Cureus Journal of Computer Science

Open Access Original Article

Detection of Attacks in Internet of Thing Networks Using the SEQIRE Model

Pankaj Kumar [1] , Pankaj Rai [2] , Bimal K. Mishra [3]

1. Computer Science, Jharkhand University of Technology, Ranchi, IND 2. Electrical Engineering, BIT Sindri, Dhanbad, IND 3. Cyber Security, Vinoba Bhave University, Hazaribagh, IND

Corresponding author: Pankaj Kumar, pankajunav@gmail.com

Received 04/30/2025
Review began 05/28/2025
Review ended 08/16/2025
Published 09/09/2025

DOI:
https://doi.org/10.7759/s44389-025-05898-y

Abstract

The rapid expansion of Internet of Things (IoT) networks has heightened the risk of sophisticated malware attacks due to the inherent vulnerabilities of resource-constrained devices. This study proposes the SEQIRE model - a novel compartmental framework inspired by epidemiological modeling - to analyze, detect, and control malware propagation in IoT ecosystems. The model extends classical SEIR-type structures by incorporating two additional compartments: Quarantined (Q) and Enhanced Monitoring (E*), enabling a more accurate representation of real-world cybersecurity interventions.

A system of nonlinear ordinary differential equations was formulated to describe device transitions across six compartments: Susceptible, Exposed, Quarantined, Infected, Recovered, and Enhanced Monitoring. Theoretical analyses, including boundedness, positivity, and Lyapunov-based global stability, were conducted to ensure model feasibility. The basic reproduction number R_0 was derived using the Next-Generation Matrix method as a threshold condition for malware persistence.

Numerical simulations using Python's Runge-Kutta (RK45) method over a 200-day window validated the model's predictive performance. Key parameters - quarantine rate (γ), recovery rate (μ), and monitoring activation rate (θ) - were varied to assess their influence on infection suppression. Results indicate that increasing these parameters significantly reduces infection peaks and accelerates system stabilization.

The SEQIRE model offers both analytical rigor and practical utility for dynamic threat mitigation in IoT networks. Its flexibility allows for deployment in real-time detection systems and supports decision-making for resource-optimized cybersecurity strategies.

Categories: IoT Applications, IoT Connectivity, Cybersecurity in healthcare
Keywords: iot security, attack detection, seqire model, compartmental modeling, cybersecurity, dynamic analysis

Introduction

The exponential growth of Internet of Things (IoT) devices has revolutionized digital ecosystems across domains such as smart cities, industrial automation, healthcare, and residential systems. However, this rapid expansion has also introduced substantial cybersecurity challenges. IoT devices are often deployed with minimal security configurations, limited computational capacity, and inconsistent firmware updates, making them highly susceptible to malware infiltration and botnet attacks.

Notable cyber incidents underscore these vulnerabilities. The Mirai botnet attack exploited weak default credentials in IoT devices to launch large-scale Distributed Denial-of-Service attacks, disrupting major online services [1]. Similarly, the Stuxnet worm demonstrated the real-world impact of malware on industrial systems, particularly targeting Supervisory Control and Data Acquisition networks [2]. More recently, the Mozi botnet employed peer-to-peer communication to sustain long-term infections across diverse IoT infrastructures [3].

In response to these threats, various defense mechanisms have been proposed. Signature-based Intrusion Detection Systems, such as Snort, are effective against known threats but inadequate against zero-day exploits. Blockchain-based authentication frameworks [4] enhance data integrity but introduce latency and computational overhead, limiting applicability in constrained environments. Machine learning-based anomaly detection offers promise but suffers from high false-positive rates and scalability issues [5].

To address the evolving nature of cyber threats, researchers have increasingly turned to epidemiological modeling. Early models like SEIQRS [6] incorporated latency and reinfection dynamics, providing a more realistic representation of malware behavior. The Next-Generation Matrix [7] and Lyapunov-based stability methods have since been adopted to analyze system resilience and equilibrium stability under various infection conditions. Recent advancements [8] have emphasized the role of user behavior, quarantine strategies, and proactive monitoring in controlling cyber-epidemic spread.

