

Modeling the Impact of Cyber Security Measure on Computer Virus Propagation in Institutional Computer Networks in Lafia, Nigeria

¹Abegye Shehu Yakubu, ²Audu.Jonathan Adoga & ³Bitrus Abene

¹Department of Mathematics and Statistics, IMAP, Lafia, Nigeria

^{2,3} Department of Computer Science, IMAP, Lafia, Nigeria

ARTICLE INFORMATION

Article history:

Published: October 2026

Keywords:

ABSTRACT

The frequent dependence of computer networks on institutions has massively promoted computer virus propagation and consequently called for the effective cybersecurity intervention. The study was developed to investigate the impact of cybersecurity measures on computer virus propagation. Six computer populations were considered: susceptible (S), protected (P), exposed (E), infected (I), quarantined (Q), and recovered (R) computers. The study examines the qualitative behavior of the model through equilibrium analysis, stability analysis, computation of the basic reproduction number, and numerical simulations. In order to determine the threshold condition for the computer virus invasion and persistence, the basic reproduction number was obtained by next-generation matrix method. The computer virus free equilibrium point was obtained and was shown to be locally asymptotically stable when the threshold quantity and the global stability was also obtained, proved to be globally asymptotically stable. Numerical simulations were conducted using MATLAB with focused on the modeled key parameters to examine the virus propagation. It was observed that increasing the transmission rate of the virus increases the virus propagation while increasing the cybersecurity effectiveness, quarantine rate and recovery rates helps to control infection. It was also noted that higher recovery rate means that infected computers can be cleaned, repaired, or restored more rapidly. Consequently, the duration for which computers remain infected is reduced, helping to suppress virus propagation throughout the institutional network. It was shown that strengthening cybersecurity protection, improving the timely quarantine of infected computers, and enhancing recovery mechanisms can substantially contribute to controlling computer virus propagation in institutional networks

1. Introduction

Due to the growing advancement of Information and Communication Technology (ICT) has consequently transformed the operations of educational institutions, government agencies, financial organizations, and private enterprises by enabling efficient data storage, communication, and service delivery. The importance of institutional computer networks have become incurable for managing academic records, financial transactions, research activities, online learning platforms, and administrative processes. However, due to the over dependence on interconnected computer systems has exposed the computer networks vulnerability to cyber threats, particularly computer viruses and other forms of malware [5]. Computer viruses are designed software programs that are malicious in nature that can easily infiltrate computer systems, replicate themselves, disrupt normal operations, compromise data integrity, degrade system performance, [2,3,13] and, in severe cases, cause substantial financial and reputational losses [4]. Due to the tremendous growth in Internet, cloud computing, wireless communication, and the Internet of Things (IoT), these viruses have become increasingly sophisticated, causing substantial financial losses, data breaches, and disruption of critical infrastructures [15]. The frequency and sophistication of cyberattacks have continued to increase globally, making cybersecurity an essential component of modern information systems.

Institutional computer networks are particularly attractive targets for cybercriminals because they often contain large volumes of sensitive information while supporting numerous users with varying levels of cybersecurity awareness [8,14]. In many developing countries, including Nigeria, institutions face additional challenges such as inadequate cybersecurity infrastructure, irregular software updates, limited financial resources, insufficient cybersecurity policies, and low levels of user awareness. According to [9,16], these factors create favorable conditions for the rapid spread of computer viruses across institutional networks, resulting in service interruptions, data breaches, unauthorized access, and significant operational disruptions. Consequently, strengthening cybersecurity measures has become a priority for institutions seeking to protect digital assets and maintain reliable network services. Cybersecurity measures such as antivirus software, firewalls, intrusion detection systems, regular security updates, network segmentation, endpoint protection, and the isolation of infected devices play a crucial role in preventing and mitigating the spread of computer viruses. Nevertheless according to [10], these security mechanisms are not always perfectly effective. Newly emerging malware variants, delayed software updates, human error, insider threats, and zero-day vulnerabilities can reduce the effectiveness of existing security controls, allowing malicious software to bypass protection mechanisms and infect previously secured computers. Understanding the interaction between virus transmission dynamics and cybersecurity interventions is therefore essential for

designing effective strategies to reduce cyber risks within institutional environments.

With the traditional cyber security that measures antivirus software, firewalls, intrusion detection systems, regular software patching, network segmentation, that facilitate user awareness campaigns has drastically reduced the impact of malware attacks [6]. However, with the increasing complexity of cyber threats also requires a quantitative framework for understanding how computer viruses spread and how different cyber security strategies influence their propagation.

Yang et al. [17] developed a deterministic mathematical model to investigate the propagation of computer viruses under limited cybersecurity resources. They examined how constraints in available resources influence virus transmission and control within computer networks. The model incorporated resource limitations into the transmission dynamics and analyzed both virus-free and virus-persistent equilibrium states. The analysis was carried out for both qualitative and numerically using MATLAB and Python simulations. The study found that limited cybersecurity resources significantly increase the persistence of computer viruses, whereas improved resource allocation enhances the effectiveness of virus containment strategies. Muthukumar et al. [7] proposed a fractional-order SEIQR malware propagation model for wireless sensor networks. They investigated malware transmission while accounting for memory effects using Caputo fractional derivatives. The authors derived all the basic stability analysis and formulated an optimal control problem with time-dependent interventions. Numerical simulations was conducted and it was shown that optimal control measures substantially reduce infection levels.

Shahini et al. [12] developed a delayed a malware propagation model for cyber-physical systems. Their work incorporated saturated incidence and treatment functions together with time delays representing temporary immunity. The study established the positivity and boundedness of solutions, determined the basic reproduction number, and investigated stability and delay-induced dynamics. Numerical experiments illustrated that time delays significantly influence malware persistence and system behavior. Raza et al. [11] proposed a delayed compartmental model consisting of susceptible, protected (antidotal), exposed, infected, quarantined, and recovered computers. They evaluated the influence of delay strategies and antivirus software on computer virus propagation. The authors established positivity and boundedness of solutions, analyzed virus-free and endemic equilibria, investigated local and global stability using the Routh–Hurwitz criterion and Lyapunov functions, and performed numerical simulations. Their findings showed that delay strategies combined with antivirus software can substantially reduce virus transmission.

