"Sustainable Green AI–Driven Cybersecurity Framework for Smart Cities: Energy-Efficient Edge-Based Intrusion Detection"

Miss. Rutuja Deepak Mokashi
School of Information Technology, Indira University, Pune

Mrs. Amruta Sakhare
School of Information Technology, Indira University, Pune

Mr. Shubham Bende
School of Information Technology, Indira University, Pune

DOI: 10.29322/IJSRP.16.02.2026.p17023
https://dx.doi.org/10.29322/IJSRP.16.02.2026.p17023

Paper Received Date: 10th January 2026
Paper Acceptance Date: 8th February 2026
Paper Publication Date: 12th February 2026

Abstract

Smart cities run on digital networks think IoT devices, edge computing, and cloud tech. But as everything gets more connected, the risk of cyberattacks just keeps climbing. Traditional AI cybersecurity tools do a decent job spotting threats, but they're power-hungry and need a lot of processing muscle. Not exactly ideal if you're trying to keep things green and ready to grow. So, here's what we're doing: rolling out a Green AI cybersecurity system. It mixes energy-saving deep learning with edge-based intrusion detection. We use things like pruning and lightweight models to cut down on energy use and computing power. Even with all these savings, the system still catches threats really well and it actually makes everything easier to scale, sturdier, and more sustainable. When we put it to the test, the results spoke for themselves. Energy use dropped a lot, but the system kept catching threats almost as well as before. Bottom line: this approach gives smart cities the strong, eco-friendly cyber defense they need to keep running smoothly.

Index Terms - Cybersecurity, Energy-Aware AI, Green AI, Intrusion Detection, Smart City Security

I. Introduction

Smart cities lean heavily on digital tech these days stuff like IoT, AI, edge computing, cloud systems, smart grids, and intelligent transportation. Put all that together, and you get cities that can track things in real time, automate routines, and run much more smoothly across areas like healthcare, energy, transit, and public safety. But the more connected everything gets, the bigger the target. Cyber threats keep growing malware, DDoS attacks, ransomware, data breaches, you name it. AI and machine learning are turning into the main tools for spotting and handling these complex threats. Still, most traditional AI-driven cybersecurity relies on deep learning models that chew up a lot of energy and computing power. That's a real problem when you need solutions that can scale up and still be sustainable for smart cities. That's where Green AI comes in. It's designed to cut down energy use and lower the carbon footprint of AI without sacrificing performance. In this paper, we introduce a Green AI-powered cybersecurity framework for smart cities. It uses energy-efficient deep learning models, edge-based intrusion detection, and smart model optimization. The goal? High detection accuracy, less energy waste.

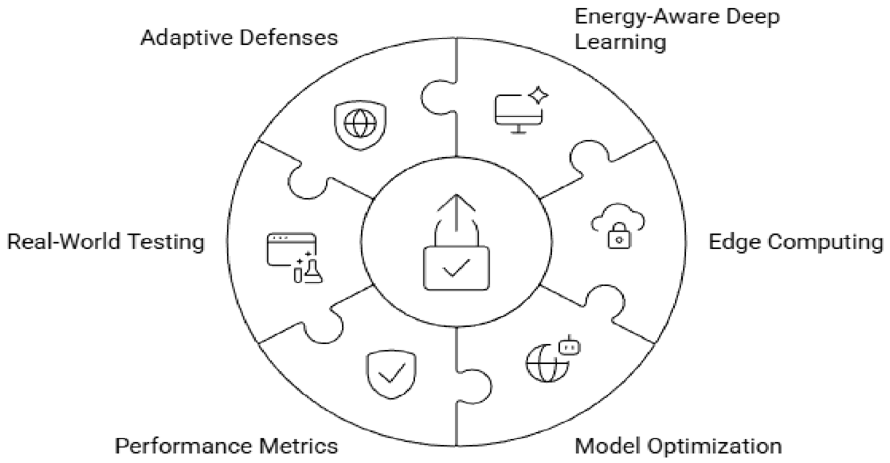

Fig. Green AI Cybersecurity Framework

II. Research Objective

- Design a Green AI-powered cybersecurity framework that keeps smart city infrastructure both secure and sustainable. The idea is to bring together energy-aware deep learning and edge computing, so everything runs smoothly without wasting power.
- Develop deep learning models that spot intrusions while using less energy and computing power. These models should stay sharp on detection no sacrificing accuracy just to save a few watts.
- Set up intrusion detection at the edge to cut down on delays, lower bandwidth use, and take the pressure off central servers. Smart cities move fast, and their security needs to keep up.
- Try out model optimization methods like pruning and lightweight architectures. The goal is to make AI-based security systems more sustainable and easier to scale.
- Look closely at how security performance stacks up against energy savings. In other words, find the right balance between keeping systems safe and keeping them efficient.
- Test the framework using real metrics things like detection accuracy, false positives, energy use, and computing demands.
- Finally, boost the system's ability to handle new and evolving cyber threats. Build adaptive, scalable AI defenses that smart cities can rely on for the long haul.

