IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 February 2023, accepted 23 March 2023, date of publication 28 March 2023, date of current version 3 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3262737

RESEARCH ARTICLE

Controlling of Fake Information Dissemination in Online Social Networks: An Epidemiological Approach

RUDRA PRATAP OJHA[1], PRAMOD KUMAR SRIVASTAVA[2], SHASHANK AWASTHI[1], (Member, IEEE), VINEET SRIVASTAVA[2], PURNENDU SHEKHAR PANDEY[3], (Senior Member, IEEE), RADHE SHYAM DWIVEDI[2], RAJESH SINGH[4], (Member, IEEE), AND ANTONINO GALLETTA[6,7,8], (Member, IEEE)

[1]Department of Computer Science and Engineering, G. L. Bajaj Institute of Technology and Management (GLBITM), Affiliated to AKTU, Greater Noida, Uttar Pradesh 201306, India
[2]Rajkiya Engineering College Azamgarh, Akbalpur, Devgaon, Azamgarh, Uttar Pradesh 276201, India
[3]Department of Electronics and Communication Engineering, G. L. Bajaj Institute of Technology and Management (GLBITM), Affiliated to AKTU, Greater Noida, Uttar Pradesh 201306, India
[4]Uttaranchal Institute of Technology, Uttaranchal University, Dehradun 248007, India
[5]Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, Mexico
[6]MIFT Department, The University of Messina, 98122 Messina, Italy
[7]INDAM Gruppo Nazionale per il Calcolo Scientifico (GNCS), 44122 Ferrara, Italy
[8]CINI, Laboratorio Informatica e Società (IeS), 00198 Lazio, Italy

Corresponding author: Antonino Galletta (angalletta@unime.it)

This work was supported in part by the Department for Drug Policies of the Presidency of the Council of Ministers (Italian Government) through the Project InstradaME under Grant CUP F49I20000100001, and in part by the Italian Ministry of Health Piano Operativo Salute (POS) Trajectory 2 "eHealth, diagnostica avanzata, medical device e mini invasività" through the Project "Rete eHealth: AI e strumenti ICT Innovativi orientati alla Diagnostica Digitale (RAIDD)" under Grant CUP J43C22000380001.

ABSTRACT Due to the fast advancement of Internet technology, the popularity of Online Social Networks (OSN) over the Internet is increasing day by day. In the modern world, people are using OSN to communicate with others around the world who may or may not know each other. OSN has become the most convenient means to transmit media (news/content) and gather or spread information in the world. The posts (contents) on OSN affect and impact people, and minds at least for some time. These contents are important because they play a crucial role in taking the decision. The posts which are available on the OSN may be information or just misinformation. The misinformation may be a type of fake news or rumour. This is very difficult for people to differentiate whether the posts are information or rumour. Therefore, the development of techniques that can prevent the transmission of false information or rumours that might harm society in any way is critical. In this paper, a model is developed based on the epidemic approach, for examining and controlling fake information dissemination in OSN. The proposed model illustrates how different misinformation debunking measures impact and how misinformation spreads among different groups. In this article, we explain that the proposed model will be able to recognize and eradicate fake news from OSN. The model is written as a system of differential equations. Its equilibrium and stability are also carefully examined. The basic reproduction number (R_0) is calculated, which is an important parameter in the study of message propagation in OSN. If $R_0 < 1$, the propagation of rumor in the OSN will be minimal; nevertheless, if $R_0 > 1$, the fake information/rumor will continue in OSN. The effects of disinformation of rumours in OSN in the real world are explored. In addition, the model covers the fake information/rumour dissemination control mechanism.

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

The comparative study shows that the proposed model provides a better mechanism to prevent the dissemination of fake information in OSN in comparison to other previous models. Extensive theoretical study and computation analysis have also been used to validate the proposed model.

INDEX TERMS Basic reproduction number, epidemic, fake information, misinformation, rumor, online social networks (OSN), stability.

I. INTRODUCTION

The modern world is moving around the Internet technology which is used to communicate the information from one location to another location in the globe. Internet is the fastest mode of information dissemination. Therefore, this is important to study the pros and cons of this technology. Internet technology is the backbone of Online Social Networks (OSN). People have been getting information quicker and faster in the past few years due to the advancement of Internet technology and the methods of obtaining information have become increasingly diversified with the uses of social media platforms such as Facebook, Instagram, Twitter, WhatsApp, Wechat, Google and microblogging sites have become a source of information exchange may be positive or negative information [1]. These platforms are used by users to connect with people from around the globe and transfer as well as share data at a very low cost. This is one of the important advantages of OSN but it is very difficult to identify whether the available data is correct information or misinformation/rumour. This is essential to understand and identify that the available information is not a rumour. The statement has no facts but disseminates widely with the wrong intention. The identification of rumours is important because they affect the personal and social lives of people [2].

In recent times, taking the example of COVID-19 disease, the different OSN platforms spread the fake information about COVID-19 [3]. The fake information about COVID-19 treatment was spreading on Facebook [4]. Due to the fake information about COVID-19 the treatment of the people badly suffered. The vaccination study for COVID-19 in the United Kingdom was affected when it was mistakenly stated that the first patient treated with the vaccine of COVID-19 had died [5]. The ramifications of this COVID-19 myth were unknown at this time because it was so new but the impact was genuine that individuals will now be more afraid to get COVID-19 vaccination. Bolsonaro president of Brazil made a false statement regarding COVID-19. This statement affected the people's health of Brazil because he is the president of the country and his statement has meaning. So the people of the country become careless. The senate committee claimed that 600000 Brazilians lost their lives due to misinformation [6]. Islam et al. [7] have presented an analysis of global media in which they analyzed the effect of misinformation on public health due to COVID-19 related rumours. Loomba et al. [8] measures the impact of online misinformation on vaccination intent in the USA and UK. Rumours have a significant influence on society [9].

People are more likely to become easy targets as a result of these realities, and they are more likely to get scared and become sad as a result of false information. They also make poor judgements based only on misinformation. Another example of the effect of fake news on people is the Zika virus. Sommariva et al. [10] discussed the influence of fake news on people concerning a well-known Zika virus case study. The authors discovered that fake news spreads quickly on OSN and tends to reach a massive audience. Verification is one of the key challenges connected with OSN.

The number of messages sent and received by the ONS users is more but the identification of message validity is very difficult. The misinformation disseminates very fast via social networks. It may be possible that due to misinformation social media may wreak havoc on peace and societal harmony [11]. Such communications, which are now referred to as fake news/rumours theses messages may be life-threatening. These messages are essentially rumours/misinformation that are disseminated in various ways with different objectives [12], [13], either for fun or malevolent intent. Unnecessary fear may grow among the public as a result of such messages and nations may suffer unnecessary panic or economic losses [14], [15]. One of the facts is that information on OSN disseminates at a rapid rate and information can spread globally within seconds [16]. There have been several occasions when the propagation of fake information on OSN has resulted in unfavourable and harmful outcomes for society. For example, two bombs exploded in the White House on April 23, 2013, wounding the US president and causing a $ 10 billion loss [17]. Another example is the ancient Mayan calendar, 21 December 2012, which was supposed to be the last date for a human being when the world will perish completely. This rumour rapidly spread in the world through OSN even after being rejected by Mayan descendants and eminent scientists of the world [18]. Hence, to minimize the loss to society as well as the nation due to rumours, it is essential to study rumour dissemination dynamics.

The spreading dynamics of rumours are similar to the epidemics [19], therefore the concept of epidemiology has been used by researchers to analyze the rumour spreading dynamics. The first classical SIR epidemic model was proposed by Kermack and McKendrick [20] in 1927 to study the spreading of infectious diseases. Afterwards, many researchers have proposed different models based on the concept of epidemic modelling for the prediction and controlling of infectious diseases. Delay and Kendal studied the rumour spreading model based on the theoretical study and practical examination of epidemic models in 1964. They noticed that there are some similarities between infectious disease spread and rumour spreading, but not exactly alike. Based on infectious disease spread, Delay and Kendal [21] proposed a classical rumour spreading model based on epidemic theory and this model was known as the DK model. In the DK model, the total population consisted of three types of population: ignorant (those people who do not know rumours), spreader (those people who know and spread rumours) and stifler (those people who know but do not spread rumours). In 1973 Maki and Thomson [22] modified the DK model and proposed an MK model to study the dynamics of rumour spread. The MK model explains the actual process of rumour propagation by classification of the contact of the direct spreader or another way. DK and MK models explain the process of rumour propagation in detail, but some important parameters which affect the process of rumour propagation were not taken into account. Based on DK, MK, and infectious disease models, considering the different aspects of rumour propagation extensive analysis has been performed on rumour propagation. Zantee [23] studied rumour propagation on small-world networks in both static and dynamic conditions. The mechanics of rumour propagation on complex social networks were explained by Nekovee et al. [24]. The researchers looked at how rumours propagate in various network topologies, including scale-free networks, uncorrelated scale-free networks, and random graphs. The authors discovered a threshold value to prove that below a certain level of a threshold value, a rumour could not successfully propagate in a specific OSN. The other factors which affect the spreading of rumour are network topology, activity of spreader, hesitating mechanism, forgetting mechanism, forget-remember mechanism, etc. [25].

