**Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Step-by-Step Approach with Zero-Day Detection and Adversarial Robustness Benchmarks**

Medard Anjei Nyemb  
*College of Computing.  
Illinois Institute of Technology  
Chicago, llinois*  
manjeinyemb@hawk.illinoistech.edu

Michael Owusu Jackson  
*College of Computing.*  
Illinois Institute of TechnologyChicago, llinois   
mowusujackson@hawk.illinoistech.edu

3rd Puya Pakshad  
*College of Computing.*  
Illinois Institute of TechnologyChicago, llinois  
ppakshad@hawk.illinoistech.edu

***Abstract*—** **In addition to changing many facets of contemporary life and industry, the quick expansion of IoT devices has increased intricate security flaws. Even though previous hybrid frameworks and other security solutions have proven effective against well-known dangers including spoofing, illegal access, and Denial-of-Service (DoS) assaults. Frequently, they are not strong enough to fend off adversarial and zero-day attacks. The growing complexity and volume of IoT devices are proving too much for traditional, centralized security systems to handle, which leads to poor intrusion detection, high latencies, and increased energy usage. We suggested a hybrid security framework that uses a step-by-step approach with adversarial robustness benchmarks and zero-day detection to overcome these issues. The method combines blockchain technology with artificial intelligence (AI) in IoT networks.**

**By leveraging a lightweight consensus protocol for device authentication and data integrity and deep learning models for realtime intrusion detection, our approach achieves a detection precision of 95.2% for phishing attacks. Additionally, our solution reduces authentication latency by 66.6% to 15 ms in largescale networks with 1000 devices and decreases energy consumption by 31.8% compared to traditional approaches. This hybrid framework provides a scalable and efficient security solution for IoT networks, enhancing both security and operational efficiency.**

**We first verify the model's performance on established parameters, such as low energy consumption, low latency, and high detection accuracy, using the UNSW-NB15 dataset. Next, we present our new benchmarks: an Adversarial Robustness Benchmark to evaluate the framework's resilience to deliberately altered, evasive samples, and a ZeroDay Detection Benchmark to gauge its capacity to detect hitherto undiscovered attack types.The outcomes show that in addition to performing well on standard criteria, our approach is more resilient and robust against complex and unforeseen threats.This study creates a new, more rigorous benchmark for assessing security solutions in extensive IoT networks.**

**In this paper, we focus on reviewing and comparing recent studies that have been proposed for “Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection.” This paper addresses three research questions and highlights the research gaps and future directions. This paper aims to increase the knowledge base for enhancing IoT security, recommend future research, and suggest directions for future research.**

Keywords—Blockchain, Artificial Intelligence (AI), Internet of Things (IoT), Zero-Day Detection, Adversarial Robustness, Network Security, Data Integrity, Deep Learning Model, Intrusion Detection Systems, Deep Learning Models

# Introduction

The Internet of Things (IoT) has significantly changed how many consumers, commercial services, applications, and industries run their businesses or work flows. IoT has been used in a variety of industrial systems, such as healthcare, agriculture, and smart industries of aggregated networks to achieve goals of intelligent recognition, positioning, tracing, and management for effectiveness and efficiency of resources. However, IOT systems have also been exposed to various forms of cyberthreats and data breaches, such as denial of service (DoS), unauthorized access, etc., compromising C.I.A. (confidentiality, integrity, and availability). Security models Traditionally use, fails to meet the evolving threat landscape due to the centralised architecture employed, the increased data volume generated by current IoT networks, higher energy consumption, high latencies, restricted scalability, and insufficient threat detection. Advanced Intrusion Detection Systems (IDS) rely on static signature-based approaches, which makes them in effective against adversarial attacks (maliciously manipulated data intended to evade detection) and zero-day attacks (unseen exploits).

As a result, communication security offered by cryptographic protocols essentially fail to defend against sophisticated internal threats or anomalous behaviour from compromised devices. Recent research highlights the potential of blockchain and Artificial Intelligence (AI) as key enablers of next-generation IoT security and explores them in isolation. To resolve these challenges, this article proposes a hybrid resilient security framework designed to reinforce IoT ecosystems through a step-by step approach that integrates adversarial robustness benchmarks and zero-day threat detection, with the integration of blockchain and Artificial Intelligence (AI). machine learning models and capsule network to zero-day threat and adversarial intrusion in real time. This design comprehensively, facilitates a distributed approach where processing is efficiently handled at edge nodes, minimizing latency and optimizing resource usage, with diverse communication protocols (5G, LoRa, Zigbee, etc.) also ensuring high energy efficiency and robust protection across heterogeneous networks of a lightweight system of AI model.

This study's step-by-step evaluation methodology involves three steps: normal split, zero-day split, and adversarial testing. Normal split involves training and testing the model on all known attack classes to establish baseline performance. Zero-day split excludes one or more attack classes during training and testing, allowing the model to detect unseen threats during testing. The trained model is assessed along three essential dimensions:

**-**Normal Accuracy and F1 Score: Assesses baseline categorization ability for recognized threats.

- Zero-Day Detection Rate: evaluates the model's capacity to identify new attack types.

