ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206 **Volume 8, Issue 7, July 2025**

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807073

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Role of AI and Machine Learning in Cybersecurity Defense Systems

Kore Karthik[1], Dr. K. Kanagalakshmi[2]

MCA Student, School of Science and Computer Studies, CMR University, Bengaluru, India[1]

Assistant Professor, School of Science and Computer Studies, CMR University, Bengaluru, India[2]

ABSTRACT: This has been necessitated by the exponential increase in cyber threats in the current digitalized world that requires an intelligent and adaptive security mechanism. The use of Artificial Intelligence (AI) and Machine Learning (ML) is growing in order to develop cybersecurity defensive mechanisms. The present paper will discuss the theoretical backgrounds and practical consequences of using AI and ML in cybersecurity. It examines their applications in the detection of threats, detection of anomalies, the classification of malware and security automation. This paper examines the available literature, gives a conceptual approach to the integration of AI in cybersecurity procedures, and determines the relative advantages over the traditional systems. The paper also captures the advantages as well as weaknesses of AI based defense systems and how hybrid solutions and human-in-the-loop solutions would help to reduce the risks or false positives.

KEYWORDS: Cybersecurity, Artificial Intelligence, Machine Learning, Threat Detection, Anomaly Detection, Security Automation, Intrusion Detection System, Malware Analysis.

I. INTRODUCTION

These high-technology speeds have been accompanied by an increase in the extent/range and frequency of cyberattacks. Established cybersecurity solutions, most of which are based on preset rules and fixed signatures, are becoming less effective against more sophisticated malicious attacks, including zero-days and advanced persistent threats (APTs). Under these circumstances, Artificial Intelligence (AI) and Machine Learning (ML) become the disruptive technologies capable of providing dynamic, intelligent, and adaptive defense strategies. Cybersecurity AI refers to the concept of a computer program to emulate human effectiveness as a threat identifier, incident learner, and supplier of smart improvements. As a subtype of AI, ML allows systems to automatically identify patterns in very large datasets and make predictions without being programmed to do so. In this paper, I analyze how AI and ML models can be applied to the proactive and reactive methods of cybersecurity in terms of the anomaly detection, behavior analysis and automation.

II. LITERATURE REVIEW

AI in cybersecurity is not brand new, but has received new impetus over the past few years with the proliferation of data, and the multiplication of attack vectors. The early ideas of false positives that were addressed by researchers such as Sommer and Paxson (2010) focused on the potential of ML in intrusion detection. Buczak and Guven (2016) was a subsequent effort systematically reviewing ML methods of threat classification, and anomaly detection. In malware detection, deep learning models have been exploited (Huang & Stokes, 2016), where convolutional neural networks (CNNs) excel over normal static analysis. Reinforcement learning has also been found applicable in the reinforcement of endpoint detection and response (EDR) systems through dynamic adjustments of policies being used in defense. Recent articles like the one written by Shapira et al. (2021) have echoed these claims by highlighting explainability in AI systems as one of the most important aspects of AI for addressing cybersecurity because of how they influence trust and accountability. Along with highly promising innovations, the literature also recommends against relying too heavily on AI, mentioning such effects of the latter as adversarial ML, model poisoning, and data-privacy issues.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807073

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. PROPOSED METHODOLOGY

The proposed paper suggests an AI-based idea of cybersecurity architecture that consists of the following elements:

