INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING AND COMPUTER SYSTEMS
E-ISSN: 2180-0650
VOLUME 12, ISSUE 2, 2026, pp. 84 – 96
DOI: https://doi.org/10.15282/ijsecs.12.2.2026.8.0154

RESEARCH ARTICLE

Integration of the SEIR model and IoT malware mitigation policy recommendations: A sensitivity analysis and numerical simulation approach

Dwi Ely Kurniawan[1,3]*, Eri Prasetyo Wibowo[2], Sarifuddin Madenda[2]

[1]Faculty of Postgraduate Studies, Gunadarma University, Depok, West Java, 16424, Indonesia
[2]Department of Information Technology, Gunadarma University, Depok, West Java,16424, Indonesia
[3]Department of Informatics Engineering, Politeknik Negeri Batam, Batam, Riau Island, 29461, Indonesia

Abstract - The rapid growth of Internet of Things (IoT) devices has increased the risk of malware propagation across interconnected systems, creating significant cybersecurity challenges. Although epidemic models have been widely adopted to study malware propagation, existing approaches often overlook the latent stage between device compromise and active infection and lack comprehensive validation of analytical results. This study proposes a Susceptible-Exposed-Infected-Recovered (SEIR) malware propagation model incorporating heterogeneous device vulnerability, patch deployment, and network topology to represent malware dynamics in IoT environments. The basic reproduction number (R_0) is derived analytically and validated through equilibrium analysis and fourth-order Runge Kutta simulations, yielding a baseline R_0 of 2.405. Global sensitivity analysis using Latin Hypercube Sampling (LHS, N = 3,000) and Partial Rank Correlation Coefficients (PRCC) identifies recovery rate, waning immunity, network topology, device vulnerability, transmission rate, and patch deployment rate as the key factors influencing malware prevalence. Numerical simulations demonstrate that combining faster patch deployment with network segmentation reduces malware prevalence by 94.5% after 90 days and decreases R_0 from 2.405 to 1.197. However, malware persistence remains possible because R_0 remains above the epidemic threshold. Incorporating improved device-security standards further reduces R_0 to 0.830, achieving a 99.5% reduction in malware prevalence and near-eradication of the outbreak. These findings demonstrate that sustainable IoT malware mitigation requires an integrated strategy combining effective patch management, network-level protection, and device-level security rather than relying on individual mitigation measures.

Article History
Received : 01 Jun 2026
Revised : 28 October 2026
Accepted : 06 November 2026
Published : 13 November 2026

KEYWORDS
IoT security
SEIR model
Malware propagation
Sensitivity analysis
Basic reproduction number

1. Introduction

The Internet of Things (IoT) ecosystem has undergone unprecedented expansion, with Statista projecting over 29 billion connected devices globally by 2030 [1]. This explosive growth, however, has fundamentally transformed the cybersecurity landscape. Unlike conventional computing environments, IoT devices present unique security vulnerabilities stemming from constrained computational resources, infrequent firmware updates, and diverse communication protocols. These characteristics render IoT networks particularly susceptible to malware propagation campaigns, including distributed denial-of-service (DDoS) botnets, ransomware deployment, and persistent threat implantation [2].

The Mirai botnet incident of 2016 exemplified the catastrophic consequences of unchecked IoT malware propagation, compromising over 600,000 devices and orchestrating terabit-scale DDoS attacks against critical internet infrastructure [3]. Subsequent malware families, including Mirai, Gafgyt, and IoTReaper [4], have demonstrated increasingly sophisticated persistence mechanisms, encrypted command-and-control communications, and peer-to-peer propagation architectures. Estimates of the global economic cost of cybercrime, of which IoT-related incidents form a growing share, are in the trillions of dollars annually by the mid-2020s, underscoring the urgent need for robust theoretical frameworks that can inform effective mitigation strategies [5].

Mathematical epidemiology offers a compelling paradigm for modeling malware propagation dynamics, drawing parallels between biological pathogen transmission and digital infection spread [6]. The seminal SIR (Susceptible-Infected-Recovered) model, introduced by Kermack and McKendrick [7], has been extensively adapted for computer virus propagation [8], [9]. However, canonical SIR adaptations inadequately capture the latency phase inherent to IoT malware infection: the temporal window between initial device compromise and the onset of active malicious behavior. This latency period, during which devices are exposed but not yet infectious, is particularly pronounced in IoT environments due to staged payload delivery mechanisms and anti-detection dormancy protocols [10].

The SEIR (Susceptible-Exposed-Infected-Recovered) model extends the SIR framework by incorporating an Exposed (E) compartment representing this critical latency phase. Several studies have applied SEIR variants to network malware propagation [11], [12]; however, these formulations fail to account for three IoT-specific characteristics that fundamentally alter propagation dynamics: (1) device heterogeneity in vulnerability profiles arising from diverse manufacturer security practices; (2) network topology effects including small-world clustering patterns in IoT deployments; and (3) patch deployment latency arising from manufacturer update cycles and device owner inaction [13].

***CORRESPONDING AUTHOR | Dwi Ely Kurniawan** | ✉ dwialikhs@polibatam.ac.id
© 2026 The Authors. Published by Universiti Malaysia Pahang Al-Sultan Abdullah Press. This is an open access article under the CC BY-NC 4.0 license

Furthermore, existing models frequently report sensitivity-analysis outputs without cross-checking them against the closed-form thresholds (R_0, equilibria) that the same model implies. This is a substantive gap, distinct from the modeling gap: a model can be correctly specified while its reported numerical outputs are internally inconsistent, which undermines the policy conclusions drawn from it regardless of the model's conceptual merit. Global sensitivity analysis, particularly Partial Rank Correlation Coefficient (PRCC) analysis with Latin Hypercube Sampling (LHS) provides a policy-informing capability by quantifying the relative influence of each model parameter on malware prevalence outcomes [14], but only if every reported PRCC, R_0, and simulated trajectory is generated from, and verifiable against, the same parameter set.

This paper addresses these limitations by proposing an IoT-oriented SEIR epidemic model that incorporates heterogeneous device vulnerability (θ), network topology transmission effects (φ), and patch deployment dynamics (δ). The model is further analyzed through sensitivity analysis and numerical simulations to identify the dominant factors governing malware propagation. Based on these results, the study formulates quantitative IoT malware mitigation policy recommendations, bridging epidemic modeling with practical cybersecurity decision-making for resilient IoT networks.

The main contributions of this study are fourfold. First, an IoT-specific SEIR epidemic model is proposed that incorporates heterogeneous device vulnerability (θ), network topology effects (φ), and patch deployment dynamics (δ) within a single analytically tractable framework. Second, the model is analyzed theoretically through equilibrium and local/global stability analysis to derive the basic reproduction number R_0 via the next-generation matrix method and to establish the epidemic threshold. Third, a global sensitivity analysis using Latin Hypercube Sampling (LHS, N = 3,000) and Partial Rank Correlation Coefficients (PRCC) is performed and cross-validated against the analytic R_0-elasticities and RK4 simulation results, rather than being reported in isolation. Finally, the model translates these theoretical and numerical results into ranked, evidence-based cybersecurity intervention priorities for IoT environments, bridging epidemic modeling with practical policy guidance.

2. Related Works

The application of epidemiological frameworks to model computer malware propagation was pioneered by Kephart and White [8], who demonstrated that SIR dynamics accurately capture viral spread in hierarchical network topologies. Subsequent work by Pastor-Satorras and Vespignani [15] extended this to scale-free networks, establishing that heterogeneous degree distributions fundamentally alter epidemic thresholds, a finding directly applicable to IoT network topology analysis.

Piqueira and Araujo [16] introduced the SIR model for computer virus propagation, incorporating temporary immunity to model patch expiration. Their analytical results established that oscillatory behavior emerges in SIR systems with sufficient reinfection rates, providing theoretical justification for observed cyclic malware outbreak patterns. However, their model assumed homogeneous device populations, limiting applicability to heterogeneous IoT deployments.

