Defensive Modeling of Fake News Through Online Social Networks

Gulshan Shrivastava, *Member, IEEE*, Prabhat Kumar, *Senior Member, IEEE*, Rudra Pratap Ojha, Pramod Kumar Srivastava, Senthilkumar Mohan, and Gautam Srivastava, *Senior Member, IEEE*

***Abstract*— Online social networks (OSNs) have become an integral mode of communication among people and even non-human scenarios can also be integrated into OSNs. The ever-growing rise in the popularity of OSNs can be attributed to the rapid growth of Internet technology. OSN becomes the easiest way to broadcast media (news/content) over the Internet. In the wake of emerging technologies, there is dire need to develop methodologies, which can minimize the spread of fake messages or rumors that can harm society in any manner. In this article, a model is proposed to investigate the propagation of such messages currently coined as fake news. The proposed model describes how misinformation gets disseminated among groups with the influence of different misinformation refuting measures. With the onset of the novel coronavirus-19 pandemic, dubbed COVID-19, the propagation of fake news related to the pandemic is higher than ever. In this article, we aim to develop a model that will be able to detect and eliminate fake news from OSNs and help ease some OSN users stress regarding the pandemic. A system of differential equations is used to formulate the model. Its stability and equilibrium are also thoroughly analyzed. The basic reproduction number (R_0) is obtained which is a significant parameter for the analysis of message spreading in the OSNs. If the value of R_0 is less than one ($R_0 < 1$), then fake message spreading in the online network will not be prominent, otherwise if $R_0 > 1$ the rumor will persist in the OSN. Real-world trends of misinformation spreading in OSNs are discussed. In addition, the model discusses the controlling mechanism for untrusted message propagation. The proposed model has also been validated through extensive simulation and experimentation.**

***Index Terms*— Basic reproduction number, equilibrium, fake news, online social networks (OSNs), rumor detection, rumor propagation.**

I. Introduction

IN THE 20th century, the Internet has become the most powerful tool for communication. It facilitates efficient and effective transfer of media from one location to another. With the development of Internet technology, social networks such as Facebook, WhatsApp, Twitter, Instagram, and Google plus have become a vital platform for information exchange [1]. Nowadays, people are connected through online social networks (OSNs) and exchange information in a cost-efficient manner through data transfer. However, information exchanged on OSN platforms may comprise rumors that may affect the social lives of people [2]. Take COVID-19 as an example, where the proliferation of fake news related to the virus has left many people skeptical of any information they read information related to the virus on social media [3]. Some recent fake news related to a cure for COVID-19 has spread through Facebook [4]. Due to this type of misinformation, people from different corners of the world died. The impact of fake news on people related to a well-known Zika virus case study was presented by Sommariva *et al.* [5]. The authors found that the speed of fake news spread on OSNs is tremendous and tends to cover large audiences.

One major challenge that is associated with OSNs is verification of messages exchanged as well as the authenticity of users. Some messages that are spread through these social networks may create horrible situations regarding peace and harmony in society. Such messages, currently coined as fake news, can also be life-threatening. These kinds of messages are in essence just rumors/misinformation which are propagated through different means [6], [7] either just for entertainment or maliciously as well. Due to such messages, unnecessary anxiety uprise among the public and countries may also face economic loss [8]–[11] as is seen currently with COVID-19 [12]. This can be attributed to the fact that the rate of information dissemination on OSNs is very quick and information can spread globally within seconds [13], [14]. Several instances exist where the spread of fake news on OSNs created undesirable and detrimental situations for society. For instance, two bombs exploded in the White House injuring the U.S. president (23 April 2013) and incurring a loss of 10 billion USD [15]. Another example from India can be of a rumor on OSN that claimed, "Sonam Gupta is unfaithful." Due to this message in social networks, the personal life of a random girl whose name is Sonam Gupta was affected. Such types of comments should not be accepted in a civilized society. This is a type of public shaming on OSNs and can lead to malicious consequences even if unintended. To overcome these types of issues, Basak *et al.* [16] suggested a mechanism

Manuscript received April 28, 2020; revised July 2, 2020; accepted July 30, 2020. Date of publication August 14, 2020; date of current version November 10, 2020. *(Corresponding author: Gulshan Shrivastava.)*

Gulshan Shrivastava and Prabhat Kumar are with the Department of Computer Science and Engineering, National Institute of Technology at Patna, Patna 800005, India (e-mail: gulshanstv@gmail.com).

Rudra Pratap Ojha is with the School of Computer Science and Engineering, Galgotias University, Greater Noida 203201, India.

Pramod Kumar Srivastava is with the Department of Applied Sciences, Rajkiya Engineering College at Azamgarh, Azamgarh 276201, India.

Senthilkumar Mohan is with the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India.

Gautam Srivastava is with the Department of Mathematics and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada, and also with the Research Center for Interneural Computing, China Medical University, Taichung 40402, Taiwan.

Digital Object Identifier 10.1109/TCSS.2020.3014135

of blocking/muting of shamer's attacks on victims on Twitter. Liang *et al.* [17] investigated the rumor identification problem in microblogs. The authors proposed a method for identification of rumor rumormonger in the microblogs. Their scheme is based on the hidden behavior of users.

More recently, the drug vaccine trial in the U.K. for COVID-19 was harmed when it was falsely reported that the first patient injected with the vaccine has died [18]. The effects of this COVID-19 rumor are not yet known as it is so recent but the impact is real in the fact that people will now be more hesitant to take vaccines for COVID-19. There is a huge impact of rumors on society, individuals' daily life, during war, natural disasters, pandemics/epidemics, and within the financial market [19]–[21]. Due to these facts, people tend to become an easy target and get panicked and depressed easily over fake information. They also take wrong decisions strictly on the basis of misinformation.

There exists, different mathematical models, to study the behavior of message dynamics in social networks. In the wake of the wide scope and significance of social networks, rumor and fake news identification have become a potentially strong area of research. This urges for the development of the various mathematical models for rumor dissemination [22], [23]. In recent years, epidemic modeling on social networks is being studied.

The standard susceptible-infected-recovered (SIR) model [24] is primarily used due to its generalization and efficacy. The SIR model uses three compartments: susceptible (S), infected (I), and recovered (R). Every individual belongs to one of the three compartments and can be transferred from S to I or from I to R. This epidemic models elaborates on the dynamics of epidemics on networks and assist decision makers to alleviate the problem when an epidemic outbreaks. SIR model considers that the networks are homogeneous i.e., every node has identical relation and probability, and there is a link among any two nodes. However, the current study concludes that the community is a structure of social contact networks [25], [26] in which nodes have unusual connection and nodes have more connection inside a cluster than that between communities. Thus, when there are major numbers of infected individuals in a group of people, the rate of infection is slow. This incident is called "crowding" or "protection effect" [27], [28]. Thus, the linear forces of infection are used in the basic SIR models and they have some limitations under the typical condition. The improved SIR models consider the nonlinear forces of infection and categories spreading nature [29]. But the spreading of worms was not detected early stage, and this is one the biggest drawback of the above model.

