A Sensitivity Analysis Approach to Investigating Virus Transmission in Interconnected Computer Network

S. Mohanty, C. Parida, G. Mahanta, P.K. Nayak

Abstract— **This paper introduces an extended SEIR (Susceptible-Exposed-Infectious-Recovered) epidemic model specifically designed for computer networks, incorporating the unique dynamics associated with both symptomatic and asymptomatic nodes. These nodes represent the different stages of infection within the network, where symptomatic nodes are more likely to spread the virus, while asymptomatic nodes may still contribute to transmission despite showing no apparent signs of infection. A key focus of the study is the determination of the basic reproduction number, which quantifies the virus's potential to spread within the network. The stability analysis is conducted to investigate the conditions under which the system can maintain equilibrium at the disease-free state or transition into instability, with implications for the persistence or extinction of the virus within the network. Through numerical simulations performed in MATLAB, the model's long-term behavior is graphically illustrated, offering valuable insights into how different factors, such as the interaction between symptomatic and asymptomatic nodes, influence virus transmission and recovery rates. Furthermore, this study includes a sensitivity analysis on several critical parameters that govern the dynamics of the epidemic. By examining how variations in key parameters, such as the rates of transmission, quarantine, and recovery, affect the stability and performance of the model, we can identify which factors most strongly influence the spread of the virus. This analysis helps pinpoint critical thresholds and optimal control measures for mitigating virus outbreaks in computer networks.**

Keywords: e-epidemic model; Symptomatic nodes; Asymptomatic nodes; Basic reproduction number; Sensitive analysis.

I. Introduction

The relationship between computer viruses and mathematical epidemiology emerges from their similar patterns of spread and infection dynamics, despite differences in their host systems. Both types of viruses follow a process where an initial "host" becomes infected. The infection then spreads to other hosts, creating a chain of transmission. A computer virus spreads through infected files, emails, or websites. It targets computer systems and often causes damage or disruption. Similarly, a biological virus spreads from one person to another through various transmission modes, such as physical contact, airborne particles, or animal vectors. Despite the differences in their environments, both types of viruses propagate in strikingly similar ways. This similarity makes mathematical epidemiology models, which analyze disease transmission in populations, applicable to studying the spread of computer viruses.

Mathematical epidemiology utilizes models, such as the SIR (Susceptible-Infected-Recovered) framework, to study disease progression in populations over time. This model categorizes individuals into three groups: susceptible (vulnerable to infection), infected (currently carrying the disease), and recovered (immune or no longer infectious). By examining transitions between these groups, researchers can analyze key factors such as the rate of spread, peak infection timing, and the decline of the disease.

A similar approach can be applied to computer viruses. In this context, computers can be categorized as susceptible (not yet infected), infected (compromised by malware), and recovered (cleansed or protected through antivirus software or system updates). These models help researchers understand how quickly a virus might spread across a network. They also provide insights into virus behavior and control strategies.

Mathematical models play a crucial role in designing intervention strategies to minimize or prevent virus spread. In epidemiology, strategies such as vaccination, quarantine, and social distancing reduce transmission rates and help control outbreaks. In cybersecurity, similar measures exist. Antivirus software, firewalls, and system updates block potential infection sources and prevent viruses from spreading. Both fields also use immunization strategies. In public health, immunization refers to vaccines that prevent infections. In cybersecurity, it refers to system updates that protect against known vulnerabilities.

The study of computer viruses using mathematical epidemiology has gained increasing attention in recent years. This is due to the growing complexity and scale of digital systems. By treating computer viruses as infectious agents in network security, researchers can apply epidemiological models to simulate and predict virus behavior. These models help identify system vulnerabilities before they can be exploited. They also allow cybersecurity professionals to design proactive measures for virus containment. Understanding network structures further enhances virus spread predictions. Certain devices in a network may be more vulnerable to infection based on their role or connectivity. Similarly, in epidemiology, individuals or groups may be more susceptible due to factors like location or behavior.

In both biological and digital environments, mathematical epidemiology provides a valuable framework for understanding and controlling virus spread. By analyzing infections through models like SIR, public health authorities

Manuscript received Jan 29, 2025; revised May 25, 2025

S. Mohanty is a Research Scholar of C.V. Raman Global University, Bhubaneswar, Odisha, 752054, India (e-mail: saktiprasad20@gmail.com).

C. Parida is a Research Scholar of C.V. Raman Global University, Bhubaneswar, Odisha, 752054, India (e-mail:parchamdrakanta@gmail.com).

G. Mahanta is an Assistant Professor of Department of Mathematics, C. V. Raman Global University, Bhubaneswar, Odisha,752054, India (Corresponding author, phone: 91-8249741929; e-mail: ganeswar0385@gmail.com).

P. K. Nayak is an Assistant Professor of Mathematics Department, Sri Sathya Sai University for Human Excellence, Kalaburagi, Karnataka, 585313, India (e-mail: prasant.mu@gmail.com).

and cybersecurity experts can make informed decisions about prevention and control strategies. This connection highlights the importance of cross-disciplinary approaches in addressing global challenges, whether in public health or digital security.

The novelty of this study lies in extending the traditional SEIR model to capture the complex dynamics of computer networks. It incorporates both symptomatic and asymptomatic nodes, offering a more realistic representation of virus transmission. Different infected nodes play varied roles in the spread of infection. Additionally, the study integrates sensitivity analysis to identify critical parameters affecting network stability and virus control. This approach provides deeper insights into optimizing cybersecurity measures. By addressing these factors, this study contributes to developing more effective and adaptive cybersecurity strategies.

