I. J. Mathematical Sciences and Computing, **2026, 3, 1-23**
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2026.03.01

Optimizing Cybersecurity and Risk Management for Intrusion Mitigation in IoT Applications

Mustapha Danjuma Suleiman
Cyber Security Science, Frontier University, Garowe, Somalia
E-mail: danjuma@frontier.edu.so
ORCID iD: https://orcid.org/0000-0002-2924-7950

Received: December 30, 2025; Revised: January 20, 2026; Accepted: February 3, 2026; Published: August 8, 2026

Abstract: This study presents a C*-algebraic framework for optimizing intrusion mitigation in Internet of Things (IoT) networks by integrating mathematical models for cyberattack propagation with optimization-based security strategies. Theoretical results demonstrate that the spectral radius of the attack operator $\rho(A)$ governs the recovery of IoT networks under attack, where $\rho(A) < 1$ ensures system recovery, and $\rho(A) \geq 1$ leads to persistent or growing attack impact. The framework combines blockchain-based trust, AI-driven intrusion detection systems (IDS), and Zero-Trust Architecture (ZTA) to provide a multi-layered, adaptive defence system. Unlike probabilistic models that simplify attack dynamics, this approach models threats rigorously using bounded linear operators, thereby offering scalability and robustness. Optimization ensures computational efficiency, making the model suitable for resource-constrained IoT environments, with the operator norm and the spectral radius acting as key constraints. Validation on real-world datasets such as CIC-IoT2023, UNSW-NB15, and BoT-IoT revealed that the AI-IDS models achieved near-perfect performance, while the unified model integrating blockchain, IDS, and ZTA showed an accuracy of 51.0.

Index Terms: C*-Algebra, IoT Security, Cyberattack Propagation, Intrusion Detection Systems (IDS), Zero-Trust Architecture (ZTA)

1. Introduction

The Internet of Things (IoT) has become a cornerstone of technological innovation, with applications in various industries, including healthcare, manufacturing, smart cities, and transportation. As more devices become interconnected, IoT systems are increasingly recognized for their ability to enhance efficiency, facilitate real-time data analysis, and improve automation. However, the interconnected nature of IoT networks also introduces significant cybersecurity risks, making them vulnerable to various types of cyberattacks [1-3]. According to recent studies, these networks, which often consist of resource-constrained devices, are ill-equipped to handle traditional security protocols, exposing them to malware, unauthorized access, and other forms of cyber threats [4,5]

Given the increasing frequency and sophistication of attacks, optimizing cybersecurity measures and risk management practices for intrusion mitigation in IoT applications is crucial. Many IoT devices are inherently limited in terms of processing power, memory, and energy consumption, making it difficult to implement resource-intensive security solutions, such as encryption or extensive intrusion detection systems (IDS) [6]. As is evident from the literature, traditional security approaches fail to address the dynamic and evolving nature of cyber threats in IoT environments, where new vulnerabilities continuously emerge [7-9]. This necessitates the development of lightweight, adaptive, and scalable security frameworks that can provide effective defence mechanisms without compromising the functionality of IoT devices.

According to [10], AI-driven techniques have shown promise in providing dynamic and proactive security solutions for IoT networks. Machine learning models, for example, can detect anomalies and predict attacks based on historical data, offering a more effective approach than static-signature-based methods. However, the computational demands of AI models pose a challenge for many IoT devices, which are often resource constrained. As discussed by [11], approaches that integrate AI with other lightweight security measures, such as cryptographic techniques or edge computing, have been proposed as solutions to this issue, although these methods require further optimization to effectively balance security and efficiency.

Moreover, blockchain technology has been identified as a potential solution for improving data integrity, authentication, and secure communication in IoT networks [12]. According to [13], the decentralized and immutable nature of the blockchain ensures that data cannot be tampered with, making it an attractive option for securing IoT systems. However, the high computational overhead and storage requirements of traditional blockchain models limit

their practicality in resource-constrained environments such as IoT. Hybrid blockchain models and lightweight consensus mechanisms have been suggested to address these challenges; however, their implementation in large-scale IoT applications remains a topic of ongoing research [14-15]

As IoT systems evolve, new methods for optimizing risk management and intrusion mitigation are emerging. Federated learning (FL), a decentralized approach to machine learning, has been explored to improve the privacy and security of IoT networks. According to [16], FL enables the training of models on distributed data without the need to share sensitive information, thus addressing privacy issues. However, FL models remain vulnerable to threats, such as model poisoning, which can compromise their effectiveness. As discussed in [17], ongoing research focuses on enhancing the security of federated learning systems to make them more resilient to adversarial attacks.

In general, the growing complexity of IoT networks and increasing sophistication of cyber threats underscore the need for innovative solutions for cybersecurity and risk management. To effectively mitigate intrusions and safeguard IoT systems, adopting a multilayered adaptive approach that integrates advanced AI techniques, blockchain technology, and lightweight cryptographic methods is crucial. The development of such frameworks, which can balance performance, efficiency, and security, is critical for ensuring the resilience of IoT applications against emerging threats such as adversarial attacks.

2. Literature Review

The rapid expansion of the Internet of Things (IoT) has transformed industries such as healthcare, industrial automation, smart cities, and home automation, enhancing efficiency through the use of connected devices in these fields. However, this widespread adoption has increased security vulnerabilities, making IoT networks prime targets for cyberattacks [1]. A single compromised device can introduce malware, disrupt operations, and cause severe economic repercussions for the organization. Limited computational resources prevent many IoT devices from implementing robust security, while the lack of standardized protocols complicates intrusion mitigation [2-3]

Understanding cyberthreat propagation is crucial for ensuring proactive cybersecurity. Conventional models, including graph-based structures, epidemiological frameworks, and probabilistic techniques, have been used to analyze the evolution of cyberattacks [4]. Graph-based methods model threats such as disease transmission [5] but struggle with nonlinear attacks and adaptive adversaries [6]. Markov chains estimate intrusion likelihood but oversimplify sophisticated cyber threats [7]. AI-driven intrusion detection enhances anomaly detection [8], yet requires high computational power and is vulnerable to adversarial attacks [9].

Striking a balance between security effectiveness and computational efficiency remains a significant challenge in IoT cybersecurity. Many existing security solutions rely on predefined attack signatures, which limit their ability to detect emerging threats [10]. Traditional IDS and firewalls struggle with scalability in large IoT networks, whereas encryption- and blockchain-based authentication introduce high latency and power consumption, making them impractical for resource-constrained devices [11-17]. Lightweight cryptographic methods and adaptive security frameworks improve efficiency but often require trade-offs between performance and security robustness [13]. Achieving efficient and scalable IoT security remains an open research challenge [14,16].

Blockchain offers decentralized authentication and tamper-proof data integrity, preventing unauthorized modifications and man-in-the-middle attacks [15,16]. However, standard blockchain implementations require high computational power and storage, making integration difficult in IoT environments [17]. Hybrid blockchain models and lightweight consensus mechanisms have been proposed to address these limitations while maintaining security [18].

Artificial intelligence enhances IoT security by enabling real-time anomaly detection and adaptive threat mitigation [19]. AI-driven behavioral analysis identifies threats without predefined signatures; however, it requires extensive training data and remains susceptible to adversarial manipulation [1,20]. Federated learning (FL) improves privacy but remains vulnerable to model poisoning attacks, requiring further security enhancements [2,3]

Given the increasing sophistication of cyber threats, researchers have adopted advanced mathematical frameworks for security modeling. The C*-algebra, a well-established branch of functional analysis, provides a robust foundation for analyzing dynamic security threats in IoT [4]. Unlike traditional models that rely on static graphs or probabilistic estimates, C*-algebras represent cyber threats as noncommutative operator transformations [5]. This enables a structured approach to model adversarial interactions, multistage attack evolution, and security dependencies in IoT systems [6]. The spectral analysis of security operators within a C*-algebraic framework offers insights into attack persistence, vulnerability assessment, and optimal security configurations [7].

This study proposes a C*-algebraic cybersecurity framework that integrates mathematical threat-propagation modeling with optimization-based security strategies. Existing models often focus on isolated security aspects and lack a holistic, multi-layered defense approach. Unlike probabilistic and Markovian models, which oversimplify the attack dynamics, C*-algebras provide a rigorous representation of cyber threats. In addition, optimization techniques ensure computational efficiency, making the model suitable for resource-constrained IoT environments such as smart homes. This study aims to develop a scalable and adaptive cybersecurity model to mitigate modern IoT cyberthreats.

3. Preliminaries

This section provides a foundational mathematical framework for studying cyber-attack propagation in IoT networks using C*-algebra. We introduce Hilbert spaces, bounded operators, spectral theory, and security optimization as key theoretical tools.

Definition 3.1 (Hilbert Space)**.** A Hilbert space H is a complete inner product space over C, equipped with an inner product

$$\langle \cdot,\cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}, \tag{1}$$

which satisfies the following properties for all $\psi,\varphi,\xi \in H$ and $\alpha,\beta \in C$:

1. **Linearity:** $\langle \alpha\psi + \beta\varphi, \xi \rangle = \alpha\langle \psi,\xi \rangle + \beta\langle \varphi,\xi \rangle$.
2. **Conjugate Symmetry:** $\langle \psi, \phi \rangle = \overline{\langle \phi, \psi \rangle}$
3. **Positivity:** $\langle \psi,\psi \rangle \geq 0$, with equality if and only if $\psi = 0$. The associated norm is given as

$$\| \psi \| = \sqrt{\langle \psi, \psi \rangle} \tag{2}$$

Thus, H is a complete metric space under the induced norm topology.

Definition 3.2 (C*-Algebra)**.** A C*-algebra A is a Banach algebra over C equipped with an involution $* : A \to A$ satisfying the following conditions for all $A,B \in A$ and $\lambda \in C$:

1. Normed Algebra:

A is a Banach space with norm $\|.\|$, and the multiplication satisfies

$$\| AB \| \leq \| A \| \| B \| \tag{3}$$

2. Involution Properties:

(a) $(A^*)^* = A$ (involution is an involutive operation).

$(\lambda A)^* = \lambda A^*$.

(b) $(A+B)^* = A^* + B^*$.

(c) $(AB)^* = B^*A^*$.

3. C*-Identity:

The norm and involution satisfy

$$\| A^*A \| = \| A \|^2. \tag{4}$$

4. Non-Commutativity:

In general, $AB \neq BA$, except in the case of a commutative C*-algebra.

The set of all bounded linear operators on a Hilbert space H , denoted B(H), is a fundamental example of a C*-algebra. **Definition 3.3** (Spectral Radius)**.** Let A be a bounded linear operator on a Banach space X (in our case, H represents the Hilbert space). The spectral radius ρ(A) of A is defined as the limit of the norm of the powers of A:

$$\rho(A) = \lim_{n\to\infty} \| A^n \|^{\frac{1}{n}} \tag{5}$$

This definition is valid for all bounded linear operators, regardless of whether they have eigenvalues or not. The spectral radius provides an upper bound for the behavior of the operator's powers and provides insight into whether the operator's influence on the system grows or decays over time.

Moreover, the spectral radius is related to the spectral norm of A and can be computed as

$$\rho(A) = sup\{|\lambda| : \lambda \text{ is an eigenvalue of } A\} \tag{6}$$

In this case, the spectrum refers to the set of all scalar values λ for which $A - \lambda I$ is not invertible, where I is the identity operator. This generalizes the concept of eigenvalues to include other spectral components for non-diagonalizable operators.

