Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Deep Learning Enhanced Mathematical Model for Malware Propagation under Two-Level Security Protection

RP Chauhan
Symbiosis International University
Sumit Kumar
sumitmehta0208@gmail.com
Sarala Birla University
Devesh Tiwari
Amrita Vishwa Vidyapeetham
CH Manvitha
Amrita Vishwa Vidyapeetham

Research Article

Keywords: Malware propagation, Two-level protection, Deep neural network, Sensitivity analysis, Simulation

Posted Date: October 12th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11182851/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Deep Learning Enhanced Mathematical Model for Malware Propagation under Two-Level Security Protection

immediate

September 27, 2026

Abstract

Malware propagation poses a significant threat to the security and reliability of computer networks. This study develops a nonlinear epidemic model to investigate malware transmission under two levels of security protection, namely weak and full protection. The proposed model is qualitatively analyzed to establish the positivity and boundedness of solutions, ensuring its mathematical feasibility. The equilibrium points are derived, and their stability properties are investigated. The basic reproduction number R_0 is obtained as the principal threshold parameter governing malware persistence. Sensitivity analysis is performed to identify the parameters that have the greatest influence on R_0. Numerical simulations using the *ode45* solver are conducted to validate the analytical results and illustrate the transition between malware-free and endemic states. Furthermore, a deep neural network (DNN) is integrated to provide an independent and computationally efficient approximation of the model dynamics. The DNN demonstrates excellent predictive accuracy for the infected $I(t)$ and quarantined $Q(t)$ compartments, achieving a mean squared error (MSE) of 9.94×10^{-11} with strong regression performance. The results demonstrate that the proposed hybrid mathematical–DNN framework accurately captures nonlinear malware dynamics and provides an efficient alternative to conventional numerical ODE solvers. The framework offers a useful computational approach for cybersecurity analysis.

Keywords: Malware propagation, Two-level protection, Deep neural network, Sensitivity analysis,, Simulation

1. Introduction

The concept of malware has evolved significantly since its theoretical inception by John von Newumann in 1996. Malware is a type of malicious software designed to disrupt computer systems. It can cause problems by stealing information, damaging files, or making devices act strangely without the owner knowing. With the rapid development of Internet, malware has emerged as one of the most critical threats to network security globally [3]. Such viruses commonly spread through removable storage media like USB drives and frequently originate from suspicious emails or corrupted links that trick users into opening infected files. Once a system is compromised, it poses a serious threat to the user's privacy and data security. The nature of cyber threats has changed dramatically since the early 2000s, with modern malware such as WannaCry, NotPetya, and Ryuk demonstrating a scale and sophistication far beyond earlier computer viruses. These development highlight the need for updated models that can accurately capture the dynamics of present-day cyber threats. Common indicators of an infected system include sluggish performance, unresponsive icons, unexpected shutdowns, changes to the browser's default homepage, hidden desktop icons and turning off of the system's firewall, a critical defense mechanism [4].

Analysis of malicious software is crucial in network security as it aids in comprehending, identifying, and minimizing the impact of harmful software threats. Dynamic models are highly effective in forecasting the spread of viruses and assist in creating appropriate strategies to minimize the damage. TConventional mathematical models for malware spread are influenced by epidemiological concepts, with adaptations of SIR-type models. This strengthened the rationale for applying epidemic theory to studying malware propagation in computer network. Several mathematical models have been suggested to tackle how computer viruses spread and how to control their dynamics. For instance, in a study by Zhu et al. [10], a model known as SIR for malware propagation was introduced and examined, incorporating delays and an optimal control approach. Xiao et al. [18] developed an SIRS model to explore malware spread, considering dispersion mechanisms and time delays. Their research pinpointed critical transition points and delved into the dynamics underlying these shifts. The role of removable devices is significant in disseminating harmful elements across networks. Prajapati [11] investigated the propagation of malicious objects through networks via removable devices. Additionally, Liu et al. [12] put forth a delayed e-epidemic SEIRS malware dissemination model utilizing a general non-monotonic incidence rate. Mishra and Keshri [13] introduced the SEIR-V model, which considers that sensor nodes can either be exposed to a disease that hinders transmission or be immunized against future infections.

Mohanty et al. [16] developed the SEIAQR model under conventional antivirus defense to curb malware spread. Mishra et al. [14] proposed the SIQRS model, which excludes the latent (or exposed) phase of infection, instead allowing sensors to exhibit reduced transmission rates as a symptom of infection. In [15] Khanh developed a SIQR model capturing the propagation dynamics of worms under quarantine in wireless sensor networks. Biswal and Swain [17] introduced the SIQVD model to examine malware spread within wireless sensor networks. More recently, Choudhary et al. [1] formulated an SPIQR model to analyze malware transmission dynamics in networks, identifying strategies to control spread by regulating the reproduction number.

Deep learning is now considered a powerful approach to approximating the solutions of dynamical systems and differential equations [26]. There are several advantages of using neural networks such as immediate learning of non-linear functions from data, fast inference after training, and usage as surrogates for computationally expensive simulations [27]. The application of deep neural networks in the field of epidemiology has attracted much attention recently, in particular, in terms of predicting the spread of disease and analyzing intervention strategies [28, 29]. In this research, the authors use a feedforward neural network (deep neural network) as a fast substitute model for the suggested epidemiological model. This work aims to build a computationally efficient surrogate model that can accurately reproduce the dynamics of the infected $I(t)$ and quarantined $Q(t)$ compartments. The suggested DNN surrogate model is trained using solutions of the ODE system and is evaluated in terms of both interpolation and extrapolation cases. It can be seen that the effectiveness of DNN surrogate models in epidemiology is proved [30].

Existing malware propagation models incorporate defensive mechanisms such as quarantine, vaccination, antivirus protection, and recovery, but typically treat all protected nodes as equally secure. However, real-world computer networks may not exhibit uniform security postures, since devices differ in patch status, configuration completeness, and update frequency. To address this gap, we proposed SP_1P_2IQR framework, an extension of [1], which introduces two distinct protection states: weakly protected and fully protected nodes. Thereby capturing the varying degrees of resilience that different hosts exhibit against malware infection. Weakly protected nodes run outdated antivirus definitions, unpatched software, or minimal firewall configurations, making them susceptible to reinfection or compromise. represent fully protected nodes with significantly higher resistance. Fully protected nodes maintain up-to-date patches, robust intrusion detection, and strict access controls, offering substantially higher resistance to malware.

The specific objectives of this work are as follows:

- Formulation of SP_1P_2IQR model for malware propagation in computer networks.
- To present a qualitative analysis of the model, including non-negativity of solutions, boundedness, and existence and uniqueness of the solution.
- To identify the most influential model parameters through sensitivity analysis.
- To implement a deep neural network approach to improve the predictive accuracy of the model.

2. Mathematical Model

In this section, an epidemic-type compartmental model is formulated to describe malware propagation in a computer network. The total computer population is divided into six mutually exclusive compartments: susceptible nodes S(t), weakly protected nodes $P_1(t)$, fully protected nodes $P_2(t)$, infected nodes $I(t)$, quarantined nodes $Q(t)$, and recovered nodes $R(t)$. The size of the compartment class varies with time t but the total size of the population $N(t) = S(t) + P_1(t) + P_2(t) + I(t) + Q(t) + R(t)$.

To formulate the model, certain assumptions have been made. In particular, weakly protected computers can still become infected, although their susceptibility is reduced, whereas fully protected computers are assumed to be completely resistant to malware infection. The parameter Π denotes the entry of new computer node into the network. Susceptible nodes may acquire security protection, moving to the weakly protected class P_1 at rate α_1 or to the fully protected class P_2 at rate α_2, depending on the level of security measures adopted. Fully protected nodes are assumed to be completely resistant to malware infection, reflecting comprehensive and continuously updated defenses, whereas weakly protected nodes may lose their protection due to antivirus subscription expiry, security software failure or being disabled, or missed update cycles. Susceptible and weakly protected nodes become infected through contact with infected nodes with contact rate β. For weakly protected nodes, the transmission rate is scaled by a protection-efficacy parameter $\epsilon \in [0, 1]$. When $\epsilon = 0$, transmission proceeds at the baseline rate β. As in $\epsilon = 1$, the security protection reaches maximum effectiveness, and transmission is prevented from P_1. Weakly protected computers may lose their protection, due to expiry or failure returning to the S at rate γ. Weakly protected nodes may be upgraded to full protection through a security update at rate δ. Infected nodes transfered to the quarantine class at rate η. Infected nodes can recover through system updates, antivirus intervention, or malware removal at rate ϕ. The parameter θ represents the recovery rate of quarantined nodes. Recovered nodes may lose their acquired immunity or security status over time returning to the susceptible class at rate λ. Nodes in every compartments are removed from the network due to hardware failure, replacement, or other forms of permanent loss at the natural removal rate μ.

Incorporating the above assumptions and transition dynamics, the model is formulated as the following system of non-linear ordinary differential equations:

$$\left.\begin{array}{ll} \frac{dS}{dt} & = \Pi - \beta SI - \alpha_1 S - \alpha_2 S - \mu S + \gamma P_1 + \lambda R, \\ \frac{dP_1}{dt} & = \alpha_1 S - \delta P_1 - \gamma P_1 - (1-\epsilon)\beta P_1 I - \mu P_1, \\ \frac{dP_2}{dt} & = \alpha_2 S + \delta P_1 - \mu P_2, \\ \frac{dI}{dt} & = \beta SI + (1-\epsilon)\beta P_1 I - (\eta + \phi + \mu) I, \\ \frac{dQ}{dt} & = \eta I - (\theta + \mu) Q, \\ \frac{dR}{dt} & = \phi I + \theta Q - (\lambda + \mu) R, \end{array}\right\} \tag{2.1}$$

with the initial conditions $S(0) \geq 0, P_1(0) \geq 0, P_2(0) \geq 0, I(0) \geq 0, Q(0) \geq 0, R(0) \geq 0$, and description of the parameters are given in Table 1.

