Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 14** : 1–15.
ISSN-0037-8712
doi:10.5269/bspm.81583

A Reaction–Diffusion PDE Model for Cyberattack Propagation in Medical IoT Networks

Pankaj Kumar *, Pankaj Rai and Bimal Kumar Mishra

ABSTRACT: Medical Internet of Things (MIoT) networks are now deeply embedded in clinical environments, but their increasing connectivity also creates pathways for cyberattacks that can spread across devices rather than remain localized. Most existing studies emphasize intrusion detection or vulnerability analysis, offering limited insight into the spatio-temporal conditions under which attacks persist or die out in real hospital settings. This paper develops a reaction–diffusion partial differential equation model. By the use of reaction–diffusion partial differential equation model to study cyberattack propagation in MIoT networks while explicitly accounting for spatial device distribution, nonlinear interaction between devices, recovery through patching, and permanent isolation of compromised nodes. The proposed framework models secure, compromised, and recovered devices as spatially distributed populations. A basic reproduction number is derived to characterize a sharp threshold separating attack extinction from long-term persistence. Rigorous analysis establishes existence and uniqueness of solutions, positivity, boundedness, invariant regions, local stability of the disease-free equilibrium, and uniform persistence when the threshold is exceeded. Numerical simulations using finite difference methods validate the analytical results and reveal diffusion-driven spread, spatial clustering, and clear threshold behavior. The findings show that cyberattacks in MIoT networks behave as structured spreading processes rather than isolated events. The model provides a mathematically grounded basis for assessing cyber resilience and for designing mitigation strategies that balance vulnerability reduction, rapid recovery, and effective isolation in spatially distributed medical environments.

Keywords: Medical Internet of Things (MIoT), cyberattack propagation, reaction–diffusion model, partial differential equations, cyber-epidemic modeling, basic reproduction number, stability analysis, numerical simulation.

Contents

* Corresponding author.
2020 *Mathematics Subject Classification:* 68T07, 94A60, 90C35, 68M10, 62M45.
Submitted January 27, 2026. Published April 30, 2026.

1. Introduction

Medical Internet of Things (MIoT) systems have become a core component of contemporary healthcare infrastructure, enabling continuous monitoring, automated therapy delivery, and real-time clinical decision support. Devices such as infusion pumps, patient monitors, wearable sensors, and bedside gateways operate in tightly coupled environments where availability, integrity, and timing are critical. As connectivity increases, however, these systems become vulnerable to cyberattacks that can propagate beyond isolated devices and affect entire clinical workflows [3] [18].

Unlike conventional enterprise networks, MIoT deployments exhibit strong spatial and operational constraints. Devices are distributed across wards, corridors, and intensive care units, and communication typically relies on short-range wireless protocols and shared gateways. As a result, compromise events often emerge locally and spread gradually through trusted communication paths rather than instantaneously across the entire network. Empirical studies and incident analyses indicate that such localized propagation can escalate into persistent system-wide disruptions if not contained early [11] [12].

From a modeling perspective, these characteristics closely resemble spreading processes studied in epidemiology and network science. Classical epidemic theory established that persistence and extinction of infections are governed by threshold parameters related to transmission and recovery rates [2]. Subsequent work extended these ideas to spatial domains, showing that diffusion and local interactions can produce wave-like propagation, clustering, and long-term persistence [14]. More recent research in networked systems has demonstrated that similar threshold phenomena arise in cyber and information diffusion processes [13] [9].

Several studies have adapted epidemic and reaction–diffusion models to cyber contexts. PDE-based formulations have been shown to capture malware propagation dynamics and enable analytical stability analysis in mobile and IoT networks [19] [7] [8]. Spatial modeling of cyber-physical systems further confirms that physical deployment and communication locality strongly influence attack persistence and containment effectiveness [19]. Recent work has also framed cybersecurity as a dynamic system subject to control and resilience constraints, emphasizing the need for mathematically grounded models that go beyond detection accuracy alone [21].

Despite these advances, MIoT-specific modeling gaps remain. Most detection-oriented studies, including recent deep learning based intrusion detection frameworks, focus on identifying malicious behavior but do not analyze long-term system dynamics after compromise [5]. Compartmental IoT attack models provide useful abstractions but often assume homogeneous mixing and neglect spatial propagation effects that are inherent in clinical environments [6]. Consequently, there is limited understanding of when cyberattacks in MIoT networks inevitably die out and when they persist despite mitigation efforts. This paper addresses this gap by proposing a reaction-diffusion partial differential equation model for cyberattack propagation in Medical IoT networks. The model explicitly incorporates spatial distribution, nonlinear

device interactions, recovery through patching, and permanent isolation mechanisms. A basic reproduction number is derived to characterize a sharp threshold between attack extinction and persistence. Rigorous analytical results establish well-posedness, positivity, invariant regions, equilibrium stability, and uniform persistence, and numerical simulations validate the theoretical findings. Together, these contributions provide a principled, system-level framework for reasoning about MIoT cyber resilience in spatially distributed clinical environments.