Daley and Gani [30] explained the basics of epidemic modeling and its utilization. Epidemic modeling is used to develop a policy for controlling epidemic spread within a given population. Different strategies can be applied with the help of epidemic modeling to prevent the outbreak of epidemic disease. For example, in the specific case of COVID-19, Le *et al.* [18] used lock-down, social distancing, and quarantine techniques to combat the virus. The authors also suggested an epidemic model for the prevention of rumor spread in social networks. The authors discussed an inherited SIR model which is made up of three groups like spreaders, ignorant, and stiflers. The effect of rumor spreading in social networks is analyzed. The mechanisms for the removal of rumors (an "infection of the mind") has been explained by them. Cheng *et al.* [31] discussed the process of rumor diffusion in OSNs. For this study, the authors used the concept of epidemic modeling. In the proposed model they also assumed that there are three types of groups that exist in OSNs as noted above. In their model, the probability of infection (spreading rate of a given message) is considered as a variable and the infection is defined as a function of the strength of ties between nodes. The authors investigated the behavior of rumor spreading on the social site BlogCatalog. They also discussed weak ties as not being able to spread rumors fast and wide.

Nekovee *et al.* [32] explained the dynamics of rumor spreading on complex social networks. The authors analyzed rumor spreading in different types of network topologies such as scale-free networks, uncorrelated scale-free networks, and random graphs. The authors found a threshold value as well as observed that below this threshold value, a given rumor would not spread effectively in a given OSN.

An SIRS model [19], [22] is used for demographic linkage and related to the recovery rate in OSNs. In this model, arriving and leaving of users in the group is discussed. There could be many reasons for joining and leaving the online group. It may be due to the loss of interest or some other reasons can be there. Some new users join the group may be with good intention, or with a bad intention, such as spreading of untrusted messages in the network. A massive amount of research work on OSN is being done, including the exposure valuations, detection, and investigation of such malicious activity.

The usage of these OSN portals by the criminal group is also increasing rapidly. These users aim to spread false information, thereby creating harmful and damaging situations in the world. Due to such messages, people get affected and panicked. The high penetration rate of social networks into the daily lives of the people has led to another problem of concern. The spread of messages on the social network is very quick and it becomes a challenge to block and remove the untrusted type of messages. Hence, to protect the OSN from this type of activity, there is a need to develop models which can control the rumors and avoid the unforeseen situation in the world.

For detection and controlling of misinformation (rumor) in OSN, an susceptible-verified-infected-recovered (SVIR) model is proposed, which is inspired by the epidemic modeling of virus spreading in population [33], [34]. This model is based on different types of epidemic classes and has two layers of control mechanism to control the rumor in the social network. This model assumes that all users are susceptible that means anyone may turn a victim of misinformation or untrusted message. For protection, initially, the users are authenticated using a verified class. Hence, before accepting the request of any user, the user authentication method is applied, and the reliability of the messages from this user is evaluated in order to minimize the activities of malicious users to the OSN. If due to some reasons the verification of the user is unsuccessful then this type of user is considered to be a rumor spreader that has the potential to infect and spread unverified messages in the social network. This leads to the application of methods for removal and/or blocking of rumor as well as malicious users on the OSN.

The key objectives of the proposed model is to monitor the presence of fake news/misinformation as well as spreaders in OSNs and apply a suitable corrective method for blocking and/or removal of these types misinformation and spreaders. Our contributions can be summarized as follows:

1) formulate a mathematical model for monitoring fake news/misinformation as well as spreaders in OSNs and develop a method to prevent spreading of fake news;
2) suggest the concept of verification through verified state for verification of users in OSNs;
3) analyze the effect of a verified state on a given OSN's responsiveness and investigate its role in the prevention of fake news spreading in OSNs;
4) analyze the effectiveness of a recovered state (blocking/removing/leaving of a spreader group) on fake news as well as a spreader in OSNs;
5) investigate social network stability under various conditions and verify theoretical findings through extensive simulation results.

This article is organized into seven sections. Section II discusses related work, in Section III model formulation for OSN is presented. Section IV describes the primary properties of the model, and Section V discusses local stability and existence of positive equilibrium. In Section VI, the stability of rumor-free equilibrium is discussed, and Section VII presents simulations and result analysis. Conclusion of article and its future work are discussed in Section VIII.

II. Related Works

An enormous amount of research work has been carried out on OSN. The researchers have developed a number of models related to rumor spreading in OSN. There are many users in the OSN with varying intention. Few of them are spreading rumors in the network and others even may not be able to realize it. Therefore, to solve this, different types of methods are employed. One method is to block rumors [35]–[37], and another method is used to spread anti-rumors to diminish the effect of rumors [8], [38], but this is a grueling affair. The blocking of rumor may create a reverse effect, as it makes the people more anxious to know more about it. Some other methods are used to block rumors and spread truth [39]. In this method, first of all, the unwanted message is identified and then blocked as well as to spread the truth in OSN simultaneously. The social network is a scale-free network [40], [41] and learns rumor spreading in practical wisdom to design a heterogeneous epidemic model for the rumor dynamics. In [42], an analytical model is designed that describes positive and negative information with respect to social network and [43], [44] discusses immunization technique with weighted trust model for rumor spreading.

Some other models, like SIRS, SIS, and SEIR are also studied. All these models have different subclasses. SEIR [45] deals with a latent period with one extra exposed class. For this model, the basic reproduction number is calculated and the effect on the network is observed. The crowding and protection effect is studied in the relation of the force of infection [27]. The force of infection is used to discuss the contact rate and several infected individuals [46]. It is found that infection grows exponentially when the force of infection is high.

The improved SIR model has been discussed by Zhang *et al.* [29] who considered the variable rate of infection and the resultant function for infected individuals and nonlinear Ordinary Differential Equation (ODE) is developed. This model also discusses the crowding effect on OSN and also derives an expression for the basic reproduction number. This model has been used for the analysis of rumor spreading dynamics in social network and predicts the spreading behavior of rumor. They discussed the control strategies of rumor spread in social networks.

Zhu *et al.* [41] proposed an epidemic SIRS model, in which they described joining and leaving of users in OSNs. This article considers the dynamics of demography and the model is validated by simulation. More epidemic models are discussed related to rumors. Some of the researchers examined the temporal dynamics using the ODE [47]. Singh and Singh [48] discussed the spatial and temporal dynamics of rumor propagation and developed a strategy for countermeasures using. They used partial differential equation for the study of rumor propagation dynamics in the social network. Huang and Su [44] proposed an epidemic model for the study of news propagation on OSN and also suggested a method for controlling the rumor. They explained the effects of rumor spreading on ONS. For the study of rumor spreading in OSN, they evaluated the value of basic reproduction number and observed that if its value is less than one then the OSN will be free from unauthenticated news, otherwise unauthenticated news will be present in the OSN forever. The result of the proposed model has been verified by numerical calculation as well as simulation results.