The above literatures reviewed shows a substantial progress made on computer virus progression and the application of mathematical modeling approaches. These studies had investigated resource limitations, fractional-order dynamics, delay differential equations, cyber-physical systems, wireless sensor networks, mobile malware awareness, and saturation effects. Most of the literatures did not explicitly examined security updates, protection effectiveness, waning protection, quarantine recovery, or antivirus-based recovery as separate processes. The most recent study examined only one or two cybersecurity interventions at a time, such as resource limitations, awareness campaigns and delay effects. In this study, a deterministic compartmental model that incorporates these major cybersecurity measures within a unified mathematical framework was designed for a institutional computer networks in Lafia, Nigeria. The dynamics considered of six computer populations. It explicitly incorporates important cybersecurity mechanisms, including security updates, imperfect protection effectiveness, loss of protection over time, quarantine of infected computers, and recovery following malware removal. These features enable the model to capture the realistic dynamics of institutional computer networks where security measures reduce, but do not completely eliminate, the risk of malware transmission. The analysis of the model and validate theoretical findings were made through MATLAB simulations.

2. Mathematical Model

2.1 Model Framework

The proposed model describes the dynamics of computer virus propagation in institutional computer networks by partitioning the total computer population, $(N(t))$, into six mutually exclusive compartments: the susceptible computers represented by $S(t)$, protected computers $P(t)$, Exposed computers $E(t)$, infected computers $I(t)$, and Quarantined (isolated) computers denoted by $Q(t)$ and Recovered computers denoted by $R(t)$, where t is time. The entire population size $N(t)$ given by:

$$N(t) = S(t) + P(t) + E(t) + I(t) + Q(t) + R(t) \quad (1)$$

The SPEIQR computer virus model is based on some major assumptions. The total numbers of computers varies due to installation and retirement and available new computers enter the network susceptible to infection. It is assumed that as communication between susceptible and infected computers occurs infections become visible. Susceptible computers migrate to the protected class through cyber security awareness and software updates and infected computers can be disinfected by antivirus. Those infected computers can be isolated from the network and those computer recovered computers leave the system permanently.

Furthermore, Susceptible computers are those to vulnerable to virus infection without adequate cybersecurity protection. New computers enter the network at a constant recruitment rate (installation rate), (Λ) , while susceptible computers become protected through the implementation of cybersecurity measures, such as antivirus software, firewalls, and security updates, at rate (ω) . However, protection may diminish over time due to outdated security software, expired licenses, disabled security features, or the emergence of new malware variants, causing protected computers to return to the susceptible class at rate (α) , Susceptible computers acquire infection through contact with infectious computers at transmission rate (β) , while η is the effectiveness of cybersecurity measures $(0 < \eta < 1)$, representing the proportionate reduction in virus transmission among protected computers. Consequently, only the remaining fraction, $(1 - \eta)$, contributes to breakthrough infections in the protected class. The susceptible and protected computers get infected with computer virus are the rate of $\beta \frac{SI}{N}$ and $\beta(1 - \eta) \frac{PI}{N}$ respectively.

Upon successful transmission, computers first enter the exposed compartment, where the malicious software is present but remains inactive and incapable of spreading to other computers. Exposed computers progress to the infectious class at rate (σ) , representing the activation of the malware. Infectious computers actively propagate the virus throughout the network and may either recover directly following successful malware detection and removal at rate (γ) , or be isolated from the network through quarantine at rate

(δ). Quarantined computers undergo cleaning, repair, and security restoration before rejoining the network as recovered computers at rate (ρ). The recovered compartment consists of computers that have been successfully disinfected and restored to secure operation. Additionally, all compartments experience natural removal from the network at rate (μ), accounting for computer replacement, hardware failure, decommissioning, or permanent disconnection. This compartmental framework enables the assessment of the effectiveness of cybersecurity interventions, including security updates, protection mechanisms, quarantine policies, and malware recovery strategies, in mitigating computer virus propagation within institutional computer networks in Lafia, Nigeria.

2.2 Model Equations

Following the assumptions and the diagram describing the computer model shown below, that the ordinary differential equations for the model are stated as:

$$\begin{cases} \frac{dS}{dt} = \Lambda - \beta \frac{SI}{N} + \alpha P - \omega S - \mu S \\ \frac{dP}{dt} = \omega S - (1-\eta)\beta \frac{PI}{N} - \alpha P - \mu P \\ \frac{dE}{dt} = \beta \frac{SI}{N} + (1-\eta)\beta \frac{PI}{N} - \sigma E - \mu E \\ \frac{dI}{dt} = \sigma E - \gamma I - \delta I - \mu I \\ \frac{dQ}{dt} = \delta I - \rho Q - \mu Q \\ \frac{dR}{dt} = \gamma I + \rho Q - \mu R \end{cases} \quad (2)$$

with initial conditions $(S(0), P(0), E(0), I(0), Q(0), R(0)) \in \mathbb{R}^6$

2.3 Model Diagram

Figure 1 below denotes the transmission of computer virus by represented by arrows.