2. Literature Review

Security of Medical Internet of Things networks has attracted increasing research attention due to the safety-critical nature of healthcare environments. Existing studies largely fall into two broad categories: data-driven intrusion detection approaches and analytical or compartmental modeling approaches. While both streams contribute valuable insights, each addresses only part of the underlying problem. A significant body of work focuses on intrusion detection and attack identification using machine learning and deep learning techniques. [5] proposed a deep learning–based intrusion detection system for smart cars, demonstrating that neural models can effectively capture complex attack signatures in cyber–physical systems. Although the study is centered on vehicular networks, its relevance to MIoT lies in the shared constraints of resource-limited devices, continuous operation, and safety-critical consequences. Such approaches emphasize detection accuracy and real-time classification but offer limited insight into how attacks evolve and persist at the system level once detection fails or is delayed. Related to this direction, [6] introduced the SEQIRE model for detecting attacks in IoT networks by extending classical epidemic compartmental frameworks. This work is notable for moving beyond purely data-driven methods and incorporating state transitions that reflect different stages of compromise and recovery. However, the SEQIRE model is formulated using ordinary differential equations and assumes homogeneous mixing of devices. As a result, spatial deployment characteristics and localized attack propagation effects are not captured. Beyond these contributions, several studies have applied epidemic-inspired models to IoT and cyber–physical security analysis, highlighting nonlinear transmission dynamics and threshold behavior. These models successfully explain why certain attacks persist while others die out, but they typically neglect spatial structure and diffusion effects [17] [20]. Consequently, they are unable to explain clustering phenomena observed in real healthcare environments, where attacks often originate locally and spread gradually across physical spaces. From a system-level perspective, other researchers have examined MIoT security through architectural risk analysis and deployment studies. These works emphasize that device density, communication locality, and physical layout significantly influence attack impact and containment strategies [1]. However, such insights are rarely formalized into mathematically rigorous models that allow stability analysis or derivation of explicit persistence conditions. The existing literature reveals a clear gap. Current MIoT security models either focus on detection without addressing long-term system behavior or rely on non-spatial analytical frameworks that ignore physical deployment and communication locality. There is a lack of mathematically rigorous models that simultaneously capture spatial propagation, nonlinear attack dynamics, and threshold-driven persistence or extinction in Medical IoT networks. This work addresses this gap by formulating a reaction–diffusion partial differential equation model that explicitly incorporates spatial structure, device interactions, recovery, and isolation mechanisms. The objective is to determine precise conditions under which cyberattacks persist or die out in MIoT environments and to provide analytical guarantees supported by numerical validation.

3. System Description, Assumptions and Hypothesis

3.1. System Description:

We consider a Medical IoT network deployed inside a closed clinical environment, such as a hospital ward or an intensive care unit. The system consists of a large number of interconnected medical devices, including patient monitors, infusion pumps, wearable sensors, and gateway nodes. These devices communicate continuously to transmit physiological data and control signals. The network is spatially distributed. Devices are not concentrated at a single point. They are placed across rooms, corridors, and care units. Communication happens through short-range wireless links and centralized gateways.

Because of this structure, a cyberattack does not affect all devices at once. It spreads gradually, moving through communication paths. Once a device is compromised, it may begin to behave abnormally. It can propagate malicious packets, disrupt data transmission, or influence neighboring devices through trusted communication channels. This creates a chain reaction. One compromised node increases the risk for others. The system is assumed to operate continuously in time. Devices may be patched, isolated, or permanently disabled after detection. Some devices may recover and some do not. This dynamic behavior motivates a time-dependent and spatially dependent model rather than a static one. A conceptual overview of the system structure and attack flow is shown in Figure 1. (See Fig 1)

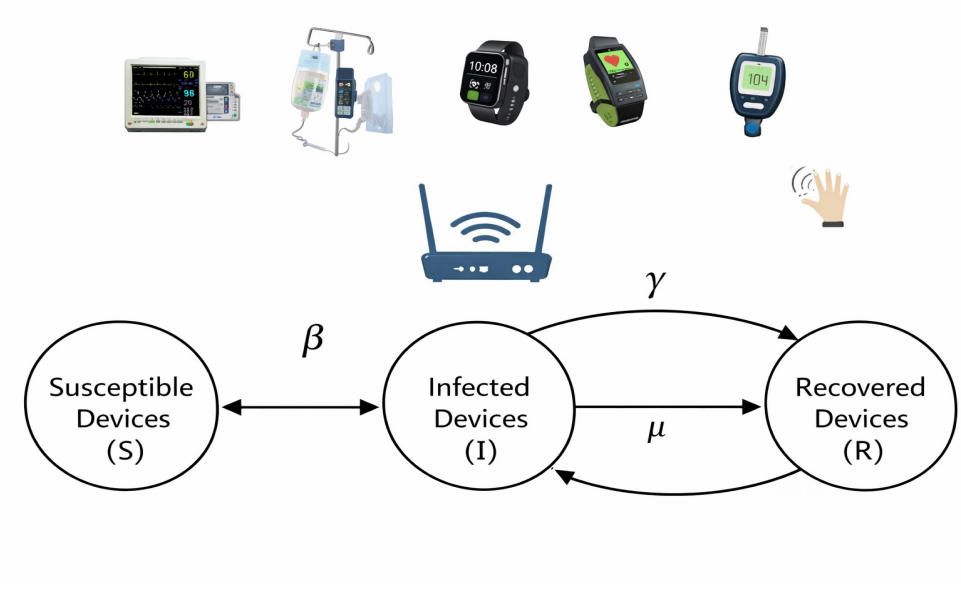

Figure 1: Overview of Medical IoT Cyberattack Dynamics

3.2. Modeling Assumptions:

To construct a tractable and analytically meaningful model, the following assumptions are made.