Dong *et al.* [49] analyzed the rumor spreading dynamics on OSN by SEIR epidemic model. They considered the varying user's number on OSN with time. The joining and deactivation rate of user in this model is discussed. They also found the basic reproduction number and exact equilibrium points of the model. The effect of user variation on rumor spreading in OSN is explained. They found that the new incoming users influence the rumor spreading rate in OSN. The proposed model is verified by simulation results. Furthermore, Zhu *et al.* [50] using the same model as in [49] obtained a local and global equilibrium as well as calculated the basic reproduction number using the next generation matrix concept. The authors explained the effect of time delay on rumor propagation and developed an effective control mechanism.

A hesitating mechanism-based SEIR model is proposed by Liu *et al.* [51] for the study of rumor spreading in OSN. They used mean field theory for analysis of rumor spreading in OSN. They discussed the rumor-free equilibrium condition and global stability of the OSN and also obtained the value of basic reproduction number. They also analyzed the effects of feedback method on rumor spreading. They established the

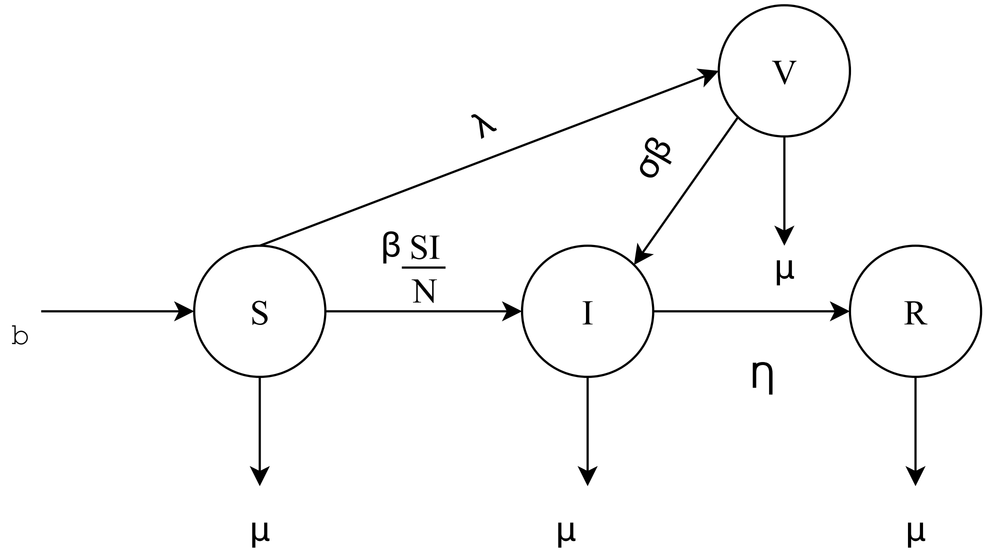

Fig. 1. States transition diagram of the proposed model.

analysis feedback mechanism to reduce the rate of rumor spreading but were not able to reduce the value of basic reproduction number.

III. Model Formulation

The proposed model considers heterogeneous network and works at two levels:

1) identify the user before joining the network;
2) identify when the user after the spreading rumor in the network.

This model investigates when rumors persist in the network [52]–[55]. In social network, users can be divided into different subclasses at any time t: susceptible $S(t)$ signify individuals who have not yet become victim of rumor but susceptible to it, infectious $I(t)$ signify the individuals that believe in untrusted message/fake news/misinformation and be active like spreader of rumor, verified $V(t)$ signify the individuals who are authenticated users, and they are not the spreader of rumor. But the spreader may be trapped, and the recovered $R(t)$ function signifies that the individuals do not believe the rumor. Moreover, those who are spreading fake news are blocked and/or removed from the OSN. The states' transition diagram of the proposed model is shown in Fig. 1.

Different states of the users in the OSN at any time t, are susceptible $S(t)$, infectious (spreader) $I(t)$, verified $V(t)$, and recovered $R(t)$ of total size $N(t)$, that is,

$$N(t) = S(t) + I(t) + V(t) + R(t) \tag{1}$$

where $S(0) = S_0, I(0) = I_0, V(0) = V_0 \forall t \geq 0$.

The dynamical transfer of subclass is described by the set of differential equation. The SIVR model is given by

$$\left.\begin{aligned} \frac{dS}{dt} &= bN - \beta\frac{SI}{N} - (\mu+\lambda)S \\ \frac{dI}{dt} &= \beta\frac{SI}{N} + \frac{\sigma\beta VI}{N} - (\mu+\eta)I \\ \frac{dV}{dt} &= \lambda S - \frac{\sigma\beta VI}{N} - \mu V \\ \frac{dR}{dt} &= \eta I - \mu R \end{aligned}\right\} \tag{2}$$

where b is the entering rate (or joining rate) of new individuals in OSN, β is the infection rate or spreading rate of rumor in OSN, μ is the rate of leaving (deactivation) of individuals from different states in OSN, λ is the verification rate or authentication rate of users in OSN, σ is the moving rate of verified individuals to the spreaders, and η is the blocking or removing rate of infected user (or leaving rate of spreader) in OSN. In order to express system of equation (2) as a portion of the entire population, and since the recovered class does not appear in the first four equations of the system (2), we use the following substitution:

$$s = \frac{S}{N}, \quad i = \frac{I}{N}, \quad \upsilon = \frac{V}{N}.$$

is used.

Hence, the resulting system of equation shall be

$$\left.\begin{aligned} \frac{ds}{dt} &= b - \beta si - (\mu+\lambda)s \\ \frac{di}{dt} &= \beta si + \sigma\beta\upsilon i - (\mu+\eta)i \\ \frac{d\upsilon}{dt} &= \lambda s - \sigma\beta\upsilon i - \mu\upsilon \end{aligned}\right\}. \tag{3}$$

IV. Basic Properties of the Model

A. Positivity of the Solution

Since the model monitors population for a different class, it is required to show that all the state variables remain nonnegative for all times.

Theorem 1: Let $\Omega = \{(s, i, \upsilon) \in R^3 : s(0) > 0\ i(0) > 0, \upsilon(0) > 0\}$ then the solution $\{s(t), i(t), \upsilon(t)\}$ of the system (3) is positive for all $t \geq 0$.

Proof: Taking the first part of (3)

$$\begin{aligned} \frac{ds}{dt} &= \alpha - \beta si - (\mu+\lambda)s \Rightarrow \frac{ds}{dt} \geq -(\mu+\lambda)s \\ &\Rightarrow \frac{ds}{s} \geq -(\mu+\lambda)dt \Rightarrow \int \frac{ds}{s} \geq \int -(\mu+\lambda)dt \\ &\Rightarrow s(t) \geq s(0)e^{-(\mu+\lambda)t} \geq 0. \end{aligned}$$

From the second part of (3)

$$\frac{di}{dt} = \beta si + \sigma\beta \upsilon i - (\mu+\eta)i \Rightarrow \frac{di}{dt} \geq -(\mu+\eta)i$$
$$\Rightarrow \frac{di}{i} \geq -(\mu+\eta)dt \Rightarrow \int \frac{di}{i} \geq \int -(\mu+\eta)dt$$
$$\Rightarrow i(t) \geq i(0)e^{-(\omega+\eta)t} \geq 0.$$