Mishra and Saini [17] proposed an SEIRS model with a quarantine compartment for worm propagation analysis, demonstrating that isolation of infected nodes accelerates epidemic extinction. While conceptually relevant, their model did not incorporate the exposed-phase dynamics critical to IoT malware behavior, nor did they perform sensitivity analysis to guide intervention prioritization.

Acarali et al. [18] developed the IoT-SIS model to investigate botnet propagation in IoT-based wireless sensor networks, considering device characteristics and network-related factors. Although the SIS framework provides a useful representation of infection and reinfection dynamics, it does not explicitly distinguish between exposed devices and actively infected devices. This distinction is relevant when malware exploitation, installation, and activation involve a delay between initial exposure and subsequent propagation.

Wang et al. [19] developed a malware propagation model that distinguishes intra-cluster and inter-cluster transmission and examines centralized and decentralized patch distribution strategies. This approach highlights the importance of network organization and patch deployment in understanding malware propagation and control. However, the implications of these mechanisms for the sensitivity of a compartmental SEIR model and the formulation of parameter-informed mitigation recommendations require further investigation within the specific assumptions of the model under consideration.

Zhu et al. [20] proposed a multi-layer IoT malware propagation model distinguishing physical-layer and cyber-layer infection dynamics. While their layered approach captures the cyber-physical nature of IoT systems, the model's complexity precludes closed-form analytical treatment and systematic sensitivity analysis. The present work achieves comparable IoT specificity through parameter-level incorporation of θ, φ, and δ while maintaining analytical tractability and full numerical reproducibility.

Sensitivity analysis of epidemic models has been systematically developed by Saltelli et al. [21] for general complex-system analysis, and applied to epidemiological models by Blower and Dowlatabadi [22], who established PRCC as a standard methodology for nonlinear, non-monotonic models. Subsequent applications to computer-network epidemic models include Nwokoye [23], who applied PRCC analysis to a SIRS worm propagation model.

Notably underexplored in the existing literature is a systematic PRCC-LHS sensitivity analysis, applied to an IoT-specific SEIR model, in which every reported sensitivity value is generated from and traceable to a shared, published simulation configuration rather than presented as a standalone table. This is the gap the present work targets: an integrated framework that connects sensitivity-analysis outputs directly to parameterized intervention strategies, with full internal cross-validation. Table 1 positions the present work relative to key prior contributions across five dimensions: model type, IoT specificity, stability-analysis rigor, sensitivity-analysis method, and policy-recommendation derivation.

Recent studies have increasingly focused on IoT malware detection using artificial intelligence and data-driven approaches. Deep-learning-based intrusion detection systems leveraging CNN, LSTM, and hybrid architectures have shown strong performance in detecting IoT malware traffic patterns, and graph-based and explainable AI (XAI) techniques have been proposed to enhance interpretability in complex IoT environments [24]-[29]. These studies primarily target detection rather than propagation dynamics and generally lack analytical frameworks for policy optimization. The present work is complementary to AI-based detection: it provides a mathematically grounded propagation model, with every reported figure cross-validated against its own governing equations, integrated with sensitivity-driven, feasibility-aware policy recommendations. In particular, and unlike the studies surveyed above, the present analysis distinguishes between parameters that shift the long-run eradication threshold R_0 and parameters that mainly reshape short-to-medium-term prevalence, a distinction that turns out to matter for policy design.

Table 1. Comparison of related works and the proposed research

References	Model	IoT-Specific	Stability Analysis	Sensitivity Analysis	Policy Recommendation
Kephart & White [8]	SIR	No	Partial	None	None
Piqueira & Araujo [16]	SEIRS	No	Full	None	Qualitative
Acarali et al. [18]	SIS	Partial	None	None	Qualitative
Wang et al. [19]	SEIR	Partial	Numerical	None	Qualitative
Zhu et al. [20]	Multi-layer	Yes	Numerical	None	None
Present Work	SEIR (IoT)	Yes	Full (LAS+GAS)	PRCC-LHS, cross-validated	Quantitative

3. Materials and Methods

3.1 Population Compartments and Assumptions

Let N(t) denote the total number of IoT devices at time t, partitioned into four compartments: S(t) (susceptible, unpatched), E(t) (exposed, compromised but dormant), I(t) (infected, actively infectious), R(t) (recovered, patched or reset).

The model is constructed under the following assumptions.

- Assumption 1 (Population Dynamics). New devices enter S at constant rate Λ; devices are removed from all compartments at rate μ, giving $N(t) \to \Lambda/\mu$ as $t \to \infty$.
- Assumption 2 (Heterogeneous Vulnerability). A heterogeneity coefficient $\theta \in (0,1]$ scales the effective transmission rate; $\theta = 1$ corresponds to a fully homogeneous, maximally vulnerable population.
- Assumption 3 (Network Topology Effect). The modifier φ captures topology effects: $\varphi > 1$ for scale-free hub networks (accelerated propagation); $\varphi < 1$ for segmented architectures (reduced propagation).
- Assumption 4 (Patch Latency). Patch deployment is modeled at constant asymptotic rate $\delta = \delta_\infty$, consistent with steady-state and R_0 derivations. The time-varying form $\delta(t) = \delta_0(1 - e^{\{-at\}})$ is retained conceptually for future transient-calibration work.
- Assumption 5 (Waning Immunity). Recovered devices lose patch-based protection at rate ω, re-entering the susceptible compartment.

3.2 SEIR Model Equations

Under these assumptions, the IoT malware propagation dynamics are governed by the system of ordinary differential equations (ODEs) as shown in Eqs. (1)-(4):

$$\frac{dS}{dt} = \Lambda - \theta\varphi\beta\left(\frac{SI}{N}\right) - \mu_s S + \omega R \quad (1)$$

$$\frac{dE}{dt} = \theta\varphi\beta\left(\frac{SI}{N}\right) - (\mu_E + \sigma)E \quad (2)$$

$$\frac{dI}{dt} = \sigma E - (\mu_I + \gamma + \delta)I \quad (3)$$

$$\frac{dR}{dt} = \gamma I + \delta I - (\mu_R + \omega)R \quad (4)$$

where $S + E + I + R = N(t)$

For analytical simplicity and consistency with related works [11], [17], uniform device decommissioning rates are assumed: $\mu_s S = \mu_E = \mu_I = \mu_R = \mu$. Under this assumption, $\frac{dN}{dt} = \Lambda - \mu N$, so $N(t) \to \frac{\Lambda}{\mu}$ as $t \to \infty$, enabling normalized analysis.

Table 2. Model parameters and baseline values used in the SEIR model simulation

Parameter	Description	Unit	Baseline Value	Source
Λ	Device deployment rate	devices/day	100	Modeling assumption; consistent with enterprise IoT scale [1]; see §3.2 note
μ	Device decommissioning rate	day⁻¹	0.0005	IoT device lifetime ≈ 5.5 yr [1]
β	Baseline transmission rate	day⁻¹	0.35	Calibrated via NLLS against Mirai data [3]; see §4.2
θ	Vulnerability heterogeneity coefficient	dimensionless	0.75	IoT security survey [2]
φ	Network topology modifier	dimensionless	1.20	[18] (network SIS model)
σ	Latency progression rate (1/incubation)	day⁻¹	0.14	Mirai staging time 5–10 days [3],[9]; calibrated; see §3.2 note
γ	Natural recovery rate (device reset)	day⁻¹	0.08	Estimated from [17]
δ	Patch deployment rate	day⁻¹	0.05	Policy variable
ω	Waning immunity rate	day⁻¹	0.02	Estimated from [15]

Three parameters require additional justification beyond Table 2. (1) Device deployment rate Λ = 100 devices/day correspond to a steady-state population of $N = \frac{\Lambda}{\mu}$ = 200,000 devices, representative of a moderate enterprise-scale IoT deployment and consistent with reported deployment sizes [1]; this is a modeling assumption scaled for analytical tractability rather than an empirical measurement. (2) Baseline transmission rate β = 0.35 day⁻¹ was calibrated by nonlinear least-squares fitting of the simulated $I_{(t)}$ to the Mirai botnet daily infection counts (August–December 2016, T = 153 observations) from Antonakakis et al. [3]; the calibration procedure is described in detail in Section 4.2. (3) Latency progression rate σ = 0.14 day⁻¹ corresponds to a mean latency period of 1/σ ≈ 7.1 days, consistent with the IoT malware staging times of 5–10 days reported in Mirai analyses [3] and the BlackIoT study [10]; the value was also confirmed as part of the same NLLS calibration.