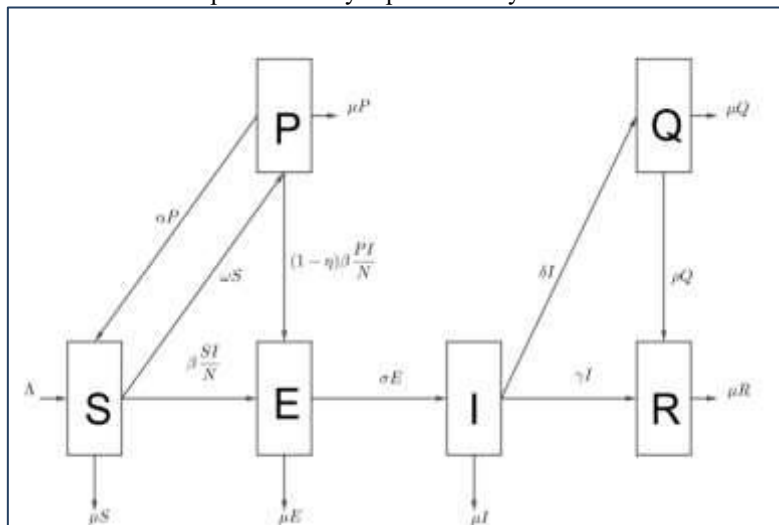


Figure 1: Schematic Diagram of computer model.

Table 1: Parameters Description with Values

Parameters	Description	Values	References
Λ	Installation rate of new computers	8 computers/day	[11]
β	Virus transmission rate	0.65 day ⁻¹	[17]
η	Protection effectiveness	0.85	[11]
ω	Rate of installing security updates	0.08 day ⁻¹	[8]
σ	Progression from exposed to infected	0.25 day ⁻¹	[11]
γ	Antivirus recovery rate	0.20 day ⁻¹	[7]
δ	Quarantine rate	0.15 day ⁻¹	[17]
ρ	Recovery rate from quarantine	0.12 day ⁻¹	[11]
μ	Retirement rate of computers	0.005 day ⁻¹	[17]
α	Loss of protection rate	0.02 day ⁻¹	[11]

2.4 Basic Properties of the Model

For the computer virus transmissions shown in equation 1 to be suitable and meaningful like the usual diseases epidemiological models then it is essential to show that all the state variables are non-negative at time t . This consequently implies that for all time $t \geq 0$ the solutions of equation (2) remain positive.

2.4.1 Positivity of Solutions

Theorem 2.4: If $S_0 \geq 0, P_0 \geq 0, E_0 \geq 0, I_0 \geq 0, Q_0 \geq 0$ and $R_0 \geq 0$, then it follows that equation 2 is non-negative solution for all $t \geq 0$.

Proof: Hence, solving the susceptible population in equation 2 using integrating factor gives:

$$S(t) \geq S(0)e^{-(\omega+\mu)t} \geq 0 \quad (3)$$

Equation 3 connotes that $S(t)$ remains positive as long as $t > 0$. Similarly the solution of the others populations is given as: $P(t) \geq P(0)e^{-(\alpha+\mu)t} \geq 0, E(t) \geq E(0)e^{-(\sigma+\mu)t} \geq 0, I(t) \geq I(0)e^{-(\delta+\mu)t} \geq 0, Q(t) \geq Q(0)e^{-(\rho+\mu)t} \geq 0, R(t) \geq R(0)e^{-\mu t} \geq 0$. This implies that all these populations remains positive as long as $t > 0$. Therefore, the theorem is proved.

2.4.2 Feasible Region

Summing all the ordinary differential equations (ODEs) in equation 2 above, we have $\frac{dN}{dt} = \Lambda - \mu N$ which follows that $N(t) \leq \frac{\Lambda}{\mu}$ by solving the ordinary differential equation obtained from the equation 2. Hence the feasible region is $\Omega = \{(S, P, E, I, Q, R): N \leq \frac{\Lambda}{\mu}\}$, which is positively invariant.

3. Disease – Free Equilibrium and Basic Reproduction Number (BRN)

The disease – free equilibrium of the proposed SPEIQR model is obtained by setting $E = I = Q = R = 0$ and so $S^* = \frac{\Lambda(\alpha+\mu)}{\mu(\omega+\alpha+\mu)}, P^* = \frac{\Lambda\omega}{\mu(\omega+\alpha+\mu)}$. It follows then that the DFE is $E_0 = (S^*, P^*, 0, 0, 0, 0)$. We proceed further to obtain the basic reproduction number using the next generation matrix method was adopted in [1]. Therefore, the basic reproduction number the model is obtained by $\mathcal{R}_0 = \rho(FV^{-1})$ where ρ represent the spectral radius of the matrix for the next generation. Let F represent the Jacobian of $\mathcal{F}_i$ where $\mathcal{F}_i$ denotes the rate of new infection progressing into the compartment i and V represent the Jacobian of $\mathcal{V}_j$ where $\mathcal{V}_j$ is the rate of transfer of infections from infected compartment to another compartment j respectively. Hence,

$$F = \begin{bmatrix} 0 & \beta \frac{(S^* + (1-\eta)P^*)}{N^*} \\ 0 & 0 \end{bmatrix} \text{ and } V = \begin{bmatrix} \sigma + \mu & 0 \\ -\sigma & \gamma + \delta + \mu \end{bmatrix} \text{ so, } \mathcal{R}_0 = \rho(FV^{-1}) = \beta \frac{(S^* + (1-\eta)P^*)}{N^*}$$

$$\mathcal{R}_0 = \frac{\beta\delta[\alpha + \mu + (1 - \eta)\omega]}{\mu(\alpha + \mu)(\omega + \alpha + \mu)(\gamma + \delta + \mu)} \quad (4)$$

Equation (4) shows the expected number of secondary infections caused by one infected computer introduced into a fully susceptible network. The elimination of computer virus becomes possible when $\mathcal{R}_0 < 1$ and persists when $\mathcal{R}_0 > 1$.

3.1 Stability of Computer Disease – Free Equilibrium

In this section we shall examine the nature of stability for the computer virus-free equilibrium of the SPEIQR model at E_0 of the computer virus model

Theorem 1: The SPEIQR model at $E_0 = \left(\frac{\Lambda(\alpha+\mu)}{\mu(\omega+\alpha+\mu)}, \frac{\Lambda\omega}{\mu(\omega+\alpha+\mu)}, 0, 0, 0, 0\right)$ is locally asymptotically stable when $\mathcal{R}_0 < 1$ and unstable if $\mathcal{R}_0 > 1$.