From third part of (3)

$$\frac{d\upsilon}{dt} = \lambda s - \sigma\beta\upsilon i - \mu\upsilon \Rightarrow \frac{di}{dt} \geq -\mu\upsilon \Rightarrow \frac{d\upsilon}{\upsilon} \geq -\mu dt$$
$$\Rightarrow \int \frac{d\upsilon}{\upsilon} \geq \int -\mu dt \Rightarrow \upsilon(t) \geq \upsilon(0)e^{-\upsilon t} \geq 0.$$

□

B. Basic Reproduction Number (R_0)

The basic reproduction number R_0 is an important parameter to characterize the transmission of rumor in the social network. In our consideration, there are three infected classes (s, i, υ), so for finding parameter R_0 [56], [57]. Here, only three equations of the system in (3) are considered

$$\left.\begin{aligned} \frac{ds}{dt} &= b - \beta si - (\mu+\lambda)s \\ \frac{di}{dt} &= \beta si + \sigma\beta\upsilon i - (\mu+\eta)i \\ \frac{d\upsilon}{dt} &= \lambda s - \sigma\beta\upsilon i - \mu\upsilon \end{aligned}\right\}. \tag{4}$$

After linearization of (4), get

$$\left.\begin{matrix} \frac{ds}{dt} \\ \frac{di}{dt} \\ \frac{d\upsilon}{dt} \end{matrix}\right\} = (F - V)\begin{bmatrix} s \\ i \\ \upsilon \end{bmatrix} \tag{5}$$

where

1) F represents rates of infection of rumors;
2) V represents the rate of transmission of rumors in the social network, are given by

$$F = \begin{pmatrix} \beta s_0 + \sigma\beta\upsilon_0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{6}$$

and

$$V = \begin{pmatrix} (\mu+\eta) & 0 & 0 \\ \sigma\beta\upsilon_0 & \mu+\sigma\beta i_0 & -\lambda \\ \beta s_0 & \sigma & (\mu+\lambda) \end{pmatrix}. \tag{7}$$

So, the basic reproduction number

$$R_0 = \frac{b\beta(\mu+\sigma\lambda)}{\mu(\lambda+\mu)(\mu+\eta).} \tag{8}$$

V. Existence of Positive Equilibrium

For equilibrium points

$$\frac{ds}{dt} = 0; \quad \frac{di}{dt} = 0; \quad \frac{d\upsilon}{dt} = 0.$$

Moreover, on a simple calculation, the equilibrium points are given as

$$P_0 = (s_0, i_0, \upsilon_0) = \left(\frac{b}{(\mu+\lambda)}, 0, \frac{\lambda b}{\mu(\mu+\lambda)}\right) \tag{9}$$

for rumor-free state.

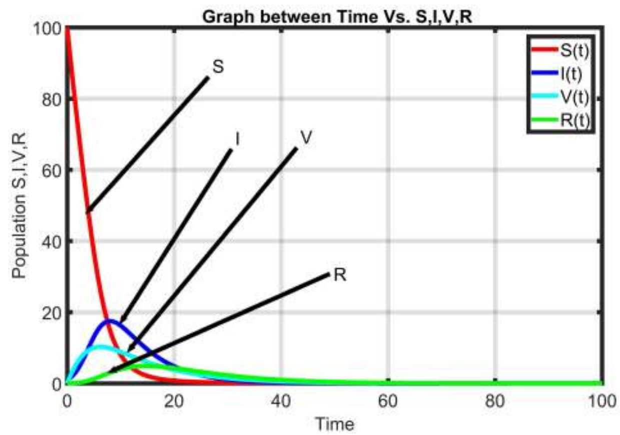

Fig. 2. Dynamic characteristics of the system when $R_0 < 1$ ($b = 0.015$; $\beta = 0.01$; $\mu = 0.1$; $\lambda = 0.04$; $\eta = 0.05$; and $\sigma = 0.004$).

VI. Stability of the Rumor Free Equilibrium Stage

Theorem 2: The system of equation (2) is locally asymptotically stable if all its eigenvalues are less than zero at rumor-free equilibrium P_0.

Proof: At rumor-free equilibrium point P_0, the Jacobian matrix is

$$J(P_0) = \begin{pmatrix} -(\mu+\lambda) & -\beta s_0 & 0 \\ 0 & \beta s_0 + \sigma\beta\upsilon_0 - (\mu+\eta) & 0 \\ \lambda & 0 & -\mu \end{pmatrix}. \tag{10}$$

Eigenvalues of (10) are: $\omega_1 = -\mu$, $\omega_2 = (R_0 - 1)(\mu+\eta)$, $\omega_3 = -(\mu+\lambda)$. It is clear that $\omega_1 < 0$, $\omega_2 < 0$, and $\omega_3 < 0$ if $R_0 < 1$. Therefore, the system is locally asymptotically stable at rumor-free equilibrium point P_0 Otherwise, when $R_0 > 1$ the value of ω_2 will be nonnegative and the system becomes unstable. □

Theorem 3: When R_0 is less than or equal to one, the rumor-free equilibrium P_0 is globally asymptotically stable.

Proof: A suitable Lyapunov function L to establish the global stability of the rumor-free equilibrium is defined as $L = \omega I$.

The derivative of the Lyapunov function with respect to time t is

$$\dot{L} = \omega\dot{i} = \omega(\beta si + \sigma\beta\upsilon i - (\mu+\eta)i)$$
$$\leq \omega[(\mu+\eta)R_0 - (\mu+\eta)] \leq \omega(\mu+\eta)(R_0 - 1)i.$$

If $R_0 \leq 1$, then $\dot{L} \leq 0$ holds. Furthermore, $\dot{L} \leq 0$ if and only if $I = 0$. Therefore, the most extensive invariant set in $\{(s, i, \upsilon) \in \Gamma : \dot{L} \leq 0\}$ is the singleton set $\{P_0\}$. Hence, the global stability P_0 follows from LaSalle's [58] invariance principle, when $R_0 \leq 1$. □

VII. Results and Analysis

The proposed work is simulated using `MATLAB` on a 3-GHz Intel Xeon system running UBUNTU 19.2 LTS with 16-GB RAM. The dynamism of the message act as a hurdle to prevent the rumor rather than taking a corrective measure is hurdle. The results of simulation are illustrated in Figs. 2–4, which shows the dynamic nature of different class of users in OSN,

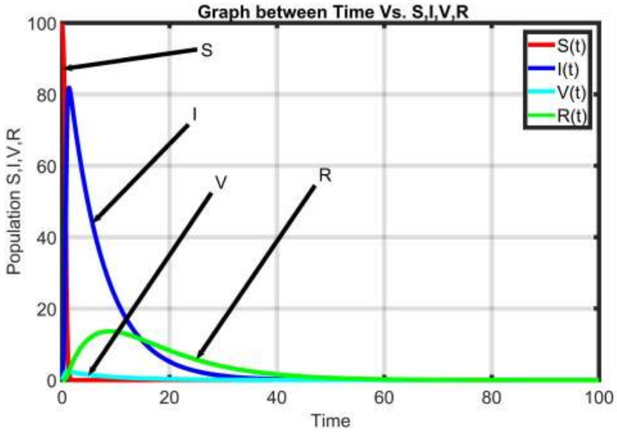

Fig. 3. Dynamic characteristics of the system when $R_0 < 1$ ($b = 0.015$; $\beta = 0.07$; $\mu = 0.1$; $\lambda = 0.04$; $\eta = 0.06$; and $\sigma = 0.05$).

