STM JOURNALS

International Journal of
Computer Science Languages

ISSN: 3048-944X
Volume 3, Issue 2, 2025
July–December
DOI (Journal): 10.37591/IJCSL

https://journals.stmjournals.com/ijcsl

Research IJCSL

AI for Cybersecurity: Deploying Machine Learning for Network Traffic Anomaly Detection

Priyanshi Nahar*

Abstract

The growing sophistication of cyberattacks and the growth of network traffic necessitate sophisticated anomaly detection methods. This study overviews the use of artificial intelligence (AI) and machine learning (ML) to counter these challenges, as noted in current studies. It analyses supervised learning (SVM, Decision Trees), unsupervised learning (K-means, DBSCAN), and deep learning (CNNs, RNNs, Auto-encoders) approaches, considering their strengths and weaknesses. The research integrates current developments in AI/ML-based network anomaly detection, critically evaluating corresponding challenges like data quality, computational complexity, and interoperability of the model. As illustrated through methods like CNNs and RNNs successfully identifying complex patterns, AI and ML provide improved functionalities in anomaly detection. Yet, concerns like the need for high-quality labeled data (for supervised learning) and difficulty in parameter tuning (for unsupervised learning) persist. Deep learning techniques are associated with challenges of computational expense and interoperability. This study presents a state-of-the-art evaluation of AI and ML in the area, outlining upcoming trends. It suggests future research avenues for optimizing model structures, enhancing interoperability and solving scalability problems to transcend current limitations and improve the efficiency of network anomaly detection systems. This review provides beneficial information for practitioners and scholars working to enhance network security using advanced detection techniques.

Keywords: Anomaly detection, ensemble techniques, feature engineering, performance quantification, integration complexities

INTRODUCTION

The growth in network traffic and the increasing complexity of cyber threats emphasize the importance of sophisticated and reliable anomaly detection methods. Traditional techniques, traditionally based on predefined rules and statistical models, find it difficult to cope with changing network anomalies and cyberattacks. As a result, there is a significant move towards cutting-edge technologies such as AI and ML in order to support anomaly identification and countermeasures. These technologies offer effective tools for analyzing vast volumes of network data, identifying patterns, and predicting anomalies with very high accuracy. They are better suited to dealing with the dynamic and multidimensional nature of network traffic, where conventional approaches falter. AI and ML in anomaly detection cover a range of methods, including supervised, unsupervised, and deep learning [1]. Each has its strengths and weaknesses. For example, supervised learning models need labelled data and can perform high accuracy in familiar situations. Unsupervised learning models are best at finding unknown patterns without any knowledge. Deep learning, which can handle complex data structures using architectures such as CNNs and RNNs, demonstrates outstanding success in real-time anomaly detection. All these

***Author for Correspondence**
Priyanshi Nahar
E-mail: priyanshinahar13@gmail.com

Student, Department of Computer Science Engineering, Rajasthan College of Engineering for Women, Jaipur, Rajasthan, India

Received Date: April 23, 2025
Accepted Date: July 15, 2025
Published Date: August 25, 2025

Citation: Priyanshi Nahar. AI for Cybersecurity: Deploying Machine Learning for Network Traffic Anomaly Detection. International Journal of Computer Science Languages. 2025; 3(2): 1–10p.

developments notwithstanding, there are still challenges, such as data quality, computational demands, and interoperability of AI models [1]. Table 1, intends to present an overall analysis of recent techniques used in detecting anomalies within network traffic with a focus on the contribution and influence of AI and ML.

LITERATURE REVIEW

Anomaly detection of network traffic has come a long way from simple rule-based and statistical techniques to advanced AI and machine learning techniques [2]. Simple thresholds were used by early intrusion detection systems to determine anomalies, but increasing attack sophistication made more adaptive mechanisms necessary. Recent developments underscore the breakthrough role played by AI in network security, with deep learning offering robust capabilities for high-level feature extraction from raw traffic. Convolutional Neural Networks and Recurrent Neural Networks have proven especially effective in identifying subtle anomalies that are not caught by traditional methods. Unsupervised learning methods such as clustering and dimensional reduction assist in discovering hidden patterns and novel attack vectors [3].