- **Spatial Continuity:** The MIoT network is modeled as a continuous spatial domain $\Omega \subset R^2$. This abstraction allows the use of partial differential equations to capture spatial propagation effects.
- **Device State Classification:** Each device belongs to one of three states. This classification has been widely used in cyber-epidemic modeling and provides a clear analytical structure [16]:
  - Secure or susceptible (S)
  - Compromised or infected (I)
  - Recovered or isolated (R)
- **Attack Propagation Mechanism:** Cyberattacks propagate through communication links. The spread is not instantaneous. It depends on proximity, communication frequency, and protocol weaknesses. These effects are modeled using diffusion terms.
- **Closed Environment:** The clinical network is assumed to be closed. No new devices enter during the observation period, and compromised devices do not leave the system. This justifies the use of no-flux boundary conditions.
- **Recovery and Isolation:**Compromised devices may recover through patching or be isolated by security mechanisms. Some devices may be permanently disabled if the damage is severe.

- **Homogeneous Parameters:** For analytical clarity, infection and recovery parameters are assumed to be spatially uniform. This assumption is relaxed later during numerical validation.

These assumptions are standard in reaction-diffusion systems and are sufficient to capture the essential behavior of cyberattack spread in MIoT environments [14] [10].

3.3. Mathematical State Variables:

Let $x \in \Omega x$ denote the spatial position and $t \geq 0$ denote time. We define:

- $S(x,t)$: density of secure (susceptible) MIoT devices
- $I(x,t)$: density of compromised devices
- $R(x,t)$: density of recovered or isolated devices

The total device density satisfies:
$S(x,t) + I(x,t) + R(x,t) = N(x)$
where $N(x)$ represents the local device number.

3.4. Research Hypothesis:

Cyberattacks in Medical IoT networks exhibit spatio-temporal propagation behavior that can be accurately modeled using a reaction-diffusion partial differential equation framework. The persistence or extinction of such attacks is governed by a threshold parameter analogous to the basic reproduction number. In other words, the attack does not merely occur. It spreads and this spread follows a predictable mathematical structure. If the reproduction number exceeds a critical threshold, the cyberattack persists within the MIoT network. If it remains below that threshold, the attack eventually dies out. This hypothesis will be formally supported using analytical results, including lemmas on positivity and invariance, and theorems on equilibrium stability.

3.5. Justification for the PDE Framework:

Ordinary differential equation models assume complete mixing of devices. This assumption is unrealistic in hospital settings, where physical layout and communication constraints matter. Devices located in different rooms or wards do not interact equally. Unlike graph-based or agent-based MIoT security models, the proposed framework enables analytical threshold derivation and stability guarantees in a spatially explicit setting. Reaction-diffusion equations naturally incorporate both local interactions and spatial spread. They have been successfully applied to biological epidemics and, more recently, to cyber-physical systems [15] [8] [7]. Therefore, a reaction-diffusion PDE framework is not a modeling luxury.

4. Mathematical Model Formulation

4.1. Spatial Domain and Time Scale:

Let $\Omega \subset R^2$ denote the spatial domain representing a clinical environment such as a hospital ward or an intensive care unit. Devices are distributed across this domain in a non-uniform manner. Time is represented by $t \geq 0$. A two-dimensional spatial domain is sufficient to capture spatial interaction effects caused by communication range, gateway placement, and physical separation between devices. Similar spatial abstractions have been used in both epidemiological diffusion models and cyber-physical security studies [19] [15] [14].

4.2. Reaction-Diffusion Cyberattack Model:

Based on the assumptions, cyberattack dynamics are modeled using the following system of reaction-diffusion partial differential equations:

$$\begin{aligned} \frac{\partial S(x,t)}{\partial t} &= D_S \nabla^2 S(x,t) - \beta S(x,t) I(x,t), \\ \frac{\partial I(x,t)}{\partial t} &= D_I \nabla^2 I(x,t) + \beta S I(x,t) - (\gamma + \mu) I(x,t), \\ \frac{\partial R(x,t)}{\partial t} &= D_R \nabla^2 R(x,t) + \gamma I(x,t). \end{aligned}$$

The diffusion terms represent the spatial spread of attack influence through communication links and routing mechanisms. Diffusion does not imply physical movement of devices. It reflects information flow and malware transmission across the network. The nonlinear interaction term βSI models the compromise process, where secure devices become infected due to interaction with compromised devices. Similar nonlinear terms have been widely used in cyber-epidemic and malware propagation models [21] [10] [16]. The recovery term γI represents security responses such as firmware updates, intrusion detection actions, or automated remediation. The parameter μ accounts for permanent device isolation or failure due to severe compromise. The model conserves total device density up to removal through isolation, ensuring physical consistency of the system.

4.3. Model Parameters and Interpretation:

The parameters appearing in the model have clear cyber-security interpretations:

- D_S, D_I, D_R: diffusion coefficients reflecting communication intensity, routing frequency, and network topology
- β: cyber infection rate, associated with vulnerability exposure and attack capability
- γ: recovery rate due to patching and security intervention
- μ: permanent removal or isolation rate

All parameters are assumed to be positive constants. This assumption is standard in reaction-diffusion systems and allows analytical results to be derived without unnecessary technical complications [14].