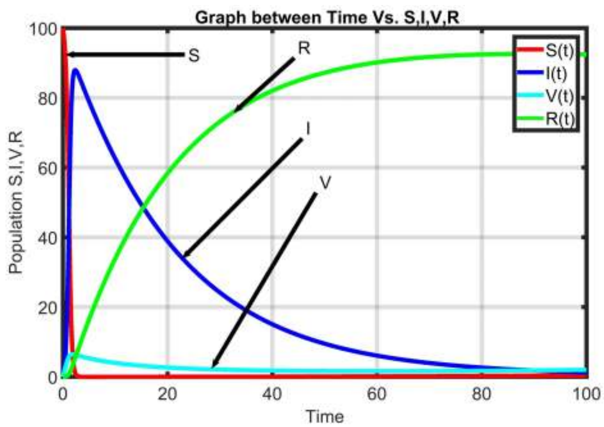

Fig. 4. Dynamic characteristics of the system when $R_0 > 1$ ($b = 0.05$; $\beta = 0.04$; $\mu = 0.001$; $\lambda = 0.06$; $\eta = 0.05$; and $\sigma = 0.02$).

susceptible (S), infectious (I), recovered (R), and verified (V) class with respect to time (t). In this analysis, it is ascertained that initially rumor (infection) increases with time and achieve the maximum value. After that, it begins to disappear with time and become zero. This shows that the system is asymptotically stable in these conditions. The basic reproduction number in case 1 (value taken for Fig. 2) and (value taken for Fig. 3) are 0.007154 and 0.05012, respectively. These values are less than 1, so untrusted message disappears from the social network. This result validates Theorems 2 and 3. Fig. 4 demonstrates that rumor persists in the system continuously and in case 2, the value of basic reproduction number (1.414336) is greater than 1. In this situation, unwanted messages will spread in the social network.

Fig. 5 shows the dynamic relationship between susceptible and verified individuals. The number of verified users increases in the social network under the given conditions. From Fig. 5, it is observed that as the rate of verification increases then the number of verified users increases in the network. Therefore, in this case the chances of unwanted message propagation will be very less or will not propagate in the network. However, this verification cannot ensure that the verified user will not propagate unwanted message in the network. They may be victimized by other unauthenticated user and may be moved into the category of spreader.

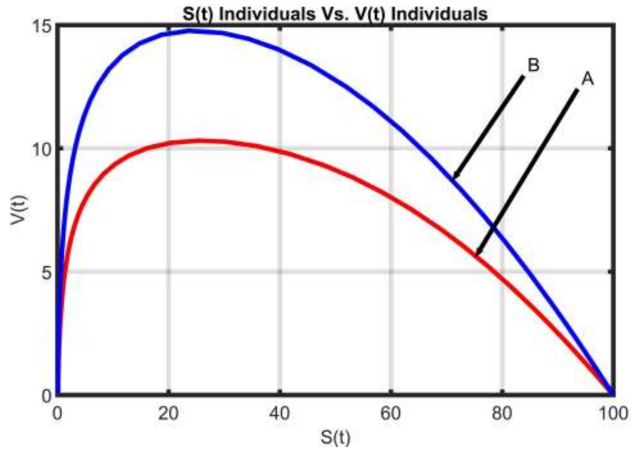

Fig. 5. Effect of verification on the system under different conditions A ($b = 0.015$; $\beta = 0.01$; $\mu = 0.1$; $\lambda = 0.04$; $\eta = 0.05$; and $\sigma = 0.004$) and B ($b = 0.015$; $\beta = 0.01$; $\mu = 0.1$; $\lambda = 0.06$; $\eta = 0.05$; and $\sigma = 0.003$).

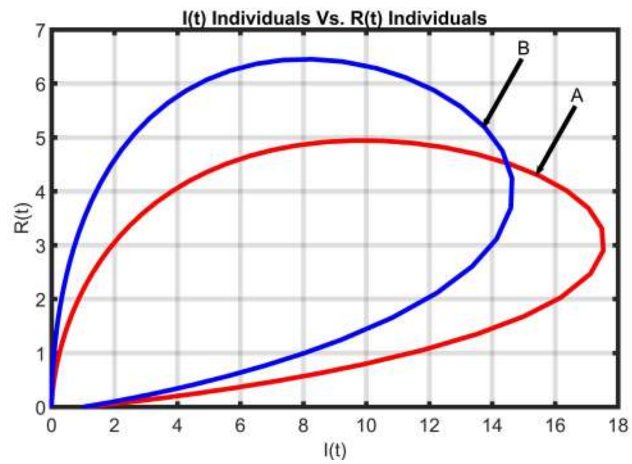

Fig. 6. Effect of elimination of unwanted messages of the system under different condition A ($b = 0.015$; $\beta = 0.01$; $\mu = 0.1$; $\lambda = 0.04$; $\eta = 0.05$; and $\sigma = 0.004$) and B ($b = 0.015$; $\beta = 0.01$; $\mu = 0.1$; $\lambda = 0.04$; $\eta = 0.08$; and $\sigma = 0.004$).

Fig. 6 shows that if the rate of recovery increases, then the number of infected (unwanted) messages (or users) gets eliminated from the network. From this figure, it is observed that as the rate of removal or blocking of unwanted messages (or users) increases then the number of spreaders will be decreed from the network. This technique can be used to prevent unwanted messages (or users) propagation in the network.

The trend of real-world spread of misinformation on social networks is similar to what we experienced and show in our simulation results. Lohr [59] reported on the basis of the research of Vosoughi *et al.* [60] and prepared a chart of fake news trends on Twitter. The technology related to the fake news report is reported in their works [59], [60]. Fig. 7 describes how the misinformation spread in Twitter reaches to a maximum and then starts to experience a decline. Depending on the type and activeness of the specific spreader, the news will exist endemically in OSNs and may be blocked and removed by the social site which will end its spread. There are two stories discussed in the report. Two stories related to

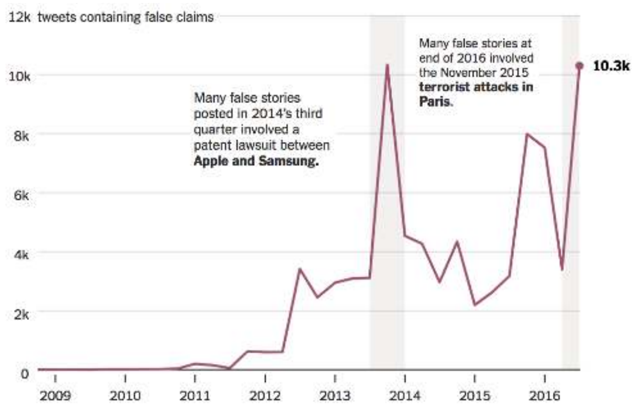

Fig. 7. Spreading trend of misinformation in OSN.

misinformation can be referenced by interested readers directly in their works.