The historical evolution indicates a transition from statistical averages to rule-based systems, and ultimately to neural networks that can learn from enormous datasets and adjust to changing threats. These neural networks introduced a new paradigm in anomaly detection by providing the ability to handle enormous amounts of data while adapting to changing threat landscapes. The integration of AI and ML has revolutionized network security capabilities to the extent that dynamic adaptation to ever-changing threats is now possible [4–6].

Studies continue to show that AI/ML-based detection performs better compared to conventional methods, but despite this, problems remain. Among these are large labeled training datasets requirements, computationally expensive nature of advanced models, and lacking interoperability. Recent studies address model optimization, enhanced interoperability, and combating scalability in a bid to alleviate these problems as well as advance network security from ever-evolving threats [7–10].

OBJECTIVE

The main objective of this study is going to be an in-depth review of modern approaches that detect anomalies in network traffic by utilizing Artificial Intelligence (AI) and Machine Learning (ML). This study's objectives encompass the following:

- *Synthesizing Recent Research:* Review recent advancements in network anomaly detection with the aid of AI and ML and present it as a uniform overview of all current methodologies.
- *Highlight Technological Advancements:* Identify and discuss the key technological advancements brought by AI and ML to the detection and mitigation of network anomalies.
- *Identify and Analyze Challenges:* Critically analyze the challenges faced by the implementation of AI and ML in the network anomaly detection, such as data quality-related issues, high computational demands, and lack of model interoperability.
- *Future Research Directions:* Possible future research directions to aid in the elimination of challenges being currently encountered and increase the efficiency of network anomaly detection systems.

Table 1. Review of network anomaly detection techniques.

Approach	Strength	Challenges	Reference
AI and ML (Supervised, Unsupervised, DL)	Ability to analyze vast amounts of data: Adaptation to new threats	Data quality issues, Computational requirements, Model interoperability	Smith and Johnson (2023) [12]
Deep Learning	Real-time anomaly detection, Handling complex data structures	High computational cost-Limited interoperability	Park *et al*. (2022) [13]

With these objectives, this study hopes to make a contribution towards both the realm of academic research and the applied fields within network security, through insight that can be informative to guide future work towards augmenting network anomaly detection with AI and ML.

METHODOLOGY

This research uses an exhaustive approach to explore and assess the use of AI and ML in network anomaly detection. The methodology consists of a systematic literature review that includes scholarly publications, conference papers, and industry reports published in the last 10 years. This review seeks to summarize recent research into network anomaly detection methods based on AI and ML, giving an integrated account of current practices.

The study will outline and discuss different AI and ML methods used in network traffic analysis. The methods will be classified into supervised learning (e.g., SVM, Decision Trees), unsupervised learning (e.g., K-means, DBSCAN), and deep learning (e.g., CNNs, RNNs, Autoencoders). For each type, the research will discuss the underlying algorithms, their advantages, and their disadvantages when used for anomaly detection.

A central aspect of the methodology is a comparative evaluation of the techniques identified. This will evaluate their effectiveness, strengths, and weaknesses in capturing network anomalies, taking into consideration aspects such as precision, computational complexity, scalability, and interoperability. In addition, the research will critically evaluate the challenges of implementing AI and ML for network anomaly detection, including challenges with data quality, computational resources, and model interoperability. The ultimate purpose is to possess potential future research avenues focused on conquering such challenges and enhancing the efficiency of network anomaly detection systems. This review will provide worthwhile insights that can guide and inform future work towards improving network anomaly detection via AI and ML.

CNN AND RNN IN MACHINE LEARNING

Convolutional Neural Networks (CNNs)

- Designed for the processing of structured grid data such as images.
- Important characteristics include convolutional layers applying filters to find patterns.
- Utilize pooling layers to down-sample while retaining vital features.

In network security, CNNs are able to identify patterns within packet data or graphical network traffic.

Recurrent Neural Networks (RNNs)

- For the processing of sequential data.
- Are capable of processing inputs of variable length.
- Variants such as LSTM and GRU are used to deal with long-term dependencies.
- RNNs in network security perform best in processing time-security network data and finding anomalies based on temporal patterns.

Both architectures have been useful in network anomaly and associations in traffic data that are not picked up by conventional approaches.