4.4. Boundary and Initial Conditions:

The MIoT network is assumed to operate in a closed clinical environment. As a result, no device state crosses the boundary of the spatial domain. This leads to no-flux (Neumann) boundary conditions:

$$\nabla \mathrm{S}(x,t) \cdot n = \nabla \mathrm{I}(x,t) \cdot n = \nabla \mathrm{R}(x,t) \cdot n = 0, x \in \partial\Omega, \quad t > 0.$$

where n denotes the outward normal vector.
Initial conditions are defined as:

$$S(x,0) = S_0(x), I(x,0) = I_0(x), R(x,0) = 0, \quad x \in \Omega .$$

The initial compromised population $I_0(x)$ is assumed to be small and spatially localized. This reflects realistic scenarios in which cyberattacks begin from a limited number of entry points, such as a compromised gateway or infected update server [4] [8] [7].

4.5. Disease-Free Equilibrium:

The disease-free equilibrium represents a secure operating state of the MIoT network, where no devices are compromised. It is given by:

$$E_0 = (S^*, I^*, R^*) = (N, 0, 0).$$

This equilibrium serves as a baseline for analyzing system stability and attack persistence. Its stability properties are examined in the following section through analytical techniques.

4.6. Rationale for the Model Structure:

The proposed model closely resembles spatial epidemic systems, which is intentional. Cyberattacks in MIoT networks share key characteristics with biological infections, including nonlinear transmission, threshold behavior, and spatial clustering. Reaction-diffusion frameworks allow these features to be captured in a mathematically rigorous way. More importantly, they enable the derivation of a reproduction number and stability conditions, which are difficult to obtain using purely simulation-based security models [19] [15] [21].

5. Analytical Results

This section establishes the mathematical validity of the proposed reaction-diffusion model and rigorously analyzes the conditions under which cyberattacks persist or disappear in Medical IoT networks. The analysis proceeds step by step. First, we address the well-posedness of the system. Then we study positivity, boundedness, equilibrium behavior, and threshold dynamics governed by the reproduction number.

Existence and Uniqueness of Solutions

It is necessary to confirm that the model admits a well-defined solution.

Theorem 5.1: Existence and Uniqueness: For any non-negative initial conditions

$$S(x,0) = S_0(x), I(x,0) = I_0(x), R(x,0) = R_0(x),$$

with $S_0, I_0, R_0 \in L^2(\Omega)$, the reaction–diffusion system admits a unique, global solution

$$(S(x,t), I(x,t), R(x,t)) \in C\left([0,\infty); L^2(\Omega)\right).$$

Proof: The diffusion operators are linear and uniformly elliptic under Neumann boundary conditions. The reaction terms are locally Lipschitz continuous in (S, I, R). Hence, by standard parabolic PDE theory, a unique local solution exists. Global existence follows from the boundedness. Therefore, the solution exists for all $t > 0$ and is unique [14].

5.1. Positivity of Solutions:

The system must preserve physical meaning, meaning device densities cannot become negative.

Lemma 1: Positivity of Solutions

If the initial conditions are non-negative, then

$S(x,t) \geq 0, I(x,t) \geq 0, R(x,t) \geq 0, Forallx \in \Omega$ *and* $t > 0$.

Proof: When any state variable reaches zero, its corresponding reaction term is non-negative. For example, at $I = 0$, the infection term vanishes and no negative forcing is present. Combined with Neumann boundary conditions, the parabolic maximum principle prevents solutions from crossing into the negative region. Hence, non-negativity is preserved.

5.2. Invariant Region and Boundedness:

Next, we establish that the total device population remains bounded.

Lemma 2: Invariant Region The set
$D = \{(S, I, R) \in \mathbb{R}^3_+ \ : \ S + I + R \leq N(x)\}$
is positively invariant under the system dynamics.

Proof: Summing the three equations of the model yields
Let

$$U(x,t) = S(x,t) + I(x,t) + R(x,t).$$
$$\frac{\partial U}{\partial t} = D_S \nabla^2 S + D_I \nabla^2 I + D_R \nabla^2 R - \mu I.$$

Integrating over Ω and applying the no-flux boundary conditions removes the diffusion terms. Since $\mu I \geq 0$, the total population does not increase. Thus $U(x,t) \leq N(x)$ for all $t > 0$. This guarantees boundedness and supports global existence.

5.3. Disease-Free Equilibrium:

The disease-free equilibrium corresponds to a secure MIoT system:

$$E_0 = (S^*, I^*, R^*) = (N, 0, 0).$$

This equilibrium represents normal network operation without active cyberattacks.

5.4. Derivation of the Basic Reproduction Number:

To characterize attack persistence, we derive the basic reproduction number R_0. Let the infected equation be written as

$$\frac{\partial I}{\partial t} = F(I) - V(I),$$

where

$$F(I) = \beta N I, \quad V(I) = (\gamma + \mu)I - D_I \nabla^2 I.$$

The next-generation operator is defined as

$$K = FV^{-1}.$$

The basic reproduction number is given by the spectral radius of K:

$$R_0 = \rho(K) = \frac{\beta N}{\gamma + \mu}.$$

This quantity represents the expected number of secondary compromised devices generated by one infected device in an otherwise secure network.

5.5. Local Stability of the Disease-Free Equilibrium:

Theorem 5.2 (Local Stability): If $R_0 < 1$, the disease-free equilibrium E_0 is locally asymptotically stable.

Proof: Linearizing the infected equation around E_0 yields

$$\frac{\partial I(x,t)}{\partial t} = D_I \nabla^2 I(x,t) + (\beta N - \gamma - \mu) I(x,t).$$

The principal eigenvalue of the diffusion operator under Neumann conditions is zero. Stability depends on the sign of $\beta N - (\gamma + \mu)$. If $R_0 < 1$, all eigenvalues are negative, and perturbations decay exponentially. Hence, the system returns to the disease-free equilibrium.