As the popularity of OSN is increasing the speed of fake information dissemination also speeds up exponentially in comparison to traditional networks. Therefore, Rumour/fake information detection and prevention measures have become a potentially significant field of research as a result of the enormous extent and relevance of OSN. This encourages the researchers to develop diverse mathematical models for rumour propagation detection. Shah [26] utilized the SI model to detect the source of fake information in the network. Zhan et al. [27] proposed an SIS model to analyze the dynamics of information diffusion in a complex network. Abdullah and Wu [28] utilized the SIR model to explain the spreading dynamics of news on Twitter. They identified the factors that can affect the particular news spreading on Twitter. Dhar et al. [18] proposed an SEI model to investigate the spreading dynamics of news in OSN. They analyzed the impact of wrong news propagation on people. The method of detection and control of unauthenticated news propagation in OSN was discussed. Dong et al. [29] proposed SEIR to analyze the propagation of rumour in OSN considering the different sizes of the population. They also analyzed the impact of new users and other factors in OSN. The model describes the behaviour of the exposed class of users in OSN. The extended SEIR model was proposed by Zhao et al. [30] to analyze the information propagation dynamics in OSN. They studied the effect of the homepage on the propagation speed of information in OSN. The equilibrium state of the system was analyzed and obtained two equilibrium points. One of the important control parameters basic reproduction number of the model was obtained, which was used to analyze the spreading dynamics of information in OSN. To prove the proposed model they use a case study and numerical simulations. To protect the OSN from fake information spreading it is necessary to verify the users who want to join social media platforms. Srivastava et al. [31] proposed a susceptible-verified-infected-recovered (SVIR) model to prevent the spread of misinformation in OSN. The concept of user or message authentication through the verified class was introduced. They also analyzed the global and local stability of the OSN. The value of the basic reproduction number was also obtained by them to describe the status of fake information in OSN. These models are useful to analyze the rumour spreading in OSN.

Nowadays criminal groups are using OSN portals to spread rumours or fake information. These users intend to disseminate incorrect information, resulting in dangerous and detrimental situations throughout the world. People are impacted and scared as a result of such communications. The increasing penetration rate of social networks into people's daily lives has resulted in a new source of concern. The propagation of information on social media is extremely rapid. It is very difficult to prevent and remove untrustworthy content. As a result, developing models that can manage rumours and avoid unanticipated situations in the world is necessary to safeguard the OSN from this sort of activity.

To control the fake information/rumour dissemination in OSN by use of the concept of epidemic modelling, we proposed a Susceptible - Verified - Exposed - Infectious - Recovered/Removed (SVEIR) model. In the proposed model, this is assumed that all the users of the OSN are in the susceptible category and they can be a victim of fake information or rumour. To prevent malicious users in OSN the verification of users are important. Therefore, a method of user verification is applied to authenticate the users, those who want to join OSN. Due to the variety of users in OSN, verification of all types of users are very difficult. So, those users who are not verified can be considered exposed users of the OSN. It might be that some of the users have been verified in OSN by use of wrong information and are kept in the observation because in OSN there is no physical verification of the users. After some time, the exposed users turn into a spreader and they have the potential to infect and spread fake information in the OSN. Hence, to preclude fake information dissemination and the unwanted user activities in the OSN, apply the techniques of removal and/or blocking of malicious users as well as fake information.

The proposed model's main goals are to keep a watch on the presence of fake information/rumour and spreaders in OSN and to implement an appropriate corrective mechanism for blocking and/or removing these forms of fake information and spreaders.

The following is a summary of our contributions:

1) Devise a technique to prevent the transmission of fake information by developing a mathematical model for monitoring spreaders and fake information in OSN.
2) Apply the user's authentication mechanism in OSN by using the concept of verification through the verified class.
3) Analyse the impact of a verified state on an OSN's responsiveness and its function in preventing the dissemination of fake information in OSN.
4) Study the importance of the exposed state in controlling fake information dissemination in OSN. The exposed state provides the mechanism to detect rumours early and take corrective action on time.
5) Investigate the effect of a recovered state (blocking, deleting, or leaving a spreader group) on fake information and a spreader in OSN.
6) Analyse the stability of rumour-free equilibrium and rumour-prevailing equilibrium and verify theoretical conclusions with comprehensive simulation results.

The rest of this article is organized as follows. In Section II, related work is discussed, and model formulation for OSN and its fundamental characteristics are presented in Section III, while local and global stability of the proposed model is discussed in Section IV, simulations and experimental analysis, as well as comparative studied, are presented in Section V. Fake information dissemination control technique and sensitivity analysis of the parameters are presented in section VI. Section VII discusses the conclusion and future work.

II. RELATED WORK

Online social networks have been the subject of a tremendous amount of study. To analyze the process of fake information or rumour dissemination in OSN, the researchers have presented several rumour-spreading models. In the OSN, there are numerous types of users with various intentions. A few of them are spreading fake information on the OSN and others may not even be aware of it. So, different techniques can be used to tackle the problem of fake information dissemination in the OSN. One way is to block the rumour [32], while another is to propagate anti-rumour to reduce the impact of rumour [14], although both are time-consuming and costly mechanisms. The suppression of rumour may have the opposite effect, increasing people's desire to know more about it. Other techniques are employed to combat rumours and disseminate the facts [33] especially done by the government in case of emergency. In this technique, the undesirable message is first recognized and then stopped, as well as spreading the truth in OSN at the same time. Escalante and Odehnal [34] proposed a SIRS epidemic model to study the effect of two rumours spread on a social network. They discussed the effect of counteracting rumours from the original rumour spread. The stability analysis along with rumour-free and rumour-endemic equilibrium is discussed. They performed the numerical analysis of a model for validation.

Jiang and Yan [35] analyzed the rumour spreading on OSN using the SIR model. The number of spreaders changes dynamically in the OSN, this has been taken into account in the analysis. For the determination of rumour spreading trend in the OSN obtained the value of basic reproduction number R_0. The value of R_0 determines the status of the rumour in the OSN. If $R_0 > 1$, the rumour will persist in the OSN. Otherwise, disappear from the OSN when $R_0 < 1$. For controlling rumour spreading in the OSN they suggested a mechanism for susceptible users' immunization. Huo et al. [36] considered the activity of the spreader and proposed an I2SR model for the study of rumour spreading in homogeneous networks. They also discussed the local stability and global stability of equilibrium. The numerical simulation has been performed to analyze the effect of different parameters on the spreading of rumours. Zhao and Wang [37] proposed an ISRW model for the analysis of rumour spreading in OSN. This model took into account the rumour spreading methods between individuals and from medium-to-individuals. The stability of the system is established. Sensitivity analyses of the different parameters are also carried out.

The social network is a scale-free network that learns rumour spreading in practical knowledge to develop a heterogeneous epidemic model [38] for rumour dynamics. Moreno et al. [39] proposed models and examined the effects of network topology on rumour propagation rate in a scale-free network. In an epidemic SIRS model, Zhu et al. [40] described the joining and departure of users in OSN. The model is validated by simulation. Huang and Su [41] developed an improved SIR epidemic model for the study of news dissemination on OSN, as well as a mechanism for rumour management. They discussed the consequences of rumour spreading on ONS. They calculated the value of the basic reproduction number (R_0) to determine the rumour spreading status in OSN and found that if R_0 is less than one, the OSN will be free of unauthenticated news, but if R_0 is greater than one, unauthenticated news will remain in the OSN indefinitely. Numerical calculations have also been used to verify the suggested model's results.