III. Methodology

- The research selects the combination of datasets carefully to elucidate diversified cases of cybersecurity.
- To detect network, level intrusions, the study uses the CICIDS2017 dataset which is a rich source of attack patterns and very suitable for testing traditional network security mechanisms. In addition, the study leverages IoT, oriented smart city traffic datasets to reflect device, level attacks and thus, address the growing challenge of securing urban interconnected systems.
- The model architecture incorporates traditional as well as energy, efficient methods. Classical networks including CNNs, LSTMs, and Autoencoders serve as a baseline for the performance benchmarking, whereas Green AI models, e.g., pruned CNNs, quantized LSTMs, and knowledge, distilled networks, are deployed to save the computation and energy consumptions with only marginally sacrificed detection accuracy.
- In order to save energy the following actions are taken: primacy is given to edge, based inference so that the reliance on the cloud is reduced; the model is changed dynamically according to even momentary variations in the workload; and, federated learning is conducted on a regular basis so that the model updating is both privacy, preserving and resource, efficient.
- Initiation to dual, metric used to measure different aspect of performance, the security metrics (accuracy, precision, recall, F1, score, and detection latency) were first combined with sustainability metrics, such as energy consumption (Joules), CPU/GPU utilization, carbon footprint, model size, and inference time, to yield comprehensive performance result both in terms of threat detection and operational efficiency.

IV. Problem Identification and Research Motivation

Deep learning models keep smart cities secure, but they eat up a lot of energy. That's a real problem, especially when you think about how many devices, sensors, cameras, and more rely on limited power and processing at the edge. Most of these devices just can't handle heavy-duty AI, especially in real time. Right now, there's no single framework that tackles everything at once: energy use, detection accuracy, efficiency, and resilience. Researchers usually pick one, either they chase better security or they try to build lightweight AI. Hardly anyone brings energy efficiency and strong protection together under one roof. This article changes that. It introduces a Green AI approach that cuts down on energy drain without sacrificing detection power. It's a step toward smarter, greener, and safer cities.

Proposed Green AI Enabled Cybersecurity Framework

The Green AI, enabled cybersecurity framework put forward aims to deliver energy, efficient, scalable, and intelligent threat detection in smart city environments. The architecture combines edge intelligence, energy, aware deep learning, and optimization techniques to keep computational and energy overhead extremely low while attaining high detection accuracy. Four connected layers, as shown below, make up the framework.

1. Smart City Device & Edge Layer

This layer consists of IoT devices, sensors, smart meters, surveillance systems, and edge nodes that constantly produce diverse data streams. Since these devices are limited in terms of computational capacity and energy, only very preliminary data processing and the extraction of features are done on the edge locally. To allow for early threat detection, reduce the transmission of raw data, and lower network congestion, lightweight intrusion detection mechanisms are deployed.

2. Edge Intelligence & AI Security Layer

The Edge Intelligence layer incorporates energy, aware deep learningbased intrusion detection systems (IDS) that help analyze network traffic and device behavior in real, time. Lightweight models such as pruned Convolutional Neural Networks (CNNs) and quantized Long Short, Term Memory (LSTM) networks are utilized, thus giving them the ability to spot anomalies and cyber, attacks efficiently. By executing intrusion detection at the local level, this layer guarantees low latency, rapid reaction times, and enhanced scalability, which are essential features of smart city infrastructures.

3. Green AI optimization layer

This layer aims at minimizing the computational complexity and energy usage of AI models while maintaining high detection accuracy. It introduces advanced optimization methods like model pruning, quantization, parameter sharing, knowledge distillation, and dynamic model selection. These techniques can drastically decrease model size, cost of inference, and power consumption and thus can support ongoing monitoring and eco, friendly cybersecurity operations even in less powerful environments.

4. Cloud Intelligence & Threat Response Layer

The Cloud Intelligence layer handles model training intervals, whole world threat analytics, and response system coordination. Federated learning is a method whereby the models get updated through collaboration while the amount of data transferred is kept minimal and user privacy is maintained. Threats that have been detected receive risk, based priority scores, thus, automated mitigation strategies as well as timely response actions can be facilitated. Then the updated lightweight models are sent back to edge devices in a secure manner to keep up with the adaptive and latest protection.