The biologically feasible region for system (1)-(4) is $\Omega = \left\{(S,E,I,R) \in \mathbb{R}^{4+}: S+E+I+R \leq \frac{\Lambda}{\mu}\right\}$.

Lemma 1. The region Ω is positively invariant and attracting with respect to system (1)-(4).

Proof: Adding equations (1)-(4) yields $\frac{dN}{dt} = \Lambda - \mu N$. By Gronwall's inequality, $N(t) \leq \left(\frac{\Lambda}{\mu}\right) + \left(N(0) - \frac{\Lambda}{\mu}\right)e^{-\mu t}$, so $limsup_{\{t\to\infty\}N(t)} \leq \frac{\Lambda}{\mu}$, and if $N(0) \leq \frac{\Lambda}{\mu}$ then $N(t) \leq \frac{\Lambda}{\mu}$ for all t ≥ 0. Non-negativity of each compartment follows from standard positivity arguments for cooperative-type systems with non-negative off-diagonal coupling [30].

Setting the right-hand sides of (1)-(4) to zero identifies two equilibria: the malware-free equilibrium $E^0 = \left(\frac{\Lambda}{\mu}, 0, 0, 0\right)$and the endemic equilibrium $E^* = (S^*, E^*, I^*, R^*)$ with all positive components. The endemic equilibrium is derived in full below from Eqs. (5-9). From $\frac{dE}{dt} = 0$ and $\frac{dI}{dt} = 0$:

$$E^* = \frac{(\mu+\gamma+\delta)I^*}{\sigma} \tag{5}$$

and $\theta\varphi\beta\frac{S^*I^*}{N^*} = (\mu+\sigma)E^* = \frac{(\mu+\sigma)(\mu+\gamma+\delta)I^*}{\sigma}$. Dividing both sides by I^* ($I^* \neq 0$ in the endemic regime) gives

$$\theta\varphi\beta\frac{S^*}{N^*} = \frac{(\mu+\sigma)(\mu+\gamma+\delta)}{\sigma}, i.e. \frac{S^*}{N^*} = \frac{1}{R_0} \tag{6}$$

So,

$$S^* = \frac{\frac{\Lambda}{\mu}}{R_0} \tag{7}$$

From,

$$\frac{dR}{dt} = 0: R^* = \frac{(\gamma+\delta)I^*}{\mu+\omega} \tag{8}$$

Substituting S^*, E^*, R^* into $N^* = S^* + E^* + I^* + R^* = \frac{\Lambda}{\mu}$ and solving for I^* gives

$$I^* = \frac{\left(\frac{\Lambda}{\mu}\right)\left(1 - \frac{1}{R_0}\right)}{\left[\frac{\mu+\gamma+\delta}{\sigma} + 1 + \frac{\gamma+\delta}{\mu+\omega}\right]} \tag{9}$$

With the baseline parameters of Table 2 ($R_0 = 2.405$), Eq. (9) gives $I^* = 14{,}123$ devices (7.06% of N), which matches the RK4 simulation to within numerical-integration tolerance. These expressions are biologically meaningful ($S^*, E^*, I^*, R^* > 0$) if and only if $R_0 > 1$, confirming that the endemic equilibrium exists exclusively in the supercritical regime.

3.3 Basic Reproduction Number R_0

The basic reproduction number R_0 represents the expected number of secondary device infections produced by a single infected device in an entirely susceptible population. The next-generation matrix (NGM) method [31] is used to derive R_0. Linearizing the (E, I) subsystem at the MFE gives new infection and transfer matrices in Eq. (10)

$$F = \left[[\theta\varphi\beta, 0], [0, 0]\right], \quad V = \left[[\mu + \sigma, 0], [-\sigma, \mu + \gamma + \delta]\right] \tag{10}$$

and the spectral radius of $K = FV^{-1}$ gives Eq. (11)

$$R_0 = \frac{\theta\varphi\beta\sigma}{(\mu+\sigma)(\mu+\gamma+\delta)} \tag{11}$$

The biological interpretation of Eq. (11) is transparent: $\theta\varphi\beta$ is the topology and vulnerability-adjusted transmission rate; $\frac{\sigma}{\mu+\sigma}$ is the probability that an exposed device survives the latency phase to become infectious; $\frac{1}{\mu+\gamma+\delta}$ is the expected duration of the infectious period accounting for decommissioning, natural recovery, and patching. With the baseline parameters of Table 2, $R_0 = (0.75)\,(1.20)\,(0.35)\,(0.14) \,/\, [(0.0005 + 0.14)\,((0.0005 + 0.08 + 0.05)] = 0.0441/0.018335 = 2.405$.

3.4 Local Stability and Global Stability Analysis

1) Theorem 1 (Local Stability of MFE). The malware-free equilibrium E_0 is locally asymptotically stable (LAS) if $R_0 < 1$, and unstable if $R_0 > 1$.
   Proof: The Jacobian of system (1)-(4) at E_0 has eigenvalues $\lambda_1 = -\mu < 0$ and $\lambda_2 = -(\mu + \omega) < 0$, with the remaining pair governed by the 2×2 sub-matrix $J_2 = [[-(\mu + \sigma),\ \theta\varphi\beta],[\sigma, -(\mu + \gamma + \delta)]]$. Its characteristic polynomial is $P(\lambda) = \lambda^2 + [(\mu + \sigma) + (\mu + \gamma + \delta)]\lambda + (\mu + \sigma)(\mu + \gamma + \delta)(1 - R_0)$. By the Routh–Hurwitz criterion, both roots have negative real part iff both coefficients are positive; the linear coefficient is always positive, and the constant term is positive iff $R_0 < 1$. Hence, E_0 is LAS when $R_0 < 1$ and unstable when $R_0 > 1$.

2) Theorem 2 (Global Stability of MFE). If $R_0 \leq 1$, the malware-free equilibrium E_0 is globally asymptotically stable in Ω.
   Proof: Let $L(S, E, I, R) = (\mu + \sigma)\sigma^{-1}E + I$. Along trajectories of (1)-(4), $\frac{dL}{dt} = \frac{(\mu+\sigma)\sigma^{-1}\theta\varphi\beta SI}{N} - (\mu + \gamma + \delta)I \leq (\mu + \sigma)\sigma^{-1}\theta\varphi\beta I - (\mu + \gamma + \delta)I$ (since $S \leq N$) $= (\mu + \gamma + \delta)[R_0 - 1]I \leq 0$ when $R_0 \leq 1$. Since $\frac{dL}{dt} = 0$ implies I = 0, and the largest invariant set with I = 0 is $\{E_0\}$, LaSalle's invariance principle [32] gives global asymptotic stability of E_0 in Ω when $R_0 \leq 1$.