CHALLENGES IN IMPLEMENTING AI AND ML FOR ANOMALY DETECTION

Integrating artificial intelligence (AI) and machine learning (ML) into anomaly detection methods has transformed the process, especially network traffic analysis. Yet, some challenges hinder smooth integration and application of these technologies [14]. The following section discusses the most important hurdles in the application of AI and ML for anomaly detection, such as data quality and labeling issues, computational complexity and resource requirements, interoperability and explainability of models, and flexibility to accommodate changing threats.

Data Quality and Labeling Problems

The performance of AI and ML models is greatly dependent on the quality of input data. In anomaly detection, having high-quality data that well reflects normal behavior is essential. However, collecting and preparing such data is a big challenge. The process typically includes determining what is "normal" behavior, which may be subjective and network-dependent. Labeling anomalies also takes expertise and time, further making the data preparation process difficult. These concerns highlight the need for strong data collection and annotation processes to provide effective anomaly detection systems.

Computational Complexity and Resource Demands

The deployment of AI and ML models for real-time anomaly detection requires high computational power. Algorithms are really complex, especially deep learning models, so powerful hardware and efficient software frameworks are required. In addition, continuous monitoring and updating the models in line with new patterns is a constant resource demand as reported by Jeon and Park [15]. These challenges raise the need to develop scalable solutions that align performance with resource utilization such that the anomaly detection system remains operational even when resources are scarce or in constant fluctuation [16].

Model Interoperability and Explainability

While AI and ML provide sophisticated capabilities for anomaly detection, their black-box nature tends to complicate it to determine the decision-making process [7]. This transparency limitation can prevent users and administrators from trusting the system, as they might need to be explained about the anomalies that are identified [8]. Model interoperability and explainability are therefore imperative, allowing stakeholders to understand why anomaly detections have been made and modify their behavior accordingly [9]. Efforts towards creating more transparent models, for example, using explainable AI (XAI) methods, are necessary to overcome this challenge.

Adaptability to Changing Threats

Network environments are dynamic, with new types of threats emerging constantly. Ensuring that AI and ML-based anomaly detection systems remain effective against these evolving threats is a significant challenge [10]. Models trained on historical data may fail to recognize novel attack patterns, necessitating continuous training and adaptation.

Additionally, the emergence of new cyber threats at a very fast rate means that static sets of rules and conventional anomaly detection can become outdated very rapidly. This challenge must be addressed through adaptive learning mechanisms that allow models to learn effectively from new data and dynamically update their knowledge about normal behavior [11–14].

OVERVIEW OF THE PROPOSED THEORETICAL FRAMEWORK

This research propounds a hypothesis in a clever manner to enhance network anomaly detection to improve cybersecurity. This blueprint blends traditional approaches and new technology. It employs elements such as planning features, transference of machine learning models, and group practices in combination with deep brain structures to identify patterns promptly and monitor behavior in real-time that enables it to perform efficiently regardless of changes that may circulate around it. This platform employs components of renowned theories and models to address the weaknesses of the old methods. It also capitalizes on their strengths [17].

The most important component of the plan is a dynamic system that expands with emerging cyber threats. This ensures it remains effective with time [9]. This section will thoroughly contrast the suggested framework with current theories, emphasizing how it complements existing models and adds new aspects to contribute to the dynamic environment of network anomaly detection. As illustrated in Figure 1, this comparison is intended to illustrate the subtle strengths and innovations this framework offers to the field of cybersecurity.