V. Identify, Research And Collect Idea

The notion behind this research arose as a natural extension of two hot, topic trends in smart cities: IoT and edge computing getting more embraced, and the rising demand for sustainable, energy, efficient AI. A smart city relies on an extensive network of devices such as sensors, cameras, smart meters, and autonomous vehicles, which all contribute to the generation of huge amounts of data that inevitably need to be processed in real time. While traditional AI, driven cybersecurity solutions have been proved to be very efficient in threat detection, they also require great computing power and a lot of energy, which is why they can hardly be used on energy, constrained edge devices.

The investigation also took into account an idea known as Green AI, which advocates for energy, saving, lower carbon footprint, and sustainability in AI model creation. The researchers made a review of recent studies on intrusion detection systems (IDS), deep learning for cybersecurity, edge computing, and energy, efficient AI. It immediately became evident that there is hardly any comprehensive framework that would incorporate detection performance, energy efficiency, and scalability simultaneously. In fact, most of the existing solutions either try to accomplish high, accuracy IDS practically ignoring energy consumption or come up with a lightweight model that, thus, undermines security.

Out of this deliberation, the essential concept was crystallized: to design a Green AIpowered cybersecurity framework for smart cities that can take advantage of energy, aware deep learning, edge, based intrusion detection, and model optimization (pruning, quantization, and knowledge distillation) to deliver secure, scalable, and sustainable protection.

VI. Write down Your Studies and Findings

- Dataset Analysis: The study that is discussed here chose CICIDS2017 for the network, level attack setting and IoT smart city traffic datasets for device, level attacks. CICIDS2017 includes various types of attacks, such as DDoS, Brute Force, and Web attacks, thus it is a good fit for benchmarking conventional IDS.

- Meanwhile, IoT, specific datasets mainly deal with the device, level attacks, thus they are a great reflection of real, life situations in smart cities. By combining these two, the framework can be exposed to a wide range of threats at both the network and device levels.
- Model Development: Classic deep learning architectures (CNNs, LSTMs, Autoencoders) were used as baseline models to give an initial performance level of detection that can be obtained by standard methods. Green AI variants such as pruned CNNs, quantized LSTMs, and knowledge, distilled networks, were tested for their effectiveness in reducing energy combustion and computational overhead, while still delivering comparable accuracy.
- Energy Optimization Strategies: The focus was on performing inference at the edge to be less dependent on the cloud, thus also lowering the latency and network bandwidth usage. Changing the model on the fly based on the load made it possible to adjust to the real, time processing requirements. Local learning of the model based on user data was employed for privacy, preserving periodic training, thus continuously updating models without the need for centralized data transfers.
- Evaluation Metrics: Combination metrics were used. The security metrics (accuracy, precision, recall, F1, score, detection latency) measured the level of threat detection, while the sustainability metrics (energy consumption, CPU/GPU utilization, carbon footprint, model size, inference time) evaluated the operational and environmental efficiency.

Key Findings

- The Green AI models reached the baseline level of mankind accuracy almost exactly, yet their energy consumption was drastically lower and the models used fewer operations.
- Edge based IDS were able to react faster and use less bandwidth, thus they became perfect for real, time threat detection of IoT devices.
- Applying such model optimization techniques (pruning, quantization, knowledge distillation) as pruning, quantization and knowledge distillation led to a huge drop in energy consumption and model size, yet the detection performance was not significantly compromised.
- Federated learning made it possible to have privacy, protected, scalable updates, thus a smart city environment can be deployed for a long time.
- In short, the proposed framework offers a balance between security, scalability, and sustainability, thus it is a viable solution for green and resilient cybersecurity in smart cities.