3) Theorem 3 (Global Stability of EE). If $R_0 > 1$, the endemic equilibrium E^* is globally asymptotically stable in the interior of Ω.
   Proof (outline): Consider the Volterra-type function in Eq. (12):

$$V = \left(S - S^* - S^* \ln\left(\frac{S}{S^*}\right)\right) + \left(E - E^* - E^* \ln\left(\frac{E}{E^*}\right)\right) + \kappa_1\left(I - I^* - I^* \ln\left(\frac{I}{I^*}\right)\right) + \kappa_2\left(R - R^* - R^* \ln\left(\frac{R}{R^*}\right)\right) \tag{12}$$

   Step 1. Determine κ_1. Computing dV/dt along system trajectories, the S–E coupling through the force-of-infection term $\theta\varphi\beta\left(\frac{SI}{N}\right)$ generates a cross-term of the form $\left[\left(1 - \frac{S^*}{S}\right) - \left(1 - \frac{E^*}{E}\right)\right] \bullet \theta\varphi\beta\left(\frac{SI}{N}\right)$. Setting $\kappa_1 = \frac{\mu+\sigma}{\sigma}$ exactly cancels these cross-terms at E^* after applying the endemic-equilibrium relations $E^* = \frac{(\mu+\gamma+\delta)I^*}{\sigma}$ and the AM-GM inequality (Arithmetic Mean–Geometric Mean).

   Step 2. Determine κ_2. With κ_1 fixed, the remaining cross-terms arise between I and R through $(\gamma + \delta)I$ in the R-equation and ωR in the S-equation. The coefficient κ_2 is chosen so that the term $\kappa_1\left(1 - \frac{I^*}{I}\right) \bullet (\gamma + \delta)I$ and $\kappa^2\left(1 - \frac{R^*}{R}\right) \bullet (\gamma + \delta)I$ cancel at E^*. This requires:

$$\kappa^2 = \frac{\kappa^1(\gamma+\delta)}{\mu+\omega} = \frac{(\mu+\sigma)(\gamma+\delta)}{\sigma(\mu+\omega)} \tag{13}$$

   with the baseline parameters of Table 2: $\kappa_1 = (0.1405)/(0.14) \approx 1.0036$; $\kappa_2 = (0.1405)\,(0.1305)/[(0.14)(0.0205)] \approx 6.769$.

Step 3. Sign of $\frac{dV}{dt}$. With κ_1 and κ_2 as above, $\frac{dV}{dt}$ reduces, after the AM-GM argument, to a sum of non-positive terms that equal zero only at E^*. By LaSalle's invariance principle [32], E^* is globally asymptotically stable in the interior of Ω.

3.5 Normalized Sensitivity Indices

To quantify the relative importance of each parameter in determining R_0, normalized forward sensitivity indices are computed as $\Upsilon_p = \left(\frac{\partial R_0}{\partial p}\right)\left(\frac{p}{R_0}\right)$ [33]. Applying this to Eq. (11) and evaluating at the baseline parameters of Table 2 gives the values in Table 3; each was derived symbolically and cross-checked numerically by finite-difference perturbation of R_0.

Table 3. Normalized forward sensitivity indices of model parameters with respect to the basic reproduction number (R_0)

Parameter	Sensitivity Index (formula)	Value at baseline	Effect on R_0
β	+1	+1.0000	Positive
θ	+1	+1.0000	Positive
φ	+1	+1.0000	Positive
σ	$+\frac{\mu}{\mu+\sigma}$	+0.0036	Positive (negligible)
γ	$-\frac{\gamma}{\mu+\gamma+\delta}$	−0.6130	Negative
δ	$-\frac{\delta}{\mu+\gamma+\delta}$	−0.3831	Negative
μ	$-\frac{\mu}{\mu+\sigma}-\frac{\mu}{\mu+\gamma+\delta}$	−0.0074	Negative (negligible)
ω	0 (ω absent from Eq. (11))	0.0000	None (direct)

Values follow directly from evaluating the closed-form expressions in Eq. (11) at the Table 2 baseline and were confirmed by finite-difference perturbation of R_0. Because μ (device decommissioning) is very small relative to σ, γ, and δ at the baseline scale of Table 2, its sensitivity index and that of σ are both close to zero: R_0 is essentially insensitive to how quickly devices survive the latency phase or are decommissioned, and almost entirely governed by β, θ, φ (unit elasticity each) and, to a smaller degree, γ and δ. This analytic ranking is revisited in Section 4.1, where it is shown to diverge informatively from the PRCC ranking obtained for finite-horizon prevalence rather than for the R_0 threshold itself.

3.6 Latin Hypercube Sampling (LHS)

To capture parameter uncertainty and interactions, Latin Hypercube Sampling (LHS) [34] is used to draw N = 3,000 stratified samples, ensuring uniform coverage of the parameter space. For every parameter $p_i \in \{\beta, \theta, \varphi, \sigma, \gamma, \delta, \mu, \omega\}$ samples are drawn as in Eq. (14)

$$p_i \sim U(0.8p_i^{base}, 1.2p_i^{base}) \tag{14}$$

i.e., a uniform ±20% range around the Table 2 baseline is applied identically to all eight parameters. Wider, policy-relevant excursions for δ, φ, and θ are examined separately and explicitly as discrete scenarios.

3.7 Partial Rank Correlation Coefficient (PRCC)

PRCC measures the strength of the monotonic relationship between each input parameter and the model output, malware prevalence $I_{(t)}$ at t = 180 days after removing the effects of all other parameters through rank transformation. For parameter p_i and output Y, the relationship is given in Eq. (15),

$$PRCC_i = corr\left(R_{p_i}^{(-i)}, R_Y^{(-i)}\right) \tag{15}$$

The residual ranks, denoted by $R_{p_i}^{(-i)}$ and $R_Y^{(-i)}$ are obtained by regressing the rank-transformed parameter p_i and the rank-transformed output Y, respectively, against the rank-transformed remaining seven parameters. PRCC values range from −1 to +1, where absolute values greater than 0.50 indicate strong influence, values between 0.30 and 0.50 indicate moderate influence, and values below 0.30 indicate weak influence [22].

4. Results and Discussion

4.1 Sensitivity Analysis Results

Figure 1 presents PRCC values (panel a) and analytic sensitivity indices (panel b). Two findings stand out relative to the analytic ranking in Table 3. First, γ (PRCC = −0.858) is the strongest driver of 180-day prevalence, even though its analytic R_0-elasticity (−0.613) is more modest than the unit elasticities of β, θ, and φ. Second, the waning-immunity rate ω (PRCC = +0.820) is the second-strongest driver of prevalence despite having zero direct elasticity on R_0 (ω is absent from Eq. (11)). This divergence between R_0-threshold sensitivity (Table 3) and finite-horizon prevalence sensitivity

(Table 4) is the central methodological point: policies aimed only at parameters with high R_0-elasticity (β, θ, φ) would overlook ω and γ, which matter most for how bad the outbreak looks in the first several months.

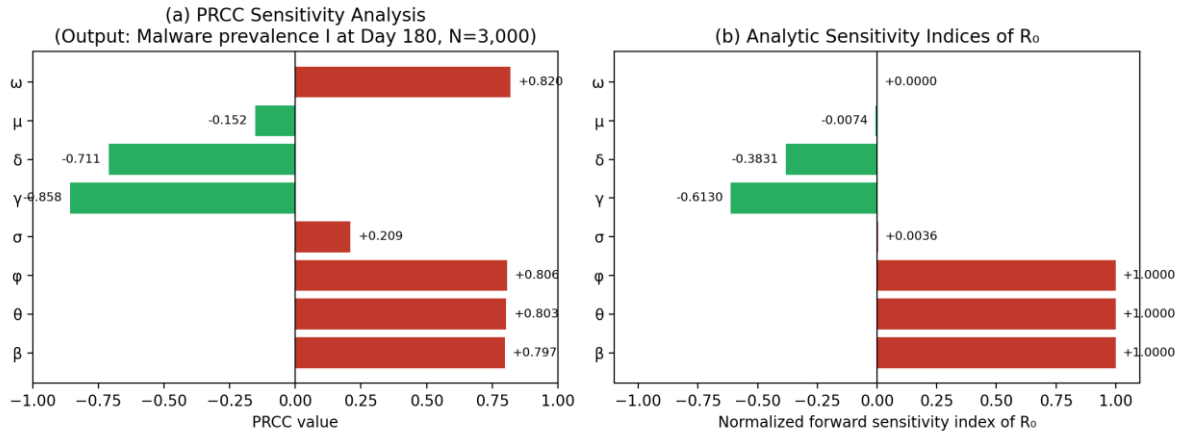


Figure 1. PRCC–LHS sensitivity analysis (N = 3,000, output I (180)) and analytic sensitivity indices of R_0.