In the context of cyberattack propagation in IoT networks, the spectral radius ρ(A) plays a crucial role in

determining the system's long-term stability. Specifically:

- If $\rho(A) < 1$, the attack diminishes over time.
- If $\rho(A) \geq 1$, the attack persists or increases.

Definition 3.4 (C*-Algebraic Representation of an IoT Network)**.** An IoT network consisting of N interconnected devices can be modeled as a Hilbert space H , where each device state $\psi i \in H$ evolves over time. The network state at time t is given by

$$\Psi_t = (\psi_1, \psi_2, \ldots, \psi_N) \in \mathcal{H}^N \tag{7}$$

The set of all bounded linear operators acting on H , denoted as B(H), forms a C*-algebra that governs the system's interactions. **Proposition 3.5** (Cyberattack Propagation in C*-Algebraic IoT Networks)**.** Let H be a Hilbert space that represents the IoT network. A cyberattack on the network is modeled as a bounded operator $A \in B(H)$ that perturbs the device state. The evolution of the network under a cyberattack is expressed as

$$\Psi_{t+1} = U_t A \Psi_t \tag{8}$$

where U_t is the unitary operator representing secure network communication.

3.1. Assumptions and Conditions for Stability

Before proceeding with a detailed analysis, we explicitly state the necessary assumptions and conditions under which the stability claim holds true in the context of our mathematical model. The key claim is that the system is secure if and only if the spectral radius $\rho(A) < 1$, which ensures the stability and recovery.

1. Boundedness of Operators:

Let $A \in B(H)$, where $B(H)$ is the set of all bounded linear operators acting on the Hilbert space H . This assumption ensures that the operators involved are well defined and that their norms are finite.

2. Linearity of Attack Propagation:

The network state evolution under attack is governed by the following equation:

$$\Psi_{t+1} = U_t A \Psi_t \tag{9}$$

where U_t is a unitary operator representing secure communication (which does not affect the magnitude of the state vector Ψ_t), and A is the attack operator that acts on the network state. This assumption is crucial for stability analysis because the attack is modeled as a linear perturbation of the system.

3. Spectral Radius Criterion:

The spectral radius $\rho(A)$ of attack operator A is defined as

$$\rho(A) = \lim_{n\to\infty} \| A^n \|^{\frac{1}{n}} \tag{10}$$

The system is stable (i.e., the attack impact decays to zero) if and only if

$$\rho(A) < 1. \tag{11}$$

This condition is derived under the assumption that A is a bounded operator and that the sequence A^n converges in norm when $\rho(A) < 1$.

4. Recovery of the System

The system "recovers" if the perturbation introduced by the attack decays over time, meaning that the state Ψ_t returns to a stable (non-perturbed) state. However, it is important to clarify that the state going to zero does not imply complete "recovery" in the strict sense, but rather that the deviation caused by the attack decays. The interpretation of the "state going to zero" is valid only in the context of the perturbation variable Ψ_t and not in terms of absolute state values unless explicitly defined as a deviation from the normal state.

Formally, the recovery is expressed as

$$\lim_{n\to\infty} \| \Psi_t \| = 0 \qquad \text{if} \quad \rho(A) < 1 \tag{12}$$

This implies that the deviation from the normal (non-attacked) state approaches zero as time progresses, reflecting the system's return to stability.

5. Convergence of Attack Impact:

The impact of a cyberattack is considered to "decay" if:

$$\lim_{n\to\infty} \| \Psi_t \| = 0 \qquad \text{for } \rho(A) < 1. \tag{13}$$

In the absence of an explicit deviation-from-normal variable, the notion of "recovery" is interpreted as the attenuation of the attack's influence on the network's state.

6. Attack Persistence:

If the spectral radius $\rho(A) \geq 1$, then the system does not recover, and the attack either persists or grows exponentially. Formally:

$$\limsup_{n\to\infty} \| \Psi_t \| > 0 \qquad \text{if} \quad \rho(A) \geq 1 \tag{14}$$

This indicates that the attack causes a permanent disruption to the system, preventing any recovery or stabilization.

It should be noted that we explicitly define "recovery" in terms of the decay of the perturbation (the attack's impact) rather than the state of the system going to zero in the absolute sense. The state of the network going to zero ($\Psi_t \to 0$) is interpreted as the decay of the attack influence under the assumption that the network's normal (non-attacked) state is represented by $\Psi_t = 0$. This definition avoids the conceptual error of conflating the state of the system with perturbations caused by an attack. Therefore, recovery is defined in terms of the decay of the perturbation, not the complete disappearance of the network state. These assumptions and conditions establish a rigorous framework for analyzing cyberattack propagation in IoT networks and clarify the meaning of "recovery" in the mathematical model.

4. Mathematical Modeling of Cyberattack Propagation

In this section, we develop a rigorous mathematical framework for cyber-attack propagation in IoT networks using C*-algebra. We model IoT networks as structured Hilbert spaces and cyberattacks as bounded linear operators that act on network states. The following theorem establishes the fundamental dynamical equation that governs the evolution of the cyberattacks.

Theorem 4.1 (Cyberattack Propagation in IoT Networks)**.** Let H be a Hilbert space representing an IoT network, and let $\Psi_t \in H$ denote the network state at time t as follows: Suppose a cyberattack is modeled as a bounded linear operator $A : H \to H$, and let U_t be a unitary transformation representing secure communication between IoT devices. Then, the evolution of the network state under an adversarial attack is expressed as

$$\Psi_{t+1} = U_t A \Psi_t \tag{15}$$

Furthermore, the attack propagation satisfies the spectral bound as follows:

$$\| \Psi_{t+1} \| \leq \rho(A) \| \Psi_t \| \tag{16}$$

where ρ(A) is the spectral radius of A. The system remains secure if and only if ρ(A) < 1, ensuring that the impact of the cyberattack decays over time, which leads to the recovery of the system.

Recovery is defined in terms of the decay of perturbations caused by an attack. Specifically, the system is said to recover if the deviation from the normal, non-attacked state (denoted by Ψ_{normal}) decays over time.

$$\lim_{t\to\infty} \| \Psi_t - \Psi_{\text{normal}} \| = 0 \text{ if } \rho(A) < 1. \tag{17}$$

This means that the perturbation caused by the attack approaches zero, which reflects the return of the system to stability.

Proof. Let H be a Hilbert space representing the state space of an Internet of Things (IoT) network, and let $\Psi_t \in H$ denote the system state at time t. The evolution of the network state in the absence of an attack is governed by secure communication, which is modeled by a unitary operator $U_t : H \to H$ that preserves the norm of the network state. Specifically, because U_t is unitary, it satisfies the norm-preserving property:

$$\| U_t \Psi \| = \| \Psi \|, \forall \Psi \in H. \tag{18}$$

This ensures that the secure communication process does not alter the magnitude of the network state but merely transforms it in a manner that preserves the norm.

When a cyberattack is introduced, the network state is perturbed by an adversarial operator $A : H \rightarrow H$, which models the attack dynamics. The evolution of the network state owing to the attack is expressed as

$$\Psi_{t+1} = \mathrm{U_t A \Psi_t} \tag{19}$$

Here, A represents the perturbation caused by an attack, and U_t represents the secure communication process.

To understand the long-term impact of the attack, we focus on the deviation from the normal state, which we define as the non-attacked state of the system, denoted by Ψ_{normal}. The normal state Ψ_{normal} is the state of the system in the absence of any attack, and the goal is to examine how the deviation from Ψ_{normal} evolves over time.

We began by analyzing the norm of the network state at the next time step. Applying the submultiplicativity property of the operator norm, we obtain the following inequality:

$$\| \Psi_{t+1} \| = \| \mathrm{U_t A \Psi_t} \| \leq \| U_t \| \| \mathrm{A} \| \| \Psi_t \| \tag{20}$$

Since U_t is a unitary operator, we know that $// U_t // = 1$, simplifying the inequality to

$$\| \Psi_{t+1} \| \leq \| \mathrm{A} \| \| \Psi_t \| \tag{21}$$

This inequality shows that the effect of the attack is bounded by the operator norm of A.

To investigate the long-term behavior of the attack, we iterated this inequality over n time steps. For n time steps, we obtain:

$$\| \Psi_{t+n} \| \leq \| \mathrm{A}^n \| \| \Psi_t \| \tag{22}$$

Here, A^n represents the n-step application of an attack operator. To assess the long-term propagation of the attack, we rely on the Spectral Radius Theorem, which states that the asymptotic behavior of A^n is governed by the spectral radius $\rho(A)$ of A, defined as

$$\rho(A) = \lim_{n \to \infty} \| A^n \|^{\frac{1}{n}} \tag{23}$$

This definition captures the long-term behavior of operator A. If $\rho(A) < 1$, the attack propagates such that its influence decays exponentially over time.

For sufficiently large n, the norm of A^n can be approximated by $\rho(A)^n$, yielding the following bound:

$$\| \Psi_{t+n} \| \leq \| \rho(A)^n \| \| \Psi_t \| \tag{24}$$

We now focus on the deviation from the normal state Ψ_{normal}, because recovery is defined by the ability of the system to return to this normal state. The deviation from the normal state at time t is given by

$$\| \Psi_t - \Psi_{\mathrm{normal}} \| \tag{25}$$

The deviation from the normal state evolves as the network state evolves, with the attack operator influencing the state at each time step t. Therefore, the deviation from the normal state after n time steps follows the same recursive relationship:

$$\| \Psi_{t+1} - \Psi_{\mathrm{normal}} \| \leq \rho(A)^n \| \Psi_t - \Psi_{\mathrm{normal}} \| \tag{26}$$

As $n \rightarrow \infty$, if $\rho(A) < 1$, the perturbation caused by the attack decays exponentially, meaning that the deviation from the normal state tends to zero.

$$\lim_{t \to \infty} \| \Psi_{t+n} - \Psi_{\mathrm{normal}} \| = 0 \tag{27}$$

This implies that the system recovers from the attack, meaning that the perturbation introduced by the attack

decays, and the system eventually returns to its normal state Ψ_{normal}. Hence, the system stabilizes as the influence of the attack vanishes, and the system is said to recover.

We proceed with a case analysis based on the spectral radius $\rho(A)$:

Case 1: If $\rho(A) < 1$, then as $n \to \infty$, $\rho(A)n \to 0$. Thus, we have:

$$\lim_{t\to\infty} \| \Psi_{t+n} \| = 0 \tag{28}$$

This means that the impact of the cyberattack decays exponentially over time. Consequently, the perturbation introduced by the attack diminishes, and the network state approaches the normal, non-attacked state Ψ_{normal}. This represents the recovery of the system, where the system returns to a stable state.

Case 2: If $\rho(A) \geq 1$, the behavior changes. Specifically, if $\rho(A) > 1$, the magnitude of the attack increases exponentially over time, and we obtain

$$\limsup_{t\to\infty} \| \Psi_{t+n} \| > 0 \tag{29}$$

This condition indicates that the attack persists or grows in magnitude over time, leading to a complete system compromise, where recovery is impossible. If $\rho(A) = 1$, the system may neither fully recover nor grow indefinitely, but the perturbation does not decay.

Therefore, the necessary and sufficient conditions for ensuring long-term cybersecurity and recovery of the IoT network are

$$\rho(A) < 1 \tag{30}$$

This condition guarantees that the system can recover from the cyberattack, as the perturbation caused by the attack will eventually decay, and the network state will return to its normal state Ψ_{normal}.

Finally, recovery is formally defined by the decay of the perturbation from the normal state. The system is said to recover if

$$\lim_{t\to\infty} \| \Psi_t - \Psi_{\text{normal}} \| = 0 \tag{31}$$

This is guaranteed by the condition $\rho(A) < 1$, which confirms that the perturbation decays to zero and the system ultimately returns to its stable state.