5.6. Endemic Equilibrium:

When cyberattacks persist, the system approaches an endemic state. Lemma 5.4: Existence of Endemic Equilibrium:

If $R_0 > 1$, there exists a unique endemic equilibrium $E^* = (S^*, I^*, R^*)$ with $I^* > 0$.

Proof: Setting time derivatives to zero yields a nonlinear algebraic system. When $R_0 > 1$, the infection term dominates recovery. The existence and uniqueness of the endemic equilibrium follow from standard fixed-point and monotonicity arguments for reaction-diffusion systems. The detailed functional-analytic construction is omitted for brevity, as it closely follows established results in spatial epidemic modeling.

5.7. Persistence of Cyberattacks:

Theorem 5.3: Uniform Persistence:
If $R_0 > 1$, then

$$\lim_{t\to\infty} inf I(x,t) > 0$$

for almost all $x \in \Omega$.

Proof: Instability of E_0 combined with positivity and boundedness implies uniform persistence by standard persistence theory for reaction–diffusion systems. The infected population cannot vanish asymptotically. The persistence result relies on classical uniform persistence theory for parabolic partial differential equations, where instability of the disease-free equilibrium, together with positivity and boundedness, ensures non-extinction of the infected class.

5.8. Analytical Interpretation:

The analytical results confirm the central hypothesis of this study. Cyberattacks in Medical IoT networks exhibit spreading behavior that is well captured by a reaction-diffusion framework rather than isolated or well-mixed models. The derived basic reproduction number R_0 acts as a sharp threshold separating extinction and persistence regimes. When $R_0 < 1$, the disease-free equilibrium is stable and cyberattacks cannot sustain themselves. When $R_0 > 1$, the system admits a persistent endemic state, making long-term compromise mathematically unavoidable. These results provide a rigorous foundation for the numerical validation presented in the following section.

6. Numerical Simulation and Validation

This section presents numerical simulations of the proposed reaction-diffusion model to validate the analytical results derived in Section 5. The simulations are designed specifically to verify the threshold behavior governed by the basic reproduction number, as well as the stability and persistence properties proved earlier.

6.1. Numerical Setup and Parameter Specification:

All simulations are performed using Python 3.10, with NumPy for numerical computation and Matplotlib for visualization. The numerical scheme is based on a finite difference discretization in space and an explicit Euler method for time integration. The numerical parameters and simulation settings are summarized in Table 1.

Table 1: Numerical parameters and simulation settings

Category	**Parameter(s)**	**Value(s)**
Spatial domain	Length, grid points	$(L = 10),\ (N_x = 100)$
Time discretization	Total time, time step	$(T = 20),\ (\Delta t = 0.001)$
Diffusion coefficients	$(D_S,\ D_I,\ D_R)$	0.1
Infection rate	β	$0.3 - 1.0$
Recovery rate	γ	0.5
Isolation rate	μ	0.3
Device density	N	1.0
Boundary condition	–	$Neumann(no - flux)$

Table 1. Numerical parameters, discretization settings, and software environment used for the simulation of the reaction-diffusion MIoT cyberattack model. All values are fixed across simulations unless explicitly stated.

Two parameter regimes are considered:

- Sub-threshold case:

$$\beta = 0.3,\ \gamma = 0.5,\ \mu = 0.3,$$

giving

$$R_0 = \frac{0.3}{0.8} = 0.375 < 1.$$

- Super-threshold case:

$$\beta = 1.0,\ \gamma = 0.5,\ \mu = 0.3,$$

giving

$$R_0 = \frac{1.0}{0.8} = 1.25 > 1.$$

The initial condition represents a mostly secure MIoT network with a small, localized infection:
$S(x,0) = N$,
$I(x,0) = 0.1 \exp\left(-\frac{(x-L/2)^2}{\sigma^2}\right)$,
$R(x,0) = 0$.
where σ controls the spatial width of the initial infection and is fixed throughout the simulations.

6.2. Spatio-Temporal Dynamics and Threshold Verification:

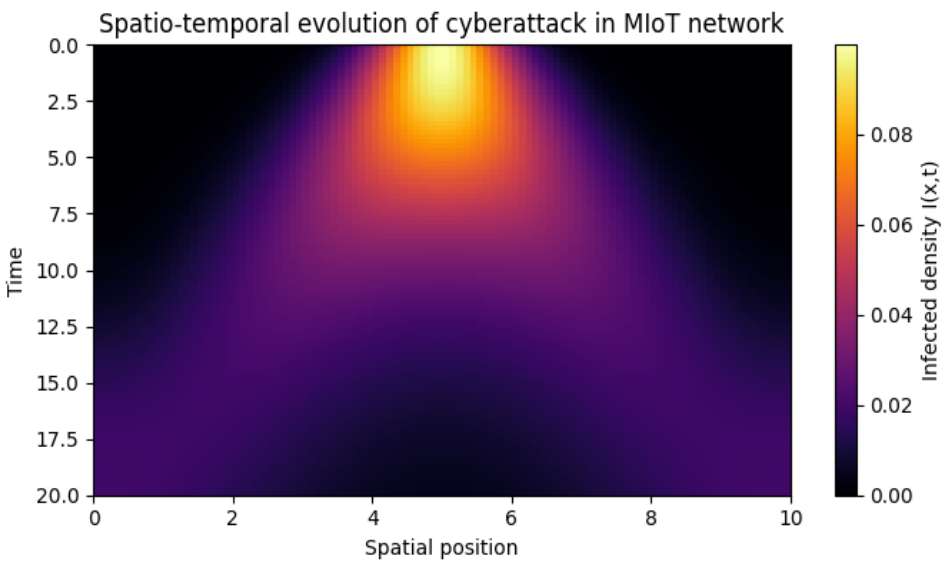

Figure 2: spatio-temporal evolution of cyberattacks in MIoT

Figure 2 illustrates the spatio-temporal evolution of the infected device density $I(x,t)$. The infection is initially localized and gradually spreads across the spatial domain due to diffusion effects. For the

