Journal of Information Systems Engineering and Management
2025, 10(14s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Advancing Cyber Threat Detection with Ai: Cutting-Edge Techniques and Future Trends

Rakhi A. Kalantri[1,2], Dr. Rajesh Bansode[3]

[1]*Research Scholar, Department of Information Technology, Thakur college of Engineering and Technology Mumbai, Maharashtra, India*
[2]*Assistant Professor, Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Navi Mumbai, Maharashtra, India*
[3]*Professor and Research Guide, Department of Information Technology, Thakur college of Engineering and Technology Mumbai, Maharashtra, India*
**Corresponding email: rakhikalantri2022@gmail.com*

ARTICLE INFO

Received: 24 Nov 2024

Revised: 15 Jan 2025

Accepted: 31 Jan 2025

ABSTRACT

The digital age has made cyberspace indispensable for economic, social, and governmental functions, thus intensifying the critical need for robust cybersecurity. Our increasing dependence on digital platforms has exposed systems to a wide array of sophisticated cyber threats, including malware, phishing, distributed denial-of-service (DDoS) attacks, ransomware, and insider threats, often motivated by financial gain, political agendas, or espionage. These challenges underscore the urgent requirement for flexible and resilient cybersecurity strategies. Traditional signature-based and rule-based detection methods, while historically foundational, are now insufficient against modern cyber risks due to their inability to detect novel and evolving threats. Consequently, recent research has focused on utilizing advanced technologies like artificial intelligence (AI), machine learning (ML), deep learning (DL), and metaheuristic algorithms. These technologies excel at processing large datasets, identifying subtle anomalies, and predicting potential vulnerabilities before they are exploited. This paper assesses the performance of a new Intrusion Detection System (IDS) developed to combat these challenges and compares its efficacy against existing systems across various network environments. Using datasets that simulate diverse network attack scenarios—including a general Network Attack Dataset, an IoT-specific attack dataset (Rt-IoT), and the UNSW-NB15 dataset the proposed IDS yielded promising results. Specifically, the system achieved high accuracy, reaching 95.95% on the Network Attack Dataset, 99.99% on the Rt-IoT dataset, and 95.35% on the UNSW-NB15 dataset. Moreover, the system demonstrated strong performance in terms of precision, recall, and F1-score across these datasets. This paper reviews the evolution of threat detection techniques, contrasting traditional methods with state-of-the-art AI-driven approaches, and integrating the performance results of our proposed IDS. It identifies key research gaps, such as scalability issues, the need for adaptive AI models capable of responding to emerging threats, and the complexities of managing diverse datasets. The study aims to guide future research, emphasizing the development of adaptive and proactive cybersecurity solutions to address the constantly changing landscape of cyber threats.

Keywords: Intrusion Detection System (IDS), Cybersecurity, Network Security, Threat Detection, Anomaly Detection, Machine Learning (ML), Deep Learning (DL), Artificial Intelligence (AI), Metaheuristic Algorithms.

1. INTRODUCTION

The digital age has profoundly reshaped society, integrating cyberspace into the foundation of economic, social, and governmental functions [1]. This widespread integration has undeniably spurred unprecedented progress in communication, information sharing, and global connectivity, fostering innovation and driving advancement across various sectors. However, our increasing reliance on digital platforms has simultaneously made systems susceptible to a constantly expanding range of sophisticated cyber threats, posing a significant challenge to the

security and integrity of vital infrastructure, sensitive information, and personal privacy [2]. The growing frequency and complexity of these attacks, often carried out by well-resourced and highly skilled adversaries, highlight the urgent need for robust and adaptable cybersecurity strategies capable of proactively mitigating potential risks and protecting digital assets in our increasingly interconnected world.

The modern cyber threat landscape is characterized by a diverse array of malicious activities, including malware infections, phishing campaigns, Distributed Denial-of-Service (DDoS) attacks, ransomware deployments, and insider threats. These attacks are frequently motivated by a complex interplay of factors, spanning from financial gain and political agendas to acts of espionage, disruption, and malicious intent [3]. Cybercriminals are in a constant state of evolution, employing increasingly sophisticated techniques to circumvent traditional security measures and exploit vulnerabilities in systems. This includes the use of advanced persistent threats (APTs), which involve stealthy and prolonged network infiltration, as well as the exploitation of zero-day vulnerabilities, for which no patches or fixes exist. The dynamic and adaptive nature of these threats makes it extremely difficult for organizations and individuals to maintain an adequate level of security, emphasizing the need for continuous innovation and proactive adaptation in cybersecurity defenses [4].