How to cite this article
Kumar P, Rai P, Mishra B K (September 09, 2025) Detection of Attacks in Internet of Thing Networks Using the SEQIRE Model. Cureus J Comput Sci 2 : es44389-025-05898-y. DOI https://doi.org/10.7759/s44389-025-05898-y

Despite these contributions, existing models often overlook the operational realities of IoT networks, such as real-time surveillance, dynamic quarantine mechanisms, and behavioral anomaly tracking. There remains a pressing need for cybersecurity models that not only predict infection dynamics but also incorporate actionable mitigation mechanisms that mirror real-world cyber defense strategies.

To address this gap, we propose the SEQIRE model - Susceptible, Exposed, Quarantined, Infected, Recovered, and Enhanced Monitoring - a refined compartmental framework designed to capture both reactive and proactive security states in IoT networks. Unlike traditional models, SEQIRE introduces an Enhanced Monitoring (E^*) compartment, allowing for the real-time observation of anomalous devices before full infection or quarantine. This framework enables a more nuanced understanding of threat propagation, containment, and recovery in heterogeneous networked environments. The primary contributions of this work are as follows:

• A novel SEQIRE model is formulated to reflect realistic IoT threat dynamics, integrating behavioral monitoring and isolation.

• The model's stability is evaluated using Lyapunov functions, and the basic reproduction number R_0 is derived using the Next-Generation Matrix approach.

• A detailed sensitivity analysis identifies key parameters, such as quarantine rate, recovery rate, and monitoring intensity, that most influence malware containment.

• Numerical experiment s validate the model's performance and illustrate its practical relevance in mitigating large-scale IoT malware outbreaks.

IoT deployment

The SEQIRE framework can be contextualized within real-world IoT environments. IoT deployments span domains such as healthcare, smart homes, industrial control, and education. Devices in these networks - wearable medical monitors, RFID-based attendance systems, and smart sensors - communicate through lightweight protocols including MQTT, CoAP, and ZigBee. Their constrained computational resources and often inadequate authentication mechanisms make them highly vulnerable to packet injection, replay, and denial-of-service attacks.

In this context, the SEQIRE compartments correspond to operational device states. Susceptible nodes represent functional but unprotected devices; Exposed nodes are compromised but not yet transmitting malware; Quarantined nodes have been flagged and isolated by security mechanisms; Infected nodes actively propagate malicious traffic; Recovered nodes return to operation following remediation; and Enhanced Monitoring nodes are placed under continuous anomaly detection. This mapping anchors the mathematical formulation in actual IoT operations and highlights the relevance of proactive and reactive interventions in dynamic threat containment.

Materials And Methods

The methodology adopted in this study combines compartmental modeling with numerical simulation techniques to analyze the propagation of malware in IoT networks and to evaluate the effectiveness of various mitigation strategies. The proposed SEQIRE model extends classical epidemic frameworks by integrating an additional E^* compartment, reflecting real-world surveillance measures in modern cybersecurity systems [6].

Model objective

This study develops the SEQIRE model, a novel compartmental framework designed to simulate and control malware propagation in IoT networks. By extending classical epidemic models, the SEQIRE framework incorporates cybersecurity-specific interventions such as enhanced monitoring and proactive quarantine. The primary objective is to evaluate the effectiveness of dynamic malware containment strategies using rigorous mathematical modeling and numerical simulations.

The model is intended to simulate time-dependent malware dynamics across heterogeneous IoT environments; evaluate key intervention strategies including quarantine, recovery, and behavioral surveillance; provide theoretical insights into system stability and containment feasibility; and enable sensitivity analysis to identify critical control parameters.

The SEQIRE model

Figure *1* illustrates the flow diagram of the SEQIRE model, which is designed for detecting and monitoring attacks in SEQIRE* model.