II. Literature Survey

The study of virus spread on networks has garnered significant attention over the years. Draief et al. [1] explored thresholds for virus propagation on networks. Their study focused on the conditions under which viruses can successfully spread. Building on this, Kephart [2] introduced a biologically inspired immune system for computers. This approach provided a foundation for protecting networks against viruses. In the context of computer networks, Kumar Nayak et al. [3] developed a dynamic E-Epidemic model. Their model captured the behavior of active infectious nodes in a network. It also highlighted the impact of node infection on network performance. Li & Wang [4] contributed to the global stability analysis in SEIR epidemic models. Their mathematical framework helped in understanding the long-term behavior of infectious diseases. This framework has also been applied to model virus transmission in computer networks. Similarly, Mishra & Jha [5] proposed a SEIQRS model for the transmission of malicious objects. Their work extended traditional epidemic models to account for the complexities of computer viruses. Mohanty et al. [6] developed a comprehensive mathematical model to analyze computer virus behavior and its stability within networks. Their study introduced new insights into virus dynamics and containment strategies. Mohanty et al. [7] also presented the SIQTRS E-Epidemic model. This model integrates additional compartments for virus propagation and recovery. It offers a more complete framework for analyzing and managing computer virus outbreaks. Newman et al. [8] investigated the role of email networks in the spread of computer viruses. Their study demonstrated how communication patterns influence virus transmission in digital environments. Piqueira & Cesar [9] focused on dynamical models for computer virus propagation. Their work provided a deep dive into the mathematical foundations of virus spread on networks. Ram et al. [10] examined the behavior of infectious nodes in a computer network through mathematical modelling. Their findings contributed to understanding virus dynamics and evaluating containment strategies. Yan & Liu [11] introduced a SEIR epidemic model with delay. They explored how transmission and recovery delays affect network stability. Ahmad et al. [12] studied the dynamic behaviours of a modified computer virus model. Their work emphasized the role of network parameters and attributes in controlling virus spread. Alderremy et al. [13] applied artificial neural networks to model the spread of computer viruses on complex networks. Their data-driven approach provided predictions on virus dynamics. Muthukumar et al. [14] focused on the optimal control of computer virus spread through partial immunization. Their study highlighted strategies to reduce virus transmission in networks. Manohara & Kumbinarasaiah [15] developed a numerical solution for a modified epidemiological model of computer viruses. They used Fibonacci wavelets to achieve accurate computational solutions. Verma & Gupta [16] investigated the effect of vaccination on the stability of wireless sensor networks against malware attacks. Their study applied epidemiological principles to cybersecurity. Finally, Ying et al. [17] explored the use of graph neural networks for virus propagation network intrusion detection. Their research introduced innovative methods for detecting and preventing virus outbreaks in networked systems.

III. NOTATIONS

$N(t) =$ The total number of nodes connected to a network of computers and actively communicating with one another.

$S(t) =$ The quantity of susceptible nodes in computer networks and their constant communication with one another.

$E(t) =$ The quantity of exposed nodes in computer networks and their constant communication with one another.

$A(t) =$ A significant number of nodes develop symptoms, and also they are capable of transmitting the virus.

$B(t) =$ A significant number of nodes never develop symptoms, but they are capable of transmitting the virus.

$I(t) =$ The quantity of infectious nodes in computer networks that are constantly communicating with one another.

$Q(t) =$ The quantity of computer network's quarantined nodes that are constantly communicating with one another.

$R(t) =$ The quantity of recoverable nodes in computer networks that are always in communication with one another.

$\Lambda =$ New nodes joining the computer network.

$\mu =$ Computer nodes not functioning because of a technical issue (not by malicious codes).

$d =$ Computer nodes not functioning because of a technical issue (by malicious codes).

$\beta =$ Enough interaction between the susceptible nodes and the infected nodes for the susceptible node to get infected.

$\gamma =$ The rate at which a non-active Exposed class becomes an infectious class.

$\lambda =$ The rate at which an active exposed class becomes an infectious class.

$P =$ Percentage of the exposed class that is active infectious.

$\alpha =$ Percentage of exposed class which are infectious.

$\sigma =$ The rate at which an infectious class becomes a quarantined class is thought to be constant.

$\theta =$ Percentage of the infected class that is quarantined.

$\psi =$ Proportion of the quarantined class that is recovered following the usage of antivirus software.

IV. Formulation of the Model and Assumptions

In the $SEABIQR$ model, the total population is divided into seven groups: susceptible $S(t)$, exposed $E(t)$, symptomatic

$A(t)$, asymptomatic $B(t)$, infected $I(t)$, quarantined $Q(t)$ and recovered $R(t)$. Susceptible individuals are those who can become infected. The infected group represents individuals infected by the computer virus and capable of spreading it. The total population at the time $N(t)=S(t)+E(t)+A(t)+B(t)+I(t)+Q(t)+R(t)$ where $N(t)$ the total population. Figure 1 depicts the transmission dynamics of the computer virus in this model, and the mathematical expressions for transmission are given by equations (1) to (7).

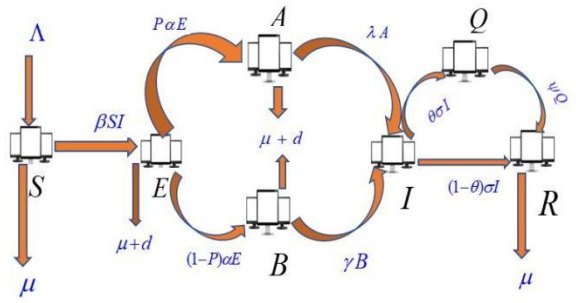

Fig.1 Schematic Diagram

$$\frac{dS}{dt}=\Lambda-SI\beta-S\mu \quad (1)$$

$$\frac{dE}{dt}=SI\beta-(\mu+\alpha+d)E \quad (2)$$

$$\frac{dA}{dt}=P\alpha E-(d+\mu+\lambda)A \quad (3)$$

$$\frac{dB}{dt}=(1-P)\alpha E-(\mu+d+\gamma)B \quad (4)$$

$$\frac{dI}{dt}=\lambda A+\gamma B-\sigma I \quad (5)$$

$$\frac{dQ}{dt}=\theta\sigma I-\psi Q \quad (6)$$

$$\frac{dR}{dt}=(1-\theta)\sigma I+\psi Q-R\mu \quad (7)$$

All the model parameters are +ve constants. Adding (1)-(7), we have, $\frac{dN}{dt}=\Lambda-(N-I-Q)\mu-d(A+E+B)$

Form the above equation, it can be seen that in the absence of the worms $E=A=B=I=Q=0, as\ \ N\to\frac{\Lambda}{\mu}.$

Thus $D_1=(S,E,A,B,I,Q):$
$S\ge 0,E\ge 0,A\ge 0,B\ge 0,I\ge 0,Q\ge 0,$

$$S+A+B+I+Q\le\frac{\Lambda}{\mu}$$

V. Basic Reproduction Number

The basic reproduction number, often denoted as R_0, is a key parameter in epidemiological modeling, including computer epidemic models. It is the average number of secondary infections that one ill individual produces in a totally susceptible community. If $R_0>1$, the infection is likely to spread, while $R_0<1$, indicates that the infection will decline. In computer models, R_0 helps assess the potential impact of interventions and guide public health responses. It is crucial for understanding the dynamics of disease spread and the effectiveness of control measures. Now we have to find the Basic Reproduction Number, From the equations (2), (3), (5) & (6) we get:

$$F=\begin{bmatrix}\beta SI\\0\\0\\0\end{bmatrix}\ \text{and V}=\begin{bmatrix}-(\mu+\alpha+d)E\\P\alpha E-(d+\mu+\lambda)A\\\lambda A+\gamma B-\sigma I\\\theta\sigma I-\psi Q\end{bmatrix}$$