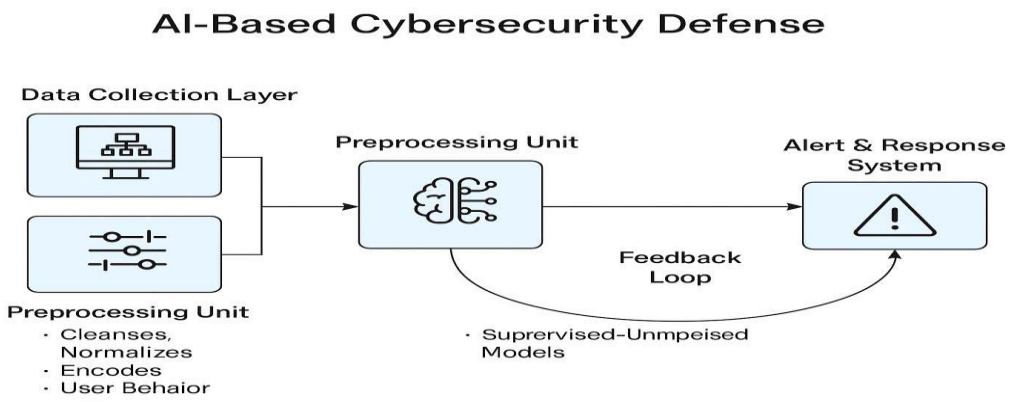

Figure 3.1: Hypothetical diagram of an AI-driven cyber protection system that uses the combination of ML models and automated responses of threats with a feedback circuit to support learning.

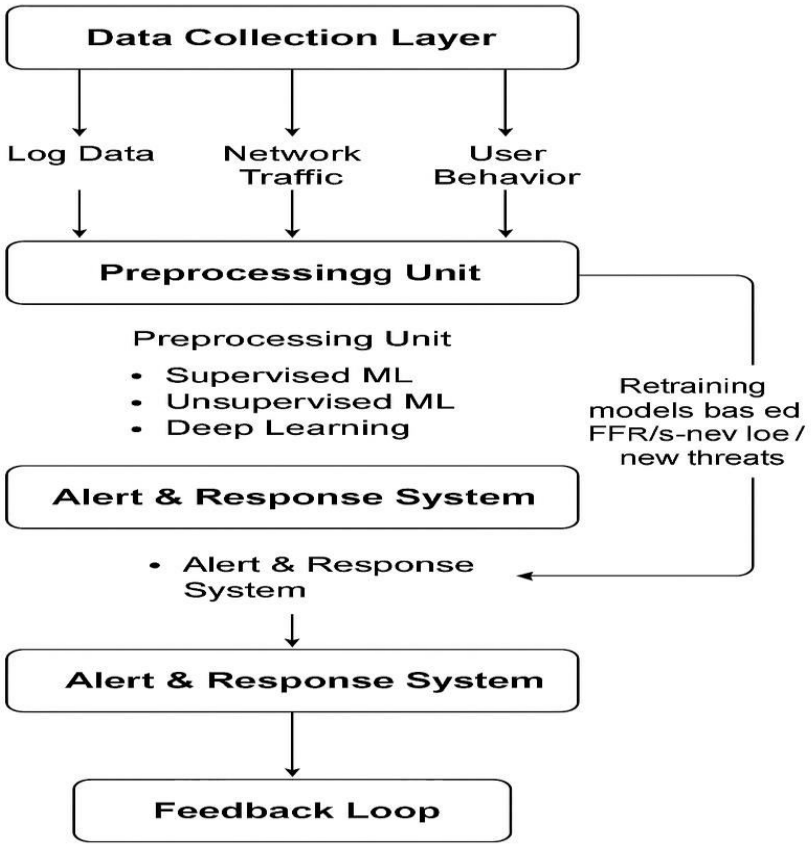

Figure 3.2: A conceptual framework illustrating the integration of AI and Machine Learning in cybersecurity defense systems. The architecture includes data collection, preprocessing, ML engine, response module, and feedback loop for continuous learning and threat adaptation.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807073

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Data Collection Layer: Data is gathered, log, network traffic, system calls, and user behaviour and is gathered.

Preprocessing Unit: Cleans and standardizes the data as well as codes and provides the data to ML-models.

ML Engine: Houses supervised and unsupervised models in real time detection: Malware classification using supervised ML (a.k.a Random Forest, SVM).