Parameters	Values
Π	Rate of entry of new computer network nodes
β	Malware transmission rate
α_1	Rate of adoption of weak protection
α_2	Rate of direct adoption of full protection
δ	Rate of upgrading to full protection
γ	Rate of loss/expiry of weak protection
ϵ	Protection efficacy against malware transmission
η	Rate of quarantine of infected computers
ϕ	recovery rate of infected computers
θ	Recovery rate of quarantined computers
λ	Rate of loss of recovery/immunity
μ	Natural disconnection rate of nodes

Table 1: Caption

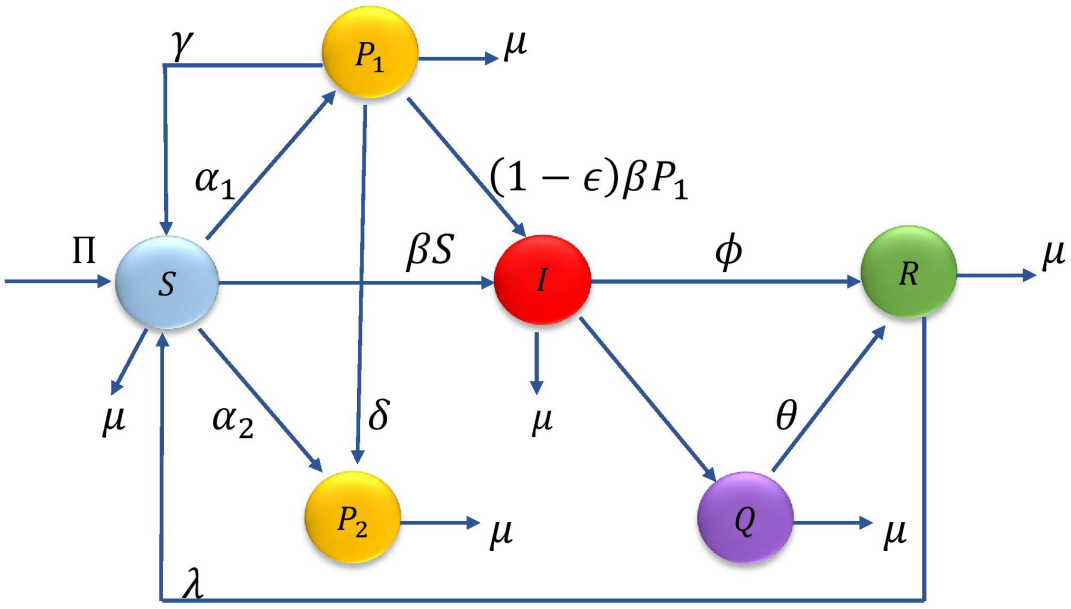


Figure 1: Flow between compartments in model (2.1)

Table 2: Parameters values for the model (2.1)

Parameter	Values	References
Π	0.20(MFE), 0.5 (EE)	[1]
β	0.30 (MFE), 0.5 (EE)	[1]
α_1	0.30	Assumed
α_2	0.10	Assumed
μ	0.05	[1]
γ	0.55	[1]
δ	0.15	[1]
ϵ	0.50	Assumed
η	0.90 (MFE), 0.25(EE)	[1]
ϕ	0.01	[1]
θ	0.65	[1]
λ	0.01	[1]

3. Elementary characteristics

3.1 Invariant region

We now show that all state variables of the model remain non-negative for given non-negative initial conditions [2].

Theorem 3.1. *All solutions are bounded and enter the region*

$$\Omega = \left\{ (S, P_1, P_2, I, Q, R) \in R_+^6 : N(t) \leq \frac{\Pi}{\mu} \right\}, \tag{3.1}$$

as $t \to \infty$.

Proof. Let $(S(t), P_1(t), P_2(t), I(t), Q(t), R(t))$ be a solution of the model with non-negative initial conditions in Ω. Since

$$N(t) = S + P_1 + P_2 + I + Q + R, \tag{3.2}$$

differentiating Eq. (3.2) with respect to time t, we obtain

$$\frac{dN}{dt} = \dot{S} + \dot{P}_1 + \dot{P}_2 + \dot{I} + \dot{Q} + \dot{R}, \tag{3.3}$$

from the model system (2.1), we get

$$\frac{dN}{dt} = \Pi - \mu N. \tag{3.4}$$

After simplification,

$$N(t) = \frac{\Pi}{\mu} + \left(N(0) - \frac{\Pi}{\mu} \right) e^{-\mu t}. \tag{3.5}$$

Taking, $t \to \infty$, we have $N(t) \leq \frac{\Pi}{\mu}$. Which implies that $0 \leq N \leq \frac{\Pi}{\mu}$, then trajectories of the model (2.1) are bounded in the region Ω. Hence, we have established that Ω is positively invariant and attracts all solution in R_+^6.

3.2 Non-negativity of solution

Theorem 3.2. *All solutions of the model with non-negative initial conditions* $(S, P_1, P_2, I, Q, R)(0) \geq 0 \in \Omega$ *remain non-negative for* $t \geq 0$ *[5, 6].*

Proof First, set $\zeta = \beta I$, from the first equation of (2.1), we have

$$\frac{dS}{dt} = \Pi - \zeta S - \alpha_1 S - \alpha_2 S - \mu S + \gamma P_1 + \lambda R,$$

or

$$\begin{aligned} \tfrac{ds}{dt} &\geq \Pi - \zeta S - \alpha_1 S - \alpha_2 S - \mu S, \\ \tfrac{ds}{dt} + (\zeta + \alpha_1 + \alpha_2 + \mu) S &\geq \Pi. \end{aligned}$$

Suppose a solution of system (2.1) exists on $[0, \infty)$, then for all $t \in [0, \infty)$, the above equation can be expressed as

$$\tfrac{d}{dt}\left(S(t) e^{\int_0^t (\zeta + \alpha_1 + \alpha_2 + \mu)(s) ds} \right) \geq \Pi e^{\int_0^t (\zeta + \alpha_1 + \alpha_2 + \mu)(s) ds}$$

implies that

$$\begin{aligned} S(t) e^{\int_0^t (\zeta + \alpha_1 + \alpha_2 + \mu)(s) ds} - S(0) &\geq \Pi \int_0^t e^{\int_0^w (\zeta + \alpha_1 + \alpha_2 + \mu)(w) dw} \\ S(t) e^{\int_0^t (\zeta + \alpha_1 + \alpha_2 + \mu)(s) ds} &\geq S(0) + \Pi \int_0^t e^{\int_0^w (\zeta + \alpha_1 + \alpha_2 + \mu)(w) dw} \\ S(t) &\geq S(0) e^{-\int_0^t (\zeta + \alpha_1 + \alpha_2 + \mu)(s) ds} \\ &\quad + \Pi e^{-\int_0^t (\zeta + \alpha_1 + \alpha_2 + \mu)(s) ds} \int_0^t e^{\int_0^w (\zeta + \alpha_1 + \alpha_2 + \mu)(w) dw} > 0. \end{aligned}$$

Hence, $S(t)$ is positive for all values of $t \in [0, \infty)$. Taking second equation of the system (2.1)

$$\begin{aligned} \frac{dP_1}{dt} &= \alpha_1 S - \delta P_1 - \gamma P_1 - (1-\epsilon)\beta I P_1 - \mu P_1, \\ \frac{dP_1}{dt} &\geq -(\delta + \gamma + (1-\epsilon)\beta I + \mu) P_1, \end{aligned}$$

Integrating inequality in the above equation by separating variables, we get

$$P_1(t) \geq P_1(0) e^{-(\delta+\gamma+(1-\epsilon)\beta I+\mu)t} \geq 0, \text{ since } (\delta + \gamma + (1-\epsilon)\beta I + \mu) > 0. \tag{3.6}$$

Third equation of the system (2.1) implies that

$$\begin{aligned} \frac{dP_2}{dt} &= \alpha_2 S + \delta P_1 - \mu P_2 \\ \frac{dP_2}{dt} &\geq -\mu P_2. \end{aligned}$$

On integrating, we obtained

$$P_2(t) \geq P_2(0) e^{-\mu t} \geq 0, \text{ since } \mu > 0. \tag{3.7}$$

Similarly, this can be proven for the compartments $I(t), Q(t)$ and $R(t)$.

3.3 Existence and Uniqueness of solution

[8] The general first-order ODE is in the form:

$$z' = g(t, z), \quad z(t_0) = z_0. \tag{3.8}$$

The following theorem is used to establish the existence and uniqueness of the solution to our model.

Theorem 3.3. *Suppose* $\mathbf{D}$ *denotes the domain*

$$|t - t_0| \leq a, |z - z_0| \leq b, \ z = (z_1, z_2, ..., z_n), z_0 = (z_{10}, z_{20}, ..., z_{n0}), \tag{3.9}$$

and suppose $g(t, z)$ *satisfies the Lipschitz condition:*

$$\|g(t, z_1) - g(t, z_2)\| \leq k\|z_1 - z_2\|, \tag{3.10}$$

whenever the pairs (t, z_1) *and* $(t, z_2) \in \mathbf{D}$ *, where* k *is a positive constant. Then, there exist a constant* $\delta^* > 0$ *such that system* (3.8) *has a unique (exactly one) continuous vector solution* $z(t)$ *of the in the interval* $|t - t_0| \leq \delta^*$*. It is important to note that condition* (3.10) *is satisfied by requirement that:*

$$\frac{\partial g_i}{\partial z_j}, \quad i, j = 1, 2, ..., n \tag{3.11}$$

be continuous and bounded in the domain $\mathbf{D}$*.*

Lemma 3.1. *If* $g(t, z)$ *has continuous partial derivative* $\frac{\partial g_i}{\partial z_j}$ *on a bounded closed convex domain* $\mathbf{R}$ *(i.e, convex set of real numbers), where* $\mathbf{R}$ *is used to denotes real numbers, then it satisfies a Lipschitz condition in* $\mathbf{R}$*. Our interest is in the domain:*

$$1 \leq \epsilon \leq \mathbf{R} \tag{3.12}$$

So, we look for a bounded solution of the form

$$0 < \mathbf{R} < \infty.$$

Theorem 3.4. *Let* $\mathbf{D}$ *denotes the domain defined in* (3.9) *such that* (3.10) *and* (3.12) *hold. Then there exists a solution of model* (2.1)*, which is bounded in the domain* $\mathbf{D}$*.*

Proof. Let

$$g_1 = \Pi - \beta SI - \alpha_1 S - \alpha_2 S - \mu S + \gamma P_1 + \lambda R, \tag{3.13}$$
$$g_2 = \alpha_1 S - \delta P_1 - \gamma P_1 - (1-\epsilon)\beta P_1 I - \mu P_1, \tag{3.14}$$
$$g_3 = \alpha_2 S + \delta P_1 - \mu P_2, \tag{3.15}$$
$$g_4 = \beta SI + (1-\epsilon)\beta P_1 I - (\eta + \phi + \mu)I, \tag{3.16}$$
$$g_5 = \eta I - (\theta + \mu)Q, \tag{3.17}$$
$$g_6 = \phi I + \theta Q - (\lambda + \mu)R. \tag{3.18}$$

Now, we want to show that $\frac{\partial g_i}{\partial z_j}, \quad i, j = 1, 2, ..., n$ are continuous and bounded. For this purpose, we explored the following partial derivatives. For class S, from Eq. (3.13);

$$\frac{\partial g_1}{\partial S} = -\beta I - \alpha_1 - \alpha_2 - \mu, \ \left|\frac{\partial g_1}{\partial S}\right| = \left| -\beta I - \alpha_1 - \alpha_2 - \mu\right| < \infty,$$
$$\frac{\partial g_1}{\partial P_1} = \gamma, \ \left|\frac{\partial g_1}{\partial P_1}\right| = |\gamma| < \infty,$$
$$\frac{\partial g_1}{\partial P_2} = 0, \ \left|\frac{\partial g_1}{\partial P_2}\right| = |0| < \infty,$$
$$\frac{\partial g_1}{\partial I} = -\beta S, \ \left|\frac{\partial g_1}{\partial I}\right| = \left| -\beta S\right| < \infty,$$
$$\frac{\partial g_1}{\partial Q} = 0, \ \left|\frac{\partial g_1}{\partial Q}\right| = |0| < \infty,$$
$$\frac{\partial g_1}{\partial R} = \lambda, \ \left|\frac{\partial g_1}{\partial R}\right| = |\lambda| < \infty.$$

For class P_1, from Eq. (3.14);

$$\frac{\partial g_2}{\partial S} = \alpha_1, \ \left|\frac{\partial g_2}{\partial S}\right| = |\alpha_1| < \infty,$$
$$\frac{\partial g_2}{\partial P_1} = -\delta - \gamma - (1-\epsilon)\beta I - \mu, \ \left|\frac{\partial g_2}{\partial P_1}\right| = \left| -\delta - \gamma - (1-\epsilon)\beta I - \mu\right| < \infty,$$
$$\frac{\partial g_2}{\partial P_2} = 0, \ \left|\frac{\partial g_2}{\partial P_2}\right| = |0| < \infty,$$
$$\frac{\partial g_2}{\partial I} = 0, \ \left|\frac{\partial g_2}{\partial I}\right| = |0| < \infty,$$
$$\frac{\partial g_2}{\partial Q} = 0, \ \left|\frac{\partial g_2}{\partial Q}\right| = |0| < \infty,$$
$$\frac{\partial g_2}{\partial R} = 0, \ \left|\frac{\partial g_2}{\partial R}\right| = |0| < \infty.$$

Now for class P_2, from Eq. (3.15);

$$\frac{\partial g_3}{\partial S} = \alpha_2, \ \left|\frac{\partial g_3}{\partial S}\right| = |\alpha_2| < \infty,$$
$$\frac{\partial g_3}{\partial P_1} = \delta, \ \left|\frac{\partial g_3}{\partial P_1}\right| = |\delta| < \infty,$$
$$\frac{\partial g_3}{\partial P_2} = -\mu, \ \left|\frac{\partial g_3}{\partial P_2}\right| = |-\mu| < \infty,$$
$$\frac{\partial g_3}{\partial I} = 0, \ \left|\frac{\partial g_2}{\partial I}\right| = |0| < \infty,$$

$$\frac{\partial g_3}{\partial Q} = 0, \ \left|\frac{\partial g_2}{\partial Q}\right| = |0| < \infty,$$
$$\frac{\partial g_3}{\partial R} = 0, \ \left|\frac{\partial g_2}{\partial R}\right| = |0| < \infty.$$

Likewise, the same outcome can also be established for the classes I, Q and R. This confirms that all partial derivatives are continuous and bounded. Consequently, by Theorem (3.3), we conclude that system (2.1) possesses a unique solution within the region $\mathbf{D}$.