Let t=βSI u=0 v=0 w=0

Then $F=\begin{bmatrix}\frac{\partial t}{\partial E}&\frac{\partial t}{\partial A}&\frac{\partial t}{\partial I}&\frac{\partial t}{\partial Q}\\\frac{\partial u}{\partial E}&\frac{\partial u}{\partial A}&\frac{\partial u}{\partial I}&\frac{\partial u}{\partial Q}\\\frac{\partial v}{\partial E}&\frac{\partial v}{\partial A}&\frac{\partial v}{\partial I}&\frac{\partial v}{\partial Q}\\\frac{\partial w}{\partial E}&\frac{\partial w}{\partial A}&\frac{\partial w}{\partial I}&\frac{\partial w}{\partial Q}\end{bmatrix}=\begin{bmatrix}0&0&\beta S&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$

$$V=\begin{bmatrix}\frac{\partial t}{\partial E}&\frac{\partial t}{\partial A}&\frac{\partial t}{\partial I}&\frac{\partial t}{\partial Q}\\\frac{\partial u}{\partial E}&\frac{\partial u}{\partial A}&\frac{\partial u}{\partial I}&\frac{\partial u}{\partial Q}\\\frac{\partial v}{\partial E}&\frac{\partial v}{\partial A}&\frac{\partial v}{\partial I}&\frac{\partial v}{\partial Q}\\\frac{\partial w}{\partial E}&\frac{\partial w}{\partial A}&\frac{\partial w}{\partial I}&\frac{\partial w}{\partial Q}\end{bmatrix}$$

Where $t=-(\mu+d+\alpha)E$
$u=P\alpha E-(\mu+d+\lambda)A$
$v=A\lambda+B\gamma-\sigma I$
$w=I\theta\sigma-\psi Q$

Let X=(E,A,I,Q)

$\Rightarrow\frac{dX}{dt}=F-V$

Therefore,

$$V=\begin{bmatrix}(\mu+d+\alpha)&0&0&0\\-P\alpha&(\mu+d+\lambda)&0&0\\0&-\lambda&\sigma&0\\0&0&-\theta\sigma&\psi\end{bmatrix}$$

Now,

$|V|=(\mu+d+\alpha)(\mu+d+\lambda)\sigma\psi$
$\neq 0$

So V^{-1} exist
Now,

$$Adj.V=\begin{bmatrix}(\mu+\lambda+d)\sigma\psi&P\psi\alpha\sigma&P\psi\alpha\lambda&P\theta\sigma\alpha\lambda\\0&(\mu+\alpha+d)\sigma\psi&(\mu+\alpha+d)\lambda\psi&(\mu+d+\alpha)\lambda\theta\sigma\\0&0&(\mu+\alpha+d)(\mu+\lambda+d)\psi&(\mu+\alpha+d)(\mu+\lambda+d)\theta\sigma\\0&0&0&(\mu+\alpha+d)(\mu+d+\lambda)\sigma\end{bmatrix}^T$$

$$\Rightarrow AdjV = \begin{bmatrix} (\mu+\lambda+d)\sigma\psi & 0 & 0 & 0 \\ P\alpha\sigma\psi & (\mu+\alpha+d)\sigma\psi & 0 & 0 \\ P\alpha\lambda\psi & (\mu+d+\alpha)\lambda\psi & \begin{matrix}(\mu+d+\alpha)\\(\mu+\lambda+d)\psi\end{matrix} & 0 \\ P\alpha\lambda\theta\sigma & (\mu+\alpha+d)\lambda\theta\sigma & \begin{matrix}(\mu+\alpha+d)\\\theta\sigma(\mu+\lambda+d)\end{matrix} & \begin{matrix}(\mu+\alpha+d)\\(\mu+\lambda+d)\sigma\end{matrix} \end{bmatrix}$$

Therefore,

$$V^{-1} = \frac{1}{\begin{matrix}(\mu+\alpha+d)\\(\mu+\lambda+d)\sigma\psi\end{matrix}} \begin{bmatrix} (\mu+d+\lambda)\sigma\psi & 0 & 0 & 0 \\ P\alpha\sigma\psi & (\mu+\alpha+d)\sigma\psi & 0 & 0 \\ P\alpha\lambda\psi & (\mu+\alpha+d)\lambda\psi & \begin{matrix}(\mu+\alpha+d)\\(\mu+\lambda+d)\psi\end{matrix} & 0 \\ P\alpha\lambda\theta\sigma & (\mu+\alpha+d)\lambda\theta\sigma & \begin{matrix}(\mu+\alpha+d)\\\theta\sigma(\mu+\lambda+d)\end{matrix} & \begin{matrix}(\mu+\alpha+d)\\(\mu+\lambda+d)\sigma\end{matrix} \end{bmatrix}$$

The next generation matrix is,

$$K = F.V^{-1}$$

$$= \frac{1}{\begin{matrix}(\mu+d+\alpha)\\(\mu+d+\lambda)\sigma\psi\end{matrix}} \begin{bmatrix} 0 & 0 & \beta S & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} (\mu+d+\lambda)\sigma\psi & 0 & 0 & 0 \\ P\psi\alpha\sigma & (\mu+d+\alpha)\sigma\psi & 0 & 0 \\ P\psi\alpha\lambda & (\mu+\alpha+d)\lambda\psi & \begin{matrix}(\mu+d+\alpha)\\(\mu+d+\lambda)\psi\end{matrix} & 0 \\ P\alpha\lambda\theta\sigma & (\mu+\alpha+d)\lambda\theta\sigma & \begin{matrix}(\mu+\alpha+d)\\\theta\sigma(\mu+\lambda+d)\end{matrix} & \begin{matrix}(\mu+\alpha+d)\\(\mu+\lambda+d)\sigma\end{matrix} \end{bmatrix}$$

$$K = \begin{bmatrix} \frac{\beta SP\alpha\lambda}{(\mu+d+\alpha)(\mu+d+\lambda)\sigma} & \frac{\beta S\lambda}{(\mu+d+\lambda)\sigma} & \frac{\beta S}{\sigma} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Now finding the eigenvalues K,

$$\Rightarrow |K - \lambda_* I| = 0$$

$$\Rightarrow \begin{bmatrix} \frac{\beta SP\alpha\lambda}{(\mu+d+\alpha)(\mu+d+\lambda)\sigma} - \lambda_* & \frac{\beta S\lambda}{(\mu+d+\lambda)\sigma} & \frac{\beta S}{\sigma} & 0 \\ 0 & -\lambda_* & 0 & 0 \\ 0 & 0 & -\lambda_* & 0 \\ 0 & 0 & 0 & -\lambda_* \end{bmatrix} = 0$$

One eigen value of K is:

$$\lambda_* = \frac{\beta SP\alpha\lambda}{(\mu+d+\alpha)(\mu+d+\lambda)\sigma}$$

Therefore,

$$R_0 = \frac{\beta SP\alpha\lambda}{(\mu+d+\alpha)(\mu+d+\lambda)\sigma}$$

Which is the Basic reproduction number of our developed model.