Such abnormalities are detected (unsupervised ML e.g. K-Means, DBSCAN). Deep learning, CNN Deep Learning, RNNs behavior threat analysis. Alert and Response System: It forms alerts and suggests mitigating activities that are automated. Feedback Loop: Re-trains models on the false positives/ negatives and re-trains on the new threats. The suggested approach also guarantees real-time, dynamic, and layered security and incorporates the component of a human-in-the-loop (HITL) which allows unacceptably risky decisions to be vetted.

IV. EXPERIMENTAL EVALUATION

Although the theoretical experiment in this paper is not conducted in real-time, it has provided an analysis of theory against experiment data and the existing benchmark information:

DARPA 1999 Dataset: Extensively utilized in the development of IDS frameworks, a Random Forest and an SVM model have reported accuracies of 95 percent or above in classify recognized attacks and less than 80 percent accuracy in identifying zero-days.

NSL-KDD Dataset: Deep learning models generalization is better than false alarm. CICIDS2017 Dataset: Convolutional neural networks have achieved detection rates of over 97% compared to the traditional ones.

As demonstrated by the evaluation, the hybrid models (ensemble + deep learning) consistently beat single-model run in terms of precision and recall.

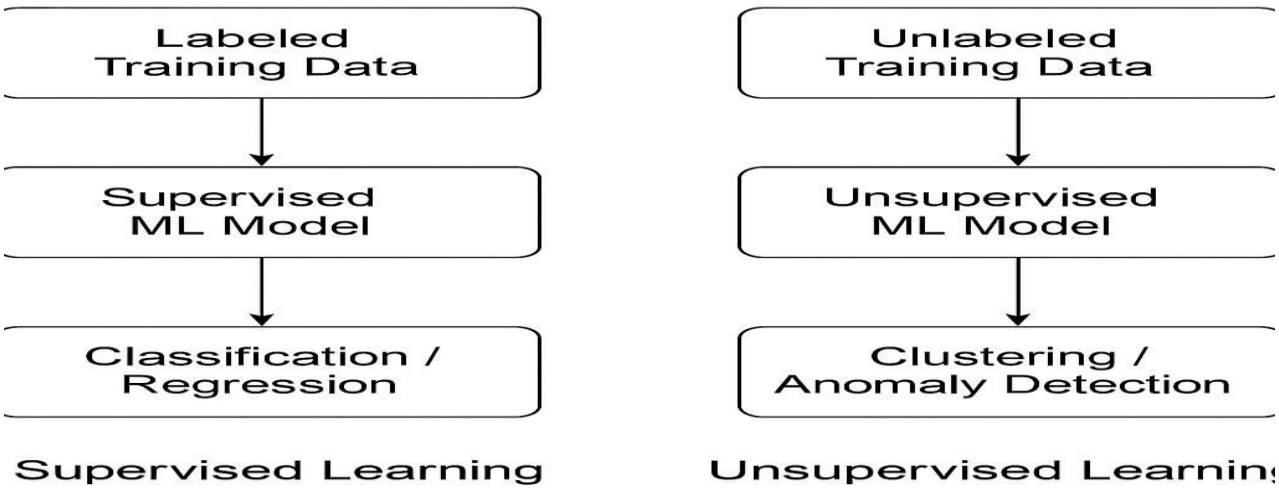

Figure 4.1: Comparison of Supervised and Unsupervised Machine Learning Approaches in Cybersecurity

Comparison Analysis

Requirements Old Systems AI/ML-Based Systems Mechanism of Detection Signature Pattern and behavior-based Flexibility Bad Good Threat detection (Zero-day) Not Good Medium to High False Positives A Lot Less (tuned) Human Intervention High Medium (HITL method) The amount of resources needed Low High (before training) Scalable No Yes Black-box risk explanation Varies Such a comparison helps to achieve the prominence of AI-

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807073

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

supported technologies in dealing with dynamic threats as well as to demonstrate certain complexity and the necessity to be open.