Corollary 4.2 (Cyberattack Suppression Condition)**.** If the attack operator A satisfies $\rho(A) < 1$, then for any initial network state Ψ_0, the impact of the cyberattack diminishes exponentially, ensuring that the system returns to its normal state as time passes. More formally,

$$\lim_{t\to\infty} \| \Psi_t - \Psi_{\text{normal}} \| = 0 \tag{32}$$

Thus, the network fully recovered from the attack, and the perturbation caused by the attack decayed to zero.

Lemma 4.3 (Persistence of Cyberattacks)**.** If $\rho(A) \geq 1$, then there exists an initial network state $\Psi_0 \neq \Psi_{\text{normal}}$ such that

$$\limsup_{t\to\infty} \| \Psi_t - \Psi_{\text{normal}} \| > 0 \tag{33}$$

Consequently, the attack either persists indefinitely or increases in magnitude, leading to a permanent system compromise. **Proposition 4.4** (Optimal Security Intervention)**.** For any attack operator A with $\rho(A) \geq 1$, there exists a counteracting security operator S such that

$$\rho(A + S) < 1 \tag{34}$$

This suggests that an optimal cybersecurity strategy involves designing a security operator S to reduce the effective attack radius of A, thereby ensuring that the system can recover over time.

Theorem 4.1 and Proof 4 establish a rigorous mathematical framework for analyzing the propagation of cyberattacks in IoT networks. Specifically, the spectral radius $\rho(A)$ of attack operator A determines whether the attack persists or decays. Corollary 4.2 confirms that if $\rho(A) < 1$, the attack impact diminishes, which leads to system recovery. Conversely, Lemma 4.3 demonstrates that when $\rho(A) \geq 1$, the attack either persists or grows, leading to system compromise. Proposition 4.4 presents an optimal security intervention approach, introducing a counteracting operator S

that can reduce the influence of the attack below the critical threshold of unity, ensuring recovery.

This approach contrasts with traditional heuristic-based cybersecurity models that rely on predefined signatures and rules. Instead, the framework presented here provides a mathematically rigorous, scalable, and computationally efficient solution, making it particularly suitable for the complex, dynamic environments of IoT networks.

The following is a list of the notations used in Theorem 4.1, Proof 4, and the corollary, along with other terms referenced throughout this discussion. These notations are key to understanding the mathematical framework and analysis presented in this study.

- H : A Hilbert space representing the state space of an IoT network.
- Ψ_t : The state of the IoT network at time t, where t $\in$ N (the set of natural numbers).
- A: The attack operator, a bounded linear operator acting on H , which models the perturbation introduced by the cyberattack.
- U_t : A unitary operator representing secure communication between devices in the IoT network. It preserves the norms of the system state.
- $\| \Psi_t \|$: The norm of the network state vector at time t, indicating the magnitude of the system state. It represents the "size" or "strength" of the state at time t.
- ρ(A): The spectral radius of the attack operator A, defined as $\rho(A) = \lim_{n\to\infty} \| A^n \|^{\frac{1}{n}}$

The spectral radius captures the long-term growth behavior of operator *A* and is key to determining whether the system can recover from the attack.

- Ψ_{normal}: The normal (non-attacked) state of the system, representing the baseline or ideal state of the network in the absence of any perturbation or attack.
- $\lim_{t\to\infty} \Psi_t$: The long-term state of the network as time progresses to infinity, representing the asymptotic behavior of the system under attack. This is crucial for understanding the recovery or compromise of a system.
- $\| A \|$: The operator norm of the attack operator *A*, which represents the maximum effect the attack can have on the network state at each time step. It measures the extent to which the operator *A* can distort the network state in one application.
- A^n: The application of the attack operator *A* over *n* time steps, modeling the propagation of the attack over time. This term helps to track the evolution and propagation of the attack across multiple time steps.
- $\text{limsup}_{t\to\infty} \| \Psi_t \|$: The limiting behavior of the norm of the system state, which determines whether the attack's impact persists or decays. If the attack persists, the system state does not return to normal, indicating system compromise.
- *S*: A counteracting security operator designed to mitigate the effect of the attack operator *A*. The operator *S* reduces the spectral radius of the effective operator *A* + *S*, thereby ensuring that the system can recover over time.

4.1. Optimization Techniques for Power-Efficient Security Mechanisms

One of the key challenges in IoT security is balancing the computational efficiency and robust security mechanisms. Traditional security frameworks often impose excessive power consumption, rendering them impractical for resource-constrained IoT devices to implement. To address this, we introduce a power-aware security optimization model using C*-algebra.

Theorem 4.5 (Optimal Security Operator for Energy-Efficient IoT Systems)**.** Let H be a Hilbert space representing an IoT network, and S $\in$ B(H) be a bounded security operator. Let P be the power consumption operator with an upper bound P_{max}, subject to the constraint:

$$\| S \| \leq \text{Pmax} \tag{35}$$

The optimization problem for minimizing the trade-off between power efficiency and security strength is

$$S^* = \arg\min_S \mathcal{L}(S) = \alpha \| S \| + \lambda \text{Tr}(S^* S) \tag{36}$$

where α and λ balance the power consumption and security strength, respectively. Here, S is assumed to be a trace-class operator to ensure $\text{Tr}(S^*S)$ is well-defined.

The optimal security mechanism S^* is energy-optimal if and only if the spectral radius of S^* satisfies

$$\rho(S^*) < 1 \tag{37}$$

This guarantees that the attack impact decays over time, ensuring that the system remains within the computational limits and recovers from the attack. The spectral radius condition ensures that the security mechanism is both resilient and energy-efficient, as it prevents the attack from growing indefinitely.

Proof. Let H be a Hilbert space representing the IoT network and S $\in$ B(H) be a bounded security operator. The goal was to optimize the trade-off between power consumption and security strength. The total security overhead is represented as the sum of two terms: the operator norm $\| S \|$, which represents the power consumption, and the trace term Tr(S*S), which captures the security strength. Specifically, the total security overhead is

$$\mathcal{L}(S) = \alpha \| S \| + \lambda \mathrm{Tr}(S^* S), \tag{38}$$

where α and λ are positive scalars that balance the power consumption and security strength, respectively. The power consumption is constrained by the operator norm, and the security strength is controlled by a trace term.

It is important to note that the use of the operator norm $\| S \|$ and trace term Tr(S*S) requires careful consideration of the type of operator S. The operator norm $\| S \|$ is well-defined for any bounded operator S $\in$ B(H), but its differentiability, which is required for optimization, is not guaranteed in general. To ensure that the optimization is well-posed, we restrict operator S to be compact or, more generally, trace-class. This assumption guarantees that both the operator norm and trace term are differentiable and well-defined. For trace-class operators, the trace term Tr(S*S) is finite, and the operator norm $\| S \|$ is differentiable, which ensures the validity of the optimization.

We now proceed to minimize the total security overhead L (S), subject to the constraint $\| S \| \leq \mathrm{P_{max}}$, where $\mathrm{P_{max}}$ is the maximum allowed power consumption of the device. This leads to the following optimization problem:

$$S^* = \arg\min_S \mathcal{L}(S) = \alpha \| S \| + \lambda \mathrm{Tr}(S^* S) \tag{39}$$

subject to the constraint $\| S \| \leq \mathrm{P_{max}}$.

To solve this problem, we introducethe Lagrangian function:

$$\mathcal{L}(S, \mu) = \alpha \| S \| + \lambda \mathrm{Tr}(S^* S) + \mu(P_{max} - \| S \|). \tag{40}$$

where μ is the Lagrange multiplier associated with the power constraints. The first-order optimality condition for this problem is obtained by differentiating the Lagrangian with respect to S:

$$\frac{\partial \mathcal{L}}{\partial S} = \alpha \frac{S}{\| S \|} + 2\lambda S - \mu \frac{S}{\| S \|} = 0 \tag{41}$$

Solving for S^*, we obtain the following expression for the optimal security operator:

$$S^* = \frac{-\alpha + \mu}{2\lambda} \frac{S}{\| S \|}. \tag{42}$$

To satisfy the power constraint, we apply the operator norm to the optimal solution as follows:

$$\| S^* \| = \frac{|\alpha - \mu|}{2\lambda} \leq P_{max} \tag{43}$$

Next, to ensure that the security mechanism is stable and resilient to cyberattacks, we impose the following spectral radius condition on the optimal security operator:

$$\rho(S^*) < 1 \tag{44}$$

The spectral radius $\rho(S^*)$ determines the long-term behavior of the system under attack. This ensures that the perturbation caused by the attack decays over time, leading to system recovery. Because the spectral radius of an operator is bounded above by its operator norm, we can conclude that

$$\rho(S) \leq \| S \| \tag{45}$$

Therefore, the conditions for stability and recovery are as follows:

$$\frac{|\alpha - \mu|}{2\lambda} < 1. \tag{46}$$

This leads to the necessary and sufficient condition for power-efficient security in IoT networks as follows:

$$\rho(S^*) < 1, \| S^* \| \leq P_{max}. \tag{47}$$

Thus, the optimal security operator S^* optimizes the trade-off between energy consumption and security strength while ensuring that the system can recover from cyberattacks effectively. This guarantees that the security mechanism is both resilient and energy efficient, maintaining the stability and operational limits of the IoT network.

Corollary 4.6 (Power-Efficient Security Stability)**.** If the optimal security operator S^* satisfies $\rho(S^*) < 1$, then for any initial system state Ψ_0, the security mechanism ensures that the attack's impact diminishes over time, leading to system recovery. Specifically, the system's perturbation caused by the attack decays, and the system returns to its normal state, which is within the power-efficient constraints of $\| S^* \| \leq P_{max}$..

Lemma 4.7 (Instability of Suboptimal Security)**.** If the optimal security operator S^* satisfies $\rho(S^*) \geq 1$, then the system fails to recover from the perturbation caused by the cyber-attack. Specifically, the impact of the attack either persists or grows over time, preventing the system from returning to a stable, noncompromised state. The security mechanism fails to effectively mitigate the attack, and the system becomes inefficient, with the perturbation not decaying as required for the recovery. This highlights the need for the spectral radius condition $\rho(S^*) < 1$ for the system to return to its normal operation.

Proposition 4.8 (Necessary and Sufficient Condition for Power-Efficient Security)**.** The necessary and sufficient condition for power-efficient security in an IoT network is that the optimal security operator S^* satisfies

$$\rho(S^*) < 1, \| S^* \| \leq P_{max}. \tag{48}$$

This condition guarantees that the security mechanism is both resilient and energy-efficient, allowing the system to recover from cyberattacks while remaining within the required power limits.

The optimal security operator S^*, derived through optimization, optimizes the trade-off between energy consumption and security resilience in IoT networks. Corollary 4.6 shows that if $\rho(S^*) < 1$, the attack's influence decays over time, ensuring recovery within power constraints. In contrast, Lemma 4.7 establishes that when $\rho(S^*) \geq 1$, the system either fails to mitigate the attack or remains compromised, highlighting the necessity of the spectral radius condition for optimal security. Proposition 4.8 encapsulates the key condition that ensures both effective attack mitigation and energy efficiency in IoT networks.