The effect of the exposed state on ONS is described by Dong et al. [29] using the SEIR model. They took into account the variation of OSN users over time. In this model, the user's joining and deactivation rates are explored. They also determined the model's basic reproduction number and exact equilibrium points. In OSN, the impact of user variety on rumour diffusion is explained. They noticed that the number of new users who joins OSN has an impact on the rate at which rumours propagate. Simulation findings back up the proposed model.

TABLE 1. Symbols and their meaning.

S(t)	Susceptible signify individuals who have not yet become victim of rumour but susceptible to it.
E(t)	Exposed (infected, but not yet infechous).
I(t)	Signify the individuals that believe in untrusted message/fake news and be active spreader of rumour.
V(t)	Signify the individuals who are authenticated users in OSN.
R(t)	Signify the individuals who has come out from spreader group.

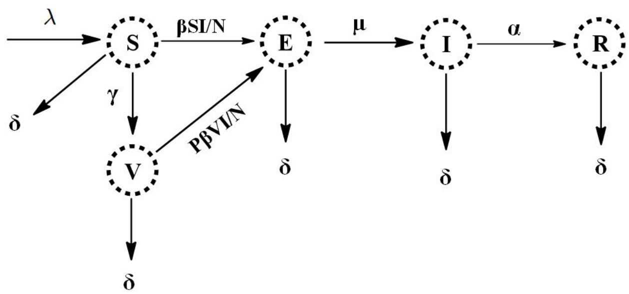

FIGURE 1. Different states of Users in the OSN.

TABLE 2. Used parameters and their meaning.

λ	is the joining rate of user in OSN.
δ	is the rate of leaving (deactivation) of users from different subclass of OSN.
β	is the rate of infection / spreading of rumour in OSN.
α	is the rate of removing / blocking of spreader (infectious) users in OSN.
ρ	is the moving rate of verified users to the exposed type of users.
μ	is the converting rate of exposed users into spreader.
γ	is the rate of verification of susceptible users.

III. FORMULATION OF THE MODEL AND PRELIMINARIES

The rumour propagation flow of the proposed model is given in Fig. 1. The meaning of the different states of the proposed model is described in Table 1.

From the above propagation rule, the rumour spreading SEIVR model in OSN is divided into the following differential equations.

$$\begin{aligned}\frac{dS(t)}{dt} &= \lambda N - \frac{\beta SI}{N} - (\delta+\gamma)S\\ \frac{dV(t)}{dt} &= \gamma S - \frac{\rho\beta VI}{N} - \delta V\\ \frac{dE(t)}{dt} &= \frac{\beta SI}{N} + \frac{\rho\beta VI}{N} - (\mu+\delta)E\\ \frac{dI(t)}{dt} &= \mu E - (\alpha+\delta)I\\ \frac{dR(t)}{dt} &= \alpha I - \delta R \end{aligned} \tag{1}$$

Let $s = S/N$, $e = E/N$, $i = I/N$, $v = V/N$, $r = (R)/N$ denote the proportion of the users S,E,I,R and V to the total numbers of users respectively. Therefore, $s+e+i+v+r = 1$ After straight forward calculation, the resulting system of equation shall be

$$\begin{aligned}\frac{ds(t)}{dt} &= \lambda - \beta si - (\delta+\gamma)s\\ \frac{dv(t)}{dt} &= \gamma s - \rho\beta vi - \delta v\\ \frac{de(t)}{dt} &= \beta si + \rho\beta vi - (\mu+\delta)e\\ \frac{di(t)}{dt} &= \mu e - (\alpha+\delta)i\\ \frac{dr(t)}{dt} &= \alpha i - \delta r \end{aligned} \tag{2}$$

The meaning of the symbols used in model formulation is explained in Table 2. From Eq. 2 it is clear that users of class r do not appear in the first four equations of Eq. 2. It means that four equations are independent of the fifth equation for study is

$$\begin{aligned}\frac{ds(t)}{dt} &= \lambda - \beta si - (\delta+\gamma)s\\ \frac{dv(t)}{dt} &= \gamma s - \rho\beta vi - \delta v\\ \frac{de(t)}{dt} &= \beta si + \rho\beta vi - (\mu+\delta)e\\ \frac{di(t)}{dt} &= \mu e - (\alpha+\delta)i \end{aligned} \tag{3}$$

A. SEIVR MODEL ANALYSIS

Positivity of the Model Since the model monitor number of users for a different class, it is clear that all state variables in the different class remain positive at all times.

Theorem 1: $\Omega = (s,e,i,v)\,\epsilon R_+^4 : s(0) > 0, e(0)>0, i(0) >0, v(0)$ is possible for all $t \geq 0$. *Proof:* Considering the first equation of system (2), we get

$\frac{ds(t)}{dt} \geq -(\delta+\gamma)s \Rightarrow s(t) \geq s_0 e^{-(\delta+\gamma)t} \geq 0$

which shows that $s(t)$ may remain positive for all $t \geq 0$. In the similar way, we can $i(t) \geq 0$, $v(t) \geq 0$, $r(t) \geq 0$ Which proves the Theorem 1.

B. EQUILIBRIUM POINTS

We will analyze two types of behaviour of the SEIRV model, one behaviour where the rumour persists in the system i.e $E \neq 0, I \neq 0$ and the other in which rumour is completely removed i.e $E = I = 0$ The rumour free equilibrium of the system (3) is given by setting all derivatives to zero with $i = 0$ and $e = 0$. $P_0^{RFE} = (s_0^{RFE}, e_0^{RFE}, i_0^{RFE}, v_0^{RFE}) = (\frac{\lambda}{\gamma+\delta}, 0, 0, \frac{\gamma\lambda}{\delta(\gamma+\delta)})$

C. BASIC REPRODUCTION NUMBER R_0

R_0 is calculated by using the next-generation matrix [42]. The components e and I of the system (3) are explicit with rumour propagation. The matrices $\mathbb{F}$, $\mathbb{V}$ represent new rumours and transitions, given by

$$\mathbb{F} = \begin{bmatrix} (\beta s_0 + \rho\beta v \\ 0 \end{bmatrix}^i$$

$$\mathbb{V} = \begin{bmatrix} (\mu+s)e \\ (\alpha+\delta)i - \mu e \end{bmatrix}$$

Their corresponding Jacobian matrix at a rumour-free state is

$$\widetilde{\mathbb{F}} = \begin{bmatrix} 0 & \beta s_0 + \rho\beta v_0 \\ 0 & 0 \end{bmatrix}$$

$$\widetilde{\mathbb{V}} = \begin{bmatrix} \mu+\delta & 0 \\ -\mu & \alpha+\delta \end{bmatrix}$$

The basic reproduction number R_0 is the dominant eigenvalue of the matrix $\mathbb{F}\,\mathbb{V}^{-1}$. That gives
$R_0 = \frac{\beta s_0+\rho\beta v_0}{(\alpha+\delta)(\mu+\delta)}\mu$
Representing the value of S_0 and V_0 in (4), we get
$R_0 = \frac{\beta\lambda\mu(\delta+\rho\gamma)}{\delta(\gamma+\delta)(\alpha+\delta)(\mu+\delta)}$

IV. STABILITY ANALYSIS OF THE PROPOSED MODEL

Local and Global Stability Analysis at Rumour-Free Equilibrium:

Local and Global stability analyses at rumour-free equilibrium P_0^{RFE} of the proposed model are analyzed with help of the Jacobian matrix. $\left(\frac{\lambda}{(\gamma+\delta)(\mu+\delta)}, 0, 0, \frac{\gamma\lambda}{\delta(\gamma+\delta)}\right)$

The Jacobian matrix at P_0^{RFE} is given by

$$J(P_0^{RFE}) = \begin{bmatrix} -(\delta+\gamma) & 0 & -\beta s_0^{RFE} & 0 \\ 0 & -(\delta+\mu) & \beta s_0^{RFE}+\rho\beta v_0^{RFE} & 0 \\ 0 & \mu & -(\delta+\alpha) & 0 \\ \gamma & 0 & -\rho\beta v_0^{RFE} & -\delta \end{bmatrix}$$

Theorem 2: At rumour free equilibrium $P_0^{RFE} = \left(\frac{\lambda}{(\gamma+\delta)}, 0, 0, \frac{\gamma\lambda}{\delta(\gamma+\delta)},\right)$ If $R_0 < 1$ then the OSN model (3) is locally asymptotically stable otherwise unstable when $R_0 > 1$