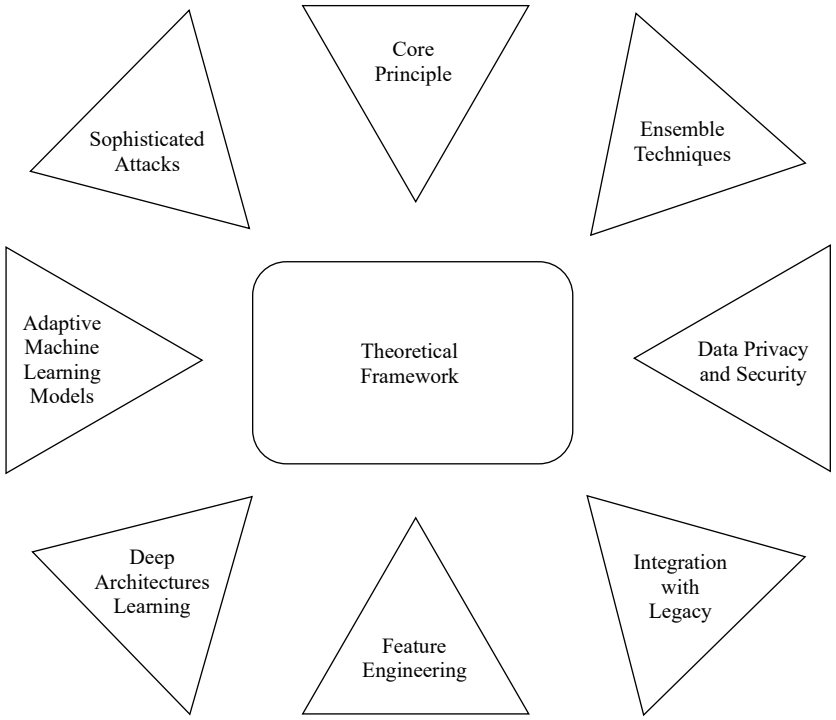

Figure 1. Theoretical framework.

Applications of Theoretical Framework

The theoretical framework established for incorporating machine learning (ML) into industrial network anomaly detection provides a blueprint for implementing sophisticated cybersecurity measures in real-world environments. Its usage spans different industrial sectors, addressing sector-specific challenges and delivering tangible advantages.

Adaptive Machine Learning Model Implementation

Scenario Implementation

In the scenario of a manufacturing facility, where the security of the Operational Technology (OT) network is most critical, the deployment of adaptive machine learning (ML) models marks a significant leap in enhancing cybersecurity. These advanced ML models are not static; they are designed to continuously learn and evolve in response to the changing landscape of network data. This dynamic nature allows them to detect even the most subtle anomalies that could signify emerging cyber threats, including those that are new or evolving.

Implications

The implementations of adaptive ML models changes the cybersecurity strategy from reactive to pro-active. Conventional security measures tend to investigate threats after they have occurred. Adaptive ML models, however, give an extensive, real-time analysis of network activity, enabling them to detect potential threat before they can cause harm. Ongoing adaptation to new and emerging threat patients considerably reduced the threat from advanced cyberattacks.

Using Ensemble Methods for Strong Anomaly Detection

Practical Application

In a utility company that operates a smart grid system, the use of ensemble methods like Random Forests offers an all-encompassing solution to anomaly detection. Through aggregating a multitude of algorithms, this method creates a multi-faceted detection system [8]. This improved system is not only more adapt at identifying a wide range of anomalies, from subtle to obvious, but it also combines the strengths of each algorithm, thereby providing a more nuanced and comprehensive analysis of network data.

Benefits

The most significant advantage of having experience of using ensemble techniques resides in their capability to minimize false positives and negatives. This precision in anomaly detection ensures that the utility company's smart grid operates with high efficiency and minimal disruption [9]. Through accurate identification of true threat while evicting over-reaction to non-threatening anomalies, ensemble methods such as Random Forests sustain the delicate balance required for smooth operation in complex utility networks.

Integrating Deep Learning for Anomaly Patterns of Complexity

Applications

In the complex ecosystem of automotive assembly line, where numerous sensors and devices continuously interact, deploying deep learning architectures like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) is priceless. These sophisticated models are adept at navigating and analyzing the large volumes of data generated, detecting anomalies that otherwise are difficult to detect.

Advantages

This deep learning method excels in revealing complex, subtle patterns that typically escape the notice of conventional anomaly detection techniques. It provides a more nuanced and in-depth analysis, greatly improving the assembly line's security system and ensuring a better comprehension protection against sophisticated cyber threat.

Real-Time Processing for Instantaneous Threat Response

Scenario Application

When responding to serious threats such as in the case of a telecommunications network, the implication of ML models that can accurately conduct real-time anomaly detection is vital. Such models act fast and go deeper to address cyber threats in time when they occur [16]. This instantaneous response is vital where any delay has the capacity to cause widespread system disturbance.

Benefits

Being able to respond promptly to threats is worth monitoring in enabling seamless service continuity [7]. It prevents potential financial losses and shields the company's reputation from the harmful effects of extended service outages or data breaches.