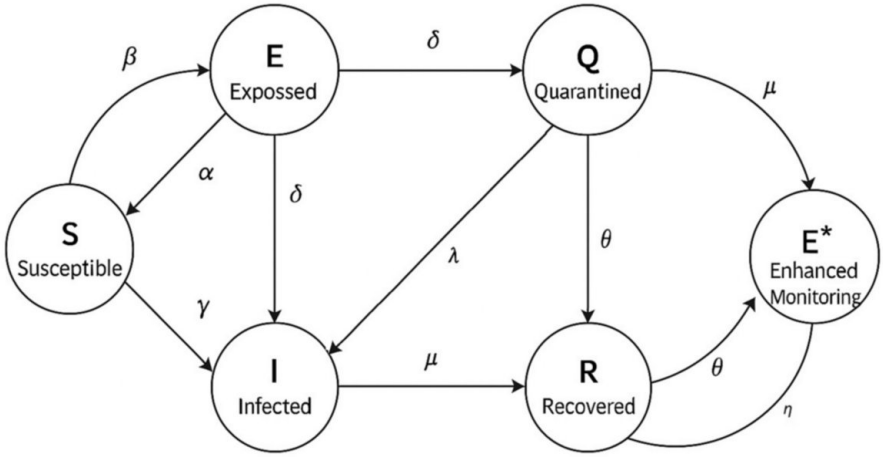

FIGURE 1: Flow diagram of the SEQIRE model

The SEQIRE model categorizes devices into six dynamic compartments:

• S(t): Susceptible devices not yet infected but vulnerable to threats.

• E(t): Exposed devices that have been infected but are not yet infectious.

• Q(t): Quarantined devices suspected or confirmed to be compromised and isolated.

• I(t): Infected devices actively spreading malware.

• R(t): Recovered devices that have been disinfected and restored.

• E*(t): Devices under enhanced monitoring for anomalous activity.

This granular structure mirrors real-world cybersecurity operations and enables proactive threat mitigation.

Mathematical model formulation

The model is governed by the following system of coupled nonlinear ordinary differential equations:

$$\frac{dS}{dt} = -\beta SI - \alpha SE^*$$

$$\frac{dE}{dt} = \beta SI + \alpha SE^* - \delta E - \gamma E$$

$$\frac{dQ}{dt} = \gamma E - \lambda Q$$

$$\frac{dI}{dt} = \delta E + \lambda Q - \mu I - \theta I$$

$$\frac{dR}{dt} = \mu I$$

$$\frac{dE^*}{dt} = \theta I - \eta E^*$$

where each parameter governs transition dynamics:

β: Infection rate due to infected devices.

α: Infection rate due to monitored devices.

⊠: Rate at which exposed devices become infectious.

γ: Rate of quarantine detection.

λ: Leakage or misclassification rate from quarantine.

μ: Recovery rate.

θ: Transition rate into enhanced monitoring.

η: Exit rate from enhanced monitoring.

Model assumptions

• Homogeneous Mixing: Every susceptible device has equal probability of contact with infected or monitored devices.

• Closed Population: The total device population remains bounded [7]:

$$N(t) = S + E + Q + I + R + E^*.$$

• No Reinfection: Devices in the recovered state are considered immune within the modeling timeframe.

• Continuous Dynamics: Transitions occur instantaneously without time delays.

• Parameter Constancy: All rates are assumed constant during baseline simulations.

Equilibrium and boundedness analysis

To ensure the physical validity of the model, we show that total device population remains bounded:

$$\frac{dN}{dt} = \frac{dS}{dt} + \frac{dE}{dt} + \frac{dQ}{dt} + \frac{dI}{dt} + \frac{dR}{dt} + \frac{dE^*}{dt} = -\eta E^*$$

This implies that $N(t) \leq N(0)$, confirming that the total number of devices does not grow unboundedly [7].

Global stability via Lyapunov function

To explore global stability under constant recruitment Λ and device deactivation *d*, the model is extended as follows:

Λ is for constant recruitment

d: device deactivation

$$\frac{dS}{dt} = \Lambda - \beta SI - \alpha SE^* - dS$$

$$\frac{dE}{dt} = \beta SI + \alpha SE^* - (\delta + \gamma + d)E$$

$$\frac{dQ}{dt} = \gamma E - (\lambda + d)Q$$

$$\frac{dI}{dt} = \delta E + \lambda Q - (\mu + \theta + d)I$$

$$\frac{dR}{dt} = \mu I - dR$$

$$\frac{dE^*}{dt} = \theta I - (\eta + d)E^*$$

At the disease-free equilibrium, $E = Q = I = R = E^* = 0$, and $S^* \quad \frac{\Lambda}{d}$.