Equilibrium Points:

In computer epidemic modelling, an equilibrium point refers to a condition where the system's variables remain unchanged over time, indicating stability in population dynamics. There are two primary types of equilibrium: the disease-free equilibrium (DFE) and the endemic equilibrium (EE). The DFE represents a scenario in which the infection has been eliminated, resulting in a stable, infection-free state. Conversely, the EE describes a situation where the infection persists at a steady level within the population, with the rate of new infections equaling the recovery rate. Analyzing these equilibria is crucial for evaluating control measures and predicting long-term disease trends.

(i) Disease-free equilibrium points:

$$E_0 = (S, E, A, B, I, Q) = \left(\frac{\Lambda}{\mu}, 0, 0, 0, 0, 0\right)$$

(ii) Endemic equilibrium points:

$$E_0^* = (S^*, E^*, A^*, B^*, I^*, Q^*)$$

$$= \left(\frac{\Lambda - aE}{\mu}, \frac{cB}{\alpha(1-p)}, \frac{Bc(1-\alpha+\alpha P)}{(1-p)b\alpha}, \frac{\sigma b\alpha I(1-p)}{\{\gamma b\alpha(1-P)+(1-\alpha+P\alpha)\lambda c\}}, \frac{R\mu}{\sigma}, \frac{R\theta\mu}{\psi} \right)$$

Where a= (μ+d+α), b=(μ+d+λ), c=(μ+d+γ)

VI. The Existence and Stability of Equilibrium

Steady states of model are given as

$$\begin{aligned} &\Lambda - \beta SI - \mu S = 0 \\ &\beta SI - (\mu+\alpha+d)E = 0 \\ &P\alpha E - (\mu+\lambda+d)A = 0 \\ &(1-P)\alpha E - (\mu+d+\gamma)B = 0 \\ &\lambda A + \gamma B - \sigma I = 0 \\ &\theta\sigma I - \psi Q = 0 \\ &(1-\theta)\sigma I + \psi Q - \mu R = 0 \end{aligned} \tag{8}$$

Theorem 1: E_0 is locally asymptotically stable and unstable if $R_0 < 1$ & $R_0 > 1$, respectively.

Proof: The linearization of the model about the disease-free equilibrium points gives

$$E_0(S, 0, 0, 0, 0, 0) = \begin{bmatrix} -\mu & 0 & 0 & 0 & -\beta S & 0 \\ 0 & -(\mu+d+\alpha) & 0 & 0 & \beta S & 0 \\ 0 & P\alpha & -(\mu+d+\lambda) & 0 & 0 & 0 \\ 0 & (1-P)\alpha & 0 & -(\mu+d+\gamma) & 0 & 0 \\ 0 & 0 & \lambda & \gamma & -\sigma & 0 \\ 0 & 0 & 0 & 0 & \theta\sigma & -\psi \end{bmatrix}$$

The eigenvalues of the above matrix are

$-\mu, -(\mu+\gamma+d), -\sigma, -(\mu+\alpha+d), -(\mu+d+\lambda), -\psi$

Negative eigenvalues show that the function is stable. Finally, the significance of -ve eigenvalues shows that the equations (1)-(7) are locally asymptotically stable at disease disease-freeequilibrium.

Theorem 2: If $R_0 < 1$ indicate that the endemic equilibrium is locally asymptotically stable.

Proof: Model linearization regarding the endemic equilibrium

Points gives

$$E_0^*(S^*, E^*, A^*, B^*, I^*, Q^*) = \begin{bmatrix} -\mu & 0 & 0 & 0 & -\beta S & 0 \\ 0 & -(\mu+d+\alpha) & 0 & 0 & \beta S & 0 \\ 0 & P\alpha & -(\mu+d+\lambda) & 0 & 0 & 0 \\ 0 & (1-P)\alpha & 0 & -(\mu+d+\gamma) & 0 & 0 \\ 0 & 0 & \lambda & \gamma & -\sigma & 0 \\ 0 & 0 & 0 & 0 & \theta\sigma & -\psi \end{bmatrix}$$

In terms of characteristic equation $|E_0^* - KI| = 0$, where K is the eigenvalue and I is the unit matrix of order 6. The matrix E_0^* has eigenvalues are: $K_1 = -\mu$, $K_2 = -\psi$, and the rest of the eigenvalues are solved by E_1^* matrix.

$$E_1^* = \begin{bmatrix} -(\mu+d+\alpha) & 0 & 0 & \beta S \\ P\alpha & -(\mu+d+\lambda) & 0 & 0 \\ (1-P)\alpha & 0 & -(\mu+d+\gamma) & 0 \\ 0 & \lambda & \gamma & -\sigma \end{bmatrix}$$

The characteristic equation of E_1^* is:

$$| E_1^* - KI | = 0$$

$$\Rightarrow B_4.K^4 + B_3.K^3 + B_2.K^2 + B_1K^1 + B_0 = 0$$

We have,

$$B_4 = 1 > 0$$

$$B_3 = 3\mu + 3d + \alpha + \lambda + \gamma + \sigma > 0$$

$$B_2 = 3\mu^2 + 6\mu d + 2\mu\lambda + 2\mu\gamma + 3\mu\sigma + 3d^2 + 2d\lambda + 2d\gamma + 3d\sigma + 2\alpha\mu + 2\alpha d + \alpha\gamma + \alpha\lambda + \alpha\sigma + \lambda\gamma + \gamma\sigma + \lambda\sigma > 0$$

$$B_1 = \mu^3 + 3\mu^2 d + \mu^2\gamma + 3\mu^2\sigma + 3\mu d^2 + 2\mu d\gamma + 8\mu d\sigma + \mu^2\lambda + 2\mu\lambda d + \mu\lambda\gamma + 2\mu\lambda\sigma + 2\mu\gamma\sigma + d^3 + d^2\gamma + 3d^2\sigma + d^2\lambda + d\lambda\gamma + 2d\lambda\sigma + 2\sigma d\gamma + \alpha\mu^2 + 2d\alpha\mu + \alpha\mu\gamma + 2\alpha\mu\sigma + \alpha d^2 + \alpha d\gamma + 2d\sigma\alpha + \alpha\lambda\mu + d\alpha\lambda + \alpha\lambda\gamma + \alpha\lambda\sigma + \alpha\sigma\gamma + \lambda\gamma\sigma - \beta SP\alpha\lambda + \alpha\gamma P - \alpha\gamma > 0$$

$$B_0 = \mu^3\sigma + 3\mu^2 d\sigma + \mu^2\gamma\sigma + 3\mu d^2\sigma + 2\mu d\gamma\sigma + \mu^2\lambda\sigma + 2d\sigma\mu\lambda + \mu\lambda\gamma\sigma + d^3\sigma + d^2\lambda\sigma + d\lambda\gamma\sigma + \alpha\mu^2\sigma + d^2\gamma\sigma + 2\alpha\mu d\sigma + \alpha\mu\gamma\sigma + \alpha d^2\sigma + \alpha d\gamma\sigma + \alpha\lambda\mu\sigma + \alpha\lambda d\sigma + \alpha\lambda\gamma\sigma - \beta SP\alpha\lambda(\mu + d + \gamma) + \alpha\gamma(P-1)(\mu + d + \lambda) > 0$$