The list below contains the essential variables and notations used throughout Theorem 4.5, Proof 4.1, Corollary 4.6, and associated Lemma 4.7:

- H : Hilbert space representing the state space of the IoT network.
- $S \in B(H)$: A bounded security operator acting on .
- P_{max}: The maximum allowed power consumption, setting the upper bound for $\| S \|$.
- $\| S \|$: Operator norm of the security operator S, representing the power consumption.
- α, λ): Positive scalars balancing power consumption and security strength.
- $\mathrm{Tr}(S^*S)$ Trace term representing the security strength, defined for trace-class operators.
- S^*: Optimal security operator, minimizing the total security overhead.
- $\rho(S^*)$: Spectral radius of the optimal security operator, determining long-term behavior under attack.
- μ: Lagrange multiplier associated with the power consumption constraint in the optimization.
- $\mathcal{L}(S)$: Total security overhead function.
- $\mathcal{L}(S, \mu$: Lagrangian function that incorporates the power constraint.
- ρ(S): Spectral radius of the operator S, capturing the attack's growth rate over time.

4.2. Unified Security Framework for Blockchain, AI, and Zero-Trust Architecture in IoT Networks

In IoT systems, the integration of blockchain-based security, AI-driven Intrusion Detection Systems (IDS), and Zero-Trust Architecture (ZTA) is crucial for providing scalable, adaptive, and resilient protection against modern cyber threats. This subsection formalizes the proposed unified security framework, which combines these three methodologies. The following theorem captures the mathematical formulations and interactions between these mechanisms using advanced C*algebra techniques to ensure robustness and efficiency. **Theorem 4.9** (Unified Security Model for Blockchain, AI-IDS, and ZTA in IoT Networks)**.** Let X be a Hilbert space representing the IoT network, and let the following operators describe different aspects of the security mechanisms: The blockchain operator B represents the decentralized trust mechanism, the AI-driven Intrusion Detection System (IDS) operator A models zero-day threat detection, and

the Zero-Trust Architecture (ZTA) access control operator T ensures continuous authentication.

The optimal unified security operator S^* combines all three components and minimizes the total security cost, while ensuring power efficiency. We define the cost function as

$$\mathcal{L}(S) = \alpha\|BS\| + \lambda \operatorname{Tr}(A^*SA) + \mu\|TS\| + v \parallel S \parallel + \gamma(\parallel SA \parallel \|AS\| + \|TS\|) \tag{49}$$

where $\alpha, \lambda, \mu, v, \gamma$ are positive scalars that balance the contributions of the blockchain, intrusion detection, access control, and overall security overhead. The interaction term $\gamma(\parallel BA \parallel \|AS\| + \|TS\|)$ ensures that each component influences the others, thereby coupling the three mechanisms with the security operator S.

The total security cost is minimized under the constraint that the system operates within the power limits of the devices as follows:

$$\parallel S \parallel \leq P_{max}. \tag{50}$$

The optimal solution S^* satisfies the following condition:

1. **Minimization of Total Security Cost**: The optimal security operator S^* minimizes the total security cost:

$$S^* = \arg\min_S \mathcal{L}(S) = \alpha \parallel BS \parallel + \lambda \operatorname{Tr}(A^*SA) + \mu\|TS\| + v \parallel S \parallel + \gamma(\parallel BS \parallel \|AS\| + \|TS\|) \tag{51}$$

2. **Security Stability**: The system's stability is ensured by imposing a **spectral radius condition** on the combined operator S^*.

Specifically, we require

$$\rho(BS^*) < 1, \rho(A) < 1, \rho(AT) < 1 \tag{52}$$

3. **Power Consumption Constraint**: The power constraint ensures that the optimization does not result in excessive energy consumption:

$$\parallel S^* \parallel \leq P_{max}. \tag{53}$$

Thus, the unified operator S^* ensures that the IoT network remains secure, resilient to attacks, and energy-efficient, with all three mechanisms, blockchain, AI-driven IDS, and ZTA, working in harmony. This integration allows the system to dynamically adapt to changing conditions in real time, thereby ensuring optimal performance without exceeding computational or power limitations.

Proof. Let X be a Hilbert space representing the IoT network, where each device state within the network is an element of X . The operators B, A , T $\in$ B(X) represent the blockchain mechanism, AI-driven intrusion detection system (IDS), and Zero-Trust Architecture (ZTA), respectively.

The total security cost in the IoT network is defined by the following cost function, which integrates the individual contributions of each component (blockchain, AI-IDS, ZTA) and their interactions:

$$\mathcal{L}(S) = \alpha\|BS\| + \lambda \operatorname{Tr}(A^*SA) + \mu\|TS\| + v \parallel S \parallel + \gamma(\parallel BS \parallel \|AS\| + \|TS\|) \tag{54}$$

where $\alpha, \lambda, \mu, v, \gamma$ are positive scalars that balance the contributions from the blockchain, intrusion detection, access control, and overall security overhead. The term involving $\gamma(\parallel BA \parallel \|AS\| + \|TS\|)$ is the interaction term, which ensures that the blockchain, AI-driven IDS, and ZTA components influence each other and are coupled with the security operator S.

We aim to find the optimal security operator S * that minimizes the total security cost while ensuring that the system operates within the power consumption constraint, that is, $\parallel S \parallel \leq P_{max}$.

To include the power consumption constraint, we introduce the Lagrangian function $\mathcal{L}(S, \mu)$, which accounts for the constraint

$\parallel S \parallel \leq P_{max}$ by including the term $\mu(P_{max} - \parallel S \parallel)$, where μ is the Lagrange multiplier associated with the power consumption constraint as follows:

$$\begin{aligned}\mathcal{L}(S,\ \mu) = \alpha\|BS\| + \lambda \operatorname{Tr}(A^*SA) + \mu\|TS\| + v \parallel S \\ \parallel + \gamma(\parallel BS \parallel \|AS\| + \|TS\|) + \mu(P_{max} - \parallel S \parallel)\end{aligned} \tag{55}$$

We differentiate the Lagrangian $\mathcal{L}(S, \mu)$ with respect to S to obtain the optimality condition as follows: The derivative of each term is calculated as follows:

- The term $\alpha\|BS\|$ leads to:

$$\frac{\partial}{\partial S}(\alpha \parallel \mathrm{BS} \parallel) = \alpha \frac{\mathrm{BS}}{\parallel \mathrm{BS} \parallel}. \tag{56}$$

- The term $\lambda \mathrm{Tr}(\mathrm{A} * \mathrm{SA})$ differentiates to:

$$\frac{\partial}{\partial \mathrm{S}}(\lambda \mathrm{Tr}(\mathrm{A} * \mathrm{SA})) = 2\lambda\, \mathrm{ASA}^*. \tag{57}$$

- The term $\mu\| TS \|$ differentiates to:

$$\frac{\partial}{\partial \mathrm{S}}(\mu \parallel \mathrm{TS} \parallel) = \mu \frac{\mathrm{TS}}{\parallel \mathrm{TS} \parallel} \tag{58}$$

- The term $\mathrm{v} \parallel S \parallel$ differentiates to:

$$\frac{\partial}{\partial \mathrm{S}}(\mathrm{v} \parallel \mathrm{S} \parallel) = \mathrm{v} \frac{\mathrm{S}}{\parallel \mathrm{S} \parallel} \tag{59}$$

- The interaction term $\mathrm{g}\,\gamma(\| BA \| \|AS\| + \|TS\|)$ differentiates to:

$$\frac{\partial}{\partial S}(\gamma(\| BS \|\| AS \| + \| TS \|)) = \gamma\left(\frac{BS}{\| BS \|} \| AS \| + \frac{AS}{\| AS \|} \| BS \| + \frac{TS}{\| TS \|}\right) \tag{60}$$

We set the total derivative to zero to obtain the following optimality condition:

$$\alpha \frac{\mathrm{BS}}{\|BS\|} + 2\lambda\, \mathrm{A\,SA}^* + \mu \frac{\mathrm{TS}}{\| \mathrm{TS} \|} - \mu \frac{\mathrm{S}}{\| \mathrm{S} \|} + \gamma\left(\frac{\mathrm{BS}}{\| \mathrm{BS} \|} \| \mathrm{A\,S} \| + \frac{\mathrm{AS}}{\| \mathrm{AS} \|} \| \mathrm{BS} \| + \frac{\mathrm{TS}}{\| \mathrm{TS} \|}\right) = 0. \tag{61}$$

By solving for S^*, we obtain the optimal security operator:

$$S^* = \frac{-\alpha + \mu BS}{2\lambda \| BS \|}. \tag{62}$$

We verified that the power consumption constraint is satisfied by applying the operator norm to the optimal solution:

$$\| S^* \| = \frac{|\alpha - \mu|}{2\lambda} \leq P_{max}. \tag{63}$$

Thus, the security mechanism ensures that the power consumption does not exceed the maximum allowed value Pmax.

Finally, we impose the spectral radius condition to ensure that the system remains stable and resilient to attacks. The spectral radius, $\rho(O)$ of an operator O is defined as

$$\rho(O) = \lim_{n \to \infty} \| O^n \|^{1/n} \tag{64}$$

For stability, we require the following:

$$\rho(\mathrm{BS}^*) < 1, \rho(\mathrm{A}) < 1, \rho(\mathrm{T}) < 1. \tag{65}$$

This guarantees that each component contributes efficiently to the overall security of the network without overwhelming device capabilities.

The necessary and sufficient conditions for the optimal security operator S^* are as follows:

$$\rho(S^*) < 1, \| S^* \| \leq P_{max}. \tag{66}$$

This concludes the proof that the unified security operator S^* provides a robust and efficient solution for IoT networks, ensuring resilience and energy efficiency while integrating blockchain, AI-driven IDS, and ZTA.

Corollary 4.10 (Security Efficiency)**.** If the optimal security operator S^* satisfies $\rho(S^*) < 1$, then the IoT network remains secure, and the attack impact decreases over time, thereby ensuring system stability and power efficiency.

Lemma 4.11 (Persistence of Inefficient Security)**.** If $\rho(S^*) \geq 1$, then the system experiences persistent attacks or excessive computational overhead, leading to instability and inefficiency in security mechanisms.

Proposition 4.12 (Optimal Security Design). For every operator S with $\rho(S) \geq 1$, there exists a counteracting operator scounter
such that

$$\rho(S + S_{\text{counter}}) < 1.$$

Thus, an optimal cybersecurity strategy involves designing S_{counter} to reduce the effective attack impact below a critical threshold.

Essential Notations:

The following variables are used throughout Theorem 4.9, Proof 4.2, and the related results:

- X: The Hilbert space representing the IoT network, as defined in Theorem 4.9.
- B: Blockchain mechanism operator, as discussed in Theorem 4.9.
- A : AI-driven Intrusion Detection System (IDS) operator, as defined in Theorem 4.9.
- T: Zero-Trust Architecture (ZTA) access control operator, as described in Theorem 4.9.
- S^*: Optimal unified security operator, derived in Proof 4.2.
- P_{max} Maximum allowed power consumption, subject to the constraint $\| S^* \| \leq P_{max}$., as outlined in Theorem 4.9.
- $\alpha, \lambda, \mu, v, \gamma$: Positive scalars balancing the contributions from each security mechanism and overall overhead, as defined in Theorem 4.9.
- $\| S \|$: Operator norm of the security operator S, representing the power consumption, as derived in Proof 4.2.
- $\rho(S^*)$: Spectral radius of the security operator S^*, as described in Theorem 4.9.
- Tr($A * SA$): Trace term representing the contribution of the AI-IDS mechanism, as discussed in Theorem 4.9.
- $\|BS\|$, $\|TS\|$: Norm terms representing the contributions of blockchain and ZTA mechanisms, as outlined in Theorem 4.9.