Proof: Using equation 2 and adopting Jacobian matrix at E_0 gives:

$$J_{E_0} = \begin{pmatrix} -(\omega+\mu) & \alpha & 0 & -\beta \frac{S^*}{N^*} & 0 & 0 \\ \omega & (\alpha+\mu) & 0 & \beta \frac{(1-\eta)P^*}{N^*} & 0 & 0 \\ 0 & 0 & -(\sigma+\mu) & \beta \frac{[S^* + (1-\eta)P^*]}{N^*} & 0 & 0 \\ 0 & 0 & \sigma & -(\gamma+\delta+\mu) & 0 & 0 \\ 0 & 0 & 0 & \delta & -(\rho+\mu) & 0 \\ 0 & 0 & 0 & \gamma & \rho & -\mu \end{pmatrix} \quad (5)$$

The characteristic equation is computed using $\det(J_{E_0} - \lambda I)$. It can be observed that equation 5 block lower triangular matrix therefore; the eigenvalues can be obtain as $\det(J_{E_0} - \lambda I) = \det(A) \det(B)$ where

$$A = \begin{pmatrix} \lambda + \sigma + \mu & -\alpha \\ -\omega & \lambda + \alpha + \mu \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} \lambda + \sigma + \mu & -\kappa & 0 & 0 \\ -\sigma & \lambda + \gamma + \delta + \mu & 0 & 0 \\ 0 & -\delta & \lambda + \rho + \mu & 0 \\ 0 & -\gamma & -\rho & \lambda + \mu \end{pmatrix}$$

where $\kappa = \beta \frac{(S^* + (1-\eta)P^*)}{N^*}$. Then the eigenvalues of the infected block can be obtained by $\det(A) = 0 \Rightarrow \lambda^2 + (\omega + \alpha + 2\mu)\lambda + \mu(\omega + \alpha + \mu) = 0$ (6)

Since $\omega, \alpha, \mu > 0$ all coefficients are positive and by quadratic formula both eigenvalues satisfy $\mathcal{R}(\lambda) < 0$. Examining the eigenvalues of the infected block with the infected subsystem (E,I) :

$$\begin{pmatrix} -(\sigma + \mu) & \kappa \\ \sigma & \gamma + \delta + \mu \end{pmatrix}. \text{ It then follows that the characteristic equation is given by } \lambda^2 + a_1\lambda + a_2 = 0 \quad (7)$$

Where $a_1 = \sigma + \gamma + \delta + 2\mu, a_2 = (\sigma + \mu)(\gamma + \delta + \mu) - \sigma\kappa$, hence,

$$a_2 = (\sigma + \mu)(\gamma + \delta + \mu)(1 - \mathfrak{R}_0) \quad (8)$$

Now using the Routh-Hurwitz criterion (RHC) for equation 5, it states that all roots have negative real parts if $a_1 > 0$ and $a_2 > 0$ since $a_1 > 0$ always and $a_2 > 0 \Leftrightarrow \mathfrak{R}_0 < 1$ the infected subsystem is locally asymptotically stable whenever $\mathfrak{R}_0 < 1$. Furthermore,

examining the remaining eigenvalues, $-(\rho + \mu)$ and $-\mu$ can be seen that the two values were both negatives. Therefore, every eigenvalues of J_{E_0} has a negative real part whenever $\mathfrak{R}_0 < 1$. Hence, the disease-free equilibrium is locally asymptotically stable whenever $\mathfrak{R}_0 < 1$ and unstable whenever $\mathfrak{R}_0 > 1$. This complete the proof. $\square$

3.2 Existence and uniqueness of the Endemic Equilibrium

In considering the endemic of the model, then let $E^* = (S^*, P^*, E^*, I^*, Q^*, R^*) \neq 0$. Then solving equation 2 in terms of the infected populations of computer virus by evaluating the necessary conditions for existence at the equilibrium point using equation 2, we have the following:

$$E^* = \frac{\gamma + \delta + \mu}{\sigma} I^*, Q^* = \frac{\delta}{\rho + \mu} I^*, R^* = \frac{1}{\mu} \left(\gamma + \frac{\rho\delta}{\rho + \mu} \right) I^*, P^* = \frac{\omega S^*}{(\alpha + \mu) + \beta(1-\eta) \frac{I^*}{N^*}}, S^* = \frac{\Lambda + \alpha P^* - \beta \frac{S^* I^*}{N^*}}{\alpha + \mu}$$

To determine I^* by taking the sum of the population of computers and substituting E^*, Q^*, R^* then,

$$N^* = S^* + P^* + C I^* \quad (9)$$

$$C = 1 + \frac{\gamma + \delta + \mu}{\sigma} + \frac{\delta}{\rho + \mu} + \frac{1}{\mu} \left(\gamma + \frac{\rho\delta}{\rho + \mu} \right)$$

Where

$$E^* = \left(S^*, P^*, \frac{\gamma + \delta + \mu}{\sigma} I^*, I^*, \frac{\delta}{\rho + \mu} I^*, \frac{1}{\mu} \left(\gamma + \frac{\rho\delta}{\rho + \mu} \right) I^* \right) \quad (10)$$

Therefore, the endemic equilibrium is

3.3 Global Stability of the model

Theorem 2: The disease was considered to exist at equilibrium point if $\mathfrak{R}_0 > 1$ and said to be globally stable.

Proof: We defined a Lyapunov function as:

$$L = E + X I \quad (11)$$

$$X = \frac{\sigma}{\gamma + \delta + \mu}$$

where

$$\dot{L} \leq (\gamma + \delta + \mu)(\mathfrak{R}_0 - 1) I$$

Hence, if $\mathfrak{R}_0 < 1$, and obviously $\dot{L} \leq 0$ with equality only at the computer disease-free equilibrium (DFE). By Lasalle's Invariance Principle, the DFE is globally asymptotically stable.