Where B_4, B_3, B_2, B_1, B_0 are positive if $R_0 > 1$ furthermore $B_3.B_2.B_1 > B_0$ By the Routh-Hurwitz stability condition is locally asymptotically stable.

Theorem 3: The disease-free equilibrium $E_0 = (S, E, A, B, I, Q) = (\frac{\Lambda}{\mu}, 0, 0, 0, 0, 0)$ of (1-7) is globally asymptotically stable in D_1 if $R_0 < 1$.

Proof: Consider a Lyapunov function

$$V_* = P\alpha E + (\mu + d + \alpha)A$$

Therefore

$$\frac{dV_*}{dt} = P\alpha\frac{dE}{dt} + (\mu + \alpha + d)\frac{dA}{dt}$$

$$= P\alpha\{\beta SI - (\mu + \alpha + d)E\} + (\mu + d + \alpha)\{P\alpha E - (\mu + d + \lambda)A\}$$

$$\leq (R_0 - 1)A(\mu + d + \alpha)(\mu + d + \lambda)$$

$$If\ R_0 < 1 \text{ then } \frac{dV_*}{dt} < 0$$

Therefore is globally asymptotically stable if $R_0 < 1$

Theorem 4**:** The endemic equilibrium point $E_0^*(S^*, E^*, A^*, B^*, I^*, Q^*)$ is globally asymptotically stable.

Proof: Let

$$L(S^*, E^*, A^*, B^*, I^*, Q^*) = M_1\frac{(S - S^*)^2}{2} + M_2\frac{(E - E^*)^2}{2} + M_3\frac{(A - A^*)^2}{2} + M_4\frac{(B - B^*)^2}{2} + M_5\frac{(I - I^*)^2}{2} + M_6\frac{(Q - Q^*)^2}{2}$$

$$\Rightarrow \frac{dL}{dt} = m_1(S - S^*)\frac{dS}{dt} + m_2(E - E^*)\frac{dE}{dt} + m_3(A - A^*)\frac{dA}{dt} + m_4(B - B^*)\frac{dB}{dt} + m_5(I - I^*)\frac{dI}{dt} + m_6(Q - Q^*)\frac{dQ}{dt} \quad (9)$$

Now substituting the differential equations (1)-(7) into (09), We get

$$\frac{dL}{dt} = M_1(S - S^*)(\Lambda - \beta SI - \mu S) + M_2(E - E^*)[\beta SI - (\mu + d + \alpha)E] + M_3(A - A^*)[P\alpha E - (\mu + d + \lambda)A] + M_4(B - B^*)[(1 - P)\alpha E - (\mu + d + \gamma)B] + M_5(I - I^*)(\lambda A + \gamma B - \sigma I) + M_6(Q - Q^*)(\theta\sigma I - \psi Q)$$

Taking out S, E, A, B, I, Q we get

$$\frac{dL}{dt} = -M_1(S - S^*)\left(\beta I + \mu - \frac{\Lambda}{S}\right) - M_2(E - E^*)\left[(\mu + d + \alpha) - \frac{\beta SI}{E}\right] - M_3(A - A^*)\left[(\mu + d + \lambda) - \frac{P\alpha E}{A}\right] + M_4(B - B^*)\left[(\mu + d + \gamma) - \frac{(1 - P)\alpha E}{B}\right] + M_5(I - I^*)\left(\sigma - \frac{\lambda A + \gamma B}{I}\right) + M_6(Q - Q^*)\left(\psi - \frac{\theta\sigma I}{Q}\right)$$

Consequently, it is evident that $M_1, M_2, M_3, M_4, M_5, M_6$ are positive integers such that $\frac{dL}{dt} \leq 0$ and the endemic equilibrium point $E_0^*(S^*, E^*, A^*, B^*, I^*, Q^*)$ is globally asymptotically stable

Example 4.1. Let β = 0.2, S=100, P=0.3, α=0.01, λ=0.02, μ = 0.05, d= 0.02, σ = 0.2. From the concept of

$$R_0 = \frac{\beta SP\alpha\lambda}{(\mu + d + \alpha)(\mu + d + \lambda)\sigma} = 0.8333 < 1.$$

Then the results of Theorems 1 and 3 hold.

Example 4.1 suggests the following outcomes,

(i) If the mean amounts of susceptible (S), exposed (E), symptomatic (A), asymptomatic (B), infected (I), quarantined (Q) and recovered (R) computers $S(t), E(t), A(t), B(t), I(t), Q(t), R(t) > 0$ at the initial time $(t = 0)$ conditions, and also close to the virus-free equilibrium E_0, the computer infection will eventually stop spreading.

(ii) We could change the β, P, α, λ, d, μ, &σ parameters so that the basic reproduction number (R_0) is smaller than one, or we might use the following suitable computer virus control measures.

1. In order To lower the contact rate β, we should be cautious while using portable storage devices like USB sticks and hard drives. We should also cut down on unneeded application services to lower the risk of virus infection.
2. We should stop using computers that have been in use for a long time in order to increase the elimination rates d.
3. We should install and use antivirus software, run routine system scans, and make sure virus libraries are maintained up to date in order to enhance investment in computer virus treatment resources and improve the recovery rate σ. Furthermore, it is essential to quickly identify and fix system flaws in order to proactively stop harmful software from infiltrating.