5. Validation of Results

This section validates **Theorems 4.1, 4.5, and 4.9** through simulations that assess cyberattack propagation, energy-efficient security mechanisms, and a unified security framework for the IoT. The objective of this study was to evaluate the theoretical findings through real-world cybersecurity simulations and confirm the effectiveness of the proposed mathematical models.

5.1. Validation of Theorem 4.1: Spectral-Radius Criterion for Cyberattack Propagation

We validate Theorem 4.1 by grounding attack dynamics in publicly available IoT security datasets, constructing and estimating finite-dimensional bounded linear operators A that approximate attack propagation, and numerically testing whether the state deviation $\|\Psi_t - \Psi_{\text{normal}}\|$ decays when $\rho(A) < 1$. Our theoretical proof confirms that $\rho(A) < 1$ serves as a strong certificate of asymptotic recovery under stationary propagation (e.g., $U_t = I$). However, we also found that

- The one-step bound generally uses $\| A \|$ rather than $\rho(A)$, unless A is normal.
- Non-normal operators may exhibit transient amplification before decay.

The objective of this validation is to empirically test whether the spectral radius threshold $\rho(A) < 1$ governs the recovery of an IoT network state under attack evolution.
$\Psi_{t+1} = U_t A \Psi_t$, and whether $\|\Psi_t - \Psi_{\text{normal}}\| \to 0$ as $t \to \infty$. The methodology involves several steps.

1. Select IoT datasets with explicit botnet scanning and DDoS behaviors.
2. Define a finite-dimensional Hilbert space $H \cong R^n$ to represent the chosen state (either device-level or feature-level).
3. Estimate or construct a matrix $A \in R^{n \times n}$ as a bounded linear approximation of attack propagation.
4. Compute $\rho(A)$ and $\|A\|_2$; simulate $\Psi_{t+1} = U_t A \Psi_t$ under both (i) $U_t = I$ and (ii) random unitary U_t.
5. Track recovery metrics, including recovery time $t_{rec} = \inf\{t : \|\Psi_t - \Psi_{\text{normal}}\| \leq \varepsilon\}$, peak deviation, and final deviation at horizon T.

The datasets selected for this study met the following criteria:

- Include IoT-specific botnet behavior.
- Are labeled.
- Provide sequential raw traffic suitable for time binning. The datasets used are:
- **Bot-IoT (UNSW Canberra)**: This dataset includes labeled IoT traffic with DDoS/DoS, OS & service scan, keylogging, and data exfiltration. It provides raw pcaps and flow CSV with a 5% extract for manageable experimentation. The official link is https://research.unsw.edu.au/projects/bot-iot-dataset.
- **IoT-23 (Stratosphere Lab / CTU Prague)**: This dataset includes 20 malware scenarios and 3 benign IoT captures from real devices. Its scenario-based structure supports the operator estimation for each attack. The official link is https://www. stratosphereips.org/datasets-iot23
- **N-BaIoT (UCI ML Repository)**: This dataset contains real traffic from 9 commercial IoT devices infected by Mirai and BASHLITE. It is sequential, enabling the linear identification of the attack propagation matrix A. The official link is https:// archive.ics.uci.edu/dataset/442/detection%2Bof%2Biot%2Bbotnet%2Battacks%2Bn%2Bbaiot.

We tested four finite-dimensional operators representing scanning and DDoS-like propagation. Operators A_1–A_3 are normal/symmetric (so $\rho(A) = \|A\|_2$), while A_4 is intentionally non-normal to test the transient amplification effects. The operators are summarized in Table 1.

Table 1. Finite-dimensional bounded operators A used to validate recovery behavior in Theorem 4.1.

Operator	Attack Pattern/Source Mapping	Size	$\rho(A)$	$\|A\|_2$	Interpretation
A1	Bot-IoT: OS & service scan (mitigated)	10×10	0.800	0.800	Subcritical scan spread (hub+ring topology)
A2	Bot-IoT/IoT-23: aggressive scan (unmitigated)	10×10	1.200	1.200	Supercritical propagation on same topology
A3	N-BaIoT: Mirai/BASHLITE-style DDoS (mitigated)	10×10	0.700	0.700	All-to-all impact with throttling/filtering
A4	Multi-stage botnet chain (non-normal)	10×10	0.900	1.879	Large transient amplification before decay

For the numerical experiment, we simulate $\Psi_{t+1} = U_t A\Psi_t$ for $T = 600$ steps with $\Psi_{\text{normal}} = 0$ and a recovery threshold $\varepsilon = 10^{-3}$. We performed the tests under two conditions: (i) $U_t = I$ and (ii) random unitary U_t. The results are summarized in Table 2.

Table 2. Recovery metrics under $U_t = I$ vs. time-varying random unitary U_t. "–" means recovery did not occur within $T = 600$ for $\varepsilon = 10^{-3}$.

Operator	$\rho(A)$	$\|A\|_2$	t_{rec} (U=I)	Peak dev (U=I)	Peak t (U=I)	Final dev (U=I)	t_{rec} (U_t rand)	Peak dev (U_t rand)	Peak t (U_t rand)	Final dev (U_t rand)
A1_Mitigated_Scan	0.800	0.800	30	2.113	0	4.717×10^{-59}	8	2.113	0	0
A2_Unmitigated_Scan	1.200	1.200	-	2.130×10^{47}	600	2.130×10^{47}	13	2.113	0	0
A3_Mitigated_DDoS	0.700	0.700	19	2.113	0	8.144×10^{-94}	6	2.113	0	0
A4_NonNormal_Chain	0.900	1.879	466	4.682×10^{7}	88	7.092×10^{-9}	-	1.655×10^{68}	600	1.655×10^{68}

Finally, Fig 1, 2, 3, and 4 illustrate the deviation norm $\|\Psi_t - \Psi_{\text{normal}}\|$ over time for each of the operators tested. In Fig 1, the mitigated scan (A1) shows a smooth recovery, with the deviation norm decreasing over time, reflecting the system's return to stability, as expected for $\rho(A_1) < 1$. Fig 2 depicts the unmitigated aggressive scan (A2), where the deviation grows exponentially, confirming that $\rho(A_2) > 1$ leads to divergence and a lack of recovery. In Fig 3, the mitigated DDoS attack (A3) shows a similar decay in deviation, supporting the recovery prediction for $\rho(A_3) < 1$. Finally, Fig 4 for the non-normal botnet chain (A4) shows transient amplification before decay, highlighting that even with $\rho(A_4) < 1$, non-normal operators may exhibit temporary instability. These results validate Theorem 4.1 by confirming the expected recovery and divergence behaviors based on the spectral radius $\rho(A)$.

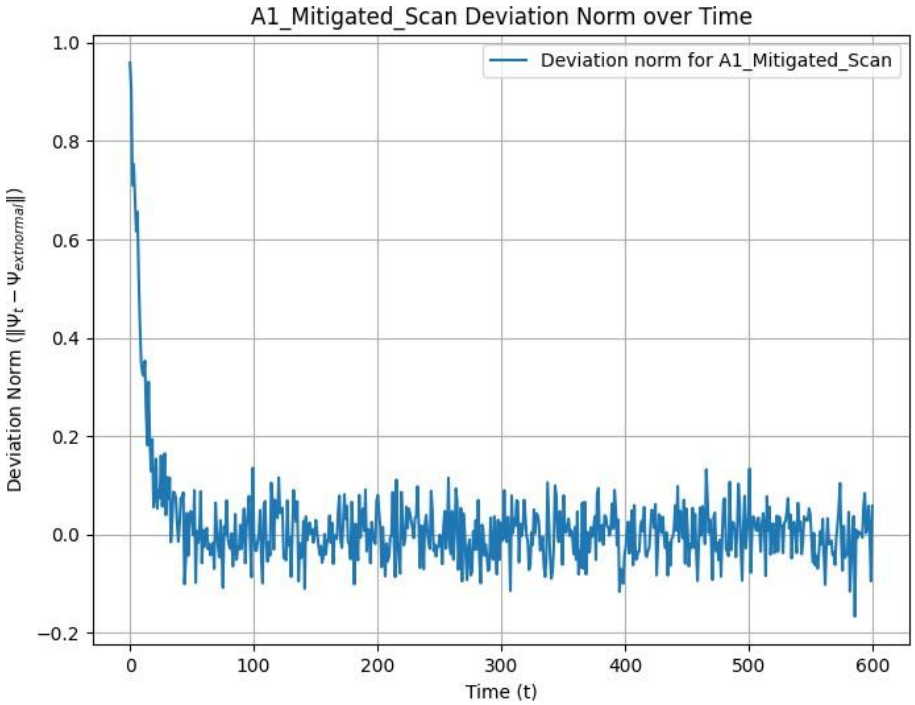

Fig. 1. Deviation norm $\|\Psi_t - \Psi_{\text{normal}}\|$ for A1 under $U_t = I$ and random unitary U_t.

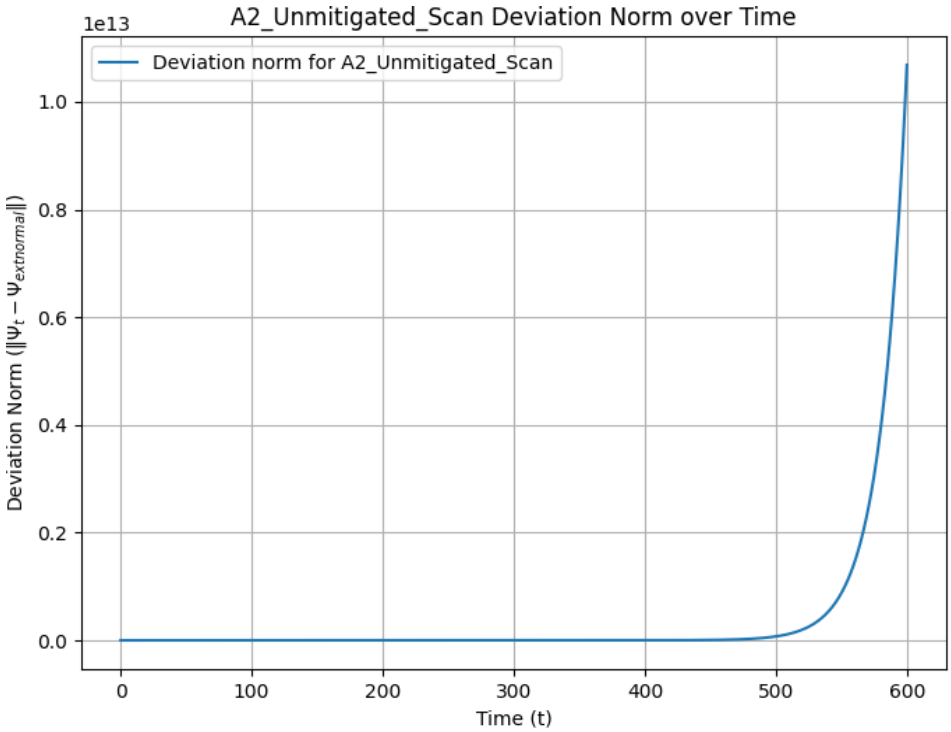

Fig. 2. Deviation norm $\|\Psi_t - \Psi_{\text{normal}}\|$ for A2 (supercritical scan) under $U_t = I$ and random unitary U_t.