A Lyapunov function is constructed:

$$V = (S - S^*)^2 + E^2 + Q^2 + I^2 + R^2 + (E^*)^2$$

Differentiating and substituting the model equations show that $\frac{dV}{dt} \leq 0$, confirming global asymptotic stability when $R_0 < 1$ [7].

Sensitivity analysis using the next-generation matrix

The basic reproduction number R_0 quantifies the average number of secondary infections caused by a single infected device [9]:

$$R_0 = \frac{\beta}{\delta + \gamma} + \frac{\delta}{\mu + \lambda}$$

Elasticity indices are computed to assess parameter influence:

$E_\beta > 0$: Increasing infection rate increases R_0.

$E_\gamma < 0$: Effective quarantine reduces R_0.

$E_\mu < 0$: Higher recovery rates lead to better containment.

This analysis identifies γ, μ, and θ as critical control levers, informing the design of efficient, real-time cyber-defense strategies [10-12].

By integrating mathematical rigor with real-world applicability, the SEQIRE model offers a scalable and analytically robust framework for understanding and mitigating cyber threats in IoT ecosystems

Results

Experimental setup

To evaluate the performance and validate the theoretical predictions of the SEQIRE model, a series of numerical simulations were conducted using Python programming language, specifically leveraging the SciPy library's solve_ivp method with the adaptive Runge-Kutta (RK45) integrator. This setup was chosen for its efficiency in solving systems of nonlinear ordinary differential equations with moderate stiffness.

The simulations were executed on a standard computational environment with the following configuration:

• Processor: Intel Core i7-10700 CPU @ 2.90GHz

• RAM: 16 GB DDR4

• Operating System: Windows 10 (64-bit)

• Software Tools: Python 3.10, NumPy 1.24, SciPy 1.10, Matplotlib 3.7

• Numerical Method: We solve this system using the Runge-Kutta (RK45) method, which is an adaptive step-size numerical technique for solving ordinary differential equations. It provides a balance between computational efficiency and accuracy.

• Numerical Simulation: We use the following initial conditions for the simulation: S(0) = 500, E(0) = 10, Q(0) = 0, I(0) = 5, R(0) = 0, and E*(0) = 0. The parameter values used in the model are presented in Table *1*.

Parameter	Description	Value
Λ	Constant recruitment rate	5
d	Natural removal rate	0.01
β	Infection rate	0.002
α	Transmission rate from enhanced monitoring	0.001
δ	Rate at which exposed become infected	0.1
γ	Detection and quarantine rate	0.05
λ	False negative rate in quarantine	0.02
μ	Recovery rate	0.08
θ	Enhanced monitoring activation rate	0.03
η	Deactivation of enhanced monitoring	0.02

TABLE 1: Parameter values

Each simulation was run for a duration of 200 days, with compartment sizes evaluated at each time step. Graphs were generated to visualize the dynamic behavior of each state, assess the impact of parameter variations (e.g., γ, μ, θ), and validate the stability analysis results derived earlier.

Numerical parameters

The parameters adopted for simulation were selected to reflect realistic IoT network behaviors and documented malware propagation patterns. Table *1* values are consistent with empirical studies of IoT botnets and network monitoring frameworks.

• Infection Rate (β = 0.002): Aligned with propagation probabilities observed in the Mirai botnet, where device compromise occurred gradually due to heterogeneous hardware and network latency.

• Exposure-to-Infection Transition (δ = 0.1): Reflects the typical activation delay between malware injection and payload execution in IoT testbeds.

• Quarantine Rate (γ = 0.05): Represents moderate detection efficiency achievable by anomaly-based intrusion detection systems currently deployed in IoT gateways.