3.4 Equilibrium Points

The malware-free equilibrium (MFE) in the absence of a virus is obtained by setting $I = 0$. Thus, the MFE is given by

$$E_0 = (S_0, P_{10}, P_{20}, 0, 0, 0), \tag{3.19}$$

where

$$P_{10} = \frac{\alpha_1 S_0}{\delta + \gamma + \sigma}, \tag{3.20}$$

$$P_{20} = \frac{\alpha_2 S_0 + \delta P_{10}}{\sigma}, \tag{3.21}$$

and

$$S_0 = \frac{\Pi(\delta + \gamma + \mu)}{(\alpha_2 + \mu)(\delta + \gamma + \mu) + \alpha_1(\delta + \mu)}. \tag{3.22}$$

Therefore, the malware-free equilibrium is

$$E_0 = \left(\frac{\Pi(\delta + \gamma + \mu)}{(\alpha_2 + \mu)(\delta + \gamma + \mu) + \alpha_1(\delta + \mu)}, \frac{\alpha_1 S_0}{\delta + \gamma + \sigma}, \frac{\alpha_2 S_0 + \delta P_{10}}{\sigma}, 0, 0, 0\right). \tag{3.23}$$

Following the next-generation matrix technique [32, 7], the basic reproduction number $\mathcal{R}_0$ of the model is derived. The model incorporates two infected compartments, namely I and Q. The rate of appearance of new infections $\mathcal{F}$ and the rate of transfer between infected compartments $\mathcal{V}$ are given by

$$\mathcal{F} = \begin{pmatrix} \beta SI + (1-\epsilon)\beta P_1 I \\ 0 \end{pmatrix}, \quad \mathcal{V} = \begin{pmatrix} (\eta + \phi + \mu)I \\ -\eta I + (\theta + \mu)Q \end{pmatrix}.$$

At the MFE point, the Jacobian matrices of $\mathcal{F}$ and $\mathcal{V}$ are calculated and given as

$$\mathrm{F} = \begin{pmatrix} \beta S_0 + (1-\epsilon)\beta P_{10} & 0 \\ 0 & 0 \end{pmatrix}, \quad \mathrm{V} = \begin{pmatrix} (\eta + \phi + \mu) & 0 \\ -\eta & \theta + \mu \end{pmatrix}. \tag{3.24}$$

The spectral radius of the next generation matrix FV^{-1} is the number $\mathcal{R}_0$, which is given by

$$\mathcal{R}_0 = \frac{\beta S_0}{\eta + \phi + \mu}\left[1 + \frac{(1-\epsilon)\alpha_1}{\delta + \gamma + \mu}\right].$$

Substituting S_0, we obtain

$$\mathcal{R}_0 = \frac{\beta\Pi(\delta + \gamma + \mu + (1-\epsilon)\alpha_1)}{(\eta + \phi + \mu)[(\alpha_2 + \mu)(\delta + \gamma + \mu) + \alpha_1(\delta + \mu)]}. \tag{3.25}$$

This expression quantifies the potential for malware spread in the computer networks.

The following theorem is established for the stability of the malware-free equilibrium.

Theorem 3.5. *The MFE point of model (2.1) is locally asymptotically stable if $\mathcal{R}_0 < 1$ and unstable if $\mathcal{R}_0 > 1$.*

Proof The Jacobian matrix of system (2.1) evaluated at the MFE E_0 is given by

$$J(E_0) = \begin{pmatrix} -(\alpha_1+\alpha_2+\mu) & \gamma & 0 & -\beta S_0 & 0 & \lambda \\ \alpha_1 & -(\delta+\gamma+\mu) & 0 & -(1-\epsilon)\beta P_{10} & 0 & 0 \\ \alpha_2 & \delta & -\mu & 0 & 0 & 0 \\ 0 & 0 & 0 & \beta S_0 + (1-\epsilon)\beta P_{10} - (\eta+\phi+\mu) & 0 & 0 \\ 0 & 0 & 0 & \eta & -(\theta+\mu) & 0 \\ 0 & 0 & 0 & \phi & \theta & -(\lambda+\mu) \end{pmatrix}. \tag{3.26}$$

The Jacobian becomes block triangular matrix. Its eigenvalues are $\lambda_1, \lambda_2, \lambda_3 = -\mu, \lambda_4 = \beta\left[S_0 + (1-\epsilon)P_{10}\right] - (\eta+\phi+\mu), \lambda_5 =$ and $\lambda_6 = -(\lambda+\mu)$, where λ_1, λ_2, are the eigenvalues of the block matrix

$$J_1 = \begin{pmatrix} -(\alpha_1+\alpha_2+\mu) & \gamma \\ \alpha_1 & -(\delta+\gamma+\mu) \end{pmatrix}. \tag{3.27}$$

The characteristic polynomial associated with J_1 is

$$\lambda^2 + A\lambda + B = 0, \tag{3.28}$$

where

$$A = \alpha_1 + \alpha_2 + \delta + \gamma + 2\mu > 0$$

and

$$B = \alpha_1(\delta+\mu) + (\alpha_2+\mu)(\delta+\gamma+\mu) > 0.$$

Therefore, by Routh-Hurwitz criteria both roots λ_1, λ_2 have negative real parts. Assuming $\mathcal{R}_0 < 1$, eigenvalue $\lambda_4 = (\eta+\phi+\mu)(\mathcal{R}_0 - 1) < 0$. Since all the parameters in the model are non- negative, it follows that the all eigenvalues of $J(E_0)$ have negative real parts when $\mathcal{R}_0 < 1$. Hence, E_0 is locally asymptotically stable.

Theorem 3.6. *In the absence of quarantine rate of infected computers, the MFE point, E_0, is globally asymptotically stable whenever $\mathcal{R}_0 < 1$.*

Proof. Define the Lyapunov function as

$$\mathcal{L}_1 = I + \frac{\eta}{\theta+\mu} Q. \tag{3.29}$$

The time derivative is given by

$$\frac{d\mathcal{L}_1}{dt} = \frac{dI}{dt} + \frac{\eta}{\theta+\mu}\frac{dQ}{dt}. \tag{3.30}$$

Substitution from the model equation (2.1)

$$\begin{aligned} \tfrac{d\mathcal{L}_1}{dt} &= [\beta SI + (1-\epsilon)\beta P_1 I - (\eta+\phi+\mu)I] + \tfrac{\eta}{\theta+\mu}[\eta I - (\theta+\mu)Q], \\ &= [\beta S + (1-\epsilon)\beta P_1 - (\eta+\phi+\mu) + \tfrac{\eta^2}{\theta+\mu}]I - \eta Q. \end{aligned} \tag{3.31}$$

at E_0, we have

$$\begin{aligned} \tfrac{d\mathcal{L}_1}{dt} &= [\beta S_0 + (1-\epsilon)\beta P_{10} - (\eta+\phi+\mu) + \tfrac{\eta^2}{\theta+\mu}]I - \eta Q \\ &= \left[(\mathcal{R}_0 - 1) + \tfrac{\eta^2}{(\theta+\mu)(\eta+\phi+\mu)}\right](\eta+\phi+\mu)I - \eta Q \end{aligned} \tag{3.32}$$

By setting $\eta = 0$, we have

$$\begin{aligned} \tfrac{d\mathcal{L}_1}{dt} &= [\beta S_0 + (1-\epsilon)\beta P_{10} - (\eta+\phi+\mu) + \tfrac{\eta^2}{\theta+\mu}]I - \eta Q, \\ &= (\mathcal{R}_0 - 1)(\phi+\mu)I. \end{aligned} \tag{3.33}$$

Hence, whenever $\mathcal{R}_0 < 1$, the Lyapunov derivative $\frac{d\mathcal{L}_1}{dt} < 0$, and hence, the MFE point is globally asymptotically stable [25].

3.5 Endemic equilibrium

Theorem 3.7. *A unique endemic equilibrium point $E^* = (S^*, P_1^*, P_2^*, I^*, Q^*, R^*)$ for the model described by the system (2.1) exists only when $\mathcal{R}_0 > 1$.*

For convenience, we define $A_1 = \delta + \gamma + \mu$, $A_2 = (1-\epsilon)\beta$, $A_3 = \eta + \phi + \mu$, $A_4 = \frac{\phi(\theta+\mu)+\theta\eta}{(\theta+\mu)(\lambda+\mu)}$, *and* $A_5 = \alpha_1 + \alpha_2 + \mu$.

The components of EE point are given as:

$P_1^* = \frac{\alpha_1 S^*}{A_1 + A_2 I^*}$,
$S^* = \frac{A_3(A_1 + k_1 I^*)}{\beta(A_1 + A_2 I^*) + A_2\alpha_1}$,
$P_2^* = \frac{\alpha_2 S^* + \delta P_1^*}{\mu}$,
$Q^* = \frac{\eta I^*}{\theta+\mu}$,
$R^* = A_4 I^*$,

and I^* is calculated by solving the quadratic equation provided for I:

$$B_2 I^2 + B_1 I + B_0 = 0.$$

where,

$$\begin{aligned} B_2 &= \beta A_2(A_3 - \lambda A_4), \\ B_1 &= A_3(\beta A_1 + A_2 A_5) - \lambda A_4(\beta A_1 + A_2\alpha_1) - \Pi\beta A_2, \\ B_0 &= \beta\Pi(A_1 + A_2\alpha_1) + \gamma\alpha_1 A_3 - A_3 A_1 A_5 \\ &= A_3 C(1 - \mathcal{R}_0), \end{aligned} \tag{3.34}$$

in which, $C = \alpha_1(\delta + \mu) + (\alpha_2 + \mu)A_1$.

Proof

To confirm the uniqueness and positivity of the equilibrium point, we prove that I is greater than zero, when $\mathcal{R}_0 > 1$ and is unique.