Conventional cybersecurity approaches, such as signature-based and rule-based detection systems, have historically served as the cornerstone of network security. These methods rely on pre-defined patterns and rules to identify known threats, essentially acting as digital watchdogs against previously documented malicious activities. While effective against attacks encountered before, they possess inherent limitations in detecting novel and evolving threats, particularly zero-day exploits and polymorphic malware that can evade signature-based detection by constantly modifying their code [5]. Moreover, these traditional systems often struggle to process the immense volume of data generated in contemporary network environments, potentially leading to bottlenecks and overlooked threats. The static nature of their detection mechanisms, depending on pre-programmed knowledge, renders them increasingly inadequate in the face of the rapidly changing cyber threat landscape, necessitating the exploration and adoption of more advanced and intelligent techniques.

To overcome the limitations of traditional cybersecurity approaches, recent research has concentrated on leveraging the power of artificial intelligence (AI), machine learning (ML), deep learning (DL), and metaheuristic algorithms. These cutting-edge technologies offer a fundamentally different approach to threat detection by enabling systems to learn from data, identify subtle anomalies, and adapt to evolving threat patterns [6]. AI-driven approaches are especially well-suited for handling the massive datasets generated by modern networks, enabling real-time analysis and identification of suspicious activities that might otherwise be missed. Machine learning algorithms can be trained to recognize complex patterns and relationships in network traffic, allowing them to detect previously unseen threats based on their behavioral characteristics. Deep learning models, with their capacity to learn hierarchical data representations, can further enhance threat detection by automatically extracting relevant features and increasing the accuracy of classification. Metaheuristic algorithms, inspired by natural processes, can be utilized to optimize the performance of AI/ML models, select relevant features, and improve the efficiency of threat detection processes, often by navigating complex search spaces to find optimal solutions.

This paper provides a thorough assessment of a new Intrusion Detection System (IDS) developed to address the challenges presented by contemporary cyber threats.

Key Contributions:

- Performance Assessment Across Diverse Datasets: The proposed IDS was tested on a variety of datasets (Network Attack, Rt-IoT, and UNSW-NB15) to prove its effectiveness and adaptability in different network environments and against various attack types.
- Improved Detection of General Network Attacks: The system significantly outperformed existing methods in detecting general network attacks, as shown by higher accuracy, precision, recall, and F1-score on the Network Attack dataset.
- Highly Effective Detection of IoT Attacks: The system achieved almost perfect results on the Rt-IoT dataset, demonstrating its strong ability to identify threats specific to Internet of Things devices.
- Consistent Performance on Complex Attack Scenarios: The system maintained comparable performance to existing methods on the UNSW-NB15 dataset, which includes a mix of modern and sophisticated attacks, showing its resilience and ability to handle challenging situations.

- In-Depth Performance Analysis: A thorough evaluation using a wide range of metrics (accuracy, precision, recall, specificity, F1-score, false negative rate, and false positive rate) was conducted to provide a detailed understanding of the system's strengths and weaknesses.

The performance of the proposed IDS is rigorously assessed using a variety of datasets representing diverse network attack scenarios, including a general Network Attack Dataset, an IoT-specific attack dataset (Rt-IoT), and the UNSW-NB15 dataset. These datasets encompass a wide range of attack types, allowing for a comprehensive evaluation of the IDS's ability to detect both common and sophisticated threats. The evaluation employs key performance metrics, such as accuracy, precision, recall, specificity, F1-score, false negative rate (FNR), and false positive rate (FPR), to provide a comprehensive assessment of the IDS's effectiveness. The results obtained from these experiments are thoroughly analyzed and compared against the performance of existing IDS solutions to demonstrate the advantages and potential contributions of the proposed system.

This research contributes to the ongoing efforts to develop more intelligent and adaptable intrusion detection systems capable of effectively mitigating the evolving landscape of cyber threats. By leveraging the power of AI and machine learning. The proposed IDS aims to bridge the gap between traditional security approaches and the increasingly sophisticated nature of modern cyberattacks. The evaluation results presented in this paper provide valuable insights into the performance characteristics of the proposed system and highlight its potential for enhancing network security in diverse environments. Furthermore, this study identifies key research gaps and challenges in the field of AI-driven threat detection, including issues related to scalability, adaptability, data management, and the need for explainable AI models. These challenges serve as a roadmap for future research directions, emphasizing the importance of developing proactive and intelligent cybersecurity solutions to combat the ever-evolving landscape of cyber threats. The goal is to create a more secure and resilient cyberspace where individuals, organizations, and governments can confidently operate without fear of cyberattacks and data breaches.