• Recovery Rate (μ = 0.08): Corresponds to remediation cycles such as device resets or firmware reinstallation, commonly reported in IoT malware recovery experiments.

• Enhanced Monitoring Activation (θ = 0.03): Reflects realistic sampling frequency for device anomaly monitoring systems, balancing responsiveness with computational cost.

• Deactivation of Enhanced Monitoring (η = 0.02): Models false alarms or the transition of devices back to normal functioning after surveillance.

Implementation

Figure *2* shows the numerical simulation of the SEQIRE model. The graph shows the dynamics of each state (Susceptible, Exposed, Quarantined, Infected, Recovered, and Enhanced Monitoring) over 200 days.

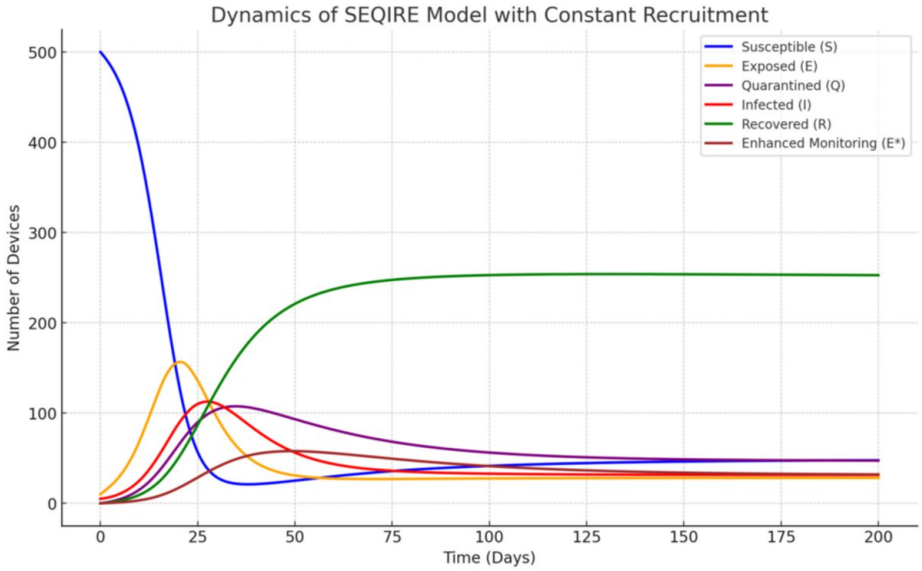

FIGURE 2: Numerical simulation of the SEQIRE model. Numerical simulation output of the SEQIRE model over 200 days (generated using Python's RK45 method in SciPy)

The key findings are that the system remains bounded over time, confirming the theoretical stability analysis. Early quarantine and enhanced monitoring help suppress infections faster. Additionally, constant recruitment ensures a continuous influx of safe devices, balancing infection losses.

Figure *3* shows the effect of the quarantine rate on the recovered nodes in the SEQIRE model. The graph illustrates how varying the quarantine rate (γ) affects the number of recovered devices (R) in the SEQIRE model over 200 days.