From the equation $B_2 I^2 + B_1 I + B_0 = 0$, we have $I = \frac{-B_1 \pm \sqrt{B_1^2 - 4B_2 B_0}}{2B_2}$. As $A_3 - \lambda A_4 > 0$, clearly B_2 is positive. When

$$\begin{aligned} \mathcal{R}_0 > 1, \quad &\Longrightarrow \ B_0 < 0 \\ &\Longrightarrow \ \tfrac{-B_1 + \sqrt{(B_1^2 - 4B_2 B_0)}}{2B_2} > 0, \text{and } \tfrac{-B_1 - \sqrt{(B_1^2 - 4B_2 B_0)}}{2B_2} < 0. \end{aligned} \tag{3.35}$$

This implies for $\mathcal{R}_0 > 1$, there exists a unique endemic equilibrium point [9].

4. Sensitivity analysis

This section presents a sensitivity analysis of the basic reproduction number $\mathcal{R}_0$. This analysis aims to identify how model parameter associated with $\mathcal{R}_0$, affects it, as measured by the sensitivity index. The normalized forward sensitivity index to a specific parameter ν is calculated by following formula [31]

$$\Upsilon_\nu^{\mathcal{R}_0} = \frac{\partial \mathcal{R}_0}{\partial \nu} \times \frac{\nu}{\mathcal{R}_0}. \tag{4.1}$$

From (4.1), the sensitivity indices of $\mathcal{R}_0$ with respect to some of the parameters are given below:

$$\begin{aligned} \Upsilon_\beta^{\mathcal{R}_0} &= 1 > 0, \\ \Upsilon_\Pi^{\mathcal{R}_0} &= 1 > 0, \\ \Upsilon_\eta^{\mathcal{R}_0} &= -\tfrac{\eta}{(\eta+\phi+\mu)} < 0, \\ \Upsilon_{\alpha_2}^{\mathcal{R}_0} &= -\tfrac{\alpha_2(\delta+\gamma+\mu)}{(\alpha_2+\mu)(\delta+\gamma+\mu)+\alpha_1(\delta+\mu)} < 0, \\ \Upsilon_\delta^{\mathcal{R}_0} &= \delta\left[\tfrac{1}{(\delta+\gamma+\mu)+(1-\epsilon)\alpha_1} - \tfrac{(\alpha_1+\alpha_2+\mu)}{(\alpha_2+\mu)(\delta+\gamma+\mu)+\alpha_1(\delta+\mu)}\right], \\ \Upsilon_\gamma^{\mathcal{R}_0} &= \gamma\left[\tfrac{1}{(\delta+\gamma+\mu)+(1-\epsilon)\alpha_1} - \tfrac{(\alpha_2+\mu)}{(\alpha_2+\mu)(\delta+\gamma+\mu)+\alpha_1(\delta+\mu)}\right], \\ \Upsilon_\epsilon^{\mathcal{R}_0} &= -\tfrac{\epsilon\alpha_1}{(\delta+\gamma+\mu)+(1-\epsilon)\alpha_1} < 0, \\ \Upsilon_\phi^{\mathcal{R}_0} &= -\tfrac{\phi}{(\eta+\phi+\mu)} < 0. \end{aligned} \tag{4.2}$$

Table 3: The values of sensitivity index of $\mathcal{R}_0$

Parameters	Sensitivity index
β	1
Π	1
η	-0.8065
α_2	-0.4348
δ	-0.2246
γ	+0.1329
ϵ	-0.1667
ϕ	-0.0323

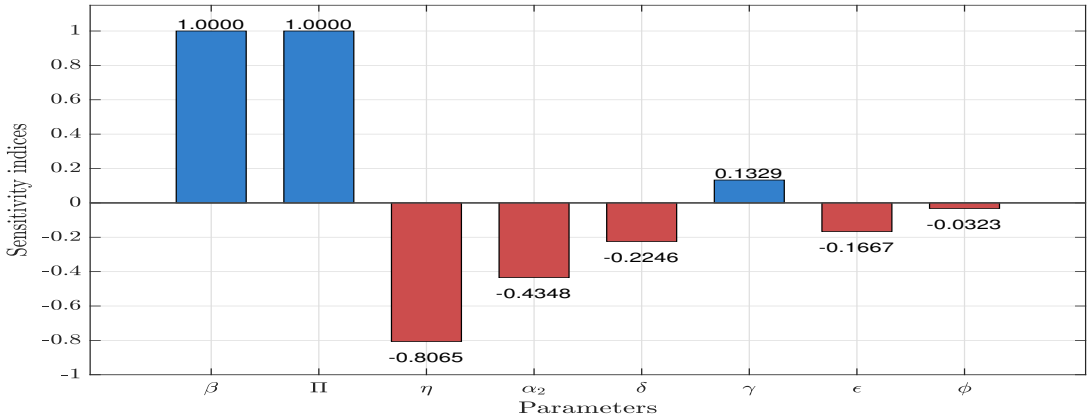


Figure 2: Sensitivity of Parameters towards $\mathcal{R}_0$

The impact of a parameter on $\mathcal{R}_0$ is directly linked to the magnitude of its sensitivity index; the higher the value, the stronger the parameter's effect. The sign of the index also indicates the direction of the impact: a positive index means that increasing the parameter raises $\mathcal{R}_0$, while a negative index suggests that an increase in the parameter lowers $\mathcal{R}_0$. Substituting the parameter values given in Table 2 into the sensitivity formula yields the corresponding sensitivity indices. The results are illustrated in Fig. 2, and the values of the sensitivity indices listed in Table 3.

The parameters that have the most significant impact on $\mathcal{R}_0$ is the quarantine rate η. The result emphasize the crucial role of the quarantine rate in the spread of malware. The value $\Upsilon_{\eta}^{\mathcal{R}_0} = -0.8064$ shows that increasing (decreasing) the quarantine rate by, say, 10%, the $\mathcal{R}_0$ decreases (increases) by 8.064%. Direct adoption of full protection α_2 is more effective at suppressing $\mathcal{R}_0$ than adopting weak protection α_1 makes sense since fully protected nodes are modeled as immune, while weakly protected ones can still be infected. Loss/expiry of weak protection γ is one of the parameter that increases $\mathcal{R}_0$ since it pushes nodes back into the fully susceptible class.

5. Result and discussion

This section presents a numerical investigation of the proposed model (2.1). Using the parameter values listed in Table 1, the basic reproduction number is calculated to be $\mathcal{R}_0 = 0.3261$, which is less than unity. This result suggests that malware cannot sustain itself within the network, and the system converges toward the malware-free equilibrium $E_0 = (0.8696, 0.3478, 2.7826, 0, 0, 0)$ over time.

Next, setting $\Pi = 0.5, \beta = 0.5, \eta = 0.25$, while holding all other parameters fixed, the reproduction number rises to $\mathcal{R}_0 = 4.2076$, exceeding unity. This implies that malware persists within the network, and the model admits a unique, stable endemic equilibrium $E = (0.5462, 0.1476, 1.5352, 1.4410, 0.5146, 5.8155)$. Now, we consider the initial values of the state variables as $S(0) = 32, P_1(0) = 6, P_2(0) = 6, I(0) = 6, Q(0) = 0, R(0) = 0$

Figs. 3 and 4 present the time evolution of the model solution about the equilibrium point for the cases $\mathcal{R}_0 < 1$ and $\mathcal{R}_0 > 1$, respectively. Fig. 3 shows that the susceptible nodes decline sharply over the first few time units before recovering slightly and settling at the positive equilibrium state. Weakly protected nodes follow a similar pattern: rapid depletion as nodes migrate to full protection or revert to the susceptible class, followed by a small rebound as inflow from S resumes, and stabilize. The fully protected nodes declining steadily throughout, with the rate of decline slowing as the susceptible and weakly protected compartments themselves approach equilibrium. The infected nodes increase intially and reachingit peak collapsing rapidly and become stable, reflecting the fact that quarantine and recovery outpace new infections. This underscores the importance of a quarantine rate and a prompt security response in preventing malware from becoming established. Quarantined nodes rising as the initial infection is detected and isolated, then declining to zero in step with. Recovered nodes, which initially increases as infection and quarantne are high and then decline and become stable.

Fig. 4 shows the susceptible nodes collapsing to a very low level almost immediately, and no rebound of the kind observed in the $\mathcal{R}_0 < 1$. The weakly protected nodes exhibiting the same behavior. Fully protected nodes declining continuously across the entire simulation after the slight increase in the statring. Ffter reaching the peak the infected nodes decline from their initial value but, in contrast to infected class in Fig. 3, flattening at a small yet strictly positive plateau near $I* = 1.4410$ rather than vanishing this, indicating that malware persists in the network at a low but steady prevalence. These results illustrate the central threshold behavior of the model whenever the effective transmission pressure keeps $\mathcal{R}_0$ below unity, the network self-clears and returns to the malware-free state, once $\mathcal{R}_0$ exceeds unity, the network instead settles into the persistent endemic state.

Fig. 5 illustrates the effect of the quarantine rate η on the infected, quarantined, and recovered compartments when $\mathcal{R}_0 > 1$. As η increases, the peak of $I(t)$ drops sharply and the infected population is driven toward steady state much faster. Quarantined $Q(t)$ shows a higher, earlier peak for larger η as more infected nodes are being intercepted, while the recovered node rises modestly with η since more nodes pass through quarantine-driven recovery. Fig. 6 shows the effect of the direct full-protection adoption rate α_2 on $I(t)$ and $R(t)$. Variation in α_2 over the range $0.1 - 0.5$ produces a marginal change in the infected and recovered curves.

To examine the combined influence of model parameters on the spread of malware, a sensitivity analysis of $\mathcal{R}_0$ is performed shown via contour and surface (3D) plots. As illustrated in Fig. 7, the joint variation of β with α_2 shows that increase in malware transmission rate leads to a significant increase in $\mathcal{R}_0$, while the increase in direct adoption of full protection suppresses it. A similar but stronger reduction in $\mathcal{R}_0$ is observed when the quarantine rate η is increased simultaneously with changes in β in Fig. 8. The (α_2 and η surface further indicates that simultaneous strengthening of complete protection and quarantine can substantially reduce the reproduction number $\mathcal{R}_0$ of malware shown in Fig. 9. The combined effect of δ and α_2 shown in Fig. 10. Fig. 11 shows that improving the effectiveness of weak protection ϵ and speeding up quarantine η can significantly reduce the reproduction potential of the malware. The surface and contour plots relating to γ and δ in Fig. 12 also show how important it is to control the loss of weak protection while encouraging the upgrading of weakly protected nodes to full protection. Overall, this analysis indicates that it is important to keep transmission low, improve protection effectiveness, increasing full-protection adoption and upgrading rates, and accelerating quarantine as all these measures together are essential for maintaining $\mathcal{R}_0$.