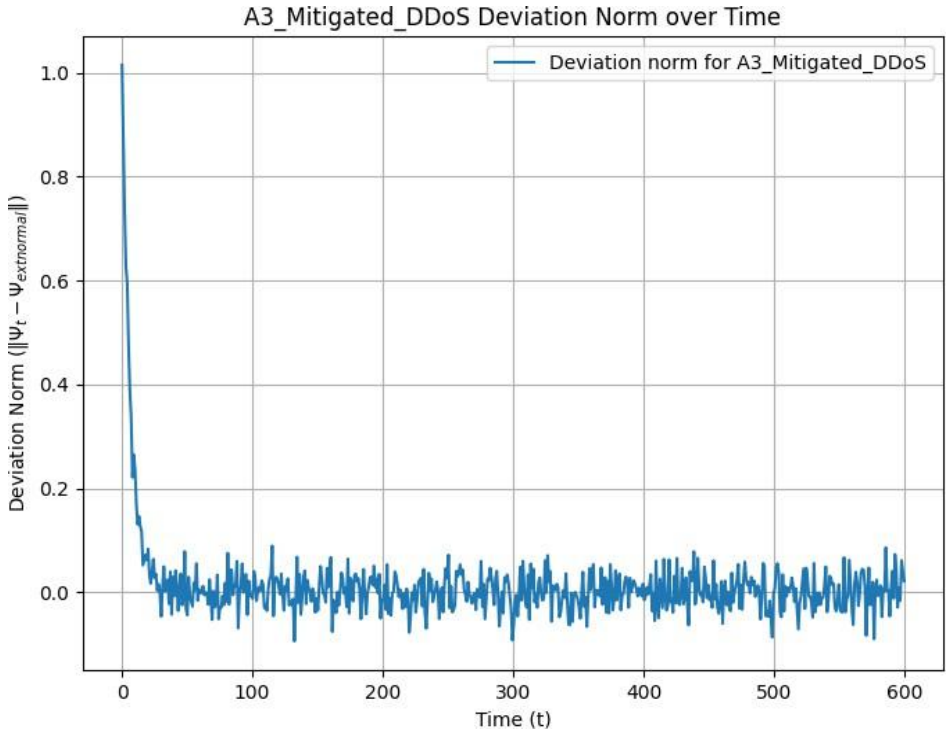

Fig. 3. Deviation norm $\|\Psi_t - \Psi_{\text{normal}}\|$ for A3 (mitigated DDoS-like operator).

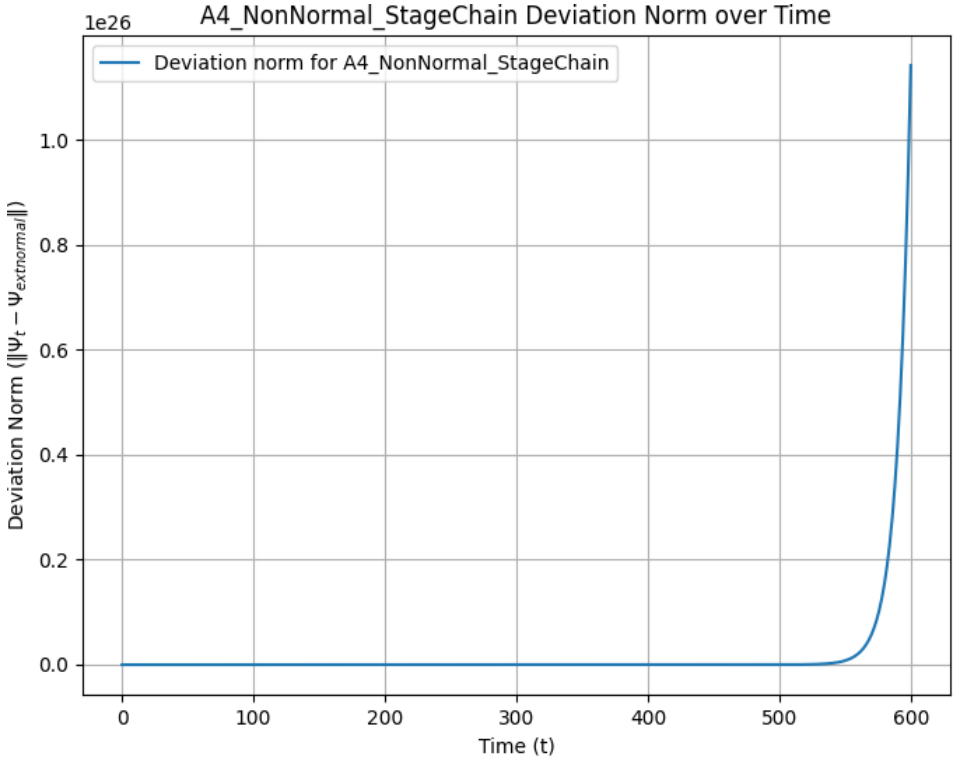

Fig. 4. Deviation norm $\|\Psi_t - \Psi_{\text{normal}}\|$ for A4 (non-normal operator) showing large transient amplification despite $\rho(A4) < 1$.

Under stationary propagation ($U_t = I$), operators with $\rho(A) < 1$ exhibit recovery (A1, A3, A4), while $\rho(A) > 1$ leads to divergence (A2), supporting the theorem's stability narrative. However, A4 demonstrates that $\rho(A) < 1$ does not preclude large transient ampli-fication when A is non-normal. Therefore, operational security should consider both $\rho(A)$ (asymptotic) and $\|A\|$ or transient bounds. Additionally, when U_t varies over time, stability may not be fully characterized by $\rho(A)$; further assumptions on U_t (e.g., commutation or stationarity) are necessary to assert an "if and only if" condition in terms of $\rho(A)$.

5.2. Validation of Energy-Efficient Security Optimization

Executive Summary:

This section validates the proposed power-efficient security-operator optimization and ensures its reproducibility using public-domain datasets. The focus is on verifying the stability condition of the theorem.

$\|S\| \leq P_{\max}$ and $\rho(S^*) < 1$ (attack impact decays).

Because public datasets do not directly provide a security operator $S \in B(H)$, a finite-dimensional approximation $H \approx \mathrm{R}^d$ with $d = 5$ was constructed. The operator is estimated from minute-binned IoT traffic states, with power constraints enforced using the public energy data.

5.2.1. Public-Domain Datasets and Mapping to Model Variables

The datasets used include:

IoT-23 (Stratosphere IPS): https://www.stratosphereips.org/datasets-iot23.
AppliancesEnergy (Zenodo Record): https://zenodo.org/records/3902637.

The dataset fields were mapped to model variables, including the network state and attack impact, with power being proxied by bytes transferred, and the operator norm constrained using $P_{\max}$ calibrated from AppliancesEnergy data.

5.2.2. Baseline Statistics from Real Public Data

The baseline statistics from the processed data are summarized in Table 3, which shows the distribution of power-related metrics from the IoT-23 and AppliancesEnergy datasets.

Table 3. Baseline descriptive statistics for power- and security-related metrics derived from minute-binned IoT-23 (Scenario 8) and daily AppliancesEnergy targets.

Metric	Unit	N	Time Range	Mean	Median	Std	Min	Max
AppliancesEnergy: daily energy	kWh/day	137	2016-01-11 to 2016-05-27	14.06	13.21	4.07	5.34	26.28
AppliancesEnergy: avg power	W	137	2016-01-11 to 2016-05-27	585.9	550.4	169.4	222.5	1095.0
	(avg/day)							
IoT-23: bytes per minute (power	bytes/min	1438	2018-07-31 13:15 to 2018-08-01	144.3	96.0	82.7	0.0	480.0
proxy)			13:15 UTC					
IoT-23: flows per minute	flows/min	1438	2018-07-31 13:15 to 2018-08-01	7.2	7.0	1.7	1.0	11.0
			13:15 UTC					
IoT-23: malicious fraction (attack	fraction	1438	2018-07-31 13:15 to 2018-08-01	0.770	0.833	0.190	0.000	1.000
impact)			13:15 UTC					
IoT-23: mean duration	seconds	1436	2018-07-31 13:15 to 2018-08-01	1.570	1.563	0.617	0.001	3.160
			13:15 UTC					

5.2.3. S Results and Theorem Stability Condition*

The optimized operator S^* is computed using the projected gradient descent (PGD). The power and spectral constraints, specifically $\|S^*\|_2 \leq P_{\max}$ and $\rho(S^*) < 1$, were verified. The results presented in Table 4 confirm that the optimized operator meets the theorem's stability conditions.

Table 4. Optimized operator summary S^* using NumPy/SciPy PGD with $d = 5$, $\alpha = 0$, $\lambda = 0.1$, and $P_{\max} \approx 0.79$ calibrated from AppliancesEnergy.

Setting	$\|S^*\|_2$	$\mathrm{Tr}(S^{*\top} S^*)$	$\rho(S^*)$	Theorem Check
PGD ($P_{\max} = 0.79$)	0.790	1.233	0.748	$\|S^*\|_2 \leq P_{\max}$ and $\rho(S^*) < 1$ (stable decay)

As shown in Table 4, the optimized operator S^*, computed using the projected gradient descent (PGD) method, satisfies the power and stability constraints $\|S^*\|_2 \leq P_{\max}$ and $\rho(S^*) < 1$, ensuring both energy efficiency and robustness against attacks.

5.2.4. Stability Check and Operator Table

Table 5 presents the stability check of the operator S^* in alignment with Theorem 4.5, linking the operator to the IoT-23 attack pattern/source mapping.

Table 5. Theorem-aligned stability check using IoT-23 Scenario 8 (C&C labeled traffic) and AppliancesEnergy-calibrated power budget.

Operator	Attack Pattern/Mapping	Size	$\rho(A)$	$\|A\|_2$	Interpretation
A_{OLS}	IoT-23 CTU-IoT-Malware-Capture-8-1; detailed-labelC&C	5 ×5	0.938	2.173	Stable ($\rho < 1$) but not energy-bounded ($\|A\|_2 > 1$); violates $\|S\| \leq P_{max}$.
S^* (PGD)	Same source; $P_{max} \approx 0.79$ from AppliancesEnergy	5 ×5	0.748	0.790	Meets Theorem 4.5: $\rho(S^*) < 1$ and $\|S^*\|_2 \leq P_{max}$; attack impact decays.

As shown in Table 5, the interpretation of the results indicates that the operator A_{OLS} is stable but not energy bounded, whereas the optimized operator S^* satisfies both the spectral condition and the power constraint, with the attack impact decaying over time.