parameter regime $R_0 > 1$, the infected population does not vanish but persists over time, forming a non-zero spatial profile even at large times. This numerical behavior is fully consistent with the persistence result established in Theorem 5.3 and confirms that cyberattacks in MIoT networks exhibit diffusion-driven spatial propagation.

Figure 3: Spatio-temporal evolution of infected devices for $R_0 < 1$.

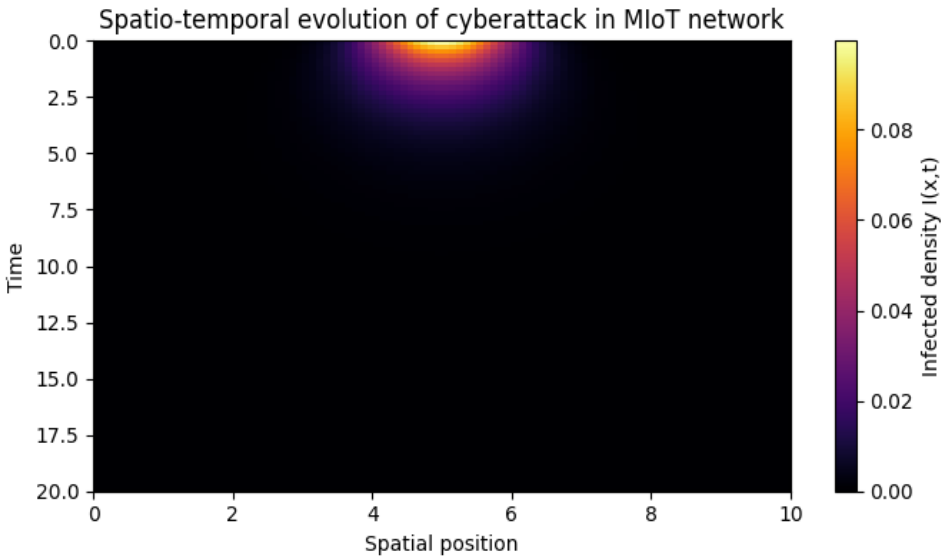

Figure 3: Spatio-temporal evolution of infected devices

Figure 3 shows the spatio-temporal evolution of the infected device density $I(x, t)$ for the sub-threshold regime $R_0 < 1$. The infection remains spatially localized at early times and rapidly decays to zero across the entire domain. No persistent infected region is observed. This numerical behavior confirms the local asymptotic stability of the disease-free equilibrium established in Theorem 5.2 and demonstrates that effective recovery and isolation mechanisms are sufficient to eliminate cyberattacks in the MIoT network.

Figure 4: The threshold diagram

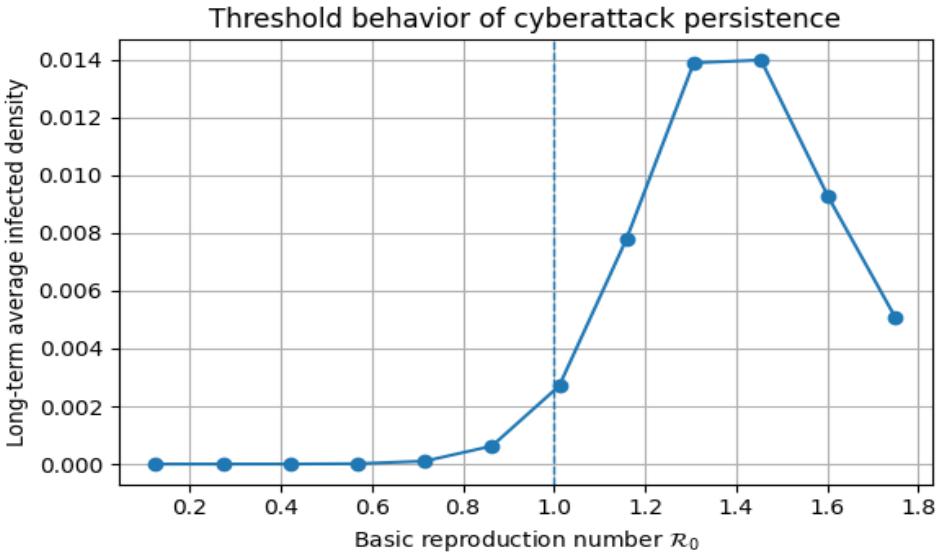

Figure 4: Spatio-temporal evolution of infected devices

Figure 4 illustrates the relationship between the basic reproduction number R_0 and the long-term average infected population. A clear transition occurs near $R_0 = 1$, confirming that R_0 acts as a sharp threshold parameter for cyberattack persistence.

6.3. Discussion and Reproducibility:

The numerical results fully support the analytical findings of Section 5. Positivity and boundedness are preserved, the disease-free equilibrium is stable when $R_0 < 1$, and sustained cyberattacks occur when $R_0 > 1$. Spatial diffusion plays a crucial role in shaping the attack dynamics, justifying the use of a PDE-based framework.