Ensuring Data Privacy and Security in ML Implementations

Application in Practice

In healthcare organizations, where patient data is sensitive and confidential, it is imperative that machine learning (ML) models are carefully designed to prevent data leakage and meet stringent privacy regulations [7]. This includes enacting strong GD-PR-grade security measures and ensuring compliance with healthcare-specific regulations such as HIPAA.

Advantages

By keeping data privacy and security at the forefront of ML implementations, healthcare organizations protect themselves not only against potential cyberattacks but also ensure complacency with legal and ethical requirements [5]. This practice is crucial in upholding the trust and integrity of the healthcare system, with patient data being confidential and secure.

The theoretical framework developed for integrating machine learning (ML) into network anomaly detection in industrial environments offers a road-map for applying advanced cybersecurity measure in real-world scenarios. Figure 2 illustrates that its application extends across various industrial sectors, addressing unique challenges and providing tangible benefits.

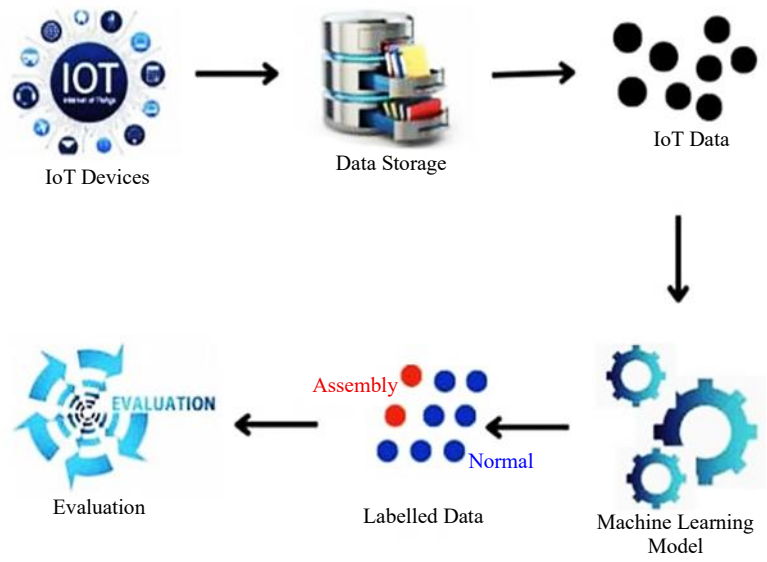

Figure 2. Machine Learning anomaly detection for cybersecurity.

TECHNOLOGICAL ADVANCEMENTS AND INNOVATIONS

For the field of network security, progress in technology has made a massive difference in how effective anomaly detection methods are. The convergence of artificial intelligence (AI) and machine learning (ML) introduced a new landscape of complexity and effectiveness in pinpointing unusual events in network flows. This is a review of the recent development in three most critical areas: real-time detection advancements, improvements in data prepossessing and feature engineering, and integration of ensemble learning and hybrid systems.

Advancements in Real-time Detection

Real-time anomaly detection has become an essential element in protecting network infrastructures against attacks. The conventional approach was through periodic scans, which were not enough for handling the dynamic and lightning-fast realities of contemporary cyberattacks. The presence of AI and ML helped create advanced algorithms that could analyze network traffic in real-time, hence limiting the window of opportunity for attackers. These technologies enable real-time identification and neutralization of anomalous behavior, preventing possible damage and ensuring the integrity of network operations [10].

FUTURE RESEARCH DIRECTIONS

As we look at the tremendous developments in anomaly detection methods in network traffic through the use of artificial intelligence (AI) and machine learning (ML), it becomes essential to think about future directions of research that can further maximize the effectiveness and usability of these technologies. This discussion identifies four key areas of future research: possible enhancements to AI and ML algorithms, better data quality and diversity, fusion of AI/ML with other security controls, and more interpretable and transparent models (Figure 3).

Possible Enhancements to AI and ML Algorithms

The ongoing development of AI and ML algorithms offers a rich area of future research. Whereas the existing models have shown unprecedented strength in recognizing anomalies, still space exists to improve and optimize them. Delving into emerging structures, such as more developed neural networks or introducing quantum computer theory, have the potential for innovations in terms of algorithm efficiency, scalability, and precision. Developing unsupervised learning algorithms capable of autonomously recognizing patterns on their own, without involving intense human interactions, could greatly advance autonomous detection of threats [8].