Proof: Two eigenvalues of the above Jacobian matrix $J(P_0^{RFE})$ are

$\lambda_1 = -\delta$, $\lambda_2 = -(\delta+\gamma)$ and the other two eigenvalues are the roots of equation

$\sigma^2 + \theta(\sigma_1+\sigma_2) - \sigma_1\sigma_2 R_0 = 0$ where $\sigma_1 = (\mu+\delta)$, $\sigma_2 = (\alpha+\delta)$

$$\lambda_3 = -\left[\frac{(\sigma_1+\sigma_2)+\sqrt{((\sigma_1+\sigma_2)^2+4\sigma_1\sigma_2R_0)}}{2}\right]$$

&

$$\lambda_4 = -\left[\frac{(\sigma_1+\sigma_2)-\sqrt{((\sigma_1+\sigma_2)^2+4\sigma_1\sigma_2R_0)}}{2}\right]$$

It is clear from the above expression that $\lambda_3 < 0$ and $\lambda_4 < 0$ when $R_0 < 1$, since all eigenvalues at P_0^{RFE}, are negative, therefore rumour-free equilibrium of the OSN model are locally asymptotically stable and if $R_0 > 1$, $\lambda_3 < 0$ and $\lambda_4 > 0$ and in this case rumour-free equilibrium P_0^{RFE} is locally asymptotically unstable.

Theorem 3: The rumour free equilibrium P_0^{RFE} is globally asymptotically stable if $R_0 \leq 1$

Proof: Consider the Lyapunov function as follows:

$$L = \tau_1 E + \tau_2 I \tag{4}$$

Now taking the first derivative of Eq. 4, we get
$\dot{L} = \tau_1\,\dot{E} + \tau_2\,\dot{I}$
$= \tau_1\{\beta si + \rho\beta vi - (\mu+\delta)e\} + \tau_2\{\mu e - (\alpha+\delta)i\}$
Let $\tau_1 = \mu$ and $\tau_2 = (\mu+\delta)$, we get
$\dot{L} = (R_0 - 1)(\alpha+\delta)(\mu+\delta)i \leq 0$
from LaSalle invariance principle [43] P_0^{RFE} is globally asymptotically stable when $R_0 \leq 1$

A. RUMOUR PREVAILING ENDEMIC EQUILIBRIUM: EXISTENCE AND UNIQUENESS

In this section, we investigate the existence and uniqueness of the endemic equilibrium. For endemic equilibrium.

$$\begin{aligned} \lambda - \beta s^* i^* - (\delta+\gamma)s^* &= 0 \\ \beta s^* i^* + \rho\beta v^* i^* - (\delta+\mu)e^* &= 0 \\ \mu e^* - (\delta+\alpha)i^* &= 0 \\ \gamma s^* - \rho\beta v i^* - \delta v^* &= 0 \end{aligned} \tag{5}$$

Let $\sigma_1 = (\delta+\mu)$, $\sigma_2 = (\delta+\alpha)$, $\sigma_3 = (\delta+\gamma)$ then from Eq. 5, we get
$s^* = \frac{\lambda}{\beta i^*+\sigma_3}$, $e^* = \frac{\sigma_2}{\mu}i^*$, $v^* = \frac{\lambda\gamma}{(\beta i^*+\sigma_3)(\rho\beta i^*+\delta)}$
replace the value of s^*, e^*, v^* in the second equation of equation 5, we get
$\tilde{q_0}i^{*2} + \tilde{q_1}i^* + \tilde{q_2} = 0$, where $\tilde{q_0} = \sigma_1\sigma_2\beta^2\rho$, $\tilde{q_1} = \sigma_1\sigma_2\delta\beta + \sigma_1\sigma_2\sigma_3\rho\beta - \mu\rho\beta^2\lambda$, $\tilde{q_2} = \sigma_1\sigma_2\sigma_3\delta[1-R_0]$

It is clear that $\tilde{q_0}$ is always positive and q_2 is negative when $R_0 > 1$, therefore from theory of equation i^* has a unique positive value when $R_0 > 1$, therefore, a unique rumour prevailing equilibrium exist when $R_0 > 1$

B. LOCAL STABILITY ANALYSIS OF RUMOUR-PREVAILING EQUILIBRIUM POINT

In this section the local stability analysis of rumour-prevailing equilibrium points $P^{*RPE} = (s^{*RPE}, e^{*RPE}, i^{*RPE}, v^{*RPE})$ is given. The Jacobian matrix is

$$J(P^{*RPE}) = \begin{bmatrix} -(\beta i^*+\gamma+\delta) & 0 & \beta s^* & 0 \\ \beta i^* & -(\mu+\delta) & \beta s^*+\rho\beta v^* & \rho\beta i^* \\ 0 & \mu & -(\alpha+\delta) & 0 \\ \gamma & 0 & -\rho\beta v^* & -(\rho\beta i^*+\delta) \end{bmatrix}$$

Theorem 4: At rumour-prevailing equilibrium P^{*RPE}, if $R_0 > 1$ then OSN model (3) is locally asymptotically stable.

Proof: In order to check the stability at the point P^{*RPE}, we will find the eigenvalues of the above matrix. The characteristics equation are given by

$$\tilde{T_0}\theta^4 + \tilde{T_1}\theta^3 + \tilde{T_2}\theta^2 + \tilde{T_3}\theta + \tilde{T_4} = 0 \tag{6}$$

where $\tilde{T_0} = 1$
$\tilde{T_1} = a_1 + a_2 + a_3 + \rho L + \delta + L$
$\tilde{T_2} = a_2a_3 + (a_2+a_3)(\rho L+\delta) - \mu N - \rho\mu M + (L+a_1)(a_2+a_3+\rho L+\delta)$
$\tilde{T_3} = a_2a_3(\rho L+\delta) + (L+a_1)(a_2a_3(a_2+a_3)(\rho L+\delta)) - (L+a_1)(\mu N+\rho\mu M) - \mu N\delta - \mu\rho M\delta - \mu NL$
$\tilde{T_4} = (L+a_1)(a_2a_3(\rho L+\delta) - \rho\mu NL - \mu N\delta - \rho M\delta - \mu NL) - N\mu\rho L^2 - N\mu\delta L - N\mu\rho Lr$ where $L = \beta i^8$, $M = \beta v^8$, $N = \beta s^8$, $a_1 = \gamma+\delta$, $a_2 = \mu+\delta$, $a_3 = \alpha+\delta$
The coefficient of Eq. 6 are satisfied using Routh - Hurwitz criteria for the fourth degree polynomial if $R_0 > 1$: which implies that all characteristic root have a negative real parts and therefore the system is locally asymptotically stable at rumour-prevailing equilibrium point $P^{*(RFE)}$.

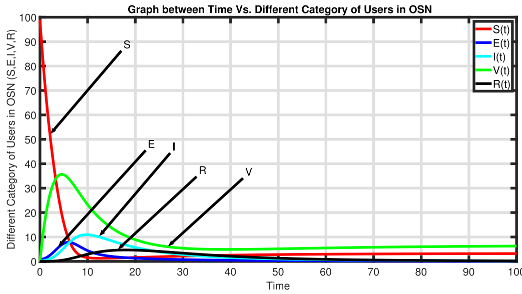

FIGURE 2. The status of users in OSN when $R_0 < 1$.

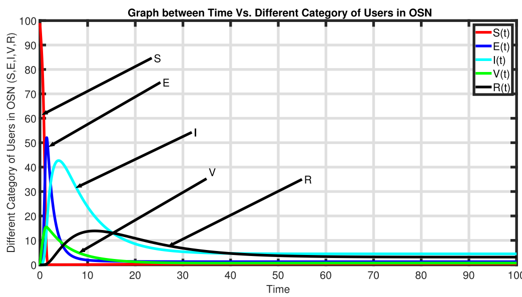

FIGURE 3. The status of users in OSN when $R_0 > 1$.

V. NUMERICAL SIMULATIONS AND ANALYSIS OF THE MODEL

In this section, numerical simulations have been undertaken to validate mathematical studies. The effect of different parameters on OSN and the controlling mechanism of fake information dissemination is explained in this section. MATLAB (R2018a) is used for the simulation of the proposed model. The state of different categories of users is changing with time which can be realized from the analysis. The dynamics of information dissemination and state of change of different categories of users in OSN are presented in Fig. 2 and Fig. 3.