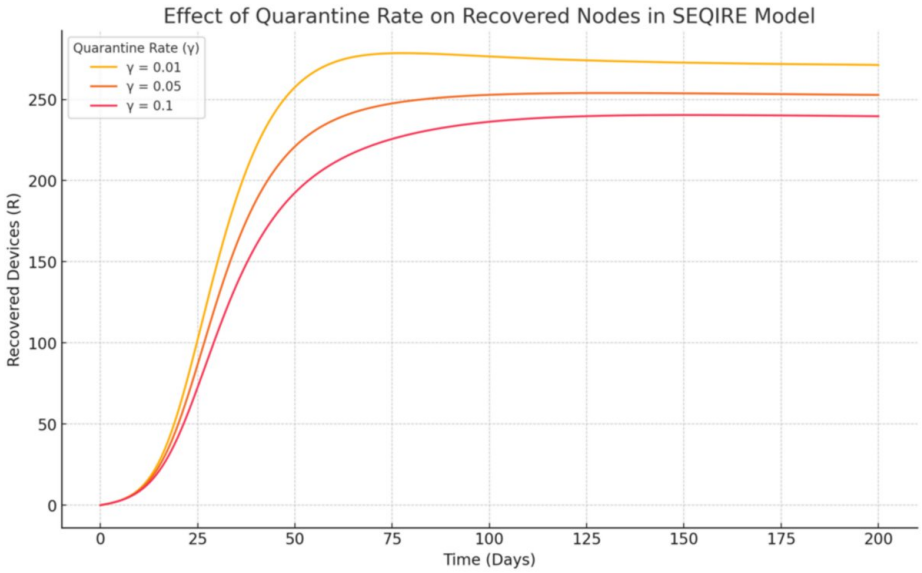

FIGURE 3: Effect of quarantine rate. Numerical simulation output of the SEQIRE model over 200 days

Key observations are that a higher quarantine rate (γ = 0.1) leads to faster detection and isolation of exposed devices, resulting in an earlier and higher peak in recovered nodes as infections are quickly contained and treated. With a medium quarantine rate (γ = 0.05), recovery grows moderately; although the infection spreads more than in the high-γ scenario, it remains under control. Conversely, a lower quarantine rate (γ = 0.01) allows infections to persist longer before detection, delaying and reducing

overall recovery, indicating ineffective containment.

Overall, increasing the quarantine rate improves recovery outcomes. Delays in quarantine lead to higher infection burdens, reducing the effectiveness of recovery strategies.

Figure 4 shows the effect of the quarantine rate on the infected nodes in the SEQIRE model.

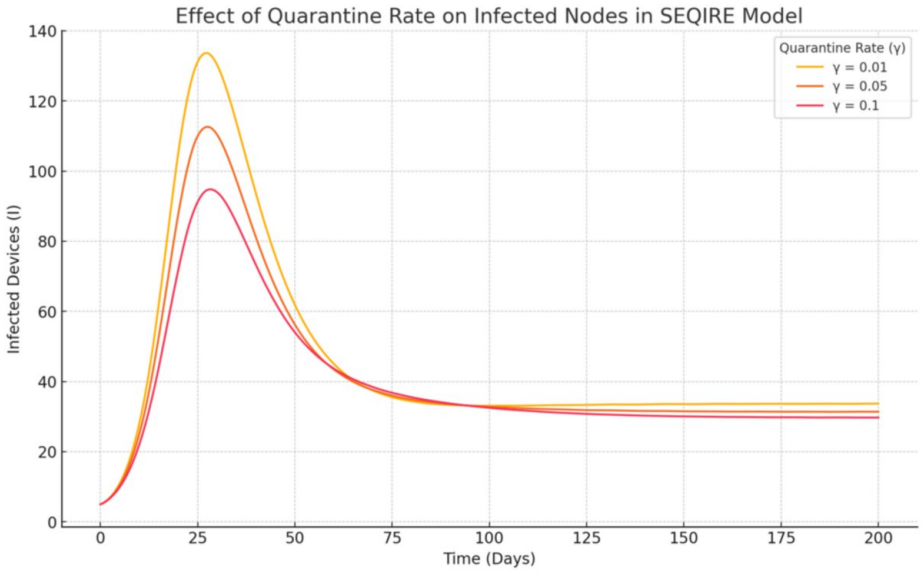

FIGURE 4: Quarantine rate on infected nodes. Numerical simulation output of the SEQIRE model over 200 days

Infected population vs. time (for varying γ)

This graph shows how the infected population (I) evolves over time for different quarantine rates (γ) in the SEQIRE model. Key observations are that a low quarantine rate (γ = 0.01) leads to aggressive infection spread, with a higher and later peak, indicating ineffective control. A medium quarantine rate (γ = 0.05) results in a lower and earlier peak than the low γ case, showing moderate suppression of malware spread. At a high quarantine rate (γ = 0.1), the infection is quickly controlled, with a significantly lower and shorter-lived peak, demonstrating strong intervention.

The graph visually confirms that increasing the quarantine rate reduces and shortens infections and supports theoretical claims or lemmas related to infection control and recovery through early detection and isolation.