4. Numerical Simulation

The numerical simulation of the computer model was performed using MATLAB to study the behavior of the system by varying key parameters. This was done by comparing cybersecurity scenarios to investigate different intervention strategies to control the

spread of computer virus among computers networks. The model developed connotes computer dynamics within institutions in Lafia (Federal University of Lafia, Isa Mustapha Agwai I Polytechnic, College of Agriculture, Science and Technology, government offices, banks, cyber cafés.). Although there is no comprehensive empirical data on malware transmission and cybersecurity rates in Lafia, however the parameter values were obtained from literatures. The initial conditions for Lafia focuses on a medium-sized institutional network obtained from the documentary record made in Lafia these were:. The initial conditions with the parameters values shown in table 1 were used for the simulations to $S(t) = 100, P(t) = 200, E(t) = 50, I(t) = 30, Q(t) = 10, R(t) = 10$ produce the graphs shown below.

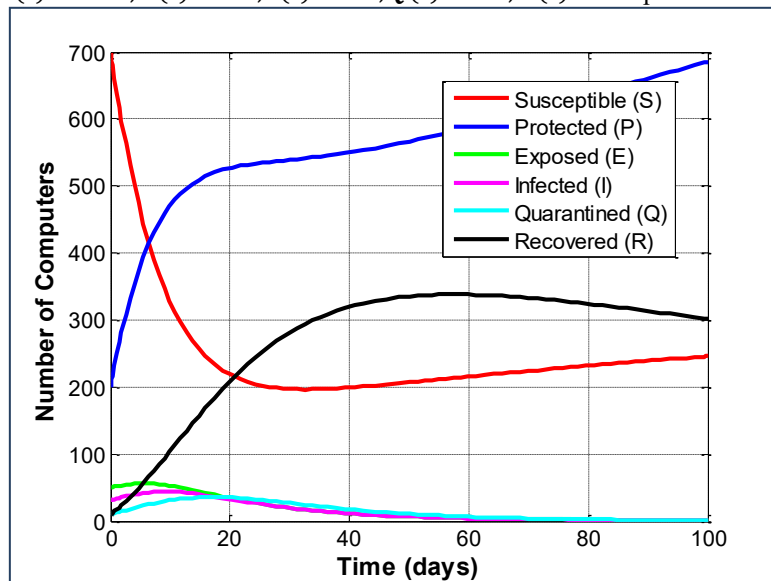


Figure 1: The plots of the entire population of computer against time

Figure 1 presents the numerical simulation of the six-compartment cybersecurity computer-virus model over a period of 100 days. The figure shows the temporal changes in susceptible (S), protected (P), exposed (E), infected (I), quarantined (Q), and recovered (R) computers. Starting from the initial populations $S=700, P=200, E=50, I=30, Q=10$, and $R=10$, the compartments change dynamically due to virus transmission, cybersecurity protection, infection, recovery, and quarantine. The simulation is based on a cybersecurity effectiveness of 0.80 and transmission rate 0.65. Overall, the figure illustrates how the different computer classes evolve over time under the specified cybersecurity conditions.

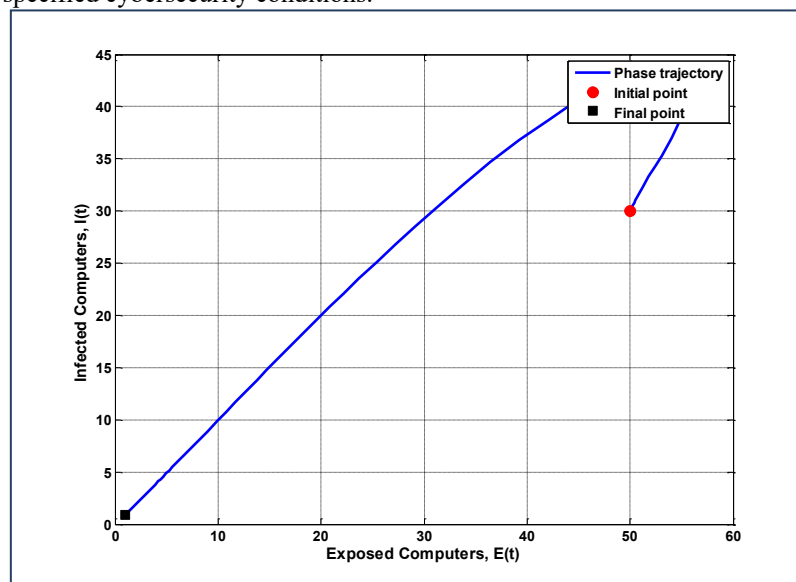


Figure 2; The phase plot between infected against exposed computers

Figure 2 presents the phase-plane relationship between the infected computers $I(t)$ and the exposed computers $E(t)$. The horizontal axis represents the number of exposed computers, while the vertical axis represents the number of infected computers. The trajectory shows how changes in the exposed computer population are associated with changes in the infected population over time. Since exposed computers progress to the infected class at the rate σ , an increase in $E(t)$ can lead to an increase in $I(t)$. The trajectory therefore provides a visual representation of the interaction between the exposed and infected classes as the system evolves. The red circle represents the initial condition, $E(0)=50$ and $I(0)=30$, while the black square represents the final state of the simulation. The movement of the trajectory toward the final state indicates the evolution of the infection dynamics under the specified parameter values, including 80% cybersecurity effectiveness ($\eta=0.80$) and transmission rate $\beta = 0.65$. It follows that, the phase plot helps to assess whether the exposed and infected computer populations tend toward a stable equilibrium as time increases.