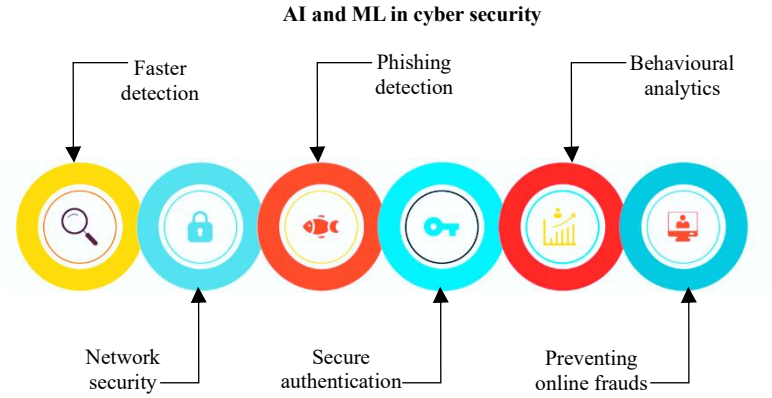

Figure 3. AI in cyber security.

Improving Data Quality and Diversification

Data quality and diversity are vital to the performance of AI and ML models. Future studies need to come up with methods for improving data quality, such as noise filtering, outlier elimination, and data augmentation. In addition, examining means to enhance data diversity, including the use of data from diverse network configurations, geographies, and industries, would enhance the models' generalization and resilience. This would prevent the risk of over-fitting into particular scenarios and increase the resilience of the models to deal with unexpected threats.

Combining AI/ML with Other Security Controls

Isolating AI and ML models from current security infrastructure restricts their efficiency. Integration of these technologies with other security protocols, including intrusion detection systems (IDS), should be an area of study in the future [13]. Such integration would allow real-time threat intelligence to be shared, thus allowing for a more unified and agile defense approach. Investigating interoperable platforms and standard protocols for data transfer between AI/ML models and legacy security tools can open the way for more integrated and efficient cybersecurity solutions.

Developing More Interpretable and Transparent Models

Although they excel at detecting anomalies, numerous AI and ML models are "black boxes" rendering it difficult to comprehend how they reach their decisions. Future work should be focused on building more interpretable and transparent models.

This should involve the exploration of explainable AI (XAI) methods that deliver insights into the decision-making capabilities of AI and ML models to enhance understanding and trust by users and stakeholders. Such developments would not only increase the transparency and accountability of anomaly detection systems but also enable users to make informed decisions about their use and management.

As we reflect upon the significant advancements in anomaly detection techniques within network traffic through the integration of artificial intelligence (AI) and machine learning (ML), it becomes imperative to consider future research directions that could further enhance the efficacy and applicability of these technologies. This discussion outlines four critical avenues for future exploration: potential improvements in AI and ML algorithms, enhancing data quality and diversity, integrating AI/ML with other security measures, and developing more interpretable and transparent models.

CONCLUSION

The intersection of Artificial Intelligence (AI) and Machine Learning (ML) has brought a new revolution in network traffic anomaly detection, revolutionizing our cyber security against cyberattacks entirely. In this study, we provide an extensive comparative survey of different AI and ML methods

and how these technologies develop to address the sophisticated needs of anomaly detection in networks. The employment of AI and ML has resulted in incredibly strong methods that are built on top of the ones that preceded them. Such supervised learning algorithms as Support Vector Machines and Decision Trees proved useful, if one is working with the cases where enormous sets of labeled data are available. Unsupervised algorithms such as DBSCAN and K-means clustering, however, tend to find hidden patterns even without knowing they are dealing with anomalies, although they tend to have difficulties with parameter adjustments and system compatibility problems.

Deep learning is simply incredible when applied to learn autonomously from enormous data. Methods such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Autoencoders can learn meaningful features end-to-end from raw input. However, these models will most probably need gigantic computational power and large memory, in real-world practice, which are constraints. Schematic representation shows the strengths, weaknesses, and optimal applications of these AI and ML methods in the anomaly detection example, providing a clear comparative framework for selecting the most suitable approach in different contexts.