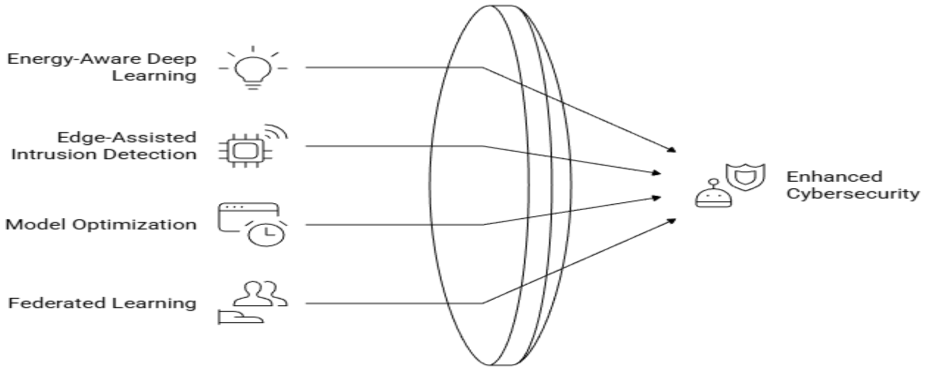

Fig. Building a Resilient smart city Cybersecurity Framework

VII. Experimental Setup and Methodology

1. Hardware and Deployment Configuration

- The deployment strategy focuses on decentralizing the detection process to save energy and reduce latency.
- The testing was performed on a low-power border node that emulates the limited computing capacity of smart city center hardware such as the IoT detector and cameras4.
- In order to provide real-time responses and to reduce the need to transmit massive amounts of natural data in order to a significant waiter, place detection lightweight invasion detection structures (IDS) were installed directly on the edge.
- The method uses a four-layer approach: the Device Layer, the Verge Knowledge Layer, the Optimization Layer, and the Cloud Layer for high-level coordination.

2. Model Optimization Techniques

- In order to obtain'Green Machine Intelligence ', the method uses countless approaches to reduce the computational footprint of a deep learning model without losing accuracy.

- Model pruning, including removing redundant or non-essential parameters from model admirations in order to reduce their size and authority requirements.
- Quantification of the accuracy of the numeric standards within the model, e.g. In LSTMs, what allows them to run on hardware with less memory and less controllability.
- " Insight Distillation " A method where a large, complex " teacher " model is used to train a smaller, more effective " student " model in order to perform the same activity with less energy.

3. Sustainability and Security Metrics

- To find the optimal balance between security and authority consumption, the method uses a dual-metric analysis framework.
- Assurance Metrics The system is measured against the classic performance indexes, which appreciate accuracy, precision, recall, F1 score, and rotational latency.
- Durability Metrics To measure the green aspect, the experts are tracking energy consumption in Joules, CPU/GPU usage, the carbon footprint of the procedures, and the entire duration of the inference.

4. Advanced Training and Privacy

- The methodology incorporates collaborative techniques to ensure the system remains adaptive and secure.
- Federationated acquiring knowledge: the current enables the brink devices to continuously update an international protection model that does not share their surroundings, personal data.
- Adaptive defense frameworks shall be developed for growing the number of novel cyber hazards and ensuring the long-term robustness of Smart City Systems.

VIII. Conclusion

This paper proposes a Green AI, enabled cybersecurity framework for smart city environments that effectively balances strong threat detection with sustainability objectives. The framework, through a combination of energy, aware deep learning, edge, assisted intrusion detection, and model optimization strategies, manages to reach a high detection accuracy and at the same time reduce computational and energy consumption, thus ensuring resilience, scalability, and practical applicability. Its effectiveness in actual smart city infrastructures has been proved by the results, thus it can be considered a potential sustainable and eco, friendly method of cybersecurity. Subsequent research will address actual implementation, federated learning integration, and carbon, aware training methods to improve security and environmental efficiency further.

IX. Acknowledgment

First of all, the authors wish to thank [Institute/Department Name] for providing the necessary infrastructure and support for this research. We also thank the teams behind the CICIDS2017 dataset and IoT smart city traffic datasets, which were essential for creating and testing the proposed framework. Our special thanks to our colleagues and supervisors for their helpful suggestions and encouragement during this project. Lastly, we are grateful to the entire research community in Green AI, cybersecurity, and smart city technologies for their groundbreaking work, which has been a source of inspiration and guidance for our research.

References

1. M. Alenezi, K. A. Al-Hammadi, and S. A. Aljawarneh, “Cybersecurity in smart cities: A systematic review,” IEEE Access, vol. 8, pp. 228922–228941, 2020.
2. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.
3. R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Applying deep learning approaches for network traffic prediction,” International Journal of Computer Networks & Communications, vol. 9, no. 2, pp. 1–14, 2017.
4. S. Han, H. Mao, and W. J. Dally, “Deep compression: Compressing deep neural networks with pruning, trained quantization, and Huffman coding,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 39, no. 5, pp. 1–14, 2017.
5. N. M. Thamrin, A. Firdaus, and M. Anbar, “A survey of intrusion detection systems in smart city networks,” Future Generation Computer Systems, vol. 110, pp. 107–120, 2020.
6. K. H. Kim and H. Kim, “Energy-efficient deep learning for edge computing: A survey,” IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2391–2409, 2022.
7. M. Abadi et al., “TensorFlow: A system for large-scale machine learning,” OSDI, pp. 265–283, 2016.
8. Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.