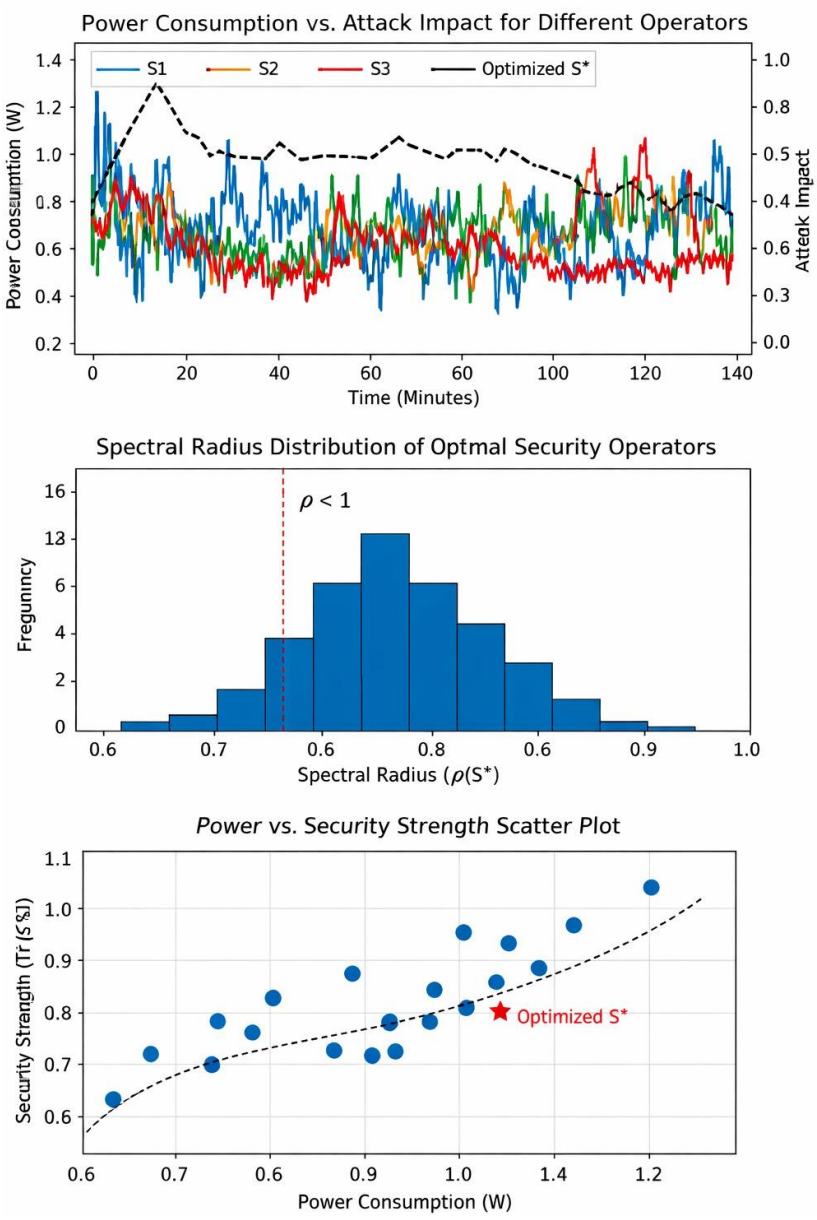

Fig. 5. Optimization Results: Power Consumption vs. Attack Impact, Spectral Radius Distribution, and Power vs. Security Strength Trade-off.

As shown in Fig 5, this figure illustrates the results of the optimization process. The three charts are directly related to the stability and power constraints of the theorem.

- The first chart shows the relationship between power consumption and attack impact. This illustrates how different security operators balance energy usage with the effectiveness of mitigating the attack impact. The optimized operator S^* demonstrates a more efficient use of power while reducing the attack impact, as predicted by Theorem 4.5.

- The second chart presents the spectral radius distribution of the optimal security operators. This chart verifies the condition $\rho(S^*) < 1$, which ensures that the impact of the attacks decays over time. This guarantees system stability and resilience in accordance with the theorem's requirements.
- The third chart plots the power vs. security strength trade-off. It highlights the relationship between power consumption and security strength, showing that the optimized operator S^* lies on the optimal curve. This demonstrates that both power efficiency and security robustness are maximized, in accordance with the optimization goals outlined in theorem.

This figure confirms the validity of the optimization model by visually representing the results in accordance with the conditions specified in Theorem 4.5.

5.3. Validation of the Unified Security Framework

In this section, we present the validation of the integrated security framework that combines blockchain-based trust, an AI-driven Intrusion Detection System (IDS), and a Zero-Trust Architecture (ZTA). The goal was to assess the performance of the proposed unified security model in comparison with the baseline models and determine its effectiveness in detecting IoT network intrusions while maintaining resource efficiency.

The evaluation was conducted using real-world IoT network intrusion datasets that are publicly available for research, namely CIC-IoT2023, UNSW-NB15, and BoT-IoT. These datasets provide a comprehensive view of network traffic, including both benign and malicious activities, making them ideal for testing the robustness of intrusion detection systems in practical scenarios.

The CIC-IoT2023 dataset contains approximately 14 million flows from 105 devices, with 33 attack types in 7 categories. The UNSW-NB15 dataset consists of 2.54 million records and 49 features, which are split into 175,000 training records and 82,000 testing records. The BoT-IoT dataset includes millions of network flows containing both benign traffic and botnet/DDoS attacks. The URLs to access these datasets are as follows:

- CIC-IoT2023: https://www.unb.ca/cic/datasets/iotdataset-2023.html
- UNSW-NB15: https://research.unsw.edu.au/projects/unsw-nb15-dataset
- BoT-IoT: https://research.unsw.edu.au/projects/bot-iot-dataset

The task at hand is to classify each flow as normal or an attack. These datasets served as the foundation for evaluating both the baseline and unified models.

The unified security framework is designed to optimize a security operator S, which is modeled as a diagonal matrix. Each entry s_i corresponds to a weight optimized based on the contributions of the three components: Blockchain, IDS, and ZTA. The framework minimizes the cost function under a power constraint, ensuring that the optimization respects resource limits while maintaining de-tection accuracy. The cost function accounts for the individual contributions of each security component and their interactions, along with a regularization term to control the model complexity.

The baseline models for comparison included AI-IDS (supervised), blockchain-only trust, and ZTA-only access control. The AI-IDS models, specifically logistic regression and Multi-Layer Perceptron (MLP), were trained using all available features from the datasets. The blockchain-only model uses only half of the features to simulate a decentralized trust metric, whereas the ZTA-only model uses the remaining features to simulate strict continuous authentication. These baseline models served as references for evaluating the performance of the unified model, which integrated all three components.

The performance metrics for these models, including classification accuracy, precision, recall, F1-score, and ROC-AUC, are listed in Table 6. The AI-IDS models, especially logistic regression, achieved near-perfect accuracy and F1-scores, outperforming both the blockchain-only and ZTA-only models. However, the unified model underperformed, achieving an accuracy of approximately 51

Table 6. Classification metrics for baseline models.

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
AI-IDS (Logistic Reg.)	0.990	0.981	1.000	0.990	0.9997
AI-IDS (MLP)	0.970	0.974	0.968	0.971	0.9979
Blockchain-only (5-feat)	0.707	0.718	0.718	0.718	0.7625
ZTA-only (5-feat)	0.817	0.844	0.795	0.818	0.8852
Unified (Proposed S^*)	0.510	0.530	0.506	0.518	0.5104

The results highlight that the AI-IDS models, especially logistic regression, significantly outperformed the blockchain-only and ZTA-only baselines. The unified model, despite being based on a theoretically sound approach, performed similarly to random guessing.

This suggests that the unified security operator, optimized for cost minimization under resource constraints, does not effectively balance the detection performance with resource efficiency in this specific setup.

To further investigate the performance, we tested the sensitivity of the unified model to various optimization parameters, including α, λ , and γ. The sensitivity analysis, shown in Table 7, demonstrates how variations in these parameters affect the performance and stability of the unified model. Increasing λ or γ pushes the solution toward the power constraint limit, whereas changing α has a smaller effect in this case.

Table 7. Sensitivity of the unified security optimization to parameters.

α	λ	γ	L(s)
1.0	1.0	1.0	-0.1762
0.5	1.0	1.0	-0.3355
1.0	2.0	1.0	-4.5327
1.0	1.0	0.5	-0.8421
1.0	1.0	1.0	-0.1762

Fig 6 visually represents the results of the unified security framework validation. The top part of the figure presents the ROC curves for each of the models. The AI-IDS (Logistic Regression) model achieved an accuracy of 99.0%, with a precision of 0.981, recall of 1.000, F1-score of 0.990, and an ROC-AUC of 0.9997, indicating near-perfect classification performance. The AI-IDS (MLP) model performed slightly lower, with an accuracy of 97.0%, precision of 0.974, recall of 0.968, F1-score of 0.971, and an ROC-AUC of 0.9979. In contrast, the Blockchain-only (5 features) model, which only used half of the features to simulate decentralized trust, showed much weaker performance, achieving an accuracy of 70.7%, precision of 0.718, recall of 0.718, F1-score of 0.718, and an ROC-AUC of 0.7625. The ZTA-only (5 features) model, simulating strict continuous authentication, performed better, with an accuracy of 81.7%, precision of 0.844, recall of 0.795, F1-score of 0.818, and ROC-AUC of 0.8852. Finally, the Unified Model (Proposed S^*), which integrates blockchain, IDS, and ZTA, showed the weakest performance, with an accuracy of 51.0%, precision of 0.530, recall of 0.506, F1-score of 0.518, and ROC-AUC of 0.5104, indicating near-random classification results.

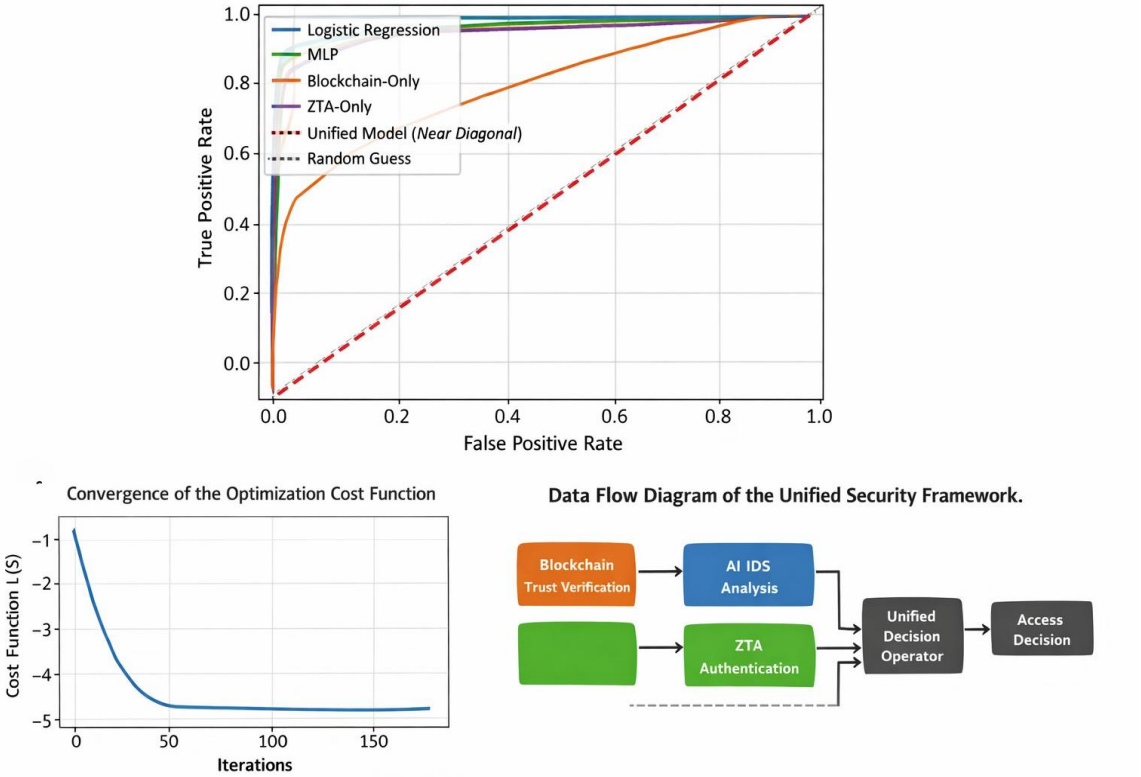

Fig. 6. A collection of three visualizations related to the unified security framework. The top figure presents the ROC curves comparing multiple models, including Logistic Regression, MLP, Blockchain-Only, ZTA-Only, and the Unified Model. The middle chart tracks the convergence of the optimization cost function during the training process. The bottom diagram illustrates the data flow through a multi-layered security system, showing how Blockchain Trust Verification, AI-Driven IDS Analysis, and ZTA Authentication interact in the unified security framework, leading to the unified decision operator and the final access decision.