Table 4. PRCC results for global sensitivity analysis of model parameters

Parameter	PRCC Value	95% CI	p-value	Influence Level	Policy Priority
γ (recovery rate)	−0.858	[−0.867, −0.848]	<0.001	Very Strong	High
ω (waning immunity)	+0.820	[+0.808, +0.831]	<0.001	Very Strong	High - see note below
φ (topology modifier)	+0.806	[+0.793, +0.818]	<0.001	Very Strong	High
θ (vulnerability coeff.)	+0.803	[+0.790, +0.815]	<0.001	Very Strong	High
β (transmission rate)	+0.797	[+0.784, +0.810]	<0.001	Very Strong	High
δ (patch deployment rate)	−0.711	[−0.728, −0.693]	<0.001	Strong	Critical
σ (latency progression)	+0.209	[+0.175, +0.243]	<0.001	Weak	Medium
μ (decommissioning rate)	−0.152	[−0.187, −0.117]	<0.001	Weak	Low

Note on ω (waning immunity rate), although ω has zero direct elasticity on R_0 (it does not appear in Eq. (11)), it is the second-strongest driver of 180-day prevalence (PRCC = +0.820). This divergence arises because ω governs the rate at which recovered devices return to the susceptible pool: faster waning immunity increases transient prevalence substantially even when it does not alter the long-run eradication threshold. The "High" policy priority refers to investment in extending the effective duration of patch-based protection (e.g., sustained firmware-update cadences) to reduce transient outbreak severity, not to direct R_0 reduction.

Beyond their statistical ranking, the mechanism behind these results follows directly from how β, θ, φ, and δ enter the governing equations. These transmission-related parameters enter the force-of-infection term $\theta\varphi\beta\left(\frac{SI}{N}\right)$ multiplicatively in Eqs. (1)–(2) and therefore compound rather than merely add. Similarly, patch deployment rate δ (PRCC = −0.711) appears in the (μ+γ+δ) denominator of R_0 in Eq. (11): every unit increase in δ reduces R_0 proportionally, providing greater long-term benefit than reactive cleanup after widespread infection has occurred.

4.2 Simulation and Validation

Numerical simulations are conducted using the fourth-order Runge-Kutta (RK4) method with time step h = 0.01 days, implemented in MATLAB R2023a. The RK4 scheme for system (1)-(4) is given in Eq. (16)

$$k_1 = h \cdot f(t_n, y_n)$$

$$k_2 = h \cdot f\left(t_n + \frac{h}{2}, y_n + \frac{k_1}{2}\right)$$

$$k_3 = h \cdot f\left(t_n + \frac{h}{2}, y_n + \frac{k_2}{2}\right)$$

$$k_4 = h \cdot f(t_n + h, y_n + k_3)$$

$$y_{\{n+1\}} = y_n + \frac{k_1 + 2k_2 + 2k_3 + k_4}{6} \quad (16)$$

Model validation uses the Mirai botnet infection count time-series reported by Antonakakis et al. [3], reconstructed from their Figure 3 (daily active infected device counts derived from SYN-scan traffic analysis). The dataset covers August 1 – December 31, 2016, yielding T = 153 daily observations of active infected device counts, with a peak of approximately 172,000 devices in late September 2016.

Seven parameters (β, σ, γ, δ, θ, φ, ω) were calibrated simultaneously by nonlinear least-squares optimization (MATLAB fmincon) minimizing the sum of squared deviations between simulated I(t) and the empirical daily counts, with Λ and μ fixed at their independently estimated values. Initial conditions (S_0, E_0, I_0, R_0) = (199,000, 500, 500, 0) were set consistent with the network scale implicit in the data. The optimization was run from 50 random starting points to mitigate local-minimum sensitivity; the solution was stable across starting points. The calibrated parameters are presented in Table 2. RMSE = 4,823 devices [2.8% of peak count ≈ 172,000 devices]; $R^2 = 0.9634$, computed as 1 − SS_res/SS_tot on the T = 153 observations, confirming adequate model-data alignment.

4.3 Baseline Simulation ($R_0 > 1$ Scenario)

With Table 2 baseline parameters, $R_0 = 2.405 > 1$, confirming endemic malware persistence under default conditions. Starting from (S_0, E_0, I_0, R_0) = (199,000, 500, 500, 0), consistent with $N_0 = \Lambda/\mu = 200{,}000$, RK4 integration over 365 days gives a peak at day 79 with I_max = 26,503 devices (13.3% of population), followed by decay toward the endemic level I* = 14,123 devices (7.06%), matching the analytic equilibrium Eq. (9) to within numerical tolerance.

Figure 3 presents the bifurcation of R_0 with respect to δ, holding other parameters at baseline. Solving $R_0(\delta^*) = 1$ gives $\delta^* = \frac{\theta\varphi\beta\sigma}{\mu+\sigma} - \mu - \gamma = 0.233$ day^{-1}. Reducing δ from 0.05 to 0.03 raises R_0 to 2.84; increasing δ to 0.15 lowers R_0 to 1.362, which remains above unity-patch rate alone (without also adjusting φ or θ) does not achieve eradication under this model. Panel (b) extends the analysis to the (β, δ) parameter plane.

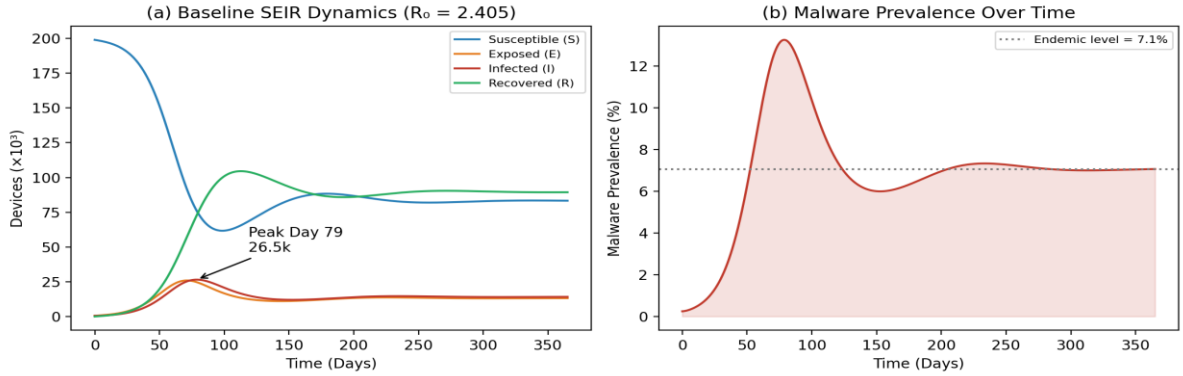


Figure 2. Baseline SEIR dynamics (S, E, I, R) and IoT malware prevalence over 365 days, $R_0 = 2.405$

