**INTRODUCTION**

IN THE 20th century, the Internet has become the most powerful tool for communication. It facilitates efficient andeffective 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 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.