

# A Broad Review of Machine Learning-Driven Approaches for Detecting and Mitigating Cyber Security Threats

Publisher: **IEEE**

[Cite This](#)

 PDF

[D. Ruban Thomas](#) ; [C. Arul Stephen](#) [All Authors](#)

24

Full

Text Views

## Abstract

### Document Sections

- I. Introduction
- II. Related Works
- III. Methodology
- IV. Introduction
- V. Conclusion

## Authors

[Figures](#)

[References](#)

[Keywords](#)

[Metrics](#)

[More Like This](#)

### Abstract:

The increasing sophistication and volume of cyber threats pose significant challenges to traditional defense mechanisms, necessitating more adaptive and intelligent solutions. This survey critically reviews machine learning (ML)-driven approaches for cybersecurity threat detection and mitigation, focusing on the limitations of current supervised and semi-supervised methods. While effective for known attacks, these models often fail to detect zero-day exploits, struggle with high-dimensional network data, and depend heavily on labeled datasets, which are often incomplete or insecure. To address these challenges, this review explores advanced unsupervised learning techniques such as deep clustering, autoencoders, and generative adversarial networks (GANs) that can extract hidden patterns from unlabeled traffic and improve anomaly detection. The paper's key contribution lies in identifying research gaps and proposing a novel direction: integrating unsupervised learning with federated and reinforcement learning frameworks to build scalable, privacy-preserving, and adaptive security systems. This study highlights the potential of such integration to enable proactive and resilient cyber defense mechanisms, offering a significant advancement in intelligent cybersecurity solutions.

**Published in:** [2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things \(ICoCI\)](#)

**Date of Conference:** 17-19 September 2025

**DOI:** [10.1109/ICoCI65217.2025.11253183](#)

**Date Added to IEEE Xplore:** 01 December 2025

**Publisher:** IEEE

▼ **ISBN Information:**

**Conference Location:** Coimbatore, India

[Sign in to Continue Reading](#)

Authors 

[D. Ruban Thomas](#)

Department of Electronics and Communication Engineering, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

[C. Arul Stephen](#)

Department of Electronics and Communication Engineering, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

Figures 

References 

Keywords 

Metrics




**Need  
Full-Text**  
access to IEEE *Xplore*  
for your organization?

**CONTACT IEEE TO SUBSCRIBE >**

The advertisement features a blue background with a white grid pattern. The text is white, with 'Need Full-Text' in a large, bold font. Below it, the text 'access to IEEE Xplore for your organization?' is in a smaller font. At the bottom, there is an orange button with the text 'CONTACT IEEE TO SUBSCRIBE >' in white.

**IEEE Personal Account**[CHANGE USERNAME/  
PASSWORD](#)**Purchase Details**[PAYMENT OPTIONS](#)  
[VIEW PURCHASED  
DOCUMENTS](#)**Profile Information**[COMMUNICATIONS  
PREFERENCES](#)  
[PROFESSION AND  
EDUCATION](#)  
[TECHNICAL INTERESTS](#)**Need Help?**[US & CANADA: +1 800  
678 4333](#)  
[WORLDWIDE: +1 732  
981 0060](#)  
[CONTACT & SUPPORT](#)**Follow**

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#)  | [Sitemap](#) | [IEEE Privacy Policy](#)

A public charity, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2026 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.