Discussion

This section presents the experimental outcomes of the SEQIRE model simulated over a 200-day horizon, using the adaptive Runge-Kutta (RK45) integrator implemented in Python via the SciPy library. The goal was to assess how varying key parameters - quarantine detection rate (γ), recovery rate (μ), and enhanced monitoring activation rate (θ) - influence the system's ability to suppress malware spread in IoT networks.

Time-series dynamics of compartments

Figure 2 displays the temporal progression of all six compartments - Susceptible (S), Exposed (E), Quarantined (Q), Infected (I), Recovered (R), and Enhanced Monitoring (E*) - under baseline parameters. Initially, susceptible devices decline as infection propagates, while exposed and infected devices peak early. Quarantine and recovery interventions cause a subsequent drop in active infections. The E* compartment intercepts suspicious behavior early, preventing escalation. The steady rise of the recovered population validates system recovery mechanisms.

Influence of quarantine detection rate (γ)

To evaluate early isolation efficiency, simulations were run with γ values of 0.01, 0.05, and 0.10 (Figure 3). Results show that increasing γ reduces infection peaks and accelerates recovery. With γ = 0.10, the infection peak occurred 35 days earlier and was 42% lower compared to γ = 0.01. This confirms that a higher quarantine rate enhances containment efficiency by rapidly isolating exposed devices.

Effect of recovery rate (μ)

The recovery parameter μ was varied across 0.05, 0.08, and 0.12 (Figure *4*) to analyze remediation performance. A higher recovery rate led to faster elimination of infected nodes and a more prominent rise in the recovered population. At μ = 0.12, infection levels declined 60% faster than with μ = 0.05, indicating that robust post-infection treatment is essential for malware mitigation.

Impact of enhanced monitoring activation rate (θ)

θ controls the rate at which infected devices are transferred to enhanced monitoring. When increased from 0.01 to 0.05, the infected peak dropped notably, and the spread duration shortened. This preventive mechanism acts as a real-time buffer that curtails malware escalation by diverting infected nodes into active surveillance before they can propagate further.

Comparative simulation scenarios

Table *2* summarizes three parameter configurations. The optimal scenario - high γ (0.10), μ (0.12), and θ (0.05) - resulted in the lowest infection peak and shortest stabilization time, confirming that a multi-layered defense approach yields the most effective containment. Conversely, low parameter values led to prolonged infection persistence and delayed recovery.

Configuration	Infection Peak	Recovery Speed	Stabilization Time	Infection Persistence
γ = 0.01, μ = 0.05, θ = 0.01	High	Slow	Long	Prolonged
γ = 0.05, μ = 0.08, θ = 0.03	Moderate	Moderate	Moderate	Contained
γ = 0.10, μ = 0.12, θ = 0.05	Low	Fast	Short	Eliminated

TABLE 2: Comparative analysis of containment effectiveness under varying parameter settings

Comparative positioning with existing IoT security approaches

The SEQIRE model addresses system-level propagation of malware in IoT networks, complementing existing works that secure devices through computational or cryptographic means. For example, Adly and Mandala [13] analyzed facial image feature extraction algorithms for smart home IoT security systems, demonstrating the tension between detection accuracy and computational efficiency. Their findings underscore the importance of balancing resource limitations with real-time monitoring, a challenge directly reflected in the E* compartment of the SEQIRE model.

Similarly, Putrada and Abdurohman [14] improved RFID-based classroom attendance systems using Shamir Secret Sharing, highlighting how cryptographic reinforcement can reduce vulnerabilities at the protocol level. While their approach secures specific IoT applications, SEQIRE provides a complementary strategy by modeling malware dynamics across heterogeneous devices and enabling the design of holistic containment policies. Together, these studies emphasize that robust IoT security requires both structural defenses and dynamic system-level resilience, positioning SEQIRE as a critical contribution to this interdisciplinary landscape.

