGES KADDOUM (Member, IEEE) received the bachelor's degree in electrical engineering from the École Nationale Supérieure de Techniques Avancés (ENSTA), France, the M.Sc. degree in telecommunications and signal processing from Telecom Bretagne (ENSTB), Brest, in 2005, and the 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 the Tier 2 Canada Research Chair of the École de Technologie Supérieure, University of Quebec, Montreal, Canada. He has published more than 150 journal and conference papers and has two pending patents. His current research interests include 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 received the Research Excellence Award of the Université du Québec in 2018 and the Research Excellence Award from the ÉTS in recognition of his outstanding research outcomes in 2019.

DUSHANTHA NALIN K. JAYAKODY (Senior Member, IEEE) received the M.Sc. degree (Hons.) in electronics and communications engineering from Eastern Mediterranean University, Turkey, under the University Graduate Scholarship, and the Ph.D. degree in electronics and communications engineering from University College Dublin, Ireland, under the supervision of Prof. M. Flanagan (Science Foundation Ireland Grant). From 2014 to 2016, he has held a Postdoctoral position at the Coding and Information Transmission Group, University of Tartu, Estonia, and the University of Bergen, Norway. Since 2016, he has been a Professor with the School of Computer Science and Robotics, National Research Tomsk Polytechnic University, Russia. He has held various visiting positions at Texas A&M University, Qatar, the University of Jyväskylä, Finland, and the National Institute of Technology, Trichy, India. He has served as the Session Chair or a Technical Program Committee Member for various international conferences, such as IEEE PIMRC 2014–2020, IEEE WCNC 2014–2020, and IEEE VTC 2015–2019.

MD. JALIL PIRAN (Senior Member, IEEE) received the Ph.D. degree in electronics and information engineering from Kyung Hee University, South Korea, in 2016. He continued his research as a Postdoctoral Research Fellow in information and communication engineering with the Networking Laboratory, Kyung Hee University. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, Seoul, South Korea. He has published a substantial number of technical papers in well-known international journals and conferences in research fields of wireless communications and networking, 5G/6G; the Internet of Things (IoT); multimedia communication; streaming, adaptation, and QoE; applied machine learning; security; and smart grid. In the worldwide communities, he has been an Active Delegate from South Korea in the Moving Picture Experts Group since 2013 and an Active Member of the International Association of Advanced Materials since 2017. He received the IAAM Scientist Medal of the year 2017 for notable and outstanding research in new age technology and innovation, Stockholm, Sweden. He has been recognized as the Outstanding Emerging Researcher by the Iranian Ministry of Science, Technology, and Research, in 2017. His Ph.D. dissertation has been selected as the Dissertation of the Year 2016 by the Iranian Academic Center for Education, Culture, and Research in the Engineering Group.

GHULAM MUHAMMAD (Senior Member, IEEE) received the B.S. degree in computer science and engineering from the Bangladesh University of Engineering and Technology, in 1997, and the M.S. degree and the Ph.D. degree in electrical and computer engineering from Toyohashi University and Technology, Japan, in 2003 and 2006, respectively. He is currently a Professor with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. His research interests include image and speech processing, smart healthcare, and machine learning. He was a recipient of the Japan Society for Promotion and Science (JSPS) Fellowship from the Ministry of Education, Culture, Sports, Science and Technology, Japan. He has authored or coauthored more than 200 publications, including IEEE/ACM/Springer/Elsevier journals, and flagship conference papers. He has two U.S. patents. He received the Best Faculty Award of the Computer Engineering Department, KSU, from 2014 to 2015. He supervised more than 15 Ph.D. and Master Theses. He is involved in many research projects as a principal investigator and a co-principal investigator. He is also affiliated to the Center of Smart Robotics Research, CCIS, King Saud University. He is an Associate Editor of the *Journal of King Saud University–Computer and Information Sciences*. He also serves as a Guest Editor for *ACM Transactions on Internet Technology*, *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, and *Multimedia Systems* journal.