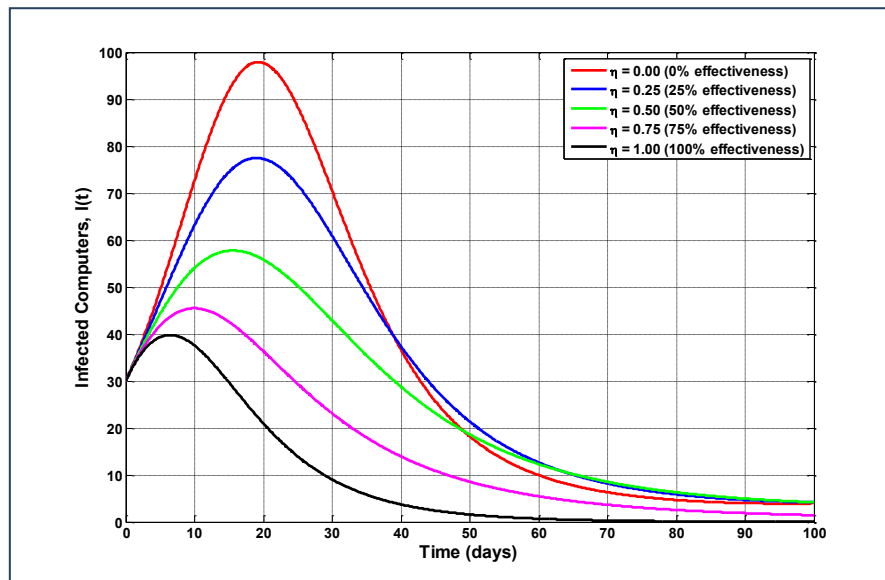


Figure 3: Illustrate the effect of varying cyber-security on infected computers

Figure 3 illustrates the effect of cybersecurity effectiveness η on the infected computer population $I(t)$ over time. Five levels of cybersecurity effectiveness are considered: $\eta=0.00, 0.25, 0.50, 0.75$, and 1.00 , representing 0%, 25%, 50%, 75%, and 100% effectiveness, respectively. The figure shows that increasing cybersecurity effectiveness generally reduces the number of infected computers. The trajectory corresponding to $\eta = 0.00$ represents the situation with no cybersecurity protection, while increasing η progressively suppresses virus propagation. The $\eta=1.00$ scenario represents complete effectiveness and produces the strongest control of infection. Thus, the simulation demonstrates that enhancing cybersecurity measures can reduce the spread and persistence of computer viruses within the network.

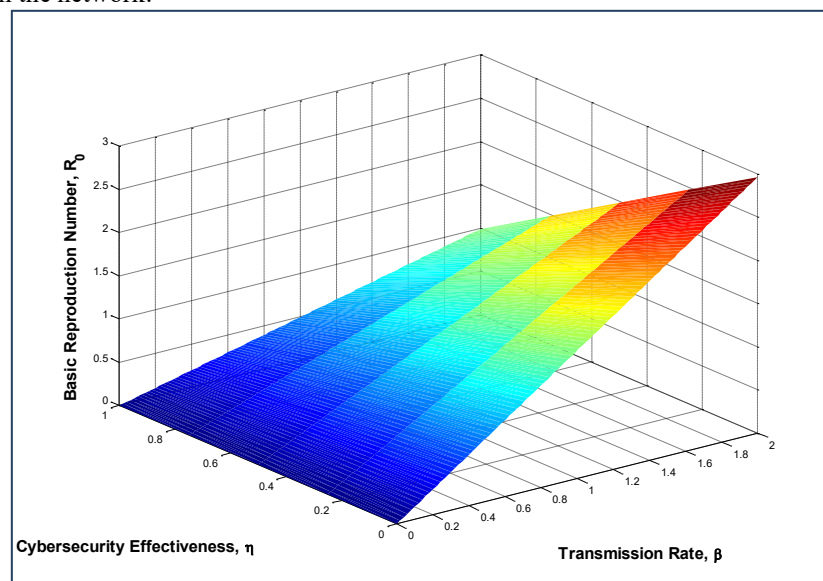


Figure 4; The surface plot of combine effect of β and η on $\mathcal{R}_0$

The 3D surface plot illustrates the combined effects of the transmission rate (β) and cybersecurity effectiveness (η) on the basic reproduction number ($\mathcal{R}_0$). The transmission rate β is represented on the x-axis, cybersecurity effectiveness η on the y-axis, and $\mathcal{R}_0$ on the z-axis. The cybersecurity effectiveness is varied at $\eta=0.00, 0.25, 0.50, 0.75$, and 1.00 , representing 0%, 25%, 50%, 75%, and 100% cybersecurity effectiveness, respectively. The plot shows that, for each of these values of η , increasing the transmission rate β results in an increase in $\mathcal{R}_0$. However, as cybersecurity effectiveness increases from $\eta = 0.00$ to $\eta = 1.00$, the corresponding value of $\mathcal{R}_0$ decreases. Thus, the surface demonstrates that weak or absent cybersecurity protection ($\eta = 0.00$) is associated with higher values of $\mathcal{R}_0$, while stronger cybersecurity protection ($\eta = 0.75$ and $\eta = 1.00$) substantially reduces $\mathcal{R}_0$. Therefore, increasing cybersecurity effectiveness can help suppress computer-virus propagation, particularly when the transmission rate is high.

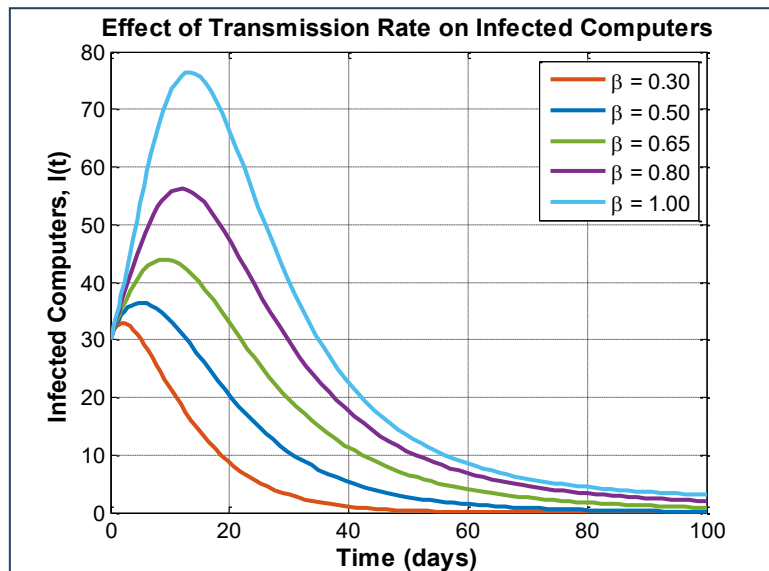


Figure 5: The plot showing the effect of varying the effect of transmission rate on infected computers

Figure 5 shows the effect of varying the transmission rate β on the infected computer population $I(t)$. The simulations were performed for $\beta = 0.30, 0.50, 0.65, 0.80$, and 1.00 , while keeping the other parameters constant. The results show that increasing the transmission rate generally leads to a higher infected computer population. This indicates that faster transmission of computer viruses increases the spread and persistence of infection within the network.