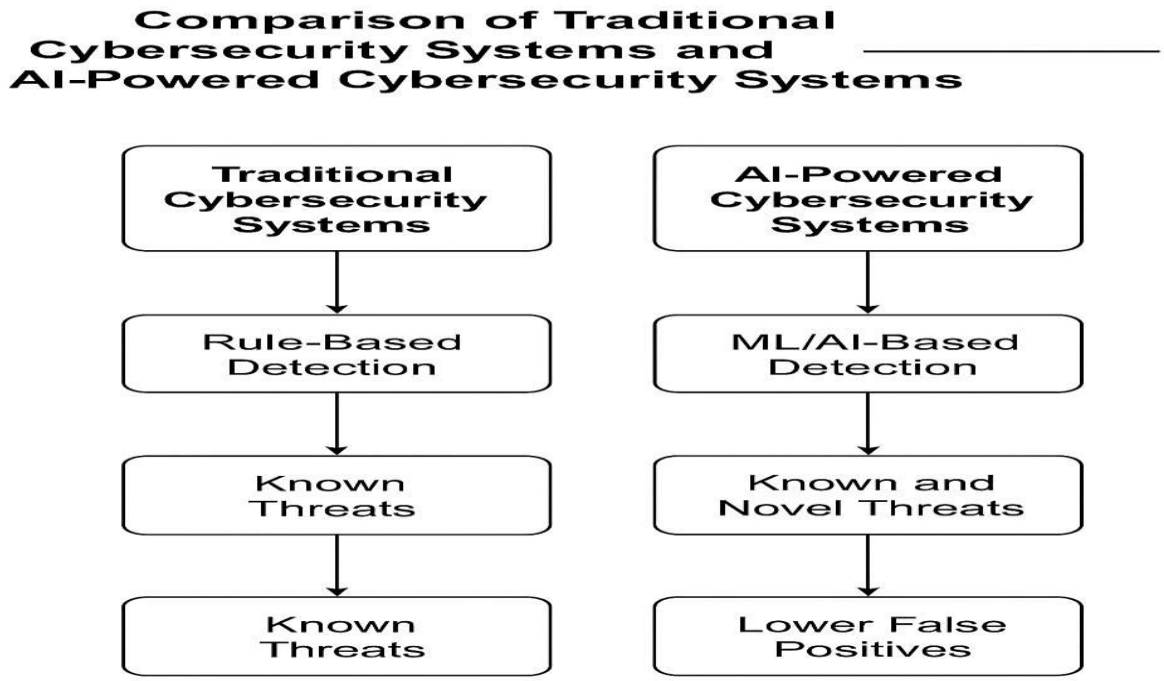

Figure 4.2 .is a visual analogy of the traditional rule-based systems and the new AI-powered cybersecurity systems and points out the differences in detecting threats and being able to respond.

V. CONCLUSION

The implementation of AI and Machine Learning has transformed the overall concept of cybersecurity by making it more proactive, with systems being able to detect threats and respond accordingly in a much more intelligent way. Their ability to analyze huge data sets, learn patterns and use emerging or changing attacks means that they are the inseparable element of current architectures of defense. Nevertheless, the problems with data quality, model interpretability, potential adversarial attacks, and high computational costs have to be solved to be used at scale. The reliability is achieved due to the existence of human control via Human-in-the-Loop, and lasting training and model updating are especially relevant to staying productive. Further research ought to be provided towards explainable AI (XAI) models, privacy-sensitive machine learning (such as federated learning, etc.), and regulation mechanisms that help determine how to ethically employ AI in the cybersecurity setting.