7. Security Interpretation and Practical Implications

The analytical and numerical results obtained in this study have direct implications for the security design and operation of Medical IoT networks. The model does not treat cyberattacks as isolated incidents. Instead, it frames them as spreading processes whose behavior is governed by measurable system parameters. The most important outcome is the existence of a clear threshold, expressed through the basic reproduction number R_0. This quantity separates safe operating regimes from unsafe ones. When $R_0 < 1$, cyberattacks cannot sustain themselves, regardless of the initial number of compromised devices. When $R_0 > 1$, persistence becomes inevitable.

7.1. Interpretation of Model Parameters in Security Terms:

Each parameter in the model corresponds to a concrete cybersecurity mechanism. The infection rate β captures vulnerability exposure. This includes weak authentication, unpatched firmware, insecure communication protocols, and excessive trust between devices. A higher value of β does not necessarily mean more attackers. It means that once an attacker gains access, propagation becomes easier. The recovery rate γ represents the effectiveness of defensive actions such as patch deployment, intrusion detection, and automated remediation.

Increasing γ does not prevent initial compromise, but it shortens the lifetime of infected devices. The isolation rate μ reflects the ability of the system to permanently remove or quarantine compromised devices. Network segmentation, device shutdown, and physical replacement all contribute to this parameter. The

diffusion coefficients represent communication structure. High diffusion corresponds to dense connectivity and frequent data exchange. While this is desirable for clinical performance, it also accelerates attack spread.

7.2. Meaning of the Threshold Condition

From a security perspective, the condition

$$R_0 = \frac{\beta N}{\gamma+\mu} < 1$$

defines a quantitative security requirement, not a heuristic guideline. This inequality shows that security can be improved in multiple ways. Reducing vulnerabilities (β) is one option, but not the only one. Increasing patching speed (γ) or isolation capability (μ) can compensate for residual vulnerabilities. The model makes this trade-off explicit. Importantly, the results show that reducing attack intensity alone is insufficient if recovery and isolation are slow. Even small initial compromises can lead to persistent infection if the system response is delayed.

7.3. Role of Spatial Structure in Medical Environments:

The numerical simulations highlight the importance of spatial structure. Infection does not spread uniformly. It forms clusters, expands through nearby devices, and persists in localized regions when mitigation is weak. This has practical consequences. Security policies that are applied uniformly across a hospital may fail to address local risk concentration. High-density device areas, such as intensive care units, are more vulnerable to diffusion-driven persistence. The reaction-diffusion framework captures this effect naturally. It explains why attacks may appear controlled in some areas while persisting in others, even under the same global security policy.

7.4. Implications for MIoT Security Design:

The results suggest several design principles. First, speed in the increasing recovery and isolation rates has a strong impact on reducing R_0. Delayed patching is mathematically equivalent to allowing the infection to reproduce. Second, connectivity must be managed, not eliminated. Diffusion-driven spread does not imply that connectivity should be reduced indiscriminately. Instead, communication patterns should be structured to limit uncontrolled propagation paths. Third, local monitoring is critical, since persistence can occur in spatial clusters, detection and response mechanisms must operate at local scales, not only at centralized gateways. These implications follow directly from the model. They are not assumptions.

8. Conclusion

This work proposed a reaction-diffusion partial differential equation framework to model cyberattack propagation in Medical IoT networks, with explicit consideration of spatial structure and temporal evolution. Unlike well-mixed or purely graph-based approaches, the proposed model captures how cyberattacks initiate locally, spread through device interactions, and either persist or disappear depending on system-level parameters. This perspective is particularly relevant for clinical environments, where device placement, communication locality, and operational continuity strongly influence security behavior. A key contribution of the study is the identification and analytical characterization of a threshold condition governed by the basic reproduction number R_0. The theoretical analysis established that when $R_0 < 1$, the disease-free equilibrium is locally asymptotically stable and cyberattacks cannot sustain themselves, regardless of the size or location of the initial compromise. In contrast, when $R_0 > 1$, the system admits a persistent endemic state in which compromised devices remain present over time. These results were rigorously supported through proofs of existence, positivity, boundedness, stability, and persistence, ensuring mathematical consistency of the model. Numerical simulations were conducted to validate the analytical findings. Spatio-temporal heatmaps demonstrated diffusion-driven attack spread and extinction, while threshold plots confirmed the sharp transition predicted at $R_0 = 1$. The strong agreement between analytical results and numerical outcomes reinforces the validity of the proposed framework and

highlights the importance of spatial effects in MIoT security analysis. The model relies on simplifying assumptions, including homogeneous parameters, deterministic dynamics, and reduced spatial dimensionality, which were adopted to ensure analytical tractability. Future work may extend the framework to incorporate device heterogeneity, stochastic effects, time delays in detection and response, and higher-dimensional spatial domains. Further integration with control strategies or clinical risk models could also enhance its applicability to real-world healthcare systems.

References

1. K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, Big healthcare data: Preserving security and privacy, *Journal of Big Data*, vol. 5, no. 1, Article 1, 2018. DOI: 10.1186/s40537-017-0110-7.

2. R. M. Anderson and R. M. May, *Infectious Diseases of Humans: Dynamics and Control*, Oxford University Press, 1991. DOI: 10.1093/oso/9780198545996.001.0001.

3. L. Coventry and D. Branley, Cybersecurity in healthcare: A narrative review of trends, threats and ways forward, *Maturitas*, vol. 113, pp. 48–52, 2018. DOI: 10.1016/j.maturitas.2018.04.008.