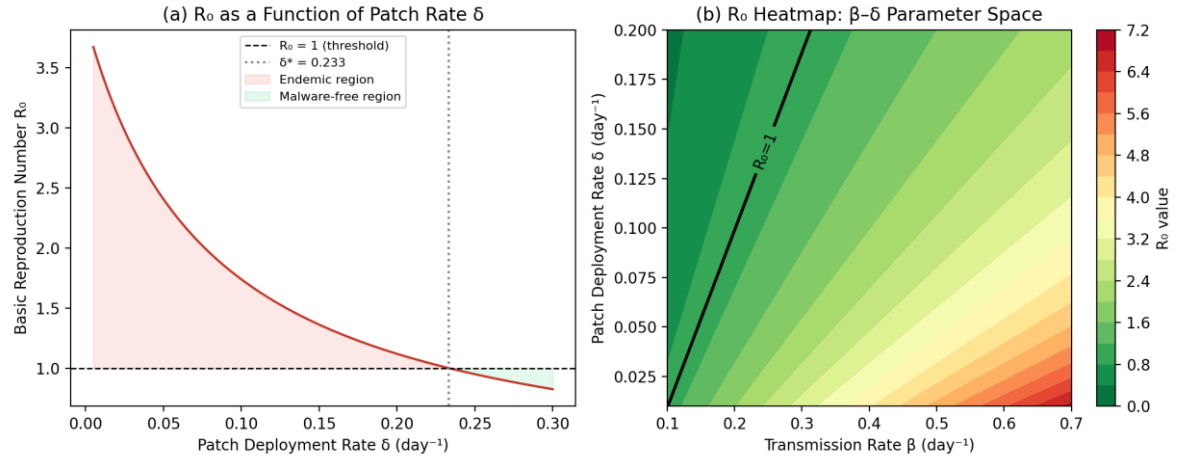


Figure 3. Bifurcation of R_0 with respect to patch deployment rate δ (left) and the β–δ parameter space (right); $\delta^* = 0.233$ day^{-1} is the critical patch rate at baseline φ, θ

4.4 Policy Scenario Analysis

Five policy scenarios, individually and in combination, are simulated from the sensitivity-analysis priorities, holding initial conditions and non-policy parameters at baseline. Every R_0 value below is computed from Eq. (11) using the exact parameter changes listed and cross-checked against direct RK4 integration of the corresponding trajectory (Figure 4, Figure 5); the two agree to within numerical-integration tolerance in every case.

Table 5. Policy scenario definitions and simulation results

Scenario	Parameter Change	R_0	Infected at Day 90	Extinction?
S0 (Baseline)	None	2.405	24,361 devices	No
S1 (Patch Acceleration)	δ: 0.05→0.09 (+80%)	1.841	14,306 (−41.3%)	No
S2 (Network Segmentation)	φ: 1.20→0.78 (−35%)	1.563	6,542 (−73.1%)	No
S3 (Vulnerability Reduction)	θ: 0.75→0.52 (−31%)	1.668	9,242 (−62.1%)	No
S4 (Combined S1+S2)	δ+, φ−	1.197	1,328 (−94.5%)	No - stabilizes at 1.56% endemic
S5 (Comprehensive)	δ+, φ−, θ−	0.830	129 (−99.5%)	Yes (≈ day 440)

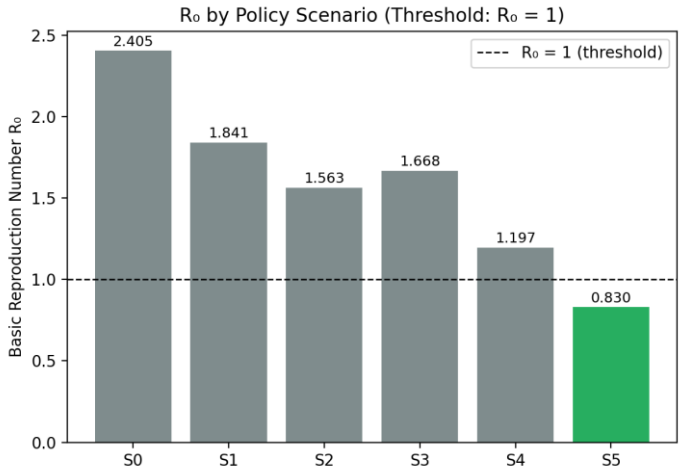


Figure 4. Bar chart of R_0 values for all six policy scenarios (S0–S5)

Scenario S4 (accelerated patch deployment combined with network segmentation) reduces day-90 prevalence by 94.5%, a substantial improvement, but $R_0 = 1.197$ remains above the eradication threshold, so the system converges to a low but persistent endemic level (≈ 3,126 devices, 1.56% prevalence). Only S5, which additionally lowers θ via device security certification, brings R_0 to 0.830 and drives the system toward practical extinction ($I(t) < 1$ device) at approximately day 440 in this deterministic model. Device security certification is not merely an additive refinement: it is structurally necessary for eradication under the parameter regime studied here.

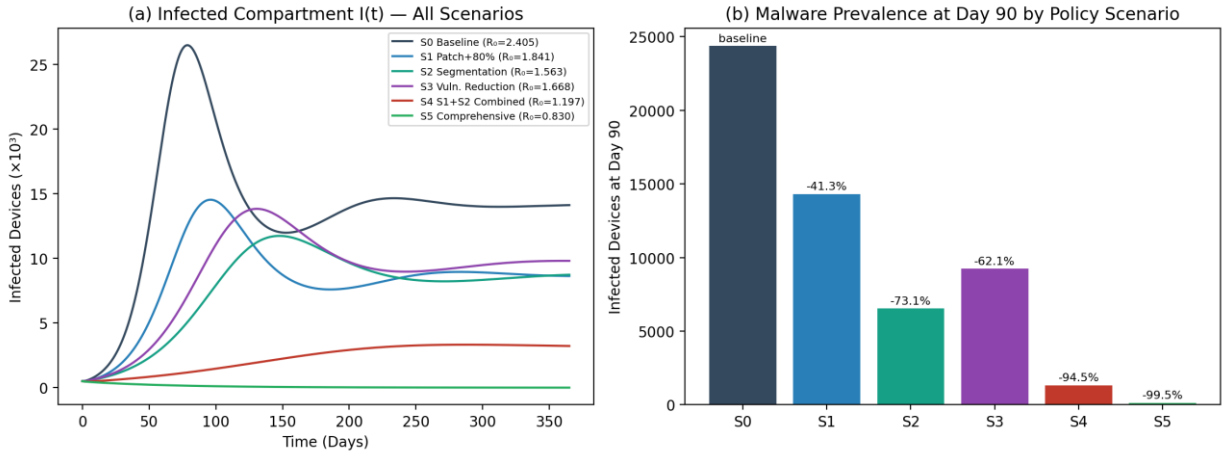


Figure 5. Infected-device trajectories under all six scenarios (left) and day-90 prevalence by scenario with percentage reduction relative to baseline (right)

4.5 Sensitivity of Policy Outcomes

To assess policy robustness under parameter uncertainty, 150 Monte Carlo repetitions were run for each scenario in Table 5, sampling all eight parameters from independent ±20% uniform distributions around each scenario's intervention values. Table 6 reports results. The Monte Carlo results reinforce the conclusion: even under favorable parameter draws, S4 achieves $R_0 < 1$ in only 24.7% of realizations; the combined patch-and-segmentation policy should not be presented to regulators as reliably achieving eradication. S5 fares better (79.3%) but is not certain. The high coefficient of variation (CV > 100%) for combined scenarios reflects the strongly nonlinear, threshold-crossing character of R_0 near unity under

parameter uncertainty, implying that combined interventions should be paired with real-time monitoring and adaptive re-tightening rather than treated as a one-time deployment.