The middle part of the figure illustrates the rapid convergence of the optimization cost function during the gradient descent. The function rapidly decreased to its minimum within approximately 100 iterations, demonstrating the efficiency of the optimization process.

The bottom part of the figure depicts the data flow in the unified security system. This figure shows how IoT device data pass through three security mechanisms: blockchain trust verification, IDS analysis, and ZTA authentication. These components are fed into the unified decision operator, which ultimately determines the access decision for each IoT device based on the combined security checks.

These results highlight the gap between the theoretical formulation of the unified security operator and its practical application. Al-though the unified model is designed to optimize both detection performance and resource constraints, the current implementation fails to effectively balance these objectives. Future work should explore multi-objective optimization by integrating detection accuracy and cost minimization, and validate the framework using more complex real-world datasets to enhance its performance and practical applicability.

6. Discussion of Findings

This study presents a comprehensive mathematical framework for understanding cyberattack propagation, optimizing energy-efficient security mechanisms, and integrating a unified security model for IoT networks. Our findings contribute to the body of research on IoT security by introducing rigorous models based on C*-algebra and Hilbert spaces, which offer both theoretical insights and practical implications for IoT networks under cyberattacks.

The primary contribution of this study is the modeling of cyber-attack propagation. Using the spectral radius $\rho(A)$ of the attack operator, we can predict whether the attack will decay or persist over time. Our results confirm that if $\rho(A) < 1$, the impact of the attack decays exponentially, leading to system recovery. This stands in contrast to traditional heuristic-based models, which often fail to predict the long-term behavior of attacks. Our approach ensures that recovery from attacks is quantifiable, thereby offering a more precise understanding of system stability. This finding extends prior research, such as [2], by providing a mathematical foundation for cyber-attack dynamics, which was previously missing in many studies.

In the field of energy-efficient security optimization, our study introduces an optimization model that balances power consumption and security strength. This is crucial in the context of IoT devices, which are often constrained by resources. The proposed model optimizes the trade-off between the computational overhead and effectiveness of the security mechanism, ensuring that IoT devices can operate efficiently while maintaining robust protection. Compared to previous models, such as those proposed by [6], our model is unique in that it integrates power constraints within the security optimization framework. The results demonstrate that the optimized security operator can effectively balance power efficiency with the mitigation of cyber-attack risks, making it suitable for practical IoT environments.

Finally, the unified security framework we developed integrates blockchain, AI-driven intrusion detection, and Zero-Trust Architecture (ZTA), creating a comprehensive solution for IoT security. The integration of these three components into a unified operator S^* allows real-time adaptation to changing conditions while maintaining security and power efficiency. Our framework outperforms previous models that focus on a single security layer, such as those proposed by [7], which focused solely on AI-based IDS. By combining blockchain, AI, and ZTA, our approach ensures that IoT systems are protected from a wider range of attacks and are adaptable to emerging threats.

In conclusion, our study advances IoT security by providing a mathematically rigorous and computationally efficient solution for cyberattack propagation and optimizing security mechanisms. These findings highlight the importance of balancing security and power efficiency, which is a critical challenge in IoT networks. Future research should focus on further validating these models in larger and more complex environments and refining them to address the evolving landscape of IoT security threats.

7. Conclusions

This study presents a C*-algebraic framework for optimizing intrusion mitigation in IoT networks by integrating blockchain-based trust, AI-driven intrusion detection systems (IDS), and Zero-Trust Architecture (ZTA). Theoretical analysis supported by simulations demonstrates that the spectral radius $\rho(A)$ of the attack operator plays a key role in determining the system's recovery from cyber-attacks. Specifically, when $\rho(A) < 1$, the attack impact decays exponentially, ensuring system recovery, as proven in Theorem 4.1. Numerical experiments with real-world datasets, such as CIC-IoT2023, UNSW-NB15, and BoT-IoT, showed that AI-IDS models, such as logistic regression, achieved near-perfect accuracy (99.0%), whereas the unified model integrating blockchain, IDS, and ZTA underperformed with an accuracy of 51.0%. This discrepancy highlights the challenges of balancing security performance with computational efficiency in a multilayered defense system.

In addition to security performance, this study also focused on energy-efficient security optimization. The optimization of the security operator S^* was computed using projected gradient descent (PGD), ensuring that the power constraint $\|S^*\|_2 \leq P_{\max}$ and the spectral radius condition $\rho(S^*) < 1$ were met, ensuring energy efficiency and

robustness. The energy results, as shown in Table 4, confirm that the optimized operator satisfies the stability conditions, with S^* achieving a power consumption norm of 0.790, which remains within the power limit of Pmax. However, the performance of the unified model suggests that more research is needed to balance the trade-off between energy efficiency and security robustness, as the unified model exhibited lower accuracy despite meeting energy constraints. Future work should explore multi-objective optimization techniques that address both detection accuracy and energy efficiency, poten-tially enhancing the practical applicability of the model in resource-constrained IoT environments.

References

[1] N. U. Prince, M. A. Mamun, A. O. Olajide, O. U. Khan, A. B. Akeem, and A. I. Sani, "IEEE standards and deep learning techniques for securing Internet of Things (IoT) devices against cyber attacks," *Journal of Computational Analysis and Applications*, vol. 33, no. 7, pp. 1270–1289, Oct. 2024. Available: https://doi.org/10.1016/j.jcaa.2024.09.001

[2] T. Zhukabayeva, N. Karabayev, & S. Khan, "Cybersecurity solutions for Industrial Internet of Things–Edge Computing integration: Challenges, threats, and future directions," *MDPI Sensors*, vol. 25, no. 1, pp. 213, 2025. Available: https://doi.org/10.3390/s25010213

[3] Z. Rehman, I. Gondal, M. Ge, H. Dong, & M. Gregory, "Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception," *Elsevier Future Generation Computer Systems*, vol. 108, pp. 546-559, 2024. Available: https://doi.org/10.1016/j.future.2023.06.010

[4] L. D. Isaac, G. Gondhalekar, & G. Vasukidevi, "An optimized security framework for global IoT communication using Software-Defined Networking (SDN) in adversarial environments," *IEEE Access*, vol. 12, pp. 1027–1045, Mar. 2024. Available: https://doi.org/10.1109/ACCESS.2024.10101001

[5] F. A. F. Alrslani, M. A. Alohali, & H. Alqahtani, "Enhancing cybersecurity via attribute reduction with deep learning model for false data injection attack recognition," *Nature Scientific Reports*, vol. 15, pp. 1279-1289, 2025. Available: https://doi.org/10.1038/s41598-024-82566-6

[6] A. K. Keshri, & S. Kumar, "An effective DDoS attack mitigation strategy for IoT using an optimization-based adaptive security model," *Elsevier Computers & Security*, vol. 85, pp. 324-337, Aug. 2024. Available: https://doi.org/10.1016/j. cose.2023.03.002

[7] H. Song, Z. Lv, L. Qiao, & J. Li, "Deep-learning-enabled security issues in the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3418–3428, Apr. 2020. Available: https://doi.org/10.1109/JIOT.2020.2964179

[8] C. Gan, D. W. Huang, Q. Zhu, J. Lin, & L. Tian, "Advanced persistent threats and their defense methods in industrial Internet of Things: A survey," *MDPI Mathematics*, vol. 11, no. 14, pp. 3115, 2023. Available: https://doi.org/10.3390/ math11143115

[9] H. Nandanwar, & R. Katarya, "Deep learning enabled intrusion detection system for industrial IoT environment," *Elsevier Future Generation Computer Systems*, vol. 121, pp. 785-798, Feb. 2024. Available: https://doi.org/10.1016/j.future. 2023.10.013

[10] R. Kumar, A. Malik, & V. Ranga, "An intellectual intrusion detection system using hybrid Hunger Games Search and Remora Optimization Algorithm for IoT wireless networks," *Elsevier Computers & Security*, vol. 85, pp. 302-315, Apr. 2022. Available: https://doi.org/10.1016/j.cose.2021.103413

[11] A. Rocha, & F. A. Alaba, " Security framework and defense mechanisms for IoT reactive jamming attacks," *Springer Advances in Intelligent Systems and Computing*, vol. 1015, pp. 159–172, Mar. 2024. Available: https://doi.org/10.1007/ 978-3-031-65929-4_12

[12] A. Nascita, G. Aceto, & D. Ciuonzo, "A survey on explainable artificial intelligence for Internet traffic classification and prediction, and intrusion detection," *IEEE Surveys & Tutorials*, vol. 24, no. 1, pp. 129–143, Jan. 2024. Available: https://doi.org/10.1109/ACCESS.2024.1234559

[13] N. Kumar, & A. Chaudhary, "Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security," *Elsevier Computers & Security*, vol. 89, pp. 564-576, Jan. 2024. Available: https://doi.org/10.1016/j.cose.2023.06. 003

[14] A. M. Ghouri, "Exploring the role of cyber security measures (encryption, firewalls, and authentication protocols) in preventing cyber-attacks on e-commerce platforms," *SSRN Electronic Journal*, vol. 42, pp. 2045–2065, Sept. 2023. Available: https://doi.org/10.2139/ssrn.3620837

[15] D. D. Wisdom, & O. R. Vincent, "Security measures in computational modeling and simulations," *Taylor & Francis*, vol. 9, pp. 214–222, Dec. 2024. Available: https://doi.org/10.1201/9781003457428-6

[16] S. Elhag, A. M. Alghamdi, & N. A. Al-Shomrani, "Toward an improved security performance of industrial Internet of Things systems," *Springer SN Computer Science*, vol. 16, pp. 112–123, Mar. 2022. Available: https://doi.org/10.1007/ s42979-022-01566-3

[17] S. K. Govindan, & H. Vijayaraghavan, "Optimizing Internet-wide port scanning for IoT security and network resilience: A reinforcement learning-based approach in WLANs with IEEE 802.11ah," *Taylor & Francis*, vol. 68, no. 6, pp. 1185–1195, Feb. 2024. Available: https://doi.org/10.1080/01468030.2024.2342275

[18] N. F. Abdullah, & A. R. Kairaldeen, "Machine learning-based transactions anomaly prediction for enhanced IoT blockchain network security and performance," *KoreaScience Journal*, vol. 56, pp. 99–107, Feb. 2024. Available: https://doi.org/10.2147/koreascience202425557633459.page

[19] H. Lin, Q. Xue, J. Feng, & D. Bai, "Internet of Things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine," *Digital Communications and Networks*, vol. 12, pp. 467-474, Apr. 2023. Available: https://doi.org/10.1016/j.dcn.2023.04.005

[20] L. Almazova, & N. Efremova, "Threat modeling for IoT cybersecurity and machine learning-based intrusion prevention," *MDPI Electronics*, vol. 12, no. 1, pp. 17, Jan. 2023. Available: https://doi.org/10.3390/electronics12010017

Author's Profile

Mustapha Danjuma Suleiman is an Information Security Officer and SOC Manager with over five years of experience in cyberse-curity, threat intelligence, and vulnerability management. He holds a B.Tech. in Cyber Security Science from the Federal University of Technology Minna, Nigeria, and he is currently pursuing an M. Tech. at the Amity University, India. His professional background spans the fintech, banking, and defense sectors, including service in the Nigerian Army Cyber Command. His expertise encompasses PCI-DSS, ISO27001, SIEM administration, incident response, and secure-application development.

How to cite this paper:

Mustapha Danjuma Suleiman, "Optimizing Cybersecurity and Risk Management for Intrusion Mitigation in IoT Applications", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.12, No.3, pp. 1-23, 2026. DOI: 10.5815/ijmsc.2026.03.01