VIII. Conclusion

The research work presented in this article proposes a mathematical model to study the dynamic spreading and controlling activities of message transmission in OSNs. The proposed model employs differential equations for investigating the effect of verification and blocking of users and the spread of messages on OSNs. The expression for basic reproduction R_0 is obtained, which is used to analyze the status of rumor in the social network. Results obtained indicates that if R_0 is less than 1, then rumors and fake news will be eliminated and OSNs gets stabilized locally. The local stability of rumor-free equilibrium is established by the Jacobian matrix. It is found that if the eigenvalues of the matrix are less than zero then the network will be asymptotically stabilize locally in nature and free from the rumors. The Lyapunov function used to establish the global asymptotic stable status of the social network. Mathematical analysis has been performed to depict the accuracy of the rumor-free equilibrium. The activities of different classes of users have also been examined in the social network. In future, the method of latent and isolation can be used for the prevention of social network from rumor spread and fake news propagation. The issues examined in this article are of direct current concern, and the pandemic COVID-19 is creating a global crisis in rumors and fake news propagating freely on OSNs which may continue until it is cured/handled. Real-world data clearly show that fake news propagation can be harmful for people, businesses, and many other facets of society. The results in this article therefore, may help solve some of the current global issues related to fake news spread.

References

[1] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, "Modeling propagation dynamics of social network worms," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 8, pp. 1633–1643, Aug. 2013.

[2] E. Lebensztayn, F. P. Machado, and P. M. Rodríguez, "On the behaviour of a rumour process with random stifling," *Environ. Model. Softw.*, vol. 26, no. 4, pp. 517–522, Apr. 2011.

[3] L. Li *et al.*, "Characterizing the propagation of situational information in social media during COVID-19 epidemic: A case study on weibo," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 2, pp. 556–562, Apr. 2020.

[4] A. Legon and A. Alsalman. *How Facebook Can Flatten the Curve of the Coronavirus Infodemic*. Accessed: Apr. 20, 2020. [Online]. Available: https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation/

[5] S. Sommariva, C. Vamos, A. Mantzarlis, L. U.-L. Dào, and D. Martinez Tyson, "Spreading the (fake) news: exploring health messages on social media and the implications for health professionals using a case study," *Amer. J. Health Edu.*, vol. 49, no. 4, pp. 246–255, Jul. 2018, doi: 10.1080/19325037.2018.1473178.

[6] G. Whitehouse, "Pete/Repeat Tweet/Retweet Blog/reblog: A hoax reveals media mimicking," *J. Mass Media Ethics*, vol. 27, no. 1, pp. 57–59, Jan. 2012.

[7] M. Kosfeld, "Rumours and markets," *J. Math. Econ.*, vol. 41, no. 6, pp. 646–664, Sep. 2005.

[8] Y. Xiao, D. Chen, S. Wei, Q. Li, H. Wang, and M. Xu, "Rumor propagation dynamic model based on evolutionary game and anti-rumor," *Nonlinear Dyn.*, vol. 95, no. 1, pp. 523–539, Jan. 2019.

[9] A. V. Banerjee, "The economics of rumours," *Rev. Econ. Stud.*, vol. 60, no. 2, pp. 309–327, Apr. 1993.

[10] K. Dietz, "Epidemics and rumours: A survey," *J. Roy. Stat. Soc., A (Gen.)*, vol. 130, no. 4, pp. 505–528, 1967.

[11] D. J. Daley and D. G. Kendall, "Stochastic rumours," *IMA J. Appl. Math.*, vol. 1, no. 1, pp. 42–55, 1965.

[12] S. Dubey *et al.*, "Psychosocial impact of covid-19," *Diabetes Metabolic Syndrome*, vol. 14, no. 5, pp. 779–788, May 2020.

[13] F. Ren, S.-P. Li, and C. Liu, "Information spreading on mobile communication networks: A new model that incorporates human behaviors," *Phys. A, Stat. Mech. Appl.*, vol. 469, pp. 334–341, Mar. 2017.

[14] T. Wang, J. He, and X. Wang, "An information spreading model based on online social networks," *Phys. A, Stat. Mech. Appl.*, vol. 490, pp. 488–496, Jan. 2018.

[15] S. Dagher, *Assad or We Burn Country: How One Family's Lust for Power Destroyed Syria*. Boston, MA, USA: London Back Pay Books, 2019.

[16] R. Basak, S. Sural, N. Ganguly, and S. K. Ghosh, "Online public shaming on Twitter: Detection, analysis, and mitigation," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 2, pp. 208–220, Apr. 2019.

[17] G. Liang, W. He, C. Xu, L. Chen, and J. Zeng, "Rumor identification in microblogging systems based on users' behavior," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 3, pp. 99–108, Sep. 2015.

[18] T. Thanh Le *et al.*, "The COVID-19 vaccine development landscape," *Nature Rev. Drug Discovery*, vol. 19, no. 5, pp. 305–306, May 2020.

[19] S. Wu, A. Das Sarma, A. Fabrikant, S. Lattanzi, and A. Tomkins, "Arrival and departure dynamics in social networks," in *Proc. 6th ACM Int. Conf. Web Search Data Mining (WSDM)*, 2013, pp. 233–242.

[20] K. Shu, H. R. Bernard, and H. Liu, "Studying fake news via network analysis: Detection and mitigation," in *Emerging Research Challenges and Opportunities in Computational Social Network Analysis and Mining*. New York, NY, USA: Springer, 2019, pp. 43–65.

[21] R. Cross, A. Parker, and L. Sasson, *Networks in the knowledge economy*. New York, NY, USA: Oxford Univ. Press, 2003.

[22] J. Cannarella and J. A. Spechler, "Epidemiological modeling of online social network dynamics," 2014, *arXiv:1401.4208*. [Online]. Available: http://arxiv.org/abs/1401.4208

[23] Y. Yao, X. Xiao, C. Zhang, C. Dou, and S. Xia, "Stability analysis of an SDILR model based on rumor recurrence on social media," *Phys. A, Stat. Mech. Appl.*, vol. 535, Dec. 2019, Art. no. 122236.

[24] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. Roy. Soc. london. A, Containing Papers Math. Phys. Character*, vol. 115, no. 772, p. 700–721, 1927.

[25] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proc. Nat. Acad. Sci. USA*, vol. 99, no. 12, pp. 7821–7826, Jun. 2002.

[26] M. E. J. Newman, "Community detection and graph partitioning," *EPL (Europhys. Lett.)*, vol. 103, no. 2, p. 28003, Jul. 2013.

[27] W.-M. Liu, S. A. Levin, and Y. Iwasa, "Influence of nonlinear incidence rates upon the behavior of SIRS epidemiological models," *J. Math. Biol.*, vol. 23, no. 2, pp. 187–204, Feb. 1986.

[28] W. Wang, "Epidemic models with nonlinear infection forces," *Math. Biosci. Eng.*, vol. 3, pp. 267–279, Jan. 2006.