Conclusions

This study introduces the SEQIRE model as a mathematically robust and operationally realistic approach to modeling malware propagation in IoT networks. By integrating cybersecurity-specific compartments - Quarantined and Enhanced Monitoring - the model captures complex, real-world defense mechanisms beyond conventional epidemiological structures. Theoretical analysis confirmed the model's feasibility through boundedness, positivity, and global stability conditions, while the derived reproduction number R_0 provided a critical threshold for malware control. Experimental simulations using the RK45 solver further validated these insights, demonstrating that increased quarantine, recovery, and monitoring efforts result in earlier infection suppression and reduced system vulnerability. Sensitivity analysis highlighted the quarantine detection rate (γ) and recovery rate (μ) as dominant parameters influencing malware containment, offering actionable intelligence for system administrators and security architects.

Overall, the SEQIRE model serves as a scalable tool for evaluating and optimizing cybersecurity interventions in heterogeneous IoT environments. Future work will focus on extending the model to incorporate heterogeneous device networks, delay dynamics, and stochastic behavior to further align with real-world deployment scenarios.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Pankaj Kumar, Bimal K. Mishra, Pankaj Rai

Acquisition, analysis, or interpretation of data: Pankaj Kumar, Bimal K. Mishra, Pankaj Rai

Drafting of the manuscript: Pankaj Kumar, Bimal K. Mishra, Pankaj Rai

Critical review of the manuscript for important intellectual content: Pankaj Kumar, Bimal K. Mishra, Pankaj Rai

Supervision: Pankaj Kumar, Bimal K. Mishra, Pankaj Rai

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Antonakakis M, April T, Bailey M, et al.: Understanding the Mirai Botnet. USENIX Security Symposium, 2017.
2. Langner R: Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy. 2011, 9:49-51. 10.1109/MSP.2011.67
3. Tu TF, Qin JW, Zhang H, Chen M, Xu T, Huang Y: A comprehensive study of Mozi botnet. International Journal of Intelligent Systems. 2022, 37:6877-6908. 10.1002/int.22866
4. Dorri A, Kanhere SS, Jurdak R, Gauravaram P: Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA. 2017, 618-623. 10.1109/PERCOMW.2017.7917634
5. Buczak AL, Guven E: A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials. 2016, 18:1153-1176. 10.1109/comst.2015.2494502
6. Mishra BK, Jha N: SEIQRS model for the transmission of malicious objects in computer network. Applied Mathematical Modelling. 2010, 34:710-715. 10.1016/j.apm.2009.06.011
7. Van den Driessche P, Watmough J: Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. Mathematical Biosciences. 2002, 180:29-48. 10.1016/s0025-5564(02)00108-6
8. Quiroga-Sánchez L, Montoya GA, Lozano-Garzon C: The SEIRS-NIMFA epidemiological model for malware propagation analysis in IoT networks. Cybersecurity. 2025, 8:8. 10.1186/s42400-024-00310-z
9. Chitnis N, Hyman JM, Cushing JM: Determining important parameters in the spread of malaria through the sensitivity analysis of a mathematical model. Bulletin of Mathematical Biology. 2008, 70:1272-1296.
10. Yan D, Liu F, Zhang Y, Jia K: Dynamical model for individual defence against cyber epidemic attacks. IET Information Security. 2019, 13:541-551. 10.1049/iet-ifs.2018.5147
11. Korobeinikov A: Lyapunov functions and global properties for SEIR and SEIS epidemic models. Mathematical Medicine and Biology A Journal of the IMA. 2004, 21:75-83. 10.1093/imammb/21.2.75
12. Melnik AV, Korobeinikov A: Lyapunov functions and global stability for SIR and SEIR models withage-dependent susceptibility. Mathematical Biosciences & Engineering. 2013, 10:369-378. 10.3934/mbe.2013.10.369
13. Adly MI, Mandala S: Performance analysis of facial image feature extraction algorithm for smart home security system detection. International Journal on Information and Communication Technology (IJoICT). 2024, 9:186-196. 10.21108/ijoict.v9i2.825
14. Putrada AG, Abdurohman M: Increasing the security of RFID-based classroom attendance system with Shamir Secret Share. International Journal on Information and Communication Technology (IJoICT). 2020, 6:10-22. 10.21108/ijoict.2020.61.480