5.1 Deep Neural Network approach for Malware Dynamics

Reasons to utilize DNN in the present research include the necessity to have a computationally inexpensive and accurate surrogate model capable of emulating the nonlinear dynamics of malware spread. The use of conventional computational methods guarantees accuracy but demands iteratively solving the problem for every simulation. On the contrary, after training, the DNN model gives instant predictions and, thus, is ideal for real-time applications in cybersecurity. Also, DNN is known for its capability to detect complex patterns and relations in high-dimensional data, which makes it able to emulate the interaction of compartments regard-

less of whether one knows the math behind them or not. We use a feedforward neural network (Deep neural network) as a quick stand-in for the proposed model (2.1). In this section, we evaluated the model under consideration using the deep neural network approach. The dynamics of the quarantined compartment $Q(t)$ and infected compartment $I(t)$ were approximated using a multi-layer feedforward neural network with five hidden layers. The network architecture is composed of four hidden layers, each with 20, 15, 10, and 5 neurons; an input layer with 12 neurons (matching to the constructed features); and an output layer with two neurons that represent the two target variables, $I(t)$ and $Q(t)$. All hidden layers utilized the hyperbolic tangent (`tansig`) activation function to add non-linearity, and the output layer used a linear (`purelin`) activation function for regression. In order to strike a compromise between model complexity and generalization capacity, this design was chosen empirically. The network architecture is summarized in Table 4 and illustrated in Fig. (13). The Levenberg-Marquardt backpropagation technique (`trainlm`), whose robustness and quick convergence make it ideal for medium-sized regression problems, was used to train the network. The Levenberg-Marquardt approach is especially useful for minimizing the mean squared error (MSE) loss function because it combines the benefits of gradient descent and the Gauss-Newton algorithm. After 936 epochs, the training procedure was stopped when the final gradient magnitude was 6.83×10^{-6} and the performance condition of MSE $\leq 1 \times 10^{-10}$ was met. The dataset comprising 500 time points (sampled from $t = 0$ to $t = 40$) was partitioned using a manual index-based division to ensure appropriate representation across training, validation, and testing phases. Specifically, 70% (350 samples) of the data was allocated for training, 15% (75 samples) for validation, and 15% (75 samples) for testing. The validation set was utilized for early stopping to prevent overfitting, while the test set provided an unbiased evaluation of the model's generalization performance. The network architecture is summarized in Table (4) and illustrated in Fig. (13). The Levenberg-Marquardt backpropagation technique (`trainlm`), whose robustness and quick convergence make it ideal for medium-sized regression problems, was used to train the network. The Fig. (15) shows the graphical representation of the comparison of actual $(ODE - 45)$ and DNN prediction for the compartment $I(t)$ and $Q(t)$ along with the prediction error and relative error for both the compartments of the model (2.1). Fig. (16) and (18) shows the neural network's training progress. At epoch 936, the network reached convergence with a final MSE of 9.94×10^{-11}, a gradient magnitude of 6.83×10^{-6}, and a mu value of 1×10^{-8}. The Levenberg-Marquardt algorithm's effectiveness for this regression job was demonstrated by the training, which was finished in two minutes and ten seconds. The performance requirement of MSE $\leq 1 \times 10^{-10}$ was effectively fulfilled. The regression plots for both compartments are shown in Fig. (17), which illustrates the relationship between actual and predicted values. The Fig. (19) shows the absolute error between ODE45 solution and DNN predication. The promise of deep learning as a computationally effective surrogate model for intricate epidemiological systems is effectively demonstrated by the suggested DNN framework. The method's efficacy in forecasting the dynamics of infected and quarantined compartments is confirmed by the excellent accuracy attained in both interpolation and extrapolation scenarios.

Table 4: Neural Network Architecture Summary

Layer	**Number of Neurons**	**Activation Function**
Input Layer	12	–
Hidden Layer 1	20	`tansig`
Hidden Layer 2	15	`tansig`
Hidden Layer 3	10	`tansig`
Hidden Layer 4	5	`tansig`
Output Layer	2	`purelin`

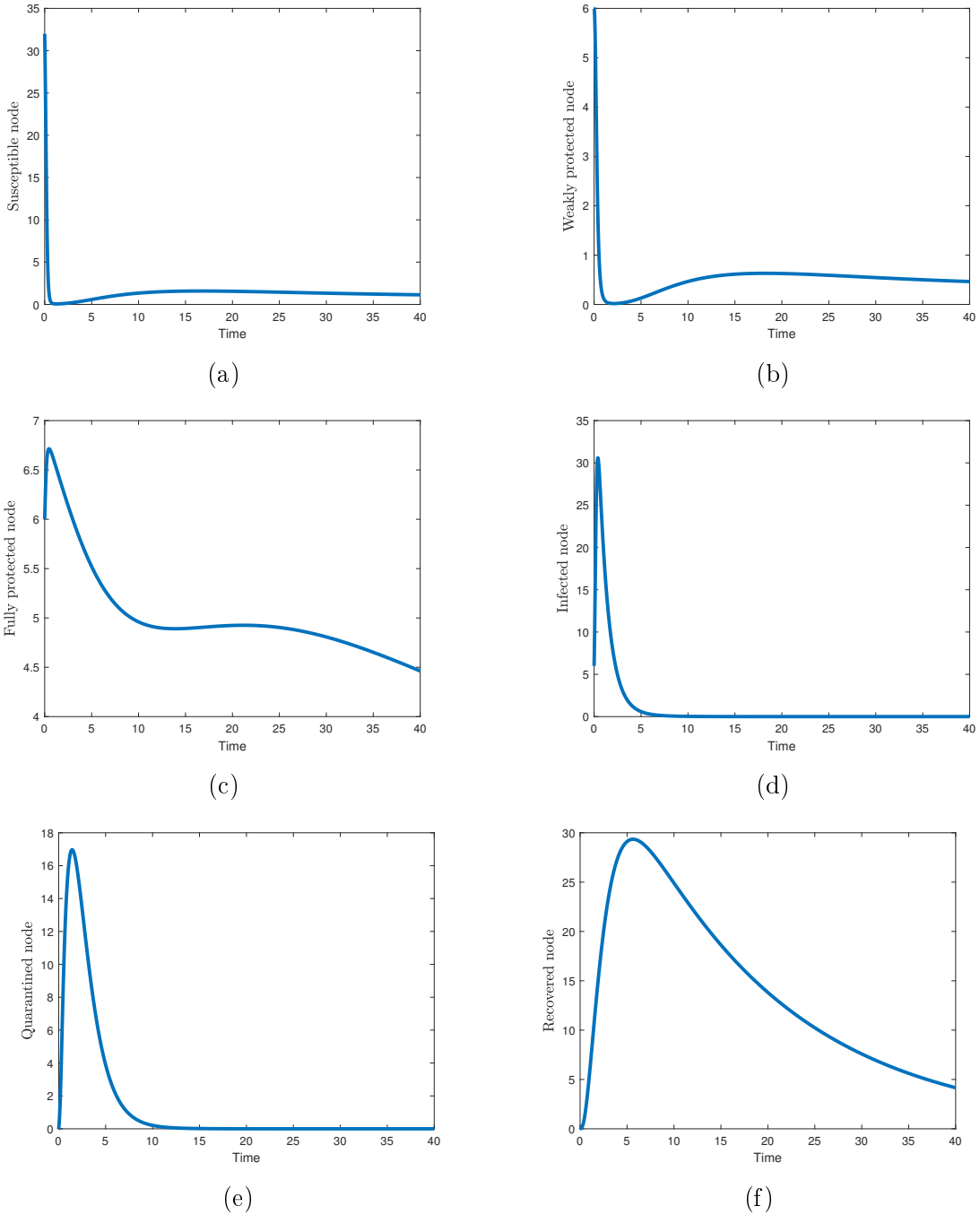


Figure 3: Graphical illustration of malware propagation with time when $\mathcal{R}_0 < 1$

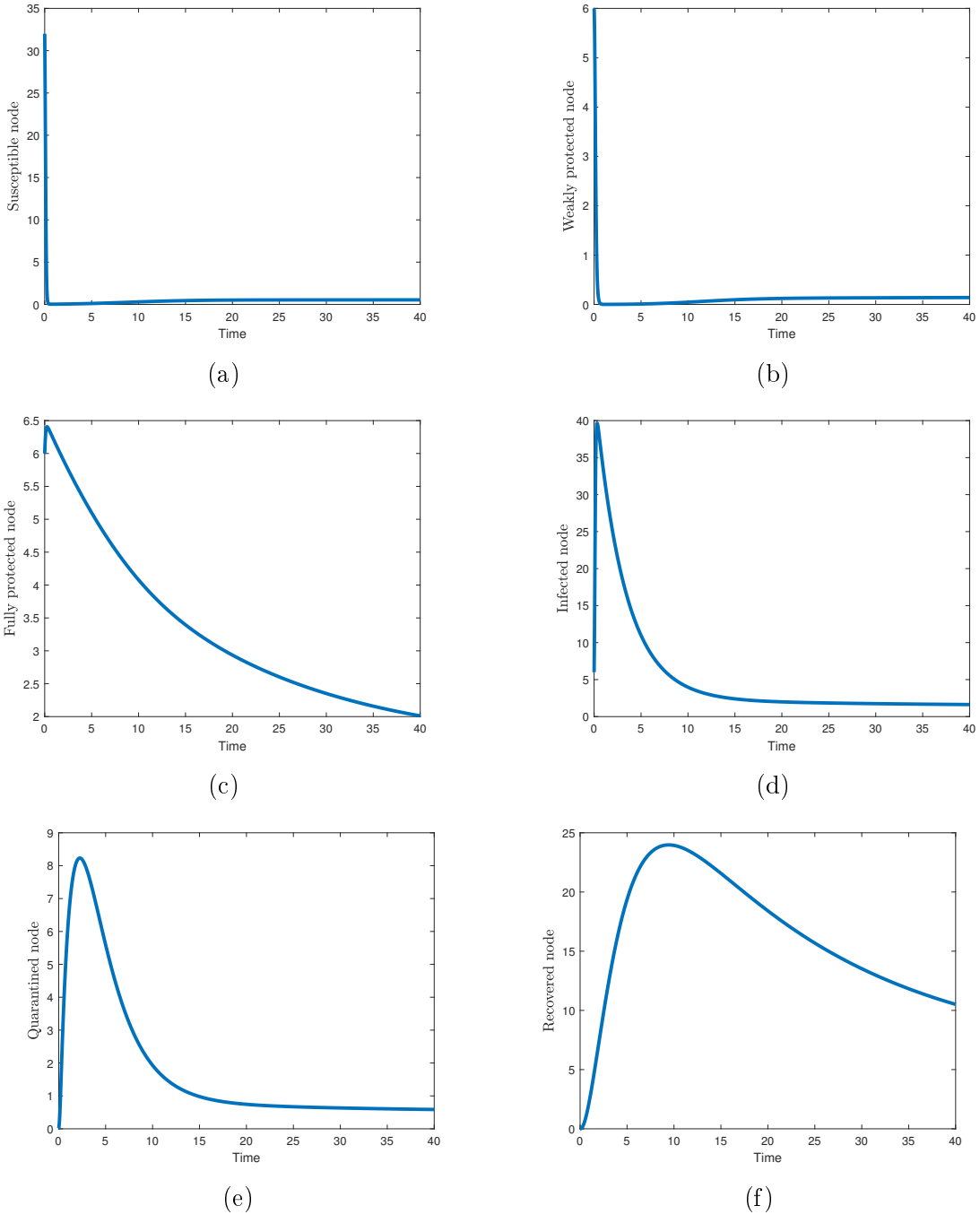
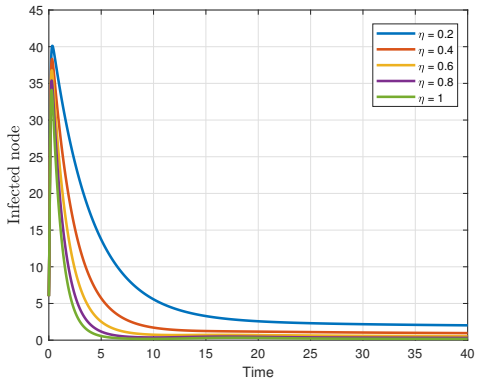
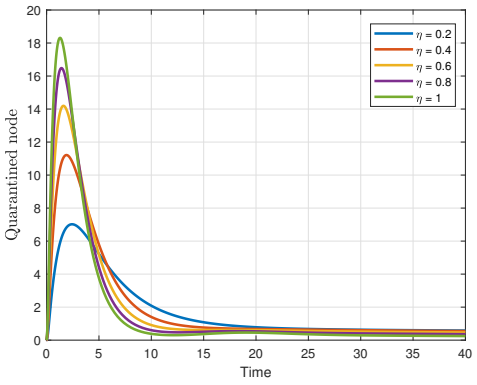