Real-world use cases like the GRAPHSEC project and Anomal-E bring real-life, in-the-wild implementation AI and ML in to network security solutions. The use cases illustrate how self-supervised learning methods and graph models can detect sophisticated patterns of behavior and anomalies without labeled training data. Broad adoption of AI-based anomaly detection in Internet of Things (IoT) networks and sensor systems are indicators of just how intertwined these technologies have become to defend vital infrastructure. Advances in real-time detection, data preprocessing, feature engineering and the design of ensemble and hybrid models in AI and ML have themselves become a cybersecurity bulwark. These advancements enhance speed and accuracy in threat detection, leverage the strengths of several algorithms, and enhance global detection networks' resilience and reliability.

Scientists, cyber security professionals, and government officials must work together in the future and leverage these technologies to their optimal extent. It will empower a confident, secure, and sustainable online future.

REFERENCES

1. Aggarwal CC, Yu PS. An effective and efficient algorithm for high-dimensional outlier detection. VLDB J. 2005 Apr; 14(2): 211–21.
2. Jiang M, Cui P, Faloutsos C. Suspicious behavior detection: Current trends and future directions. IEEE Intell Syst. 2016 Jan 22; 31(1): 31–9.
3. Akoglu L, Tong H, Koutra D. Graph based anomaly detection and description: a survey. Data Min Knowl Discov. 2015 May; 29(3): 626–88.
4. Pang G, Shen C, Cao L, Hengel AV. Deep learning for anomaly detection: A review. ACM Comput Surv. 2021 Mar 5; 54(2): 1–38.
5. Zenati H, Romain M, Foo CS, Lecouat B, Chandrasekhar V. Adversarially learned anomaly detection. In 2018 IEEE International conference on data mining (ICDM). 2018 Nov 17; 727–736.
6. Tripathi G, Abdul Ahad M, Paiva S. Sms: A secure healthcare model for smart cities. Electronics. 2020 Jul 13; 9(7): 1135.
7. Ullah W, Ullah A, Haq IU, Muhammad K, Sajjad M, Baik SW. CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks. Multimed Tools Appl. 2021 May; 80(11): 16979–95.
8. Lam J, Abbas R. Machine learning based anomaly detection for 5g networks. arXiv preprint arXiv:2003.03474. 2020 Mar 7.
9. Mokhtari S, Abbaspour A, Yen KK, Sargolzaei A. A machine learning approach for anomaly detection in industrial control systems based on measurement data. Electronics. 2021 Feb 8; 10(4): 407.
10. Diro A, Chilamkurti N, Nguyen VD, Heyne W. A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. Sensors. 2021 Dec 13; 21(24): 8320.

11. Larriva-Novo XA, Vega-Barbas M, Villagrá VA, Rodrigo MS. Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies. IEEE Access. 2020 Jan 1; 8: 9005–14.
12. Smith J, Johnson A. Leveraging Artificial Intelligence and Machine Learning for Network Anomaly Detection: A Comprehensive Review. Journal of Cybersecurity Advances. 2023; 5(2): 123–45.
13. Park C, Lee J, Kim Y, Park JG, Kim H, Hong D. An enhanced AI-based network intrusion detection system using generative adversarial networks. IEEE Internet Things J. 2022 Oct 3; 10(3): 2330–45.
14. Thota C, Manogaran G, Lopez D. Big data security framework for distributed cloud data centers. In: Cybersecurity breaches and issues surrounding online threat protection. IGI Global Scientific Publishing; Pennsylvania, USA. 2017; 288–310.
15. Jeon D, Park DG. Analysis model for prediction of cyber threats by utilizing big data technology. J Korean Inst Inf Technol. 2014; 12(5): 81–100.
16. Kostyuchenko YV, Yuschenko M. Methods and Tools of Big Data Analysis for Terroristic Behavior Study and Threat Identification: Illegal Armed Groups during the Conflict in Donbas Region (East Ukraine) in Period 2014-2015. In: Violent Extremism: Breakthroughs in Research and Practice. IGI Global Scientific Publishing; 2019; 525–537.
17. Mayhew M, Atighetchi M, Adler A, Greenstadt R. Use of machine learning in big data analytics for insider threat detection. In MILCOM 2015-2015 IEEE Military Communications Conference. 2015 Oct 26; 915–922.