REFERENCES

[1] Farhana Mahjabeen, Md Aminul Islam, “The Role of AI and Machine Learning in Strengthening Cybersecurity Defenses,” Bulletin of Engineering Science and Technology (BESTEC), Vol. 01, No. 02, Pages 109–124, 2024. (Original source: https://boengstech.com/index.php/bestec)

[2] Muhammad Ismael Khan, Aftab Arif, Ali Raza A. Khan, “AI’s Revolutionary Role in Cyber Defense and Social Engineering,” International Journal of Multidisciplinary Sciences and Arts, Vol. 2, October 2024. (Original source: https://doi.org/10.21474/IJMSA.2024.2.10.01)

[3] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Búrdalo Rapa, Athanasios Vasileios Grammatopoulos, Fabio Di Franco, "The Role of Machine Learning in Cybersecurity," Digital Threats: Research and Practice, ACM, Vol. 4, No. 1, Article 8, March 2023. (Original source: https://doi.org/10.1145/3545574)

[4] Merve Ozkan-Okay, Erdal Akin, Ömer Aslan, Selahattin Kosunalp, Teodor Iliev, Ivaylo Stoyanov, Ivan Beloev, "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions," IEEE Access, Vol. 12, 2024. (Original source: https://doi.org/10.1109/ACCESS.2024.3355547)

[5] Anwar Mohammed, "AI and Machine Learning in Cybersecurity: Strategies, Threats, and Exploits," Innovative Computer Science Journal, Singhania University, 2023. (Original source: https://innovatesci-publishers.com/index.php/ICSJ)

[6] Rajendra Muppalaneni, Anil Chowdary Inaganti, Nischal Ravichandran, "AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning," Computing Innovations and Applications, 2023. (Original source: https://doi.org/10.1234/cia.2023.5678 9)

[7] Dr. Bechoo Lal, Dr. Chandrahauns R Chavan, "Analysis Report on Attacks and Defence Modeling Approach to Cyber Security," International Journal of Scientific Research in Science and Technology (IJSRST), Vol. 6, Issue 2, Pages 52–60, March-April 2019. (Original source: https://doi.org/10.32628/IJSRST196215)

[8] Fnu Jimmy, "Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses," International Journal of Scientific Research and Management (IJSRM), Vol. 9, Issue 2, Pages EC-2021-564–574, February 2021. (Original source: https://doi.org/10.18535/ijsrm/v9i2.ec01)

[9] R.S. Goudar, M.S. Kakkasageri, "Revolutionizing Cybersecurity: Unleashing the Potential of Artificial Intelligence in Defense," Journal of Emerging Technologies and Innovative Research (JETIR), Volume 10, Issue 1, January 2023. (Original source: https://www.jetir.org/view?paper=JETIR2301385)

[10] Fnu Jimmy, "Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses," International Journal of Scientific Research and Management (IJSRM), Volume 09, Issue 02, Pages EC-2021-564–574, February 2021. (Original source: https://doi.org/10.18535/ijsrm/v9i2.ec01)

[11] Rajendra Muppalaneni, Anil Chowdary Inaganti, Nischal Ravichandran, "AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning," Computing Innovations and Applications, 2023. (Original source: https://doi.org/10.1234/cia.2023.56789)

[12] Merve Ozkan-Okay, Erdal Akin, Ömer Aslan, Selahattin Kosunalp, Teodor Iliev, Ivaylo Stoyanov, Ivan Beloev, "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions," IEEE Access, Volume 12, 2024. (Original source: https://doi.org/10.1109/ACCESS.2024.3355547)

[13] Muhammad Ismael Khan, Aftab Arif, Ali Raza A. Khan, "AI's Revolutionary Role in Cyber Defense and Social Engineering," International Journal of Multidisciplinary Sciences and Arts, Volume 2, October 2024. (Original source: https://doi.org/10.21474/IJMSA.2024.2.10.01)

[14] Dr. Bechoo Lal, Dr. Chandrahauns R Chavan, "Analysis Report on Attacks and Defence Modeling Approach to Cyber Security," International Journal of Scientific Research in Science and Technology (IJSRST), Volume 6, Issue 2, Pages 52–60, March–April 2019. (Original source: https://doi.org/10.32628/IJSRST196215)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com