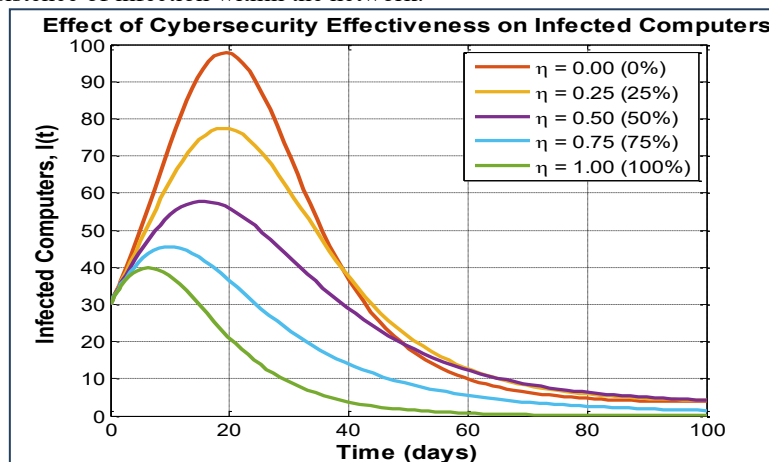


Figure 6: The plot showing the effect of cybersecurity effectiveness by varying eta

Figure 6 illustrates the effect of cybersecurity effectiveness on the infected computer population. Five effectiveness levels, $\eta = 0, 0.25, 0.50, 0.75$, and 1.00 , were considered. The simulation indicates that increasing cybersecurity effectiveness reduces virus propagation and consequently lowers the infected computer population. Thus, stronger cybersecurity protection plays an important role in controlling the spread of computer viruses.

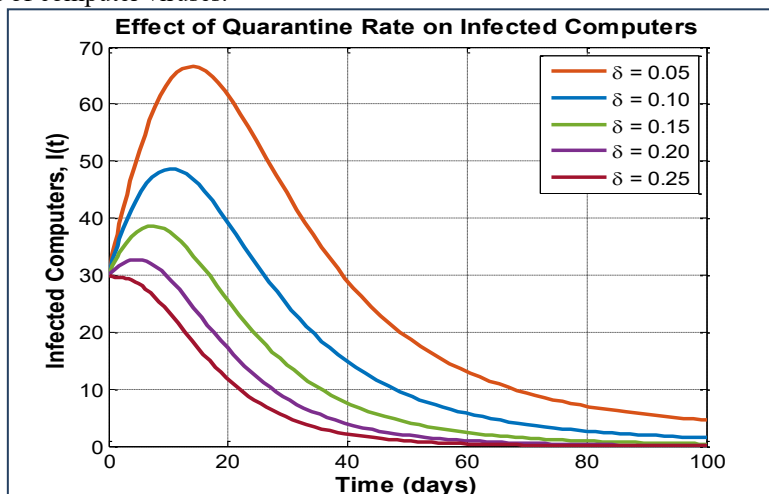


Figure 7: Illustrating the effect of Quarantine rate on infected computers

Figure 7 presents the effect of the quarantine rate δ on infected computers. The simulations considered $\delta=0.05, 0.10, 0.15, 0.20$, and 0.25 . Increasing the quarantine rate generally reduces the number of infected computers because infected computers are transferred more rapidly from the infected class to the quarantined class. This demonstrates the importance of timely isolation in controlling virus propagation.

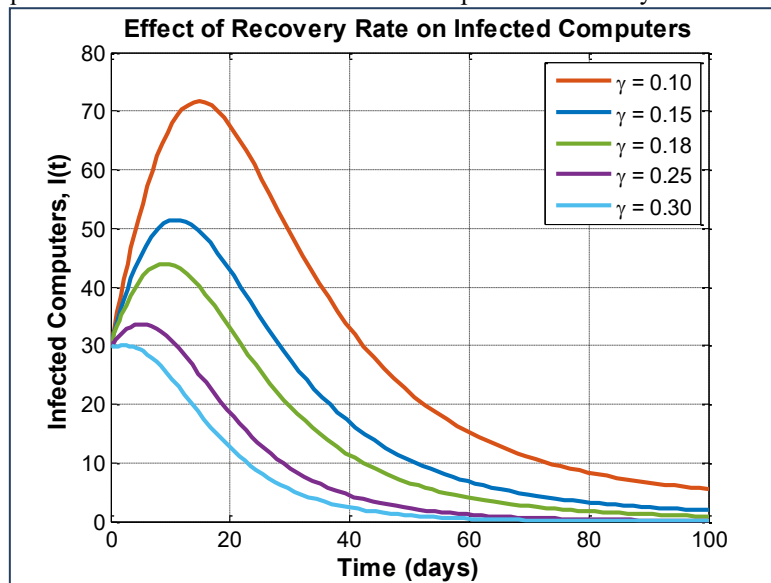


Figure 8: Shows the effect of Recovery Rate on Infected Computers.