Taking the value of different parameters are $\lambda = 1, \delta = .1, \beta = 0.05, \gamma = 0.2, \rho = 0.004, \alpha = 0.07$ and $\mu = 0.4$, after computation the value of $R_0 = .79$. Fig. 2 illustrates the different categories of users' states when $R_0 < 1$. It is concluded from Fig. 2, that the susceptible $S(t)$ category of users decreases and other categories of users increase in the OSN. But after some time $t = 20$ the number of susceptible users starts to increase and other categories of users gradually become zero when $R_0 < 1$. The infectious users (spreaders) gradually vanish from the OSN. The fake information will not survive in the OSN. This satisfies the theorem 2 that the OSN will be globally asymptotically stable. In another case, change the value of $\beta = 0.5$ and $\mu = 0.6$, the remaining values are the same, the value of $R_0 = 8.47$, which is greater than 1. In this case, as noticed in Fig. 3, the infectious users (fake information)or spreader will continuously be present in the OSN. The susceptible categories of users decline sharply and are exposed and the infectious category of users increases very quickly. After some time exposed and infectious category of users begins to decline and exposed users reach zero but infectious users become stable. In this condition, the fake information will disseminate in the OSN. This satisfies the second condition of Theorem 4. *Comparative Analysis:* The proposed model is compared with some existing models (SIR, SEIR, Extended SEIR and SIVR) under similar conditions. It is observed that a lesser number of users become a victim of fake information in comparison to other existing models. The peak becomes early in SIR and SIVR models in comparison to others. This is noted in Fig. 4 that fake information flow is very slow in the case of the proposed model. From Fig. 4, it is clear that the proposed mechanism for controlling of fake information is more suitable than these existing mechanisms.

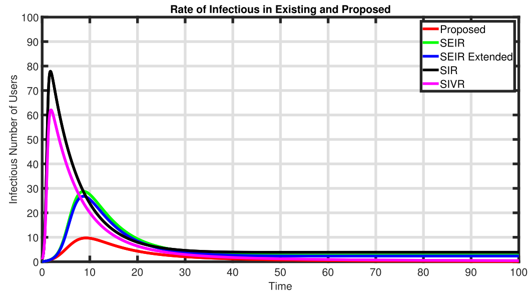

FIGURE 4. Comparison with existing models.

VI. CONTROLLING TECHNIQUE OF FAKE INFORMATION DISSEMINATION

To examine the sensitivity of R_0, to each of its parameters [44], the normalized forward sensitivity index with respect to each of the parameters is calculated:

$$R_0 = \frac{\beta\lambda\mu(\delta+\rho\gamma)}{\delta(\gamma+\delta)(\alpha+\delta)(\mu+\delta)}$$

$$\Gamma_\beta = \frac{\frac{\partial R_0}{R_0}}{\frac{\partial \beta}{\beta}} = \frac{\beta}{R_0}\frac{\partial R_0}{\partial \beta} = \frac{\beta\lambda\mu(\delta+\rho\gamma)}{R_0\delta(\gamma+\delta)(\alpha+\delta)(\mu+\delta)} = 1$$

$$\Gamma_\lambda = \frac{\frac{\partial R_0}{R_0}}{\frac{\partial \lambda}{\lambda}} = \frac{\lambda}{R_0}\frac{\partial R_0}{\partial \lambda} = \frac{\lambda}{R_0}\left[\frac{\beta\mu(\delta+\rho\gamma)}{\delta(\gamma+\delta)(\alpha+\delta)(\mu+\delta)}\right] = 1$$

$$\Gamma_\rho = \frac{\frac{\partial R_0}{R_0}}{\frac{\partial \rho}{\rho}} = \frac{\rho}{R_0}\frac{\partial R_0}{\partial \rho} = \frac{\rho}{R_0}\left[\frac{\beta\mu\rho\gamma}{\delta(\gamma+\delta)(\alpha+\delta)(\mu+\delta)}\right] > 0$$

$$\Gamma_\gamma = \frac{\frac{\partial R_0}{R_0}}{\frac{\partial \gamma}{\gamma}} = \frac{\gamma}{R_0}\frac{\partial R_0}{\partial \gamma} = \frac{\beta\mu\delta\gamma\lambda}{R_0\delta(\gamma+\delta)^2(\alpha+\delta)(\mu+\delta)}[1-\rho] > 0$$

It is clear that $\Gamma_\gamma < 0$, if $\rho > 1, \Gamma_\gamma > 0$, if $\rho < 1$ and $\Gamma_\gamma = 0$ when $\rho = 1$.

$$\Gamma_\mu = \frac{\frac{\partial R_0}{R_0}}{\frac{\partial \mu}{\mu}} = \frac{\mu}{R_0}\frac{\partial R_0}{\partial \mu} = \frac{\delta}{(\mu+\delta)} > 0$$

$$\Gamma_\alpha = \frac{\frac{\partial R_0}{R_0}}{\frac{\partial \alpha}{\alpha}} = \frac{\alpha}{R_0}\frac{\partial R_0}{\partial \alpha} = \frac{\alpha}{(\mu+\alpha)} < 0$$

It can be observed that out of these six parameters,R_0 in proportions with α, γ, ρ and μ are the most sensitive to changes in these parameters and out of four parameters one parameter α has an inversely proportional relationship with R_0. Below, let us explain how these properties of the model can be utilized to control the fake information dissemination in OSN.

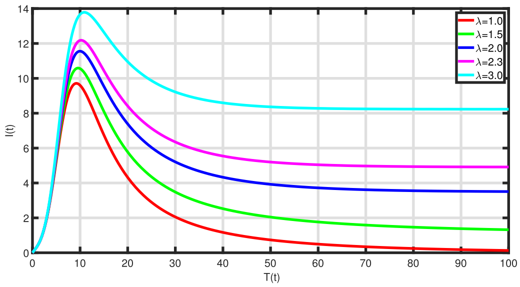

FIGURE 5. Effect of λ.

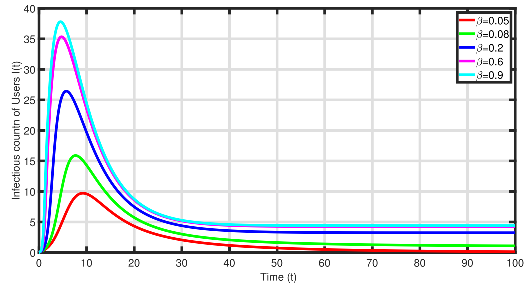

FIGURE 6. Effect of β.

A. SENSITIVITY ANALYSIS OF PARAMETERS

1) IMPACT OF NEW USER INFLOW ON THE ONLINE SOCIAL NETWORK

To investigate the impact of new user inflow on the OSN, we will maintain all other parameters constant as in the previous section and vary the value of parameter λ. Consider value of parameters $\delta = .1, \beta = 0.05, \gamma = 0.2, \rho = 0.004, \alpha = 0.07, \mu = .4$ are same and change the value of $\lambda = 1, 1.5, 2.0, 2.3$ and 3 respectively. As previously stated, the effects of fake information dissemination are represented by the tendency of the graph concerning the time given in Fig. 5. It depicts the nature of curve of $i(t)$ simultaneously w.r.t. time t for various values of λ. From Fig. 5 it is observed that, as the value of λ increases, the position of the initial peak of the $i(t)$ curve is delayed in time, and the peak value gradually decreases, but these changes are subtle. As the value of λ rises, an infectious number of users increases in the OSN. Overall, data suggest that the influx of new users has a considerable impact on fake information dissemination in the system (3). The inclusion of a higher number of new members into an OSN in a given period has been demonstrated to result in a broader scale of dissemination in the OSN.

2) IMPACT OF SPREADING RATE OF RUMOUR ON THE ONLINE SOCIAL NETWORK

In this section, we will study the effect of the spreading rate (β) on fake information dissemination in the population through OSN. The frequency of fake news/messages received by an average user in the OSN is characterized by the degree of activity of OSN.

We kept the other parameters the same as in the previous simulation and changed the parameter β. Now change the value of $\beta = 0.05, 0.08, 0.2, 0.6$ and 0.9. respectively. Figure 6 depicts the nature of the curve of $i(t)$ with the different values of time t. Fig. 6 shows that as the value of the spreading rate of fake information in OSN increases, the position of the first peak of the curve $i(t)$ emerges earlier and these variations are significant and visible. Therefore, it is clear that when the value of β will is large more susceptible users become a victim of the fake information in the OSN.