2. BACKGROUND AND RELATED WORK

Existing research relates to the creation of unique viewpoint solutions for detecting cyber attacks. Sibi Chakkaravarthy et al. (2018) investigated vulnerabilities in critical systems caused by cyber-attacks. Their work emphasized the use of firewalls and intrusion detection systems (IDS) to protect these systems but fell short of addressing modern challenges such as zero-day vulnerabilities. Similarly, Jain et al. (2017) proposed a multi-

layered security framework combining physical and digital defense strategies. However, their approach overlooked evolving attack vectors, particularly those associated with IoT ecosystems. Stojanović et al. (2019) underscored the value of feature engineering for constructing datasets aimed at detecting advanced persistent threats (APTs). Despite improving detection capabilities, their research did not address the need for dynamic datasets that adapt to real-time threats. Kaloudi et al. (2020) examined the malicious use of artificial intelligence in cyber-attacks, presenting a conceptual framework to classify such threats. While insightful, this framework lacked practical validation through real-world implementations. Ahmed et al. (2020) explored cybersecurity in IoT and multi-cloud environments, especially within healthcare systems, and proposed layered security architectures. Nevertheless, their work failed to resolve the complexities involved in securely sharing data across distributed systems. Lu et al. (2021) focused on synthetic data generation with an emphasis on privacy and fairness, but their findings had limited relevance to cybersecurity applications. Sarker et al. (2021) highlighted the role of artificial intelligence in enhancing cybersecurity within Industry 4.0 environments. They advocated for explainable AI (XAI) to increase transparency in decision-making but provided limited solutions for tackling adversarial AI-based attacks. Pagano (2024) analyzed machine learning models for anomaly detection, proposing hybrid techniques to improve accuracy. However, they identified unresolved challenges related to ensuring data quality and building models robust against adversarial manipulations. Zhang et al. (2022) developed deep learning models for securing cyber-physical systems (CPS) but found their applicability to IoT and edge computing limited. Finally, Yuchong et al. (2021) introduced a taxonomy of emerging cyber threats, offering a structured classification. However, the study lacked adaptive, real-time response mechanisms necessary for effective threat mitigation. These studies collectively provide significant insights into various facets of cybersecurity while exposing persistent gaps. They highlight the importance of advancing adaptive AI models, securing IoT frameworks, implementing real-time threat response mechanisms, and improving synthetic dataset generation for more robust and efficient threat detection. The table 1 shows the analysis of the current literature review.

Table 1: Literature review summary

References	Focus Area	Key Contributions	Proposed Solutions/Frameworks	Limitations/ Gaps Identified	Future Research Directions
S. Sibi Chakkaravarthy et al. [1]	Network Security	Examines the prevalence and impact of cyber-attacks on critical systems, offering insights into potential defense mechanisms.	Recommends using intrusion detection systems (IDS) and firewalls as part of a mitigation strategy.	Primarily addresses known threats, lacking strategies for emerging challenges like zero-day exploits.	Develop adaptive solutions to counter rapidly evolving threats using AI-driven techniques.
Jitendra Jain et al. [2]	Cybersecurity Practices	Discusses the integration of physical and digital security, highlighting key cybersecurity protocol elements.	Advocates for a multi-layered defense approach combining traditional and advanced security techniques.	Neglects newer attack vectors, such as vulnerabilities in IoT and cloud ecosystems, and lacks predictive threat analysis.	Investigate predictive analytics for threat management in hybrid security environments.
Branka Stojanović et al. [3]	Advanced Persistent Threats (APTs)	Evaluates the role of feature engineering in datasets used for detecting APTs across CPS, IoT, and cloud environments.	Offers recommendations for enhancing the quality and coverage of datasets tailored to these domains.	Does not address dynamic datasets or their applications in real-time scenarios.	Develop dynamic and adaptable datasets to improve the detection of APTs.
Nektaria Kaloudi et al. [4]	AI-Based Cyber Threats	Explores the misuse of AI in enabling advanced cyber-attacks and provides a conceptual framework for understanding them.	Proposes a classification system to categorize AI-driven threats systematically.	The framework lacks empirical validation and practical application in real-world scenarios.	Design practical tools to detect and counteract AI-powered cyber-attacks effectively.
Afsheen Ahmed et al. [5]	IoT and Multi-Cloud Security	Reviews the security challenges of IoT and multi-cloud systems in healthcare, focusing on threat identification and mitigation.	Suggests a layered security framework specifically designed for IoT healthcare systems.	Does not address the complexities of secure data sharing in interconnected IoT networks.	Research advanced data-sharing protocols and real-time threat response mechanisms for healthcare