[29] Z. Zhang, H. Wang, C. Wang, and H. Fang, "Modeling epidemics spreading on social contact networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 3, pp. 410–419, Sep. 2015.

[30] D. J. Daley and J. Gani, *Epidemic Modelling: Introduction*, vol. 15. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[31] J.-J. Cheng, Y. Liu, B. Shen, and W.-G. Yuan, "An epidemic model of rumor diffusion in online social networks," *Eur. Phys. J. B*, vol. 86, no. 1, p. 29, Jan. 2013.

[32] M. Nekovee, Y. Moreno, G. Bianconi, and M. Marsili, "Theory of rumour spreading in complex social networks," *Phys. A, Stat. Mech. Appl.*, vol. 374, no. 1, pp. 457–470, Jan. 2007.

[33] O. N. Bjørnstad, K. Shea, M. Krzywinski, and N. Altman, "Modeling infectious epidemics," *Nature Methods*, vol. 17, p. 455–456, Apr. 2020.

[34] M. Soltanolkottabi, D. Ben-Arieh, and C.-H. Wu, "Modeling behavioral response to vaccination using public goods game," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 2, pp. 268–276, Apr. 2019.

[35] R. Cohen, S. Havlin, and D. ben-Avraham, "Efficient immunization strategies for computer networks and populations," *Phys. Rev. Lett.*, vol. 91, no. 24, Dec. 2003, Art. no. 247901.

[36] Y. Yu *et al.*, "Finding spread blockers in dynamic networks," in *Proc. Int. Workshop Social Netw. Mining Anal.* New York, NY, USA: Springer, 2008, pp. 55–76.

[37] Z. He, Z. Cai, and X. Wang, "Modeling propagation dynamics and developing optimized countermeasures for rumor spreading in online social networks," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst.*, Jun. 2015, pp. 205–214.

[38] J. Xu, M. Zhang, and J. Ni, "A coupled model for government communication and rumor spreading in emergencies," *Adv. Difference Equ.*, vol. 2016, no. 1, pp. 1–15, Dec. 2016.

[39] S. Wen, J. Jiang, Y. Xiang, S. Yu, W. Zhou, and W. Jia, "To shut them up or to clarify: Restraining the spread of rumors in online social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3306–3316, Dec. 2014.

[40] D. Centola, "Failure in complex social networks," *J. Math. Sociol.*, vol. 33, no. 1, pp. 64–68, Dec. 2008.

[41] X. Zhu, Y. Nie, and A. Li, "Demographic prediction of online social network based on epidemic model," in *Proc. Asia–Pacific Web Conf.* Beijing, China: Springer, 2014, pp. 93–103.

[42] S. Wen, M. S. Haghighi, C. Chen, Y. Xiang, W. Zhou, and W. Jia, "A sword with two edges: Propagation studies on both positive and negative information in online social networks," *IEEE Trans. Comput.*, vol. 64, no. 3, pp. 640–653, Mar. 2015.

[43] M. Granovetter, "The strength of weak ties: A network theory revisited," *Sociol. Theory*, vol. 1, pp. 201–233, Jan. 1983.

[44] J. Huang and Q. Su, "A rumor spreading model based on user browsing behavior analysis in microblog," in *Proc. 10th Int. Conf. Service Syst. Service Manage.*, Jul. 2013, pp. 170–173.

[45] M. Y. Li and J. S. Muldowney, "Global stability for the SEIR model in epidemiology," *Math. Biosci.*, vol. 125, no. 2, pp. 155–164, Feb. 1995.

[46] W.-M. Liu, H. W. Hethcote, and S. A. Levin, "Dynamical behavior of epidemiological models with nonlinear incidence rates," *J. Math. Biol.*, vol. 25, no. 4, pp. 359–380, Sep. 1987.

[47] W. Zhou, X. Zhang, and X. Jiang, "AppInk: Watermarking Android apps for repackaging deterrence," in *Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur.*, 2013, pp. 1–12.

[48] A. Singh and Y. N. Singh, "Rumor dynamics with inoculations for correlated scale free networks," in *Proc. Nat. Conf. Commun. (NCC)*, Feb. 2013, pp. 1–5.

[49] S. Dong, Y-B. Deng, and Y-C. Huang, "SEIR model of rumor spreading in online social network with varying total population size," *Commun. Theor. Phys.*, vol. 68, pp. 545–552, Oct. 2017.

[50] L. Zhu, X. Zhou, and Y. Li, "Global dynamics analysis and control of a rumor spreading model in online social networks," *Phys. A, Stat. Mech. Appl.*, vol. 526, Jul. 2019, Art. no. 120903.

[51] X. Liu, T. Li, and M. Tian, "Rumor spreading of a SEIR model in complex social networks with hesitating mechanism," *Adv. Difference Equ.*, vol. 2018, no. 1, pp. 1–24, Dec. 2018.

[52] W. Fu, S. Liu, and G. Srivastava, "Optimization of big data scheduling in social networks," *Entropy*, vol. 21, no. 9, p. 902, 2019.

[53] E. D. Raj, G. Manogaran, G. Srivastava, and Y. Wu, "Information granulation-based community detection for social networks," *IEEE Trans. Comput. Social Syst.*, early access, Jan. 31, 2020, doi: 10.1109/TCSS.2019.2963247.

[54] K. Clarkson, G. Srivastava, F. Meawad, and A. D. Dwivedi, "Where's @Waldo?: Finding users on Twitter," in *Proc. Int. Conf. Artif. Intell. Soft Comput.* Springer, 2019, pp. 338–349.

[55] B. Zolfaghari *et al.*, "Content delivery networks: State of the art, trends, and future roadmap," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–34, 2020.

[56] O. Diekmann, J. A. P. Heesterbeek, and J. A. J. Metz, "On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations," *J. Math. Biol.*, vol. 28, no. 4, pp. 365–382, Jun. 1990.

[57] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Math. Biosci.*, vol. 180, nos. 1–2, pp. 29–48, Nov. 2002.

[58] J. P. LaSalle, *The Stability of Dynamical Systems*, vol. 25. Philadelphia, PA, USA: SIAM, 1976.

[59] S. Lohr. *It's True: False News Spreads Faster and Wider. and Humans are to Blame*. Accessed: Aug. 15, 2019. [Online]. Available: https://www.nytimes.com/2018/03/08/technology/twitter-fake-news-research.html

[60] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, pp. 1146–1151, Mar. 2018.

Gulshan Shrivastava (Member, IEEE) received the B.E. degree in computer science engineering from Maharishi Dayanand University, Rohtak, India, in 2008, the M.Tech. degree in information security from Guru Gobind Singh Indraprastha University (GGSIPU), Dwarka, India, in 2011, and the M.B.A. degree in information technology and finance from I. K. Gujral Punjab Technical University (IKGPTU), Kapurthala, India, in 2012. He is currently pursuing the Ph.D. degree in computer science engineering from the National Institute of Technology at Patna (Institute of National Importance), Patna, India.