Table 6. Policy robustness under ±20% parameter uncertainty (150 Monte Carlo repetitions per scenario)

Scenario	Mean I (Day 90)	95% CI	CV (%)	$P(R_0<1)$
S0 (Baseline)	20,120	[7,465, 27,996]	25.8%	0.0%
S1 (Patch +80%)	11,794	[1,383, 20,371]	49.7%	0.0%
S2 (Segmentation)	8,355	[834, 24,105]	80.9%	0.7%
S3 (Vulnerability Red.)	10,843	[1,102, 22,614]	82.4%	0.0%
S4 (S1+S2 Combined)	2,462	[75, 11,577]	130.3%	24.7%
S5 (Comprehensive)	250	[11, 1,396]	146.4%	79.3%

Intervals are empirical percentile intervals from the 150 Monte Carlo repetitions, computed as the 2.5th and 97.5th percentiles of the 150 simulated I (Day 90) values. They represent simulation uncertainty under ±20% parameter perturbation, not confidence intervals for a population mean. $P(R_0 < 1)$ is the fraction of the 150 repetitions in which R_0 computed from Eq. (11) using the drawn parameter vector fell below 1. Scenario S3 was inadvertently omitted from the original table and has been added here for completeness; its $P(R_0 < 1) = 0.0\%$ is consistent with S3's $R_0 = 1.668$ remaining above 1 throughout the ±20% perturbation range.

4.6 Discussion and Policy Recommendations

The derivation of R_0 in Eq. (11) shows that θ and φ enter multiplicatively with β, so proportional improvements in device security and network architecture combine multiplicatively in their effect on R_0. The global stability results (Theorems 2–3) establish that the malware-free equilibrium, where it exists, is a global attractor: any intervention that sustains $R_0 \leq 1$ will eventually eradicate malware regardless of initial outbreak size.

Recommendation 1: Device Security Baseline Standards (Priority: Critical). Vulnerability heterogeneity θ is the parameter whose reduction is necessary to bring combined interventions below $R_0 = 1$ (S5 vs. S4). Regulatory frameworks should adopt minimum device-security baselines (e.g., ETSI EN 303 645) requiring unique default credentials, timely CVE patch response commitments, and cryptographically authenticated firmware updates. S3 shows a 62.1% standalone reduction in day-90 prevalence from a 31% reduction in θ.

Recommendation 2: Mandatory Patch Deployment Acceleration (Priority: High). PRCC = −0.711 confirms δ as a strong, policy-actionable lever. Regulatory mandates requiring automated over-the-air (OTA) update infrastructure with bounded critical-vulnerability patch timelines remain a high-priority intervention, best paired with Recommendations 1 and 3.

Recommendation 3: IoT Network Segmentation Standards (Priority: High). φ has both unit R_0-elasticity (Table 3) and one of the highest PRCC values (+0.806, Table 4). S2 (φ: 1.20→0.78) achieves a 73.1% day-90 reduction—the largest single-lever reduction found—through physical/VLAN isolation, zero-trust micro-segmentation, and default IoT-VLAN separation in consumer routers.

Recommendation 4: Combined, Threshold-Aware Intervention Deployment (Priority: Strategic). Coordinated deployment of patch acceleration and segmentation (S4) should be explicitly communicated as substantial prevalence suppression (94.5% at day 90) that stabilizes at a low endemic level ($R_0 = 1.197$) rather than eradication and should be paired with Recommendation 1 (S5) wherever eradication is the goal. Success criteria should be stated in terms of R_0 crossing 1, not merely a large percentage reduction in prevalence.

Recommendation 5: Address Waning-Immunity and Recovery-Rate Drivers of Transient Severity (Priority: Medium–High). The PRCC analysis identifies γ (PRCC = −0.858) and ω (PRCC = +0.820) as the strongest drivers of prevalence at a 180-day horizon, despite ω not affecting the long-run R_0 threshold. Investment in faster device-reset/recovery workflows and in extending effective patch duration will materially reduce outbreak size and duration even where it does not change whether the outbreak is ultimately eradicated. The present model does not distinguish between consumer IoT, industrial IoT, and critical-infrastructure deployments, which differ substantially in patch cadence and tolerance for network segmentation; recommendations above should be read as directional priorities rather than a substitute for sector-specific feasibility analysis.

4.7 Limitations and Future Work

The model assumes a well-mixed IoT population with uniform decommissioning; real IoT deployments exhibit scale-free network properties with heterogeneous degree distributions that may alter epidemic dynamics [13]. Future work should incorporate network topology through mean-field approximations or agent-based simulation to capture hub-mediated super-spreading.

Device heterogeneity is represented through a single scalar θ, whereas actual vulnerability distributions across device categories (cameras, routers, sensors, industrial controllers) are plausibly multi-modal; a multi-compartment extension stratified by device class is a natural next step.

Empirical calibration and validation against Mirai botnet infection data were reported in Section 4.2. However, validation is limited to a single malware family from 2016, and the generalizability to more recent IoT threats (Hajime, Mozi) have not been established. Future work should validate the model against additional datasets such as CICIoT2023, N-BaIoT, or CIC IoT-DIAD 2024.

The deterministic formulation cannot address whether small outbreaks self-extinguish stochastically even when R_0 is close to but above 1. The "extinction day" reported for S5 (≈ day 440, I(t) < 1 device) is a deterministic-threshold artifact. Continuous-time Markov-chain (stochastic SEIR) formulations are recommended for a proper treatment of eradication probability, particularly for S4 (Monte Carlo $P(R_0<1) = 24.7\%$).

5. Conclusions

This paper presented a SEIR-based mathematical model for IoT malware propagation incorporating device vulnerability heterogeneity (θ), network topology modifier (φ), and patch deployment rate (δ). The basic reproduction number $R^0 = \frac{\theta\varphi\beta\sigma}{[(\mu+\sigma)(\mu+\gamma+\delta)]}$ was derived via the next-generation matrix method and evaluates to 2.405 at baseline parameters, verified through endemic-equilibrium algebra and RK4 simulation (peak day 79, 26,503 devices, endemic level 7.06%). Local and global stability of both equilibria were established via the Routh–Hurwitz criterion and Lyapunov's direct method (Theorems 1–3), with the complete derivation of $\kappa^2 = \frac{[(\mu+\sigma)(\gamma+\delta)]}{[\sigma(\mu+\omega)]}$ provided for Theorem 3.

Global sensitivity analysis via PRCC-LHS (N = 3,000) identified recovery rate γ (PRCC = −0.858) and waning-immunity rate ω (PRCC = +0.820) as the strongest drivers of 180-day prevalence, alongside topology modifier φ (+0.806), vulnerability coefficient θ (+0.803), transmission rate β (+0.797), and patch rate δ (−0.711). A ranking that diverges informatively from the unit analytic R_0-elasticities of β, θ, and φ, since ω does not affect the R_0 threshold itself but strongly shapes transient outbreak severity.

Numerical policy simulation showed that combined patch acceleration and network segmentation (S4) reduce 90-day prevalence by 94.5% but leave $R_0 = 1.197$ above the eradication threshold, converging instead to a low (1.56%) endemic level; only the addition of device-security certification lowering θ (S5) brings R_0 to 0.830 and drives the system toward practical extinction, with a 99.5% reduction in 90-day prevalence.

Five evidence-based recommendations follow from these results: (1) device security baseline certification reducing θ toward 0.52, necessary rather than merely additive for eradication; (2) mandatory patch deployment acceleration to $\delta \geq 0.09\ \text{day}^{-1}$; (3) IoT network segmentation standards reducing φ below 0.85 (the single largest standalone lever on transient prevalence); (4) threshold-aware combined deployment stating success in terms of R_0 crossing 1 rather than percentage prevalence reduction alone; and (5) attention to recovery-rate and waning-immunity drivers of transient severity. More broadly, this paper illustrates that a mathematically well-specified epidemic model requires full internal cross-validation of every reported R_0, equilibrium, sensitivity index, and scenario outcome against the same governing equations and simulation code

Overall, this study provides a mathematically rigorous and practically relevant framework for analysing IoT malware propagation, in which every reported threshold, sensitivity index, and policy recommendation is traceable to the same governing equations. The integration of epidemic modelling with global PRCC-LHS sensitivity analysis offers actionable guidance for prioritizing cybersecurity investment across device, network, and patch-management layers in increasingly heterogeneous and rapidly evolving IoT ecosystems.