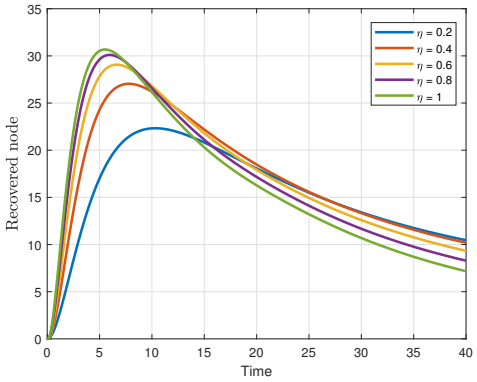
Figure 4: Graphical illustration of malware propagation with time when $\mathcal{R}_0 > 1$



(a) Infected node

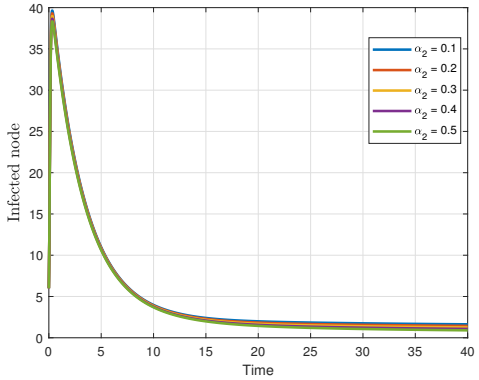


(b) Quarantined node

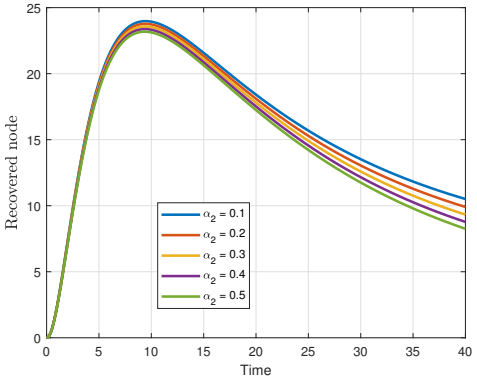


(c) Recovered node

Figure 5: Effect of different values of the quarantine rate η, on infected, quarantined and recovered nodes when $\mathcal{R}_0 > 1$

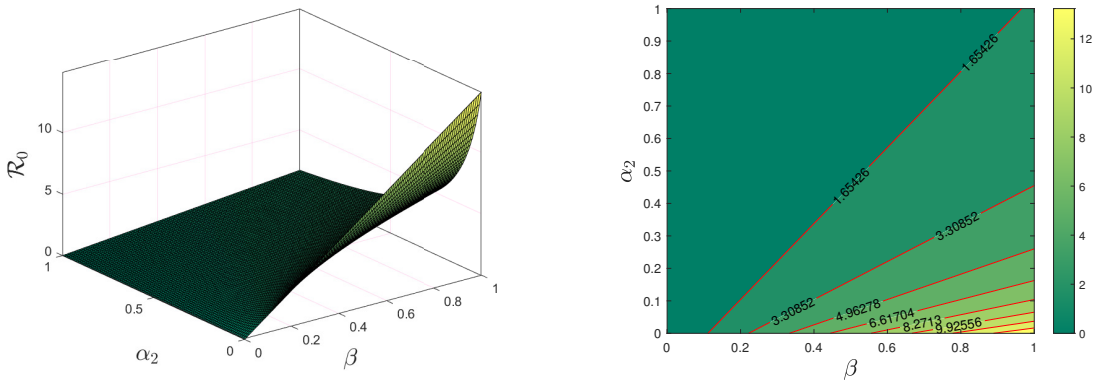


(a) Infected node



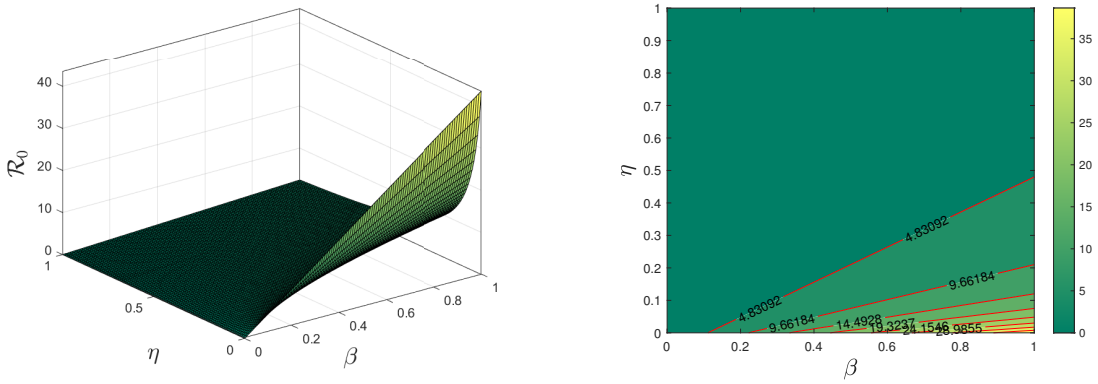
(b) Recovered node

Figure 6: Effect of full-protection adoption rate of α_2 on infected and recovered nodes, when $\mathcal{R}_0 > 1$



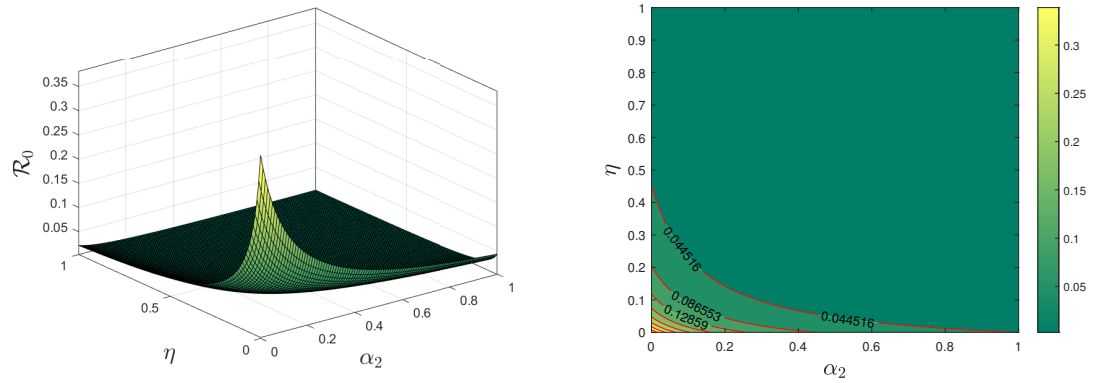
(a) (b)

Figure 7: Effects the parameters β and α_2 on $\mathcal{R}_0$



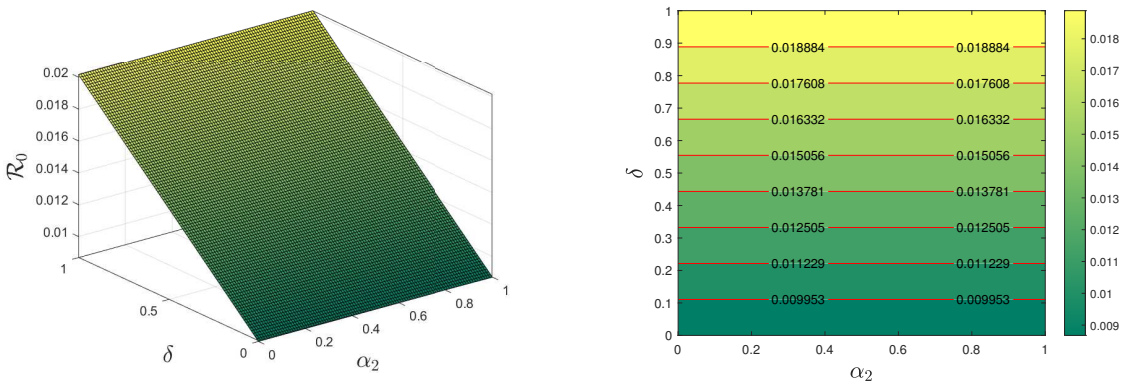
(a) (b)

Figure 8: Effects the parameters β and η on $\mathcal{R}_0$



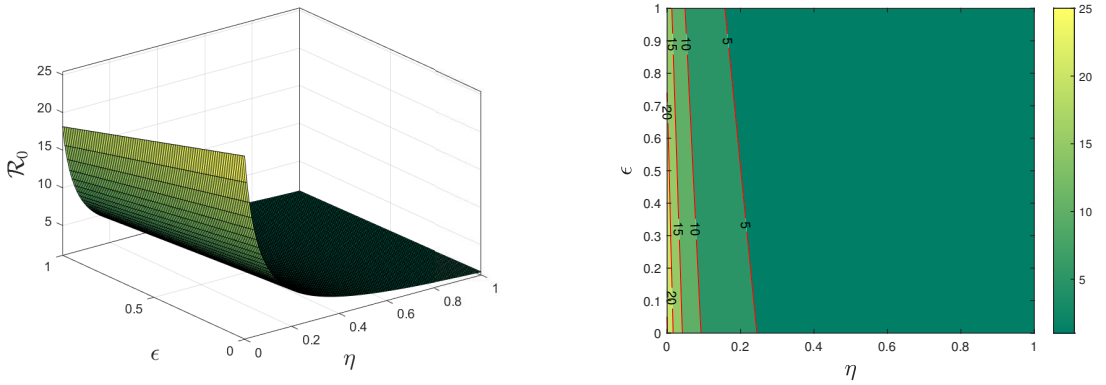
(a) (b)

Figure 9: Effects the parameters α_2 and η on $\mathcal{R}_0$



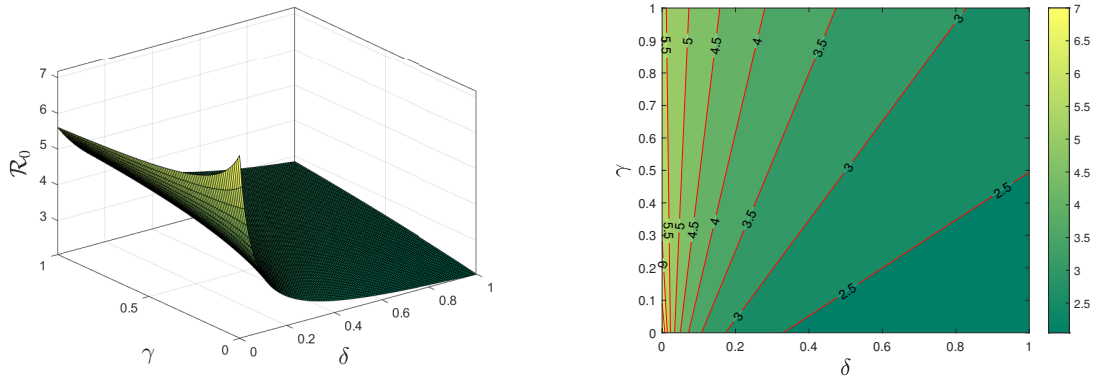
(a) (b)

Figure 10: Effects the parameters α_2 and δ on $\mathcal{R}_0$



(a) (b)

Figure 11: Effects the parameters η and ϵ on $\mathcal{R}_0$



(a) (b)

Figure 12: Effects the parameters δ and γ on $\mathcal{R}_0$

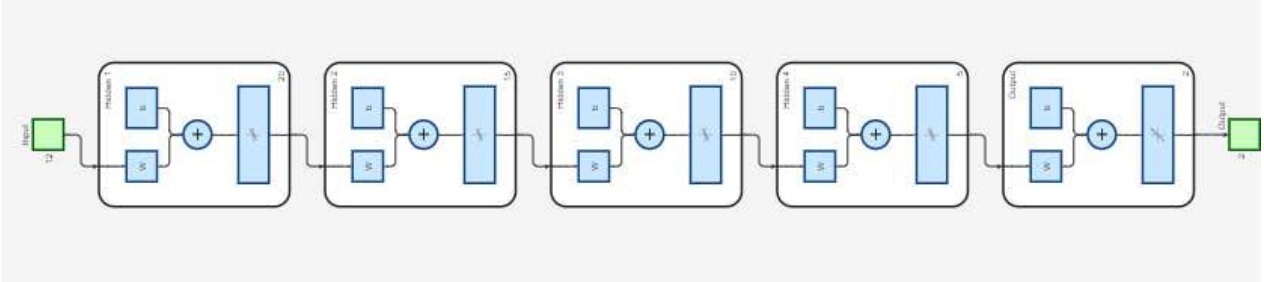


Figure 13: The deep neural network's architecture, displaying each layer's neuron counts and activation functions.