The figure illustrates the effect of varying the recovery rate γ on the population of infected computers over a period of 100 days. Five scenarios of recovery-rate were used which were: 0.10, 0.15, 0.18, 0.25 and 0.30, while keeping the other model parameters fixed. The simulation shows that an increase in the recovery rate leads to a reduction in the number of infected computers. This occurs because a higher recovery rate enables infected computers to leave the infected class more rapidly and enter the recovered class. The scenario with $\gamma = 0.30$ therefore represents the most effective recovery intervention, while $\gamma = 0.10$ represents the least effective recovery scenario. The result indicates that improving the speed and effectiveness of virus detection, cleaning, repair, and system restoration can substantially reduce the persistence of computer-virus infections in institutional networks.

5. Conclusion

A formulation of a six compartments model with isolation and vaccination of those infected with corona virus was made so as to minimize the number of people at risk with the disease and reduce its transmission. The study show that the corona-virus was transmitted through contact form those that were infected that migrated into the susceptible class. The control parameter was obtained and discussed. It was established that the disease can be eradicated if $\mathcal{R}_0 < 1$ and persisted if $\mathcal{R}_0 > 1$ which were deduce from its stability and simulation analysis. Sensitive analysis was conducted and the result shows that migration and the contact rate of those infected can lead to death of many if not checked. We also performed simulation of the model and proved graphically that effective vaccination enhances the eradication of the disease. As the rate of vaccination increases it was observed that $\mathcal{R}_0 < 1$. Also, comparing the simulation of non-infectious population, susceptible and vaccinated population, it was seen that as the disease persisted, the susceptible population goes to extinction while those vaccinated does not. It is suggested on this ground that all individual should be vaccinated against disease before its outbreak as long as the vaccine is available. Furthermore, it was noticed that without treatment, susceptible, exposed and isolated population dies off as the corona-virus persist and infected class increases grossly as more and more people becomes infected. Therefore, attention should given to treatment as one of the control measure during its outbreak. Furthermore, simulations were conducted for different levels of cybersecurity effectiveness, transmission rates, quarantine rates, and recovery rates. The results indicate that increased cybersecurity effectiveness reduces the number of infected computers, while higher transmission rates increase virus propagation. Similarly, increasing quarantine and recovery rates contributes to a reduction in the infected computer population. The $\mathcal{R}_0$ analysis further demonstrates the importance of cybersecurity effectiveness in reducing the potential for sustained virus transmission within the network. Overall, the findings show that strengthening cybersecurity protection, improving the timely quarantine of infected computers, and enhancing recovery mechanisms can substantially contribute to controlling computer virus propagation in institutional networks. The model provides a useful mathematical framework for evaluating cybersecurity strategies and supporting informed decisions on computer-network protection. A higher recovery rate means that infected computers can be cleaned, repaired, or restored more rapidly. Consequently, the duration for which computers remain infected is reduced, helping to suppress virus propagation throughout the institutional network.

References

- [1] Abegye, S. Y, Akpan C.E and Shammah S.K (2024). Dynamical Behavior of Tuberculosis Transmission of a weak and strong Latently immune Population, *IOSR Journal of Mathematics*, 20(1), 22-33
- [2] Avci, İ., Hussain, A., & Kanwal, T. (2023). Investigating the impact of memory effects on computer virus population dynamics: A fractal–fractional approach with numerical analysis. *Chaos, Solitons & Fractals*, 174.
- [3] Ayaz et al, (2025). Stochastic fractional order model for the computational analysis of computer virus. *Scientific Reports*, 15, Article 33951.

- [4] Hoang, T. (2021). Lyapunov functions for investigating stability properties of a fractional-order computer virus propagation model. *Qualitative Theory of Dynamical Systems*, 20(3).
- [5] Mishra, K., & Jha, N. (2007). Fixed period of temporary immunity after run of anti-malicious software on computer nodes. *Applied Mathematics and Computation*, 190(2), 1207–1212.
- [6] Mishra, K. & Saini, D., (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Applied Mathematics and Computation*, 188(2), 1476–1482. <https://doi.org/10.1016/j.amc.2006.11.012>
- [7] Muthukumar et al, (2024). The dynamics of the fractional SEIQR malware spread model on wireless sensor networks. *Journal of Analysis*, 32, 2349–2370. <https://doi.org/10.1007/s41478-024-00798-1>
- [8] Muthukumar, S., Senthilkumar, M., & Chinnadurai, V. (2024). Optimal control of computer virus spreading model with partial immunization. *Wireless Personal Communications*. <https://doi.org/10.1007/s11277-024-11013-6>
- [9] Piqueira, C., Araujo, O., & Monteiro, A. (2009). A modified epidemiological model for computer viruses. *Applied Mathematics and Computation*, 213(2), 355–360.
- [10] Piqueira, C., Navarro, F., & Monteiro, A. (2005). Epidemiological models applied to viruses in computer networks. *Journal of Computer Science*, 1(1), 31–34.
- [11] Raza et al, (2025). Transmission dynamics of computer virus propagation model through delay effect demonstration. *Journal of Mathematics*, 2025, Article 9971453. <https://doi.org/10.1155/jom/9971453>
- [12] Shahini et al, (2022). A spectral collocation method for computer virus spread: Case of delayed optimal control problem. *Bulletin of the Iranian Mathematical Society*, 48(2), 507–535.
- [13] Shahrear et al, (2018). Analysis of computer virus propagation based on compartmental model. *Applied and Computational Mathematics*, 7(1–2), 12–21.
- [14] Singh et al, (2018). A fractional epidemiological model for computer viruses pertaining to a new fractional derivative. *Applied Mathematics and Computation*, 316, 504–515.
- [15] Upadhyay, K., & Singh, P. (2020). Modeling and control of computer virus attacks on a targeted network. *Physica A: Statistical Mechanics and Its Applications*, 538.
- [16] Yang, L., Yang, X., & Wu, Y. (2017). The impact of patch forwarding on the prevalence of computer virus: A theoretical assessment approach. *Applied Mathematical Modelling*, 43, 110–125.
- [17] Yang, W & Chang, X. (2024). Analysis and numerical simulation of computer virus propagation model based on limited resources. *Mathematics and Computers in Simulation*, 223, 494–508. <https://doi.org/10.1016/j.matcom.2024.04.035>