He earned the certification of SCJP 5.0 from Sun Microsystems, USA. He visited at Datec Ltd., Port Moresby, Papua New Guinea (PNG), in 2010. He is currently working as a Research Scholar with the Department of Computer Science and Engineering, National Institute of Technology at Patna (Institute of National Importance). He has an ardent inclination toward the field of analytics and security. He has filled one patent, an editor/author of more than seven books, author of more than ten book chapters and 35 papers in international journals and conferences of high repute, including IEEE, Elsevier, ACM, Springer, Inderscience, IGI Global, Bentham Science, and so on. His research interests include information security, data analytics, cyber security and forensic, mobile computing, intrusion detection, and computer networks.

Mr. Shrivastava is a Life Member of the Indian Society for Technical Education (ISTE) and a Professional Member of the IEEE, Computer Society of India (CSI), Association for Computing Machinery (ACM), Special Interest Group on Data Communications (SIGCOMM), and many professional bodies. He has served as a TPC Member of International conferences worldwide. He is also serving as an Associate Editor for the *Journal of General Internal Medicine* (SCIE Indexed) and *IJDCF* (Scopus Indexed), IGI Global, and a Section Editor of *Scalable Computing* (SCPE) (Scopus Indexed). He serves for many repute journals as a guest editor, an editorial board member, an international advisory board member, and a reviewer board member. Moreover, he has also delivered the expert talk, guest lecturers in international conference and serving as a reviewer for Journals of IEEE, Springer, Inderscience, IGI Global, and so on. He is a Convener at the ICICC-2020 and the ICICC-2019, the Organizing Chair at the ICCIDA-2018, the Publication Chair at the MARC-2018, and many more. He also served as the Organizing Chair of Special Session.

Prabhat Kumar (Senior Member, IEEE) received the M.Tech. degree in information technology from Allahabad Agriculture Institute (D.U), Prayagraj, India, in 2005, and the Ph.D. degree in computer science and engineering from the National Institute of Technology Patna, Patna, India, in 2014.

He is currently an Associate Professor with the Department of Computer Science and Engineering, National Institute of Technology at Patna (NIT Patna) (Institute of National Importance), Patna, India. He is also the Professor-in-Charge of the IT Services of the Institute and has experience of more than ten years in network planning and management. His research interests include wireless sensor networks, the Internet of Things, social networks, operating systems, software engineering, E-governance, and so on.

Dr. Kumar is a Professional Member of ACM; a Life Member of the Computer Society of India (CSI), the International Association of Engineers (IAENG), the Indian Society for Technical Education (ISTE); and a Global Member of the Internet Society. He is also a member of the International Federation for Information Processing (IFIP) Working Group (WG) 6.11: Communication Aspects of the E-World as well as member of National Working Group 13 (NWG-13) corresponding to ITU-T Study Group 13 "Future Networks, with focus on IMT-2020, cloud computing, and trusted network infrastructures." He is also a former State Student Coordinator of the State—Bihar under Region II, Computer Society of India. He has several publications in various reputed journals and has published multiple papers in various international conferences. He has served as a guest editor for special issues in international journals and has also edited multiple books published by reputed international publishers. He is also in the reviewing panel of several reputed journals. He has chaired sessions at several international conferences held in India and abroad. He is also the Chairman of the Computer and IT Purchase Committee, NIT Patna. He has delivered expert talks and guest lectures at various prestigious institutes.

Rudra Pratap Ojha received the B.Tech. degree from Dr. A. P. J. Abdul Kalam Technical University at Lucknow (UPTU Lucknow), Lucknow, India, in 2004, the M.Tech. degree from the Motilal Nehru National Institute of Technology (MNNIT) at Allahabad, Allahabad, India, in 2009, and the Ph.D. degree from the National Institute of Technology (NIT), Durgapur, India, in 2019.

He is currently working as an Associate Professor with Galgotias University, Greater Noida, India. He has published more than 15 papers in international and national journals/conferences. His research interests include wireless sensor networks, real time systems, and mathematical modeling and simulation. He is working as reviewer in various reputed journals.

Dr. Ojha is a Life Member of the Computer Society of India (CSI). He has delivered expert talks and guest lectures at various prestigious institutes.

Pramod Kumar Srivastava received the Ph.D. degree in mathematics from the University of Allahabad, Allahabad, India, in 2007.

He is currently an Assistant Professor with the Department of Mathematics, Rajkiya Engineering College, Azamgarh (Affiliated to Dr.A.P.J. Abdul Kalam Technical University, Lucknow), India. He has 15 years of teaching and research experience along with Ph.D. guidance. He has several publications in various reputed international journals and international conferences. He has also published multiple books. His research interests include wireless sensor networks, mathematical modeling, and social networks.

Senthilkumar Mohan received the master's degrees in software engineering and information technology-networking and the Ph.D. degree in big data from the Vellore Institute of Technology (VIT University), Vellore, India, in 2007, 2013, and 2017, respectively.

He was a Project Associate with IIT Madras, Chennai, India, from 2009 to 2010. He is currently working as an Associate Professor with the Department of Software and System Engineering, School of Information Technology and Engineering (SITE), VIT University. He has more than 13 years of teaching and industry experience. He has published more than 30 papers in peer-reviewed reputed journals, conferences, and book chapters. His reputed publications the IEEE ACCESS, the *Journal of Parallel and Distributed Computing*, *Cybernetics and Information Technologies*, *Computer Communications*, *Computers and Electrical Engineering*, and the *Journal of Ambient Intelligence and Humanized Computing*. He is a peer reviewer for journals, such as *Software: Practice and Experience, Engineering Reports* (Wiley), the IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *International Journal of Neural Systems*, and the IEEE ACCESS. He is also a Review Board Member of *Frontiers in Medical Technology* and a Bentham Ambassador. His research interests include machine learning, cloud computing, big data, and the Internet of Things.

Dr. Mohan was a recipient of the Article of the work IEEE ACCESS. He is also a member of various professional societies like CSI and Indian Congress.

Gautam Srivastava (Senior Member, IEEE) received the B.Sc. degree from Briar Cliff University, Sioux City, USA, in 2004, and the M.Sc. and Ph.D. degrees from the University of Victoria, Victoria, BC, Canada, in 2006 and 2012, respectively.

He then taught for three years at the Department of Computer Science, University of Victoria, where he was regarded as one of the top undergraduate professors in the Computer Science Course Instruction. In 2014, he joined Brandon University, Brandon, MB, Canada, as a tenure-track position, where he is currently active in various professional and scholarly activities. He was promoted to the rank of an Associate Professor in January 2018, as he is popularly known. In his five years as a research academic, he has published a total of 100 papers in high-impact conferences in many countries and in high-status journals (Science Citation Index (SCI) and Science Citation Index Expanded (SCIE)) and has also delivered invited guest lectures on big data, cloud computing, the Internet of Things, and cryptography at many universities worldwide. His research interests include cryptography, data mining, security and privacy, and blockchain technology.

Dr. Srivastava is an editor of several SCI/SCIE journals. He has active research projects with other academics in Taiwan, Singapore, Canada, Czech Republic, Poland, and USA. He is also an Associate Editor of the world renowned IEEE ACCESS journal.