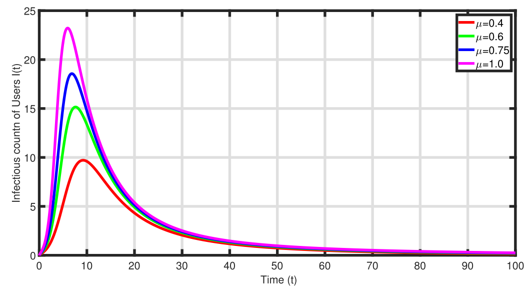

FIGURE 7. Effect of μ.

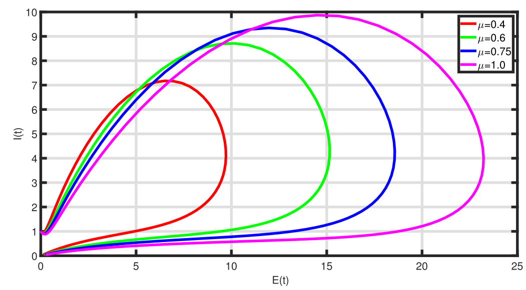

FIGURE 8. Variation in number of spreaders from Exposed individuals.

3) IMPACT OF LATENT RATE ON USERS ENTERING INTO TRANSMISSION USERS ON RUMOUR DISSEMINATION IN THE ONLINE SOCIAL NETWORK

The exposed category of individuals that believe in untrusted messages/fake news/misinformation and be active spreaders of rumours in the OSN is investigated. The other parameters remain the same as in the previous section and change parameters $\mu = 0.4, 0.6, 0.8$ and 1.0. As the value of μ increases the number of spreaders increases in the OSN. Fig. 7 shows that as the value of μ rises the number of spreaders reaches a peak quickly. In the case of a higher value higher peak value attain early.

Fig. 8 shows the relationship between $e(t)$ and $i(t)$. It is observed from Fig. 8 when the value of μ is larger more exposed (latent) users become spreader. This is also supported by Fig. 7.

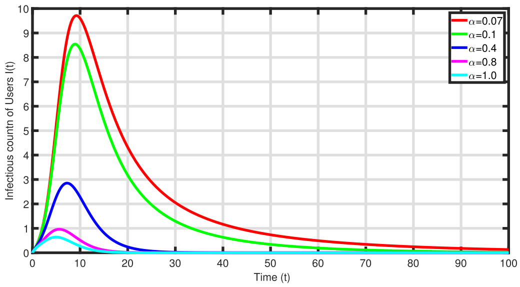

FIGURE 9. Effect of α.

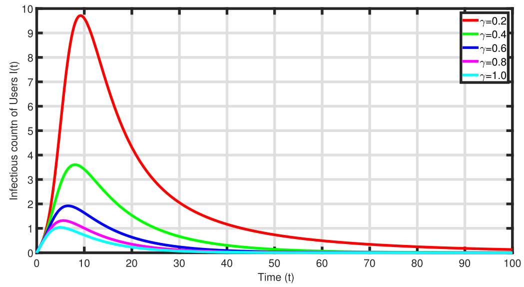

FIGURE 11. Effect of γ.

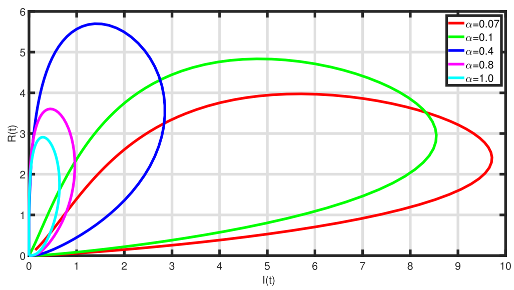

FIGURE 10. Effect of removal rate on spreaders.

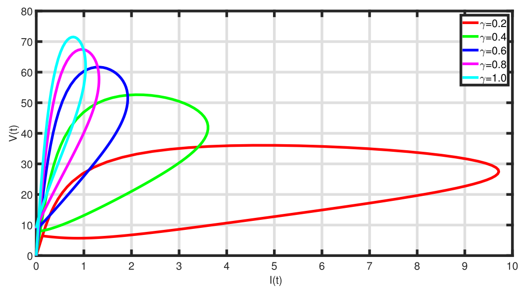

FIGURE 12. Effect of verification on spreaders.

4) IMPACT OF RECOVERY RATE ON INFECTIOUS USERS ON RUMOUR DISSEMINATION ON THE ONLINE SOCIAL NETWORK

The effect of the recovery rate on the infectious category of users that believe in untrusted messages/fake news/misinformation and are active spreaders of rumours in the OSN is analyzed. The parameters are the same as in the previous section and change the recovery parameter $\alpha = 0.07, 0.1, 0.4, 0.8$ and 1.0. As the value of α increases, the peak appears early with less number of infectious users (spreader) in the OSN which is shown in Fig. 9. The changes are obvious.

Fig. 10 illustrates the relationship between infectious users and removed/blocked users in the OSN. The result of figure 9 is supported by figure 10, in which as the value of α is increases, number of infectious users start to decrease.

5) IMPACT OF VERIFICATION OF USERS ON RUMOUR DISSEMINATION ON THE ONLINE SOCIAL NETWORK

The effect of the verification of users on OSN is an important parameter. The verified users are very sensitive to responding to any kind of information on the OSN. They first verify the information then forward, share, like and join the unknown groups on the OSN. The parameters are the same as in the previous section and change the verification parameter $\gamma = 0.2, 0.4, 0.6, 0.8$ and 1.0. As the value of γ increases the number of verified users increases in the OSN and the chance to become a victim of fake information decreases. The peak appears early with a lesser number of infectious users (spreader) in the OSN which is shown in Fig. 11. The changes are obvious.

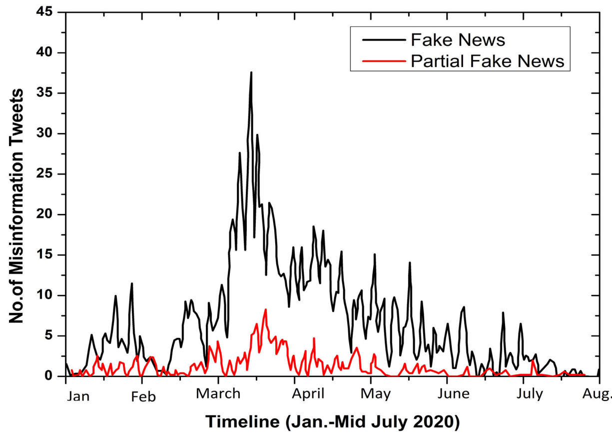

FIGURE 13. January 2020 through mid-July 2020 misleading tweets timeline [45].

Fig. 12 illustrates the relationship between infectious users and verified users in the OSN. The result of figure 11 is supported by figure 12, in which as the value of γ increases number verified users will increases, and the infectious number of users in the OSN will decrease.

Shahi et al. [45] shows the timeline of tweets with false information as shown in Fig. 13, authors showed the timeline of the false tweets made from January 2020 to mid-July 2020. The black colour shows that the false (fake news) category is spreading, while the red colour shows that the fake news is only partly true. The tweet's timeline shows that false misinformation spreads faster than partially false misinformation. From mid-March to mid-April, when COVID-19 was at its peak, the most false and partly false tweets were sent.

Misinformation tweets can be tracked by how many likes and retweets they get. Likes show how many times a user marked the tweet as a favourite, while retweets and retweets with comments show how many times a user shared the tweet. With the help of the timeline, we can see how many likes and retweets each fake tweet got. The number of retweets and favourites varies a lot, so we decided to normalise the data. We use Min-Max Normalization to put the number of likes and retweets on a scale from 0 to 1. We figured out the average number of retweets and likes for the whole month and plotted the average number of retweets and likes for both fake and partially fake for each month. The timeline analysis of normalised retweets shows that fake information gets more likes than partially fake information, especially from the middle of March to the middle of April 2020. As shown in Fig. 13, the most fake information was spread from March 16 to April 23, 2020. But for a retweet, there is no clear way to tell the difference between fake and partially fake. Overall, though, there are more likes than retweets for tweets that spread fake information.