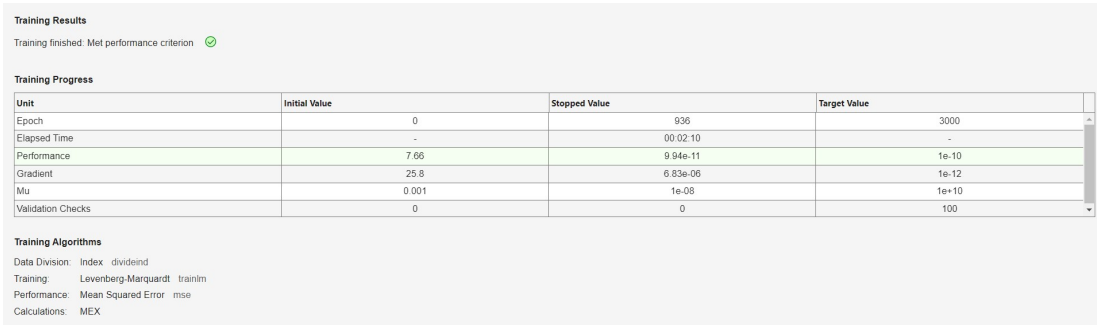


Figure 14: Training progress showing performance (MSE), gradient, and mu values over epochs. The network met the performance criterion at epoch 936.

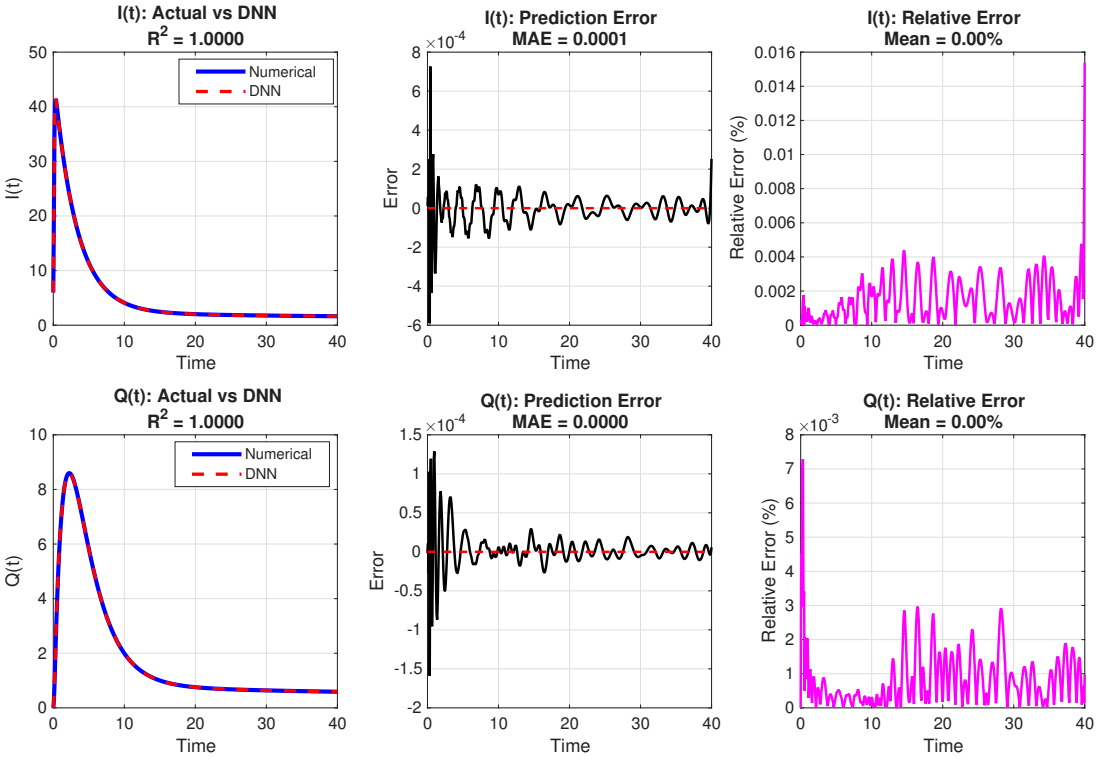


Figure 15: Comparison of DNN-predicted and ODE-45 solutions for the infected $I(t)$ and $Q(t)$ compartments, with prediction errors and relative errors

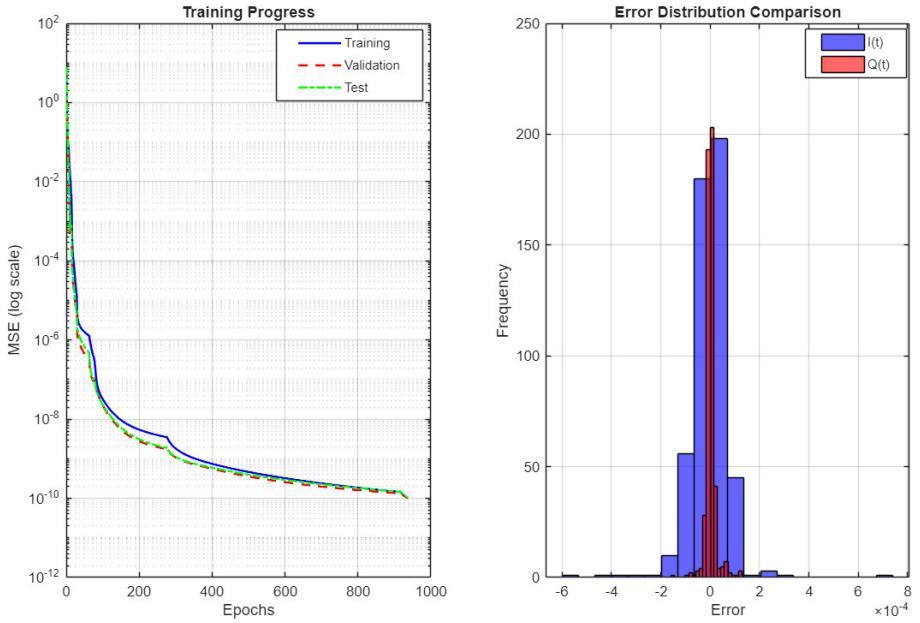


Figure 16: Training progress showing performance (MSE) and error distribution comparison.

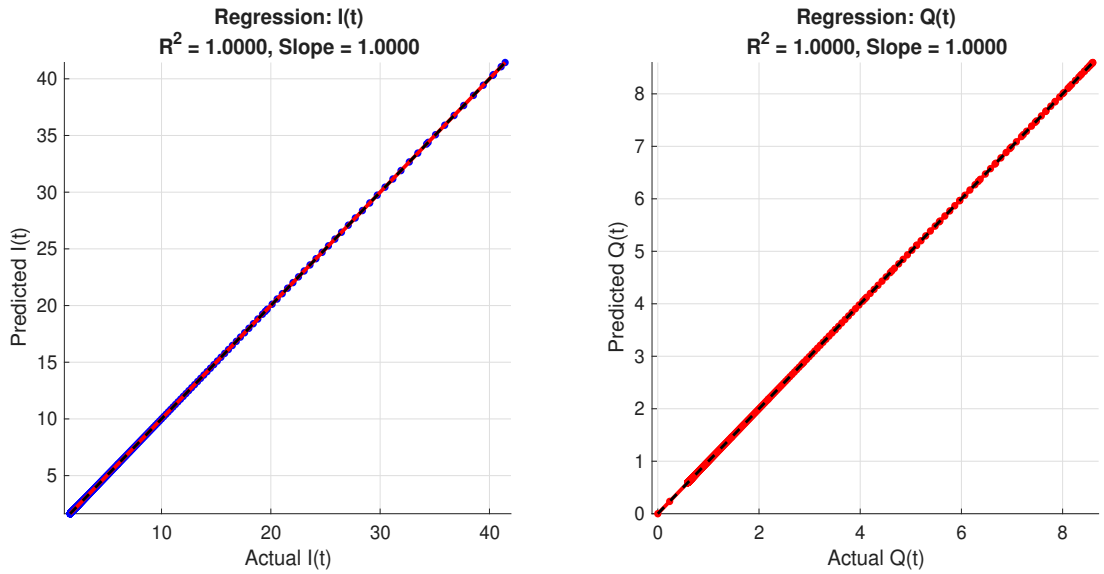


Figure 17: Regression plots of DNN predictions versus ODE-45 solutions for (a) infected $I(t)$ and (b) quarantined $Q(t)$ compartments, showing the correlation between actual and predicted values

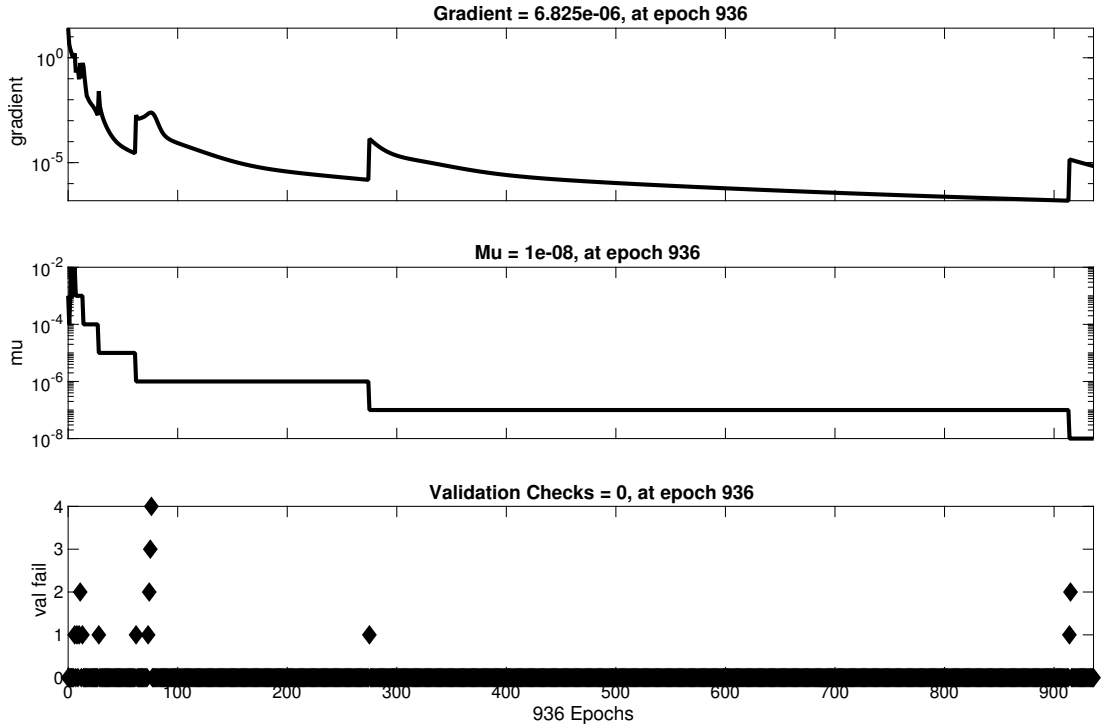


Figure 18: Training process during ANN prediction showing (a) gradient magnitude, mu parameter, and validation checks