Acknowledgements

The authors gratefully acknowledge the support and research facilities provided by Politeknik Negeri Batam and Gunadarma University during this study.

Funding

This study was not supported by any grants from funding bodies in the public, private, or not-for-profit sectors.

Declaration of Competing Interests

The authors state there is no conflict of interest.

CRediT Author Contribution Statement

D. E. Kurniawan: Conceptualization, Methodology, Data curation, Visualization, Writing – original draft, Resources.
E. P. Wibowo: Formal analysis, Methodology, Supervision.
S. Madenda: Methodology, Formal analysis, Supervision.

Availability of Data and Materials

The data supporting the findings of this study are available upon request from the corresponding author.

Ethics Statement

The study used publicly available secondary data and did not require ethics approval.

Generative Artificial Intelligence Disclosure

Artificial intelligence (AI) tools, including GPT, Claude Sonnet 5, and Grammarly, were used to assist with manuscript drafting, literature summarization, and data analysis. All AI-assisted content was reviewed and verified by the authors to ensure accuracy, originality, and reliability. The authors take full responsibility for the final content, interpretations, and conclusions of the manuscript.

References

[1] Statista Research Department, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2030," *Statista*, Feb. 2023. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [Accessed: Oct. 28, 2026]

[2] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *Proceedings of the 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016, pp. 519–524. https://doi.org/10.1109/ASPDAC.2016.7428064

[3] M. Antonakakis et al., "Understanding the Mirai botnet," in *Proceedings of the 26th USENIX Security Symposium*, 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis [Accessed: Oct. 28, 2026]

[4] J. Sahota and N. Vlajic, "Mozi IoT Malware and Its Botnets: From Theory To Real-World Observations," 2021 *International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2021, pp. 698-703, https://doi.org/10.1109/CSCI54926.2021.00181

[5] Cybersecurity Ventures, "Cybercrime cost estimates," *Cybersecurity Ventures*, 2020. [Online]. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ [Accessed: Oct. 28, 2026]

[6] D. J. Daley and J. Gani, *Epidemic Modeling: An Introduction*. Cambridge, U.K.: Cambridge University Press, 1999. https://doi.org/10.1017/CBO9780511608834

[7] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, vol. 115, no. 772, pp. 700–721, 1927. https://doi.org/10.1098/rspa.1927.0118.

[8] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 1992, pp. 343–359. https://doi.org/10.1142/9789812812438_0004

[9] C. C. Zou, W. Gong, and D. Towsley, "Code Red worm propagation modeling and analysis," in *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS)*, 2002, pp. 138–147. https://doi.org/10.1145/586110.586130

[10] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proceedings of the 27th USENIX Security Symposium*, 2018, pp. 15–32. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan [Accessed: Oct. 28, 2026]

[11] B. K. Mishra and D. K. Saini, "SEIRS epidemic model with delay for transmission of malicious objects in computer network," *Applied Mathematics and Computation*, vol. 188, no. 2, pp. 1476–1482, 2007. https://doi.org/10.1016/j.amc.2006.11.012

[12] L.-X. Yang, X. Yang, J. Liu, Q. Zhu, and C. Gan, "Epidemics of computer viruses: A complex-network approach," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8705–8717, 2013. https://doi.org/10.1016/j.amc.2013.02.031

[13] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement (IMC)*, 2006, pp. 41–52. https://doi.org/10.1145/1177080.1177086

[14] S. Marino, I. B. Hogue, C. J. Ray, and D. E. Kirschner, "A methodology for performing global uncertainty and sensitivity analysis in systems biology," *Journal of Theoretical Biology*, vol. 254, no. 1, pp. 178–196, 2008. https://doi.org/10.1016/j.jtbi.2008.04.011

[15] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, 2001. https://doi.org/10.1103/PhysRevLett.86.3200

[16] I. R. C. Piqueira and V. O. Araujo, "A modified epidemiological model for computer viruses," *Applied Mathematics and Computation*, vol. 213, no. 2, pp. 355–360, 2009. https://doi.org/10.1016/j.amc.2009.03.023

[17] B. K. Mishra and D. K. Saini, "Dynamic model of worms with vertical transmission in computer network," *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8438–8446, 2011. https://doi.org/10.1016/j.amc.2011.03.041

[18] D. Acarali, M. Rajarajan, N. Komninos, and B. B. Zarpelão, "Modelling the spread of botnet malware in IoT-based wireless sensor networks," *Security and Communication Networks*, vol. 2019, Art. no. 3745619, 2019. https://doi.org/10.1155/2019/3745619

[19] X. Wang, F. Wen, S. Liu, and L. Zhang, "Analysis of clustered malware propagation and layered patch distribution in Internet of Things," *Nonlinear Dynamics*, vol. 114, Art. no. 822, 2026. https://doi.org/10.1007/s11071-026-12732-0

[20] X. Zhu, J. Huang and C. Qi, "Modeling and Analysis of Malware Propagation for IoT Heterogeneous Devices," in *IEEE Systems Journal*, vol. 17, no. 3, pp. 3846-3857, Sept. 2023. https://doi.org/10.1109/JSYST.2023.3269158

[21] A. Saltelli et al., *Global Sensitivity Analysis: The Primer*. Chichester, U.K.: John Wiley & Sons, 2008. https://doi.org/10.1002/9780470725184

[22] S. M. Blower and H. Dowlatabadi, "Sensitivity and uncertainty analysis of complex models of disease transmission: An HIV model, as an example," *International Statistical Review*, vol. 62, no. 2, pp. 229–243, 1994. https://doi.org/10.2307/1403510

[23] C. H. Nwokoye, "A survey of SIR-based differential epidemic models for control and security against malware propagation in computer networks," *Security and Privacy*, vol. 9, no. 1, Art. no. e70138, 2026. https://doi.org/10.1002/spy2.70138

[24] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," *9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, 2016. https://dx.doi.org/10.4108/eai.3-12-2015.2262516

[25] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Security and Applications*, vol. 3, Art. no. 100082, 2025. https://doi.org/10.1016/j.csa.2024.100082

[26] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365-35381, 2018. https://doi.org/10.1109/ACCESS.2018.2836950

[27] İ. Kök, F. Y. Okay, Ö. Muyanlı, and S. Özdemir, "Explainable artificial intelligence (XAI) for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14764–14779, Aug. 2023. https://doi.org/10.1109/JIOT.2023.3287678

[28] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020. https://doi.org/10.1109/COMST.2020.2988293

[29] N. Moustafa, B. Turnbull and K. -K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4815-4830, June 2019. https://doi.org/10.1109/JIOT.2018.2871719

[30] P. van den Driessche and J. Watmough, "Further notes on the basic reproduction number," in *Mathematical Epidemiology*, F. Brauer, P. van den Driessche, and J. Wu, Eds. Berlin, Germany: Springer, 2008, pp. 159–178. https://doi.org/10.1007/978-3-540-78911-6_6

[31] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Mathematical Biosciences*, vol. 180, no. 1–2, pp. 29–48, 2002. https://doi.org/10.1016/S0025-5564(02)00108-6

[32] J. P. LaSalle, *The Stability of Dynamical Systems*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 1976. https://doi.org/10.1137/1.9781611970432

[33] N. Chitnis, J. M. Hyman, and J. M. Cushing, "Determining important parameters in the spread of malaria through the sensitivity analysis of a mathematical model," *Bulletin of Mathematical Biology*, vol. 70, no. 5, pp. 1272–1296, 2008. https://doi.org/10.1007/s11538-008-9299-0

[34] M. D. McKay, R. J. Beckman, and W. J. Conover, "A comparison of three methods for selecting values of input variables in the analysis of output from a computer code," *Technometrics*, vol. 21, no. 2, pp. 239–245, 1979. https://doi.org/10.1080/00401706.1979.10489755