VII. CONCLUSION AND FUTURE SCOPE

This article presented an epidemic model for controlling fake information dissemination in OSN. To investigate the dynamics of fake information dissemination in OSN proposed model utilized a set of differential equations which describe the various states of the users in OSN. The different types of activities in the social network need to be examined for corrective action on time that helps in the control of fake information dissemination. For controlling fake information, the latent state of users is included in the model, this type of user first identifies the authenticity of information before sharing it in a group of OSN. The impact of latent users with verification and blocking of users and the dissemination of information on OSN is discussed. The fake information can have a false impact on the people, in the long run, therefore to control the dissemination of unauthenticated information in OSN, an important threshold R_0 is defined as a basic reproduction number and its expression is computed. The R_0 is useful in the analysis of fake information status in the OSN. The analysis result shows that if $R_0 < 1$, the OSN becomes free from rumour/unauthenticated information. In this case, the status of authenticated information will remain the same with time and OSN will achieve local stability. The Jacobian matrix is used to establish rumour-free local stability. The rumour-free global asymptotic stability in OSN is also obtained by the use of the Lyapunov function. On the other hand, if $R_0 > 1$, the rumour/unauthenticated information is sustained forever in the social network. The sensitivity analysis has been also performed and explained the effect of different parameters on the dissemination of fake information in OSN. By utilising a quarantine and delay strategy sometime in the near future, it will be possible to prevent social networks from the spread of rumours and the transmission of fake news. The issues that are discussed in this article are very relevant at the moment, and the COVID-19 pandemic is generating a crisis in the dissemination of misleading information on OSNs all over the world. This crisis is likely to continue until the disease is either treated or eradicated. The dissemination of false information may be extremely harmful to individuals, organisations, and many other parts of society, as is unmistakably demonstrated by real-world events. As a result, the findings of this research have the potential to make a contribution to the solution of some contemporary global issues related to the dissemination of fake news. In the future, with the use of this approach, it will be possible to prevent the spread of fake news on the internet platforms that are used the most, such as WhatsApp and Telegram.The comparative analysis is presented in the paper and found that the proposed model ensures a better controlling mechanism of fake information dissemination in the OSN in comparison to previous models.

REFERENCES

[1] 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.

[2] M. Babaei, J. Kulshrestha, A. Chakraborty, E. M. Redmiles, M. Cha, and K. P. Gummadi, "Analyzing biases in perception of truth in news stories and their implications for fact checking," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 3, pp. 1–12, Jul. 2021.

[3] L. Li, Q. Zhang, X. Wang, J. Zhang, T. Wang, T.-L. Gao, W. Duan, K. K.-F. Tsoi, and F.-Y. Wang, "Characterizing the propagation of situational information in social media during COVID-19 epidemic: A case study on Weibo," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 2, pp. 556–562, Mar. 2020.

[4] A. Legon and A. Alsalman, *How Facebook Can Flatten the Curve of the Coronavirus Infodemic*. 2020.

[5] T. Thanh Le, Z. Andreadakis, A. Kumar, R. Gómez Román, S. Tollefsen, M. Saville, and S. Mayhew, "The COVID-19 vaccine development landscape," *Nature Rev. Drug Discovery*, vol. 19, no. 5, pp. 305–306, May 2020.

[6] J. Ricard and J. Medeiros, "Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil," *Harvard Kennedy School Misinf. Rev.*, vol. 1, pp. 1–6, Apr. 2020.

[7] M. S. Islam, T. Sarkar, S. H. Khan, A. H. M. Kamal, S. M. Hasan, A. Kabir, D. Yeasmin, M. A. Islam, K. I. A. Chowdhury, K. S. Anwar, and A. A. Chughtai, "Covid-19—Related infodemic and its impact on public health: A global social media analysis," *Amer. J. Tropical Med. Hygiene*, vol. 103, no. 4, pp. 1621–1629, 2020.

[8] S. Loomba, A. De Figueiredo, S. J. Piatek, K. De Graaf, and H. J. Larson, "Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the U.K. and USA," *Nature Human Behaviour*, vol. 5, no. 3, pp. 337–348, Feb. 2021.

[9] 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*. Springer, 2019, pp. 43–65.

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

[11] L. Meng, T. Li, X. Huang, and S. Li, "Lift the veil of rumors: The impact of the characteristics of information sources on the effectiveness of rumors spreading," *Internet Res.*, vol. 32, no. 1, pp. 90–119, Jan. 2022.

[12] 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.

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

[14] 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.

[15] A. V. Banerjee, "The economics of rumours," *Rev. Econ. Stud.*, vol. 60, no. 2, pp. 309–327, Apr. 1993.
[16] 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.
[17] S. Dagher, *Assad Or We Burn the Country: How One Family's Lust for Power Destroyed Syria*. Paris, France: Hachette, 2019.
[18] J. Dhar, A. Jain, and V. K. Gupta, "A mathematical model of news propagation on online social network and a control strategy for rumor spreading," *Social Netw. Anal. Mining*, vol. 6, no. 1, pp. 90–119, Dec. 2016.
[19] H. Sun, Y. Sheng, and Q. Cui, "An uncertain SIR rumor spreading model," *Adv. Difference Equ.*, vol. 2021, no. 1, p. 286, Dec. 2021.
[20] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. R. Soc. Lond. A, Math. Phys. Sci.*, vol. 115, no. 772, pp. 700–721, 1927.
[21] D. J. Daley and D. G. Kendall, "Epidemics and rumours," *Nature*, vol. 204, no. 225, p. 1118, Dec. 1964.
[22] D. P. Maki and M. Thompson, *Mathematical Models and Applications: With Emphasis on Social, Life, and Management Sciences*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1973.
[23] D. H. Zanette, "Critical behavior of propagation on small-world networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 64, no. 5, Oct. 2001, Art. no. 050901.
[24] 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, 2007.
[25] L. Huo, F. Ding, C. Liu, and Y. Cheng, "Dynamical analysis of rumor spreading model considering node activity in complex networks," *Complexity*, vol. 2018, pp. 1–10, Nov. 2018.
[26] D. Shah and T. Zaman, "Rumors in a network: Who's the culprit?" *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5163–5181, Aug. 2011.
[27] X.-X. Zhan, C. Liu, G. Zhou, Z.-K. Zhang, G.-Q. Sun, J. J. Zhu, and Z. Jin, "Coupling dynamics of epidemic spreading and information diffusion on complex networks," *Appl. Math. Comput.*, vol. 332, no. 9, pp. 437–448, 2018.
[28] S. Abdullah and X. Wu, "An epidemic model for news spreading on Twitter," in *Proc. IEEE 23rd Int. Conf. Tools Artif. Intell.*, Nov. 2011, pp. 163–169.
[29] 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, no. 4, p. 545, Oct. 2017.
[30] D. Zhao, J. Sun, Y. Tan, J. Wu, and Y. Dou, "An extended SEIR model considering homepage effect for the information propagation of online social networks," *Phys. A, Stat. Mech. Appl.*, vol. 512, pp. 1019–1031, Dec. 2018.
[31] G. Shrivastava, P. Kumar, R. P. Ojha, P. K. Srivastava, S. Mohan, and G. Srivastava, "Defensive modeling of fake news through online social networks," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 5, pp. 1159–1167, Oct. 2020.
[32] B. Wang, G. Chen, L. Fu, L. Song, L. Song, and X. Wang, "DRIMUX: Dynamic rumor influence minimization with user experience in social networks," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 10, pp. 2168–2181, Oct. 2017.
[33] 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.
[34] R. Escalante and M. Odehnal, "A deterministic mathematical model for the spread of two rumors," *Afrika Matematika*, vol. 31, no. 2, pp. 1–18, Sep. 2017.
[35] P. Jiang and X. Yan, "Stability analysis and control models for rumor spreading in online social networks," *Int. J. Modern Phys. C*, vol. 28, no. 5, May 2017, Art. no. 1750061.
[36] L. Huo, L. Wang, N. Song, M. Chenyang, and B. He, "Rumor spreading model considering the activity of spreaders in the homogeneous network," *Phys. A, Stat. Mech. its Appl.*, vol. 468, pp. 1–19, Feb. 2016.
[37] X. Zhao and J. Wang, "Dynamical model about rumor spreading with medium," *Discrete Dyn. Nature Soc.*, vol. 2013, pp. 1–9, Jun. 2013.
[38] S. Chen, H. Jiang, L. Li, and J. Li, "Dynamical behaviors and optimal control of rumor propagation model with saturation incidence on heterogeneous networks," *Chaos, Solitons Fractals*, vol. 140, Nov. 2020, Art. no. 110206.
[39] Y. Moreno, M. Nekovee, and A. F. Pacheco, "Dynamics of rumor spreading in complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 69, no. 6, p. 066130, Jun. 2004, doi: 10.1103/PhysRevE.69.066130.
[40] X. Zhu, Y. Nie, and A. Li, "Demographic prediction of online social network based on epidemic model," in *Proc. Asia–Pacific Web Conf.* Cham, Switzerland: Springer, 2014, pp. 93–103.
[41] 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.
[42] O. Diekmann, J. A. P. Heesterbeek, and J. A. J. Metz, "On the definition and the computation of the basic reproduction ratio R_0 in models for infectious diseases in heterogeneous populations," *J. Math. Biol.*, vol. 28, no. 4, pp. 365–382, Jun. 1990.
[43] J. P. LaSalle, *The Stability of Dynamical Systems*, vol. 25. Philadelphia, PA, USA: SIAM, 1976.
[44] L. Arriola and J. Hyman, "Lecture notes, forward and adjoint sensitivity analysis: With applications in dynamical systems, linear algebra and optimisation," Math. Theor. Biol. Inst., Tech. Rep., 2005.
[45] G. K. Shahi, A. Dirkson, and T. A. Majchrzak, "An exploratory study of COVID-19 misinformation on Twitter," *Online Social Netw. Media*, vol. 22, Mar. 2021, Art. no. 100104.