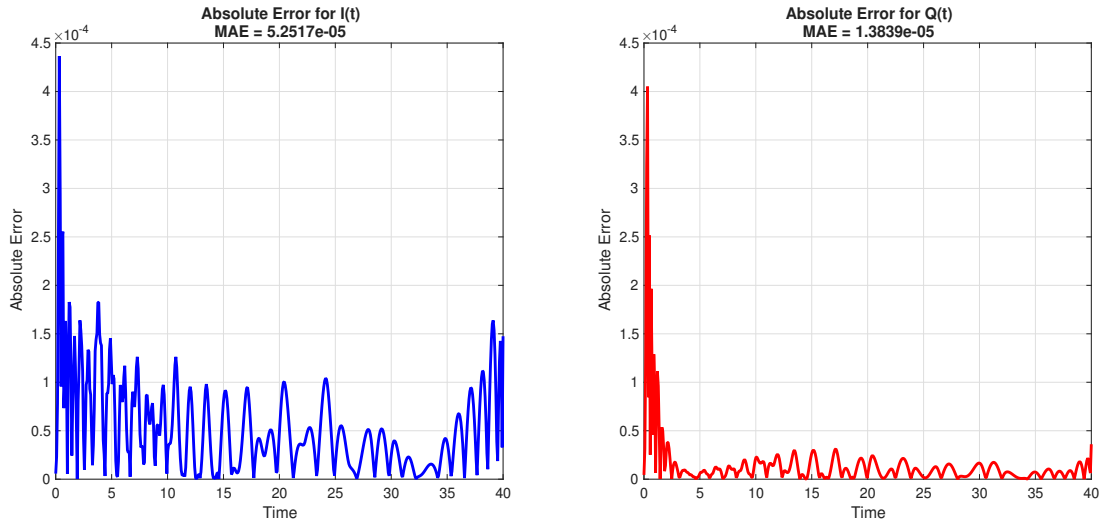


Figure 19: Absolute error between ANN predictions and ODE-45 solutions, showing errors in the order of 10^{-4}

6. Conclusions

This study developed and analyzed a nonlinear six-compartment epidemic-type model to study malware propagation in computer networks under two level of security protection. The model was shown to possess non-negative and bounded solutions, ensuring the mathematical feasibility of the proposed dynamics, while existence and uniqueness of solutions were also established. The basic reproduction number $\mathcal{R}_0$ was obtained as the principal threshold quantity governing malware persistence. The analytical results demonstrate that the malware-free equilibrium is locally asymptotically stable when $\mathcal{R}_0 < 1$, whereas if $\mathcal{R}_0 > 1$, a unique endemic equilibrium exists. The numerical simulations confirm this threshold behavior. The sensitivity analysis reveals the parameters that have the most significant impact on malware transmission. The malware transmission rate β and the network-node entry rate Π have the strongest positive effects on $\mathcal{R}_0$, whereas the quarantine rate η has the strongest negative sensitivity. These findings indicate that rapid quarantine, increased adoption of full protection, and enhanced effectiveness of security software are particularly important intervention mechanisms. Numerical simulations are facilitated by the ode45 approach. This hybrid numerical-DNN framework that has been proposed proves not only the validity of the theoretical model but also serves as an effective knowledge tool in the realm of cybersecurity applications. The findings illustrate the utilization of artificial intelligence in epidemiological modeling techniques and the facilitation of predictive analysis in the area of infectious disease dynamics. The major conclusions that were drawn from the DNN model implementation are:

- The DNN demonstrated an outstanding predictive performance with $R^2 > 0.99$ and MSE of 9.94×10^{-11} for both $I(t)$ and $Q(t)$ classes.
- The Levenberg-Marquardt optimization algorithm demonstrated an efficient training process and was able to converge in 936 epochs (2 minutes 10 seconds).
- The consistency of results obtained during training, validation, and test runs proved the high generalization ability of the model without any overfitting.
- The error analysis showed the robustness of the predictions with the maximal relative errors below 5% for all parameters and confirmed the adequacy of the model as a surrogate one.
- The hybrid approach provides fast and accurate predictions for cybersecurity problems.

The DNN is a powerful prediction tool that effectively captures nonlinearities of the malware spreading model.

Future work may extend the model by incorporating time delays, stochastic network effects, or additional security interventions to represent more realistic and dynamically changing computer-network environments.

Conflict of Interest Statement

The authors declare that they have no conflicts of interest.

Data Availability Statement

The authors can provide the data upon request.

References

[1] Md Mridul Haque Choudhury, Hemen Bharali, Dibakar Dutta, Mathematical analysis of malware propagation in computer networks using an SPIQR epidemic model, *Commun. Math. Biol. Neurosci.*, **2026**, Article ID 34 (2026).

[2] U. Ghani, B. Ahmad, S. Mahmood, A. Flah, M. Ghatasheh, I. Pergl, Nonlinear compartmental modeling of COVID-19 with dual dose vaccination using Mason graphs and variational iteration method, *Scientific Reports*, **16**(1), 4594 (2026).

[3] D. Duan, X. Yang, C. Lv, Z. Cai, Modeling and predicting malware propagation in double-layer computer networks, *IEEE Transactions on Network Science and Engineering*, **13**, 717–727 (2025).

[4] U. Khan, L. Jamel, M.H. Zubair, H.E. Khalifa, S. Aljarboa, Mathematical analysis of computer viruses through deterministic and stochastic models, *Computers & Security*, 104734 (2025).

[5] Z. Zhang, R. Gul, A. Zeb, Global sensitivity analysis of COVID-19 mathematical model, *Alexandria Engineering Journal*, **60**(1), 565–572 (2021).

[6] B.S. Ogundare, J. Akingbade, Boundedness and Stability Properties of Solutions of Mathematical Model of Measles, *Tamkang Journal of Mathematics*, **52**(1), 91–112 (2021).

[7] I. Shah, G. Ali, M. ElAffendi, Cybersecurity-Focused Modeling of Computer Virus Propagation Incorporating Removable Media, *European Journal of Pure and Applied Mathematics*, **18**(4), 6967 (2025).

[8] S.O. Sowole, D. Sangare, A.A. Ibrahim, I.A. Paul, On the existence, uniqueness, stability of solution and numerical simulations of a mathematical model for measles disease, *Int. J. Adv. Math*, **4**, 84–111 (2019).

[9] S.R. Bandekar, M. Ghosh, Mathematical modeling of COVID-19 in India and Nepal with optimal control and sensitivity analysis, *The European Physical Journal Plus*, **136**(10), 1058 (2021).

[10] L. Zhu, H. Zhao, Dynamical analysis and optimal control for a malware propagation model in an information network, *Neurocomputing*, **149**, 1370–1386 (2015).

[11] A. Prajapati, A propagation model of malicious objects via removable devices and sensitivity analysis of the parameters, in *International Conference on Cybersecurity, Cybercrimes, and Smart Emerging Technologies*, pp. 69–84, Springer (2022).

[12] J. Liu, T. Saeed, A. Zeb, Delay effect of an e-epidemic SEIRS malware propagation model with a generalized non-monotone incidence rate, *Results in Physics*, **39**, 105672 (2022).

[13] B.K. Mishra, N. Keshri, Mathematical model on the transmission of worms in wireless sensor network, *Applied Mathematical Modelling*, **37**(6), 4103–4111 (2013).

[14] B.K. Mishra, S.K. Srivastava, B.K. Mishra, A quarantine model on the spreading behavior of worms in wireless sensor network, *Transaction on IoT and Cloud Computing*, **2**(1), 1–12 (2014).

[15] N.H. Khanh, Dynamics of a worm propagation model with quarantine in wireless sensor networks, *Appl. Math. Inf. Sci*, **10**(5), 1739–1746 (2016).

[16] S. Mohanty, P.K. Nayak, S. Mohanty, Quarantine approach to defend against malicious codes in a traditional antivirus computer network, in *International Conference on Energy Systems, Drives and Automations*, pp. 345–353, Springer (2022).

[17] S.R. Biswal, S.K. Swain, Analyze the effects of quarantine and vaccination on malware propagation in wireless sensor network, *Int. J. Innov. Technol. Explor. Eng.*, **8**(10) (2019).

[18] M. Xiao, S. Chen, W.X. Zheng, Z. Wang, Y. Lu, Tipping point prediction and mechanism analysis of malware spreading in cyber–physical systems, *Communications in Nonlinear Science and Numerical Simulation*, **122**, 107247 (2023).

[19] S. Lenhart, J.T. Workman, *Optimal Control Applied to Biological Models*, CRC Press, Boca Raton (2007).

[20] L.S. Pontryagin, V.G. Boltyanskii, R.V. Gamkrelidze, E.F. Mishchenko, *The Mathematical Theory of Optimal Processes*, Interscience Publishers, New York (1962).

[21] H. Behncke, Optimal control of deterministic epidemics, *Optimal Control Applications and Methods*, **21**(6), 269–285 (2000).

[22] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, O. Klimov, Proximal Policy Optimization Algorithms, *arXiv preprint arXiv:1707.06347* (2017).

[23] V. Mnih, K. Kavukcuoglu, D. Silver et al., Human-level control through deep reinforcement learning, *Nature*, **518**, 529–533 (2015).

[24] R.S. Sutton, A.G. Barto, *Reinforcement Learning: An Introduction*, MIT Press, Cambridge (2018).

[25] Z. Alqahtani, M.H. DarAssi, Y. AbuHour, A. Almuneef, Assessing the role of vaccination in the control of hand, foot, and mouth disease transmission, *Mathematics*, **13**(2), 268 (2025).

[26] M. Raissi, P. Perdikaris, G.E. Karniadakis, Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations, *Journal of Computational Physics*, **378**, 686–707 (2019).

[27] L. Zhang, H. Schaeffer, E. Ye, Q. Li, G.E. Karniadakis, Deep learning for dynamical systems: A review, *Mechanical Systems and Signal Processing*, **144**, 106857 (2020).

[28] Y. Wang, Q. Zhang, Q. He, X. Chen, M. Cai, Neural networks for epidemic modeling: A survey, *IEEE Transactions on Neural Networks and Learning Systems*, **32**(8), 3290–3305 (2021).

[29] S. Kumar, S. Kumar, S. Momani, A deep neural network with optimization approach for a nonlinear fractional bird flu model with vaccination and treatment via spectral method, *Knowledge-Based Systems*, **312**, 115259 (2026).

[30] P. Jangir, G. Agarwal, K.S. Nisar, Fractional-order epidemic modeling with a deep neural network framework, *Scientific Reports* (2026).

[31] N. Chitnis, J.M. Hyman, J.M. Cushing, Determining important parameters in the spread of malaria through the sensitivity analysis of a mathematical model, *Bulletin of mathematical biology*, **70**(5), 1272 (2008).

[32] P. Van den Driessche, J. Watmough, Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission, *Mathematical biosciences*, **180**(1-2), 29–48 (2002).

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- RPSIRP.rar