- Adversarial Robustness: Score measures the model's resilience to manipulated or noisy inputs.

These experimental findings show how the hybrid resilient security architecture delivers high accuracy, robust performance under adversarial settings, and strong zero-day detection capabilities. These findings demonstrate the potential for merging AI and blockchain to provide robust, scalable, and intelligent security solutions for next-generation IoT ecosystems.

## The Problem STatment

Internet of Things (IoT) devices have spread so rapidly that they have created vast, linked ecosystems that are critical to modern infrastructure. However, this increase has also resulted in severe security weaknesses. Today's centralized security solutions are inadequately scalable and effective in defending these dispersed and dynamic environments against a continuously changing variety of cyber threats, such as sophisticated zero-day attacks and data poisoning.

Even while new technologies like blockchain and artificial intelligence (AI) have a lot of potential, there are many limitations to how they may be utilized alone. Despite their efficiency in danger detection, AI models are susceptible to data poisoning if the input data is not secure. Traditional blockchain technology, on the other hand, is useless for real-time threat detection in a large-volume IoT setting because to high latency and limited throughput, despite the fact that it ensures data integrity and decentralization. This issue is particularly acute when guarding against novel attacks that need a high level of adversarial robustness.

The lack of a comprehensive, hybrid security framework capable of successfully combining the  complementary strengths of blockchain and artificial intelligence to produce a solution that is not only dependable but also scalable and effective enough to meet the demands of modern IoT ecosystems creates a significant research gap. This study was motivated by our previous work titled "Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection."

## Research Motivation

Numerous sectors have undergone fundamental transformations as a result of the phenomenal expansion of the Internet of Things (IoT), resulting in sophisticated ecosystems that are critical to modern living. However, this expansion has revealed major security weaknesses, making IoT networks vulnerable to a range of cyber assaults. Because these environments are distributed, complex, and big, traditional, centralized security solutions are unsuitable for managing them and frequently serve as a single point of failure.

The explosive growth of the Internet of Things (IoT) has caused numerous industries to undergo fundamental transformations, resulting in intricate ecosystems that are essential to contemporary life. However, this growth has also revealed serious security flaws, making IoT networks easy targets for a variety of online attacks. Because these environments are distributed, complicated, and large, traditional, centralized security solutions are ill-suited to manage them.

As a result, our study is driven by the urgent need to develop a more complex and dependable solution, which is based on the core concepts of a hybrid AI and blockchain security architecture. Our primary objective is to go beyond a broad framework and provide a comprehensive, rigorous approach that is comparable to industry standards. By focusing on a model adjusted for adversarial robustness and zero-day detection, we want to provide a scalable and successful strategy to defending IoT ecosystems. This study is a vital extension of prior research, providing a practical and persuasive approach for addressing the industry's most pressing security challenges.

## Research Contribution

This study proposes and evaluates a novel hybrid security architecture, which makes numerous significant contributions to the field of IoT security. Our research, which builds on a basic understanding of hybrid AI-blockchain models, addresses specific, essential security concerns.

The key contributions are as follows:

* An Effective Hybrid Framework That Is Scalable:

We describe a unique, end-to-end solution that smoothly integrates blockchain technology for unchanging data integrity with artificial intelligence (AI) for intelligent threat detection. Our architecture is specifically built to overcome the scalability and efficiency limitations of traditional blockchain systems, making it suitable for high-volume, real-time IoT scenarios, as opposed to previous solutions that address these issues independently.

* Illustration of Synergistic Benefits:

We provide a detailed description of how merging blockchain technology and artificial intelligence produces a system that is more dependable than either alone. To prevent data poisoning, the blockchain's tamper-proof ledger provides a secure and reliable dataset for AI model training and validation. By intelligently regulating data and network traffic, AI enhances blockchain operations by reducing latency and improving throughput.

* Our model proactively detects various online

threats, including advanced adversarial and zero-day attacks, leading to a more resilient and predictive defense system compared to traditional reactive security measures.

* Practical and Optimized Approach:

We present a structured, step-by-step methodology for implementing the proposed framework, which is measured in terms of accuracy, scalability, and efficiency through a performance evaluation, a clear architectural design, and a comprehensive operational flow. Researchers and industry professionals looking to implement next-generation IoT security solutions may find this guide useful.

## Research Question

Our key research goal is how to optimize a hybrid AI-blockchain model for detecting unknown or controlled cyber risks in IoT networks beyond the trained dataset.

Supporting research questions:

* Framework Design: How can a step-by-step hybrid architecture be developed to synergistically integrate blockchain's d The Blockchain Security Ledger component decentralized integrity with AI's predictive capacity to safeguard IoT data?
* Performance and Scalability: How does this hybrid paradigm affect IoT ecosystem performance in terms of latency, throughput, and energy consumption when compared to traditional and independent security solutions?
* Threat Detection Efficacy: To what extent can the suggested model detect zero-day attacks (i.e., threats not included in the training data) and withstand adversarial attacks (where an attacker attempts to fool the AI) in real time?
* Practical Benchmarking: What critical performance metrics are required to objectively assess the model's efficacy and verify its superiority over existing methods?