RUDRA PRATAP OJHA received the B.Tech. degree from UPTU Lucknow, India, the M.Tech. degree from the Motilal Nehru National Institute of Technology (MNNIT) Allahabad, India, and the Ph.D. degree from the National Institute of Technology (NIT) Durgapur, India. He is currently with the G. L. Bajaj Institute of Technology and Management, Greater Noida, India, as a Professor with the Computer Science Engineering Department and the Head of Planning and Head of IQAC. He has published more than 20 papers in international and national journals/conferences. His research interests include wireless sensor networks, real-time systems, mathematical modeling, and simulation. He is also a reviewer of various reputed journals.

PRAMOD KUMAR SRIVASTAVA received the Ph.D. degree in mathematics from the University of Allahabad, Allahabad, India. He is currently the Dean (student welfare) with the Rajkiya Engineering College, Azamgarh (affiliated to Dr. A. P. J. Abdul Kalam Technical University, Lucknow), India. He has more than 15 years of teaching and research experience along with Ph.D. guidance. He has successfully guided one Ph.D. student and currently guiding a few more. 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. Excellence in learning has been his motto since he was a student and the proof of this was the gold medal awarded to him for securing the highest marks in his postgraduation. He has applied this motto in his teaching too, and being well-known in his genre, he has been invited to give guest lectures at reputed institutes and international conferences. He is a member of organizing committees and technical committees of many international conferences. He is renowned not only for the intellectual treasure he possesses, but also for his benevolence and altruism.

SHASHANK AWASTHI (Member, IEEE) received the M.Tech. degree in computer science and engineering from Dr. A. P. J. Kalam Technical University, Lucknow, the MCA degree from Dr. Bhimrao Ambedkar University, Agra, and the Ph.D. degree in computer science and engineering. He is currently with the G. L. Bajaj Institute of Technology and Management, Gautam Budha Nagar, India, as a Professor and the Dean (strategy) of the Computer Science Department. He has more than 18 years of teaching and research experience. He has published more than dozens of research papers in national and international journals of repute. His research interests include WSN and computer networks. He has visited more than eight countries for research purposes. He was invited as a Plenary Speaker for the 4th International Conference on Research in Intelligent and Computing in Engineering (RICE 2019), in August 2019, and the Hanoi University of Industry, Vietnam (HaUI), in 2019. He is certified by APS Germany, Center for Mechatronics, for industrial robotics, under Indo Euro Synchronization.

VINEET SRIVASTAVA received the M.Sc. degree in mathematics from Banaras Hindu University (BHU), Varanasi, India, in 2003, and the Ph.D. degree in applied mathematics from the Indian Institute of Technology (BHU) Varanasi, in 2009. 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 13 years of teaching and research experience along with Ph.D. guidance. He has several publications in various reputed international journals and international conferences. His research interests include mathematical modeling, dynamical system, fractional-order systems, and numerical techniques.

PURNENDU SHEKHAR PANDEY (Senior Member, IEEE) received the Ph.D. degree from the Indian Institute of Technology (Indian School of Mines) Dhanbad, India. Currently, he is with the Electronics and Communication Engineering Department, G. L. Bajaj Institute of Technology and Management, Greater Noida, India, as an Assistant Professor. He has more than a decade of experience in academics and research. He has published more than 55 high-quality research articles in national and international SCI journals and conferences. He has also authored a textbook titled *Power Line Carrier Communication and Arduino based Automation* (Research India Publication, 2017). He is also a JRF under the Indian Space Research Organization (ISRO)-sponsored project (Sanction ISRO/RES/3/775/18-19) with the Indian Institute of Technology (Indian School of Mines) Dhanbad. He holds eight patents published and one granted patent. His current research interests include optical sensors, nano- and biophotonics, photonic and plasmonic devices, wireless sensor networks, and biomedical engineering. He is a member of SPIE.

RADHE SHYAM DWIVEDI received the B.Tech. degree from Dr. A. P. J. Abdul Kalam Technical University at Lucknow (UPTU Lucknow), Lucknow, India, in 2008, and the M.Tech. degree from the Birla Institute of Technology Mesra, Ranchi, in 2015. He is currently pursuing the Ph.D. degree with the Motilal Nehra National Institute of Technology. He is an Assistant Professor with the Department of Applied Sciences and Humanities, Rajkiya Engineering College, Azamgarh (affiliated to Dr. A. P. J. Abdul Kalam Technical University, Lucknow), India, for the last five years. His research interests include mathematical modeling, sliding mode control, PWM control, and power converters.

RAJESH SINGH (Member, IEEE) received the B.E. degree from Dr. Bhimrao Ambedkar University, Agra, Uttar Pradesh, India, and the M.Tech. degree from RGPV, Bhopal, Madhya Pradesh, India. He is currently with the Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India, as a Professor. He has more than 18 years of experience in academics. He has 358 patents filed, including 13 granted patents (eight Australian and five Indian patents) and five PCT. He has published more than 100 research papers in refereed journals/conferences. He has published 24 authored and seven edited books in the area of embedded systems and the Internet of Things with reputed publishers like CRC/Taylor & Francis, Springer, Narosa, NIPA, River Publishers, Bentham Science, IGI Global, and NOVA Science. He has been featured by Indian and international media for smart systems and devices designed by him including OBDAS, E-Parirakshak, Kawach, 20Sec4Life, Ally, Alithis, and CT Scan Diagnosis, among which five are designed to prevent COVID-19 as per WHO guidelines. His research interests include embedded systems, robotics, wireless sensor networks, the Internet of Things, and machine learning. He received the Gold Medal from RGPV, for his M.Tech. degree. He has been honored as a keynote speaker and the session chair at international/national conferences, faculty development programs, workshops, and webinars.

ANTONINO GALLETTA (Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in computer engineering from the University of Messina, Italy, and the Ph.D. degree from the Mediterranean University of Reggio Calabria, Italy, in 2020. He is currently an Assistant Professor with The University of Messina. He is also the PI of ''InstradaME,'' an Italian project funded by the Ministry of Interior. He has coauthored more than 60 manuscripts. His research interests include the security of cloud/edge/IoT technologies for smart cities and eHealth solutions including big data management and blockchain. He is one of the members of the Technical Committee of *Computer Communication* (Elsevier). Due to his contribution to the research, he has been selected among the 200 top young researchers in mathematics and computer science to participate in the prestigious ''Heidelberg Laureate Forum,'' Heidelberg, in September 2019. He was the winner of two editions of the precious Leonardo Innovation Award, in 2018 (first place) and 2017 (second place). He is the chair of several international conferences. He was the guest editor of several SI on Q1 journals. Currently, he is an Associate Editor of *Sustainable Computing: Informatics and Systems* (Elsevier). He is a reviewer of more than 20 respected journals.

Open Access funding provided by 'Università degli Studi di Messina' within the CRUI CARE Agreement