VII. Analysis of the Results

Through a variety of graphical representations, the simulation findings offer a thorough knowledge of the infection dynamics inside the network. Every figure depicts an important facet of the epidemic's development, emphasizing the impact of several elements on the dissemination and containment of dangerous programs within the system. The functioning of the system is shown in Figure 2 when the basic reproduction number R_0 is less than 1, which signifies that the infection is successfully under control. This result implies that the antivirus software's isolation and quarantine features are effectively preventing the dangerous malware from spreading. In this situation, the infection is unable to persist, and the network stabilizes. This demonstrates how effective preventative cybersecurity techniques are in preserving network health by making sure that compromised nodes don't aid in the spread of the infection. The network's sick (A) and asymptomatic (B) nodes' movements and influences are examined in Figure 3. The overall dynamics of the infection are significantly influenced by these nodes. Containment attempts are hampered by the existence of asymptomatic nodes, which could harbor and disseminate the infection without being noticed right away. In the meanwhile, symptomatic nodes are

simpler to recognize and isolate due to their more obvious infectious behavior. The graphic emphasizes how important it is to monitor both kinds of nodes in order to implement a successful mitigation approach, since neglecting to treat asymptomatic carriers may result in undetected spread. The interaction between infected and quarantined nodes is depicted in Figure 4. The significance of prompt isolation techniques is further supported by the clear correlation between a decrease in infected nodes (I) and a rise in quarantined nodes (Q). According to the findings, quarantine regulations have a crucial role in halting the spread of the infection and avoiding additional contamination of uninfected nodes. This research shows that a clear quarantine protocol greatly improves network reliability and lessens malware's capacity to remain on the system. Figure 5 illustrates the change from infectious (I) to recovery (R) nodes. The findings demonstrate a discernible decrease in infectious nodes over time, along with a rise in recovered nodes. By examining the impact of two crucial parameters on the recovery node population, Figures 6 and 7 offer a three-dimensional view of the recovery process. The association between recovery nodes (R), infection-to-quarantine rate (σ), and time (t) is represented by the surface plot shown in Figure 6. The parameter σ denotes the constant rate at which infected nodes move into the quarantined category. The figure illustrates that a higher value of σ results in more effective infection control, enabling a greater number of nodes to recover over time. This implies that implementing a strong quarantine protocol can substantially improve recovery outcomes and limit the infection's spread throughout the network. Figure 7 explores how the number of recovered nodes (R) is influenced by the failure rate of computer nodes due to technical issues (μ) over time (t). In contrast to infections caused by malicious code, μ represents system breakdowns from hardware or software malfunctions. The figure shows that an increase in μ leads to a decline in recovered nodes, highlighting that a higher failure rate hinders the recovery process.

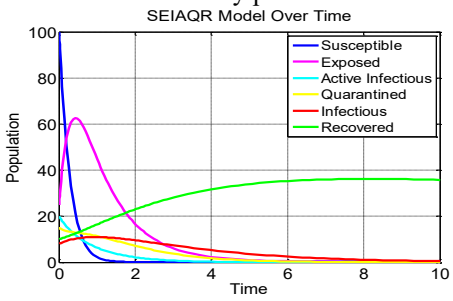

Fig.2 e-Epidemic model under isolated and quarantine defenses

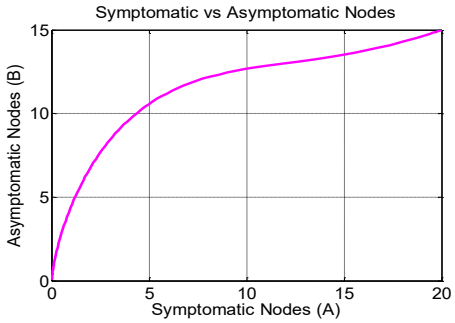

Fig. 3 Impact of A and B class nodes on the model

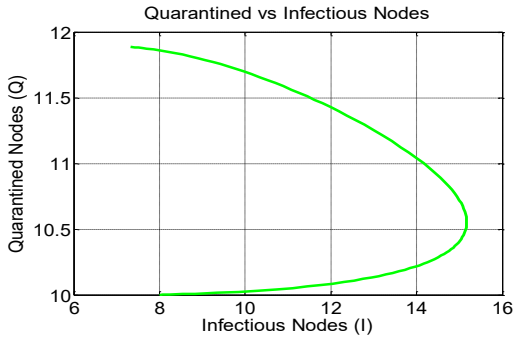

Fig. 4 Impact of Q and I class nodes on model

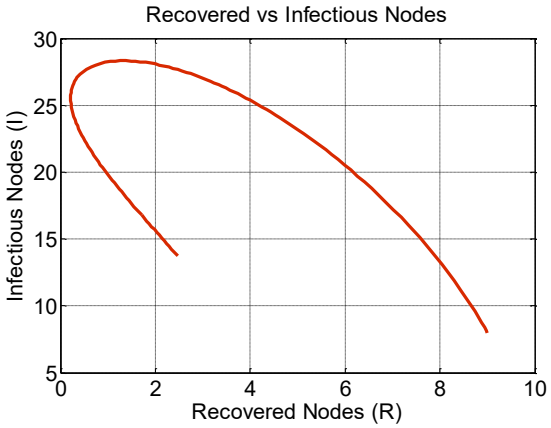

Fig. 5 Impact of R and I class nodes on the model

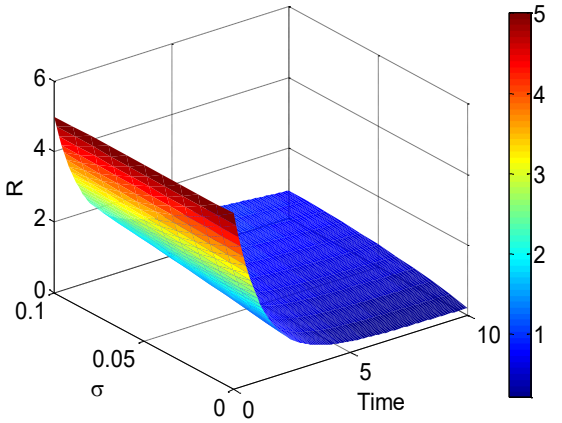

Fig.6 Surface plot w.r.t σ & t

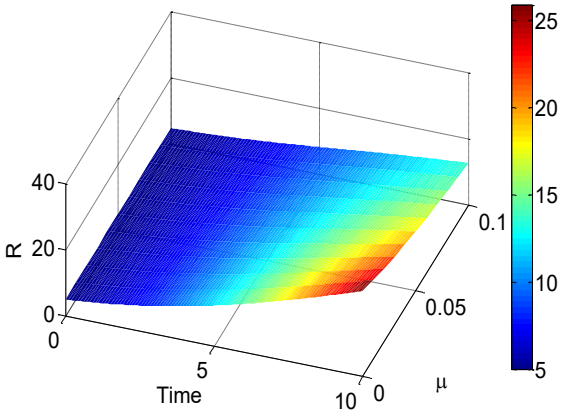

Fig.7 Surface plot w.r.t μ & t

VIII. Sensitivity Analysis

The importance of each parameter to disease transmission can be calculated through One-at-a-time (OAT) Variation methods. The OAT variation provides valuable insights into

the sensitivity of the model to each parameter, allowing researchers to identify influential parameters and understand their individual effects on the model's behavior. This method is easy to implement and provides a basic understanding of parameter sensitivity on the basic reproduction number.

$$R_0 = \frac{\beta SP\alpha\lambda}{(\mu+d+\alpha)(\mu+d+\lambda)\sigma}$$

We have determined the sensitivity index of R_0 for each of the seven parameters that determine R_0 as shown in table 1.