4. A. Humayed, J. Lin, F. Li, and B. Luo, Cyber-physical systems security: A survey, *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017. DOI: 10.1109/JIOT.2017.2703172.

5. P. Kumar, B. K. Mishra, and P. Rai, Deep learning-based intrusion detection system for smart cars, *REST Journal on Data Analytics and Artificial Intelligence*, vol. 4, no. 3, Article 11, 2025. DOI: 10.46632/jdaai/4/3/11.

6. P. Kumar, P. Rai, and B. K. Mishra, Detection of attacks in Internet of Things networks using the SEQIRE model, *Cureus Journal of Computer Science*, vol. 2, Article es44389-025-05898-y, 2025. DOI: 10.7759/s44389-025-05898-y.

7. L. Quiroga-Sánchez, G. A. Montoya, and C. Lozano-Garzón, The SEIRS-NIMFA epidemiological model for malware propagation analysis in IoT networks, *Cybersecurity*, vol. 8, Article 2, 2025. DOI: 10.1186/s42400-024-00310-z.

8. V. Kovtun, K. Grochla, M. Al-Maitah, S. Aldosary, and T. Gryshchuk, Cyber epidemic spread forecasting based on the entropy-extremal dynamic interpretation of the SIR model, *Egyptian Informatics Journal*, vol. 28, Article 100572, 2024. DOI: 10.1016/j.eij.2024.100572.

9. W. Mei, S. Mohagheghi, S. Zampieri, and F. Bullo, On the dynamics of deterministic epidemic propagation over networks, *Annual Reviews in Control*, vol. 44, pp. 116–128, 2017. DOI: 10.1016/j.arcontrol.2017.09.002.

10. B. K. Mishra and N. Keshri, Mathematical model on the transmission of worms in wireless sensor network, *Applied Mathematical Modelling*, vol. 37, no. 6, pp. 4103–4111, 2013. DOI: 10.1016/j.apm.2012.09.025.

11. A. I. Newaz, A. K. Sikder, M. Rahman, and S. Uluagac, HealthGuard: A machine learning-based security framework for smart healthcare systems, in *Proc. International Conference on Social Networks Analysis, Management and Security (SNAMS)*, pp. 389–396, 2019. DOI: 10.1109/SNAMS.2019.8931716.

12. A. A. Alli and M. M. Alam, SecOFF-FCIoT: Machine learning based secure offloading in fog-cloud of things for smart city applications, *Internet of Things*, vol. 7, Article 100070, 2019. DOI: 10.1016/j.iot.2019.100070.

13. R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, Epidemic processes in complex networks, *Reviews of Modern Physics*, vol. 87, no. 3, pp. 925–979, 2015. DOI: 10.1103/RevModPhys.87.925.

14. S. Ruan, Spatial-temporal dynamics in nonlocal epidemiological models, in *Lecture Notes in Computer Science*, pp. 87–104, Springer, 2007. DOI: 10.1007/978-3-540-34426-1_5.

15. B. Du and H. Wang, Partial differential equation modeling of malware propagation in social networks with mixed delays, *Computers & Mathematics with Applications*, vol. 75, pp. 273–286, 2018. DOI: 10.1016/j.camwa.2018.02.015.

16. R. Li, Y. Song, H. Wang, G.-P. Jiang, and M. Xiao, Reactive–diffusion epidemic model on human mobility networks: Analysis and applications to COVID-19 in China, *Physica A*, vol. 609, Article 128337, 2023. DOI: 10.1016/j.physa.2022.128337.

17. X. Zhu, J. Huang, and C. Qi, Modeling and analysis of malware propagation for IoT heterogeneous devices, *IEEE Systems Journal*, vol. 17, no. 3, pp. 3846–3857, 2023. DOI: 10.1109/JSYST.2023.3269158.

18. B. Zhai, O. N. Akande, S. Agarwal, and W. Pak, Security risk assessment of Internet of Things health devices using DREAD and STRIDE models, *Ain Shams Engineering Journal*, vol. 16, no. 11, Article 103721, 2025. DOI: 10.1016/j.asej.2025.103721.

19. J. Dou, G. Xie, Z. Tian, L. Cui, and S. Yu, Modeling and analyzing the spatial–temporal propagation of malware in mobile wearable IoT networks, *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2438–2452, 2024. DOI: 10.1109/JIOT.2023.3295016.

20. H. Cao, D.-T. Peng, and D. Yu, Modeling and controlling spatiotemporal malware propagation in mobile Internet of Things, *Applied Mathematical Modelling*, vol. 144, Article 116042, 2025. DOI: 10.1016/j.apm.2025.116042.

21. N. U. I. Hossain et al., Modeling and assessing cyber resilience of smart grid using a Bayesian network-based approach, *Journal of Computational Design and Engineering*, vol. 7, no. 3, pp. 352–366, 2020. DOI: 10.1093/jcde/qwaa029.

Pankaj Kumar,
Department of Computer science & Engineering
Jharkhand University of Technology, Ranchi,
India.
E-mail address: pankajunav@gmail.com

and

Pankaj Rai,
Department of Electrical Engineering
BIT Sindri, Dhanbad
India.
E-mail address: pkrai.ee@bitsindri.ac.in

and

Bimal Kumar Mishra,
Department of Mathematics
Vinoba Bhave University, Hazaribagh, Jharkhand
India.
E-mail address: drbimalmishra@gmail.com