Table-1: Index of parameter sensitivity of R_0

Parameter	Sensitivity Index of R_0	Sign
α	$Y_\alpha^{R_0} = \frac{\partial R_0}{\partial \alpha} \times \frac{\alpha}{R_0} = \frac{(\mu+d)}{(\mu+d+\alpha)}$	+ve
β	$Y_\beta^{R_0} = \frac{\partial R_0}{\partial \beta} \times \frac{\beta}{R_0} = 1$	+ve
λ	$Y_\lambda^{R_0} = \frac{\partial R_0}{\partial \lambda} \times \frac{\lambda}{R_0} = \frac{(\mu+d)}{(\mu+d+\lambda)}$	+ve
μ	$Y_\mu^{R_0} = \frac{\partial R_0}{\partial \mu} \times \frac{\mu}{R_0} = \frac{-\mu(2\mu+2d+\lambda+\alpha)}{(\mu+d+\alpha)(\mu+d+\lambda)}$	-ve
σ	$Y_\sigma^{R_0} = \frac{\partial R_0}{\partial \sigma} \times \frac{\sigma}{R_0} = -1$	-ve
d	$Y_d^{R_0} = \frac{\partial R_0}{\partial d} \times \frac{d}{R_0} = \frac{-d(2\mu+2d+\lambda+\alpha)}{(\mu+d+\alpha)(\mu+d+\lambda)}$	-ve
P	$Y_P^{R_0} = \frac{\partial R_0}{\partial P} \times \frac{P}{R_0} = 1$	+ve

From the table-1, it is clear that the parameters $\alpha, \beta, \lambda, P$ are all positive. So all have high sensitivity on the basic reproduction number.

Figures 8 through 11 present a comprehensive sensitivity analysis, evaluating how variations in key parameters influence infection dynamics and system functionality. By analyzing these parameters, we can identify critical factors that contribute to the network's stability and resilience against infections. Figure 8 illustrates the sensitivity of infection dynamics with respect to the quarantine rate (σ) and the speed at which an exposed group transitions into an infectious group (λ). The figure highlights that an increase in σ leads to a reduction in the infection spread, as more infectious nodes are promptly quarantined. Conversely, a higher λ accelerates the transition from exposed to infectious states, increasing infection levels. The interplay between these parameters demonstrates that effective quarantine strategies can counterbalance the rapid progression of exposure to infection, emphasizing the need for prompt intervention. Figure 9 examines the sensitivity of the system to the rate of non-functional computer nodes due to technical failures (μ). Since μ represents failures not caused by malicious codes, a higher value indicates a decline in overall system performance, independent of infection spread. The figure reveals that excessive system failures can indirectly hinder the recovery process and increase network vulnerability. This underscores the importance of maintaining system reliability through regular updates and preventive maintenance to minimize disruptions caused by technical malfunctions. Figure 10 analyses the impact of both the percentage of exposed nodes that become infectious (α) and the failure rate of computer nodes due to malicious code-induced issues (d). A higher α\alphaα increases the probability of exposed nodes transitioning into the infectious state, accelerating malware propagation. Simultaneously, an increase in d signifies that more nodes are rendered non-functional due to infections, amplifying network degradation. The sensitivity plot shows that managing both parameters effectively is crucial—limiting α through robust detection measures and controlling d through strong antivirus defenses can significantly improve network stability. Figure 11 investigates the interaction between the technical failure rate (μ) and the malicious code-induced failure rate (d). The results indicate that while both parameters contribute to system instability, their combined effects can be particularly detrimental. Networks with high μ and d values experience severe functionality loss, making it imperative to mitigate technical failures while simultaneously strengthening cybersecurity defenses.

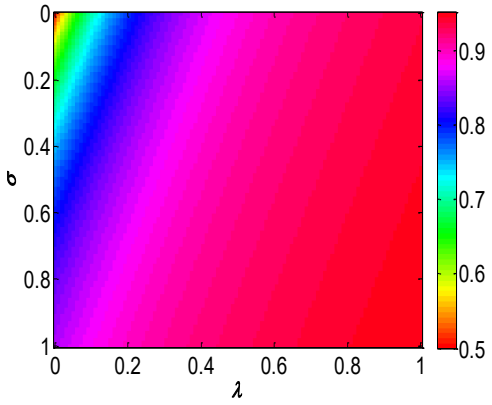

Fig. 8 Sensitivity of σ & λ

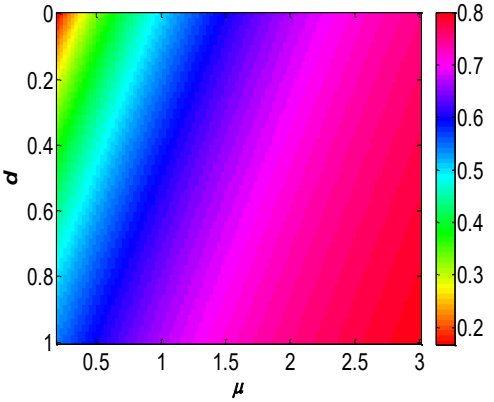

Fig. 9 Sensitivity of d & μ

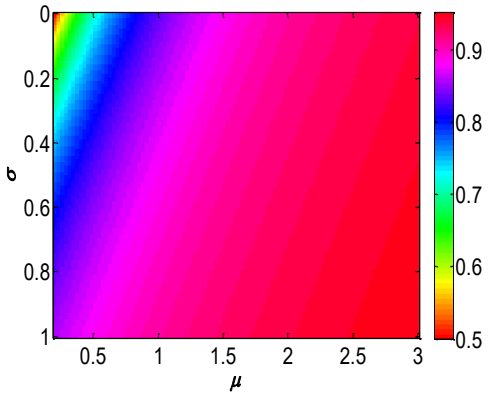

Fig. 10 Sensitivity of σ & μ

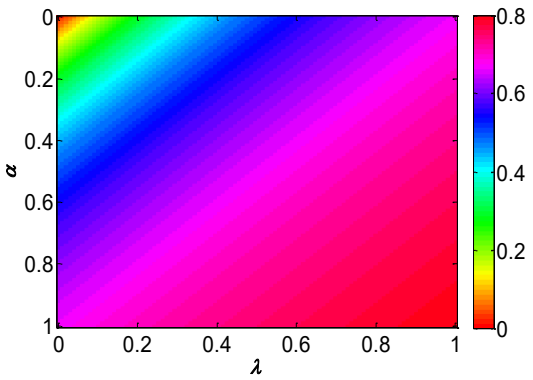

Fig. 11 Sensitivity of α & λ

IX. CONCLUSION

Our study of the SEABIQR model, supported by MATLAB simulations, has provided valuable insights into the dynamics of virus transmission within computer networks. By analyzing the system's behavior under different conditions, we have demonstrated the effectiveness of various control mechanisms in mitigating the spread of malicious codes. A key finding from our research is that the model exhibits stability at both the disease-free and endemic equilibrium points when the basic reproduction number (R_0) is below 1. This indicates that, under appropriate antivirus defenses, the spread of malware can be successfully contained, ensuring the overall security and functionality of the network.

The major outcomes of the study are as follows:

- When effective antivirus defense strategies are in place, the network remains free from epidemic spread. This reinforces the importance of proactive security measures in preventing large-scale infections.
- Asymptomatic nodes, in particular, pose a significant risk as they can continue spreading infections unnoticed, emphasizing the need for early detection mechanisms.
- An increase in quarantine rates leads to a decline in the number of actively infectious nodes which underscores the critical role of quarantine measures in containing outbreaks.
- There is a declining in infections rate as recovery processes become more effective which highlights the necessity of efficient recovery strategies, such as automated system patches and antivirus updates, to restore compromised nodes.

These findings emphasize the importance of proactive antivirus strategies in mitigating virus outbreaks in digital networks. They also demonstrate the utility of mathematical modelling and simulation in understanding and managing epidemic risks in complex systems, allowing researchers and cybersecurity professionals to design more effective intervention strategies. In addition to studying infection progression, we conducted a sensitivity analysis to identify the most influential parameters affecting virus transmission. Our analysis revealed that β, the rate at which susceptible nodes transition to the infected state, is a key factor in controlling the spread of the virus. This indicates that reducing β through strategies such as limiting exposure to malicious sources, improving early threat detection, and strengthening security protocols can significantly mitigate infection risks. Furthermore, other parameters, such as quarantine rates (σ), exposure-infection transition speed (λ), and node failure rates (μ, d), were also found to influence network stability. Understanding the interplay between these factors enables the development of optimized security strategies tailored to different network environments.

X. FUTURE SCOPE

For the computer e-epidemic model, the time delay differential equation can yield more accurate results. Expanding the effort to address the highest level of complexity in the epidemic model related to the spread of dangerous codes is also possible. Additionally, the pre-quarantine strategy can be a commendable effort to repair the malicious instructions that were communicated. As it analyses viral propagation and offers prevention in the scale-free network model, the criticality may be convergent.

REFERENCES

[1] Draief, M., Ganesh, A., & Massoulié, L., "Thresholds for virus spread on networks", *The Annals of Applied Probability*, vol. *18, no.* 2, 2008.

[2] Kephart, J. O., "A biologically inspired immune system for computers. *Artificial Life IV"*, pp123-132, 1994.

[3] Kumar Nayak, P., Mishra, D., & Ram, S., "Dynamic E-EpidEmic model for active infectious nodes in computer network", *Journal of Statistics and Management Systems*, vol. *19, no.* 2, pp247-257, 2016.

[4] Li, M. Y., & Wang, L., "Global stability in some seir epidemic models. *Mathematical Approaches for Emerging and Reemerging Infectious Diseases: Models", Methods, and Theory*, pp295-311, 2002.

[5] Mishra, B. K., & Jha, N., "SEIQRS model for the transmission of malicious objects in computer network", *Applied Mathematical Modelling*, vol. *34, no.* 3, 2010.

[6] Mohanty, S., Nayak, P. K., Paul, A. K., & Basantia, A., "Mathematical modeling for understanding computer virus behavior in a network and its stability analysis", *2023 OITS International Conference on Information Technology,* 2023.

[7] Mohanty, S., Nayak, P. K., Paul, A. K., & Basantia, A., "SIQTRS E-EpidEmic model: A comprehensive framework for analyzing and managing computer virus propagation in networks", *2023 OITS International Conference on Information Technology (OCIT),* 2023.

[8] Newman, M. E., Forrest, S., & Balthrop, J., "Email networks and the spread of computer viruses", *Physical Review E*, vol. *66, no.* 3, 2002.

[9] Piqueira, J. R., & Cesar, F. B., "Dynamical models for computer viruses propagation", *Mathematical Problems in Engineering*, vol. *2008, no.*1, 2008.

[10] .Ram, S., Nayak, P. K., & Mishra, D., "Mathematical modelling, analysis involving behaviour of infectious nodes in a computer network", *2020 International Conference on Renewable Energy Integration into Smart Grids: A Multidisciplinary Approach to Technology Modelling and Simulation (ICREISG)*, 2020.

[11] Yan, P., & Liu, S., "SEIR epidemic model with delay. *The ANZIAM Journal*", vol. *48, no.* 1, pp119-134, 2006.

[12] Ahmad, I., Bakar, A. A., Jan, R., & Yussof, S., "Dynamic behaviors of a modified computer virus model: Insights into parameters and network attributes", *Alexandria Engineering Journal*, vol. *103*, pp266-277, 2024.

[13] Alderremy, A. A., Gómez-Aguilar, J. F., Sabir, Z., Aly, S., Lavín-Delgado, J. E., & Razo-Hernández, J. R., "Numerical performances based artificial neural networks to deal with the computer viruses spread on the complex networks", *International Journal of Computer Mathematics*, vol. *101, no.* 3, pp314-330, 2024.

[14] .Muthukumar, S., Senthilkumar, M., & Veeramani, C., "Optimal Control of Computer virus Spreading model with partial immunization", *Wireless Personal Communications*, pp.1-27, 2024.

[15] Manohara, G., & Kumbinarasaiah, S., "Numerical solution of a modified epidemiological model of computer viruses by using Fibonacci wavelets", *The Journal of Analysis*, vol. *32, no.* 1, pp529-554, 2024.

[16] Verma, C., & Gupta, C. P., "Effect of vaccination on stability of wireless sensor network against malware attack: An epidemiological model", *SN Computer Science*, vol. *5, no.* 2, pp240, 2024.

[17] Ying, X., Pan, M., Chen, X., Zhou, Y., Liu, J., Li, D., ... & Zhu, Z., "Research on Virus Propagation Network Intrusion Detection Based on Graph Neural Network. *Mathematics"*, vol. 12, no. 10, pp.1534, 2024.