					IoT.
Yingzhou Lu et al. [6]	Synthetic Data	Investigates machine learning approaches for generating synthetic data, emphasizing privacy, fairness, and generalization.	Recommends best practices for creating diverse and privacy-compliant synthetic datasets.	Limited exploration of how synthetic data can be leveraged in cybersecurity.	Study how synthetic datasets can strengthen cybersecurity systems and models.
Iqbal H. Sarker et al. [7]	AI in Cybersecurity	Analyzes the use of AI methods (ML/DL) in cybersecurity within Industry 4.0, identifying research challenges.	Proposes the adoption of explainable AI to improve transparency in cybersecurity systems.	Minimal focus on adversarial AI attacks or issues related to computational efficiency.	Develop explainable and resource-efficient AI models for real-time cybersecurity applications.
Alessandro Pagano [8]	Machine Learning in Cybersecurity	Studies ML models for identifying threats, with an emphasis on anomaly detection and predictive analytics.	Introduces hybrid ML models combining supervised and unsupervised learning for anomaly detection.	Identifies issues such as data quality, interpretability, and resilience to adversarial attacks.	Enhance ML systems to address adversarial attacks while improving model transparency.
Jun Zhang et al. [9]	Deep Learning in CPS Security	Focuses on using deep learning models to safeguard CPS against cyber-attacks.	Proposes a hierarchical deep learning model for identifying CPS-specific threats.	Limited application to CPS, with no exploration of IoT or broader cross-domain scenarios.	Expand deep learning approaches to encompass IoT and edge computing for enhanced security.
Yuchong L et al. [10]	Emerging Cybersecurity Trends	Surveys the latest cybersecurity frameworks, emphasizing challenges in adapting to sophisticated attacks.	Introduces a taxonomy to classify threats based on behavioral patterns.	Lacks adaptive and real-time threat response capabilities.	Research adaptive AI-based systems for real-time threat identification and mitigation.

3. TRADITIONAL THREAT DETECTION METHODS

Research on cybersecurity threat detection encompasses a variety of methods, each with unique strengths and weaknesses. This section critically reviews the most used threat detection techniques and evaluates their effectiveness [11].

3.1 Signature-Based Detection

Signature-based detection works by comparing incoming data against a database of known attack patterns or signatures. If a match is found between the data and an existing signature, an alert is triggered. This method is

effective for identifying known threats but cannot detect new or unknown attacks [12].

Mathematical Representation:

Let S= {s_1, s_2, sn} represent a set of known signatures, where each s_i corresponds to a unique attack or malware signature. The detection process checks if the observation O matches any of the signatures in SSS.

Detection Equation:

$$P_{match}(O,S) = \begin{cases} 1 & \text{if } O \in S \\ 0 & \text{Otherwise} \end{cases}$$

Where Pmatch (O, S) represents the probability that the observation O matches a known signature from the set S.

3.2 Heuristic-Based Detection

Heuristic-based detection uses algorithms that evaluate the behavior of files or network traffic to detect potential threats. It identifies suspicious activities even when the characteristics do not exactly match predefined signatures.

Mathematical Representation:

Let F= {f_1, f_2, fm} be a set of heuristic rules or features that define the behavior of a program or network activity. A score is calculated for each observation O based on the application of these rules.

Detection Equation:

$$H(O,F) = \sum_{i=1}^{m} f_i(O)$$

where H (O, F) is the heuristic score for observation O and f_i (O) represents the value of the i^{th} feature or heuristic rule applied to O.

A threshold T is then used to determine whether the observation is benign or malicious:

If H (O, F) ≥T, then O is flagged as malicious.

3.3 Anomaly-Based Detection

Anomaly-based detection identifies threats by detecting deviations from normal behavior. A model of "normal" behavior is created, and any significant deviation from this model is flagged as suspicious [13].

Mathematical Representation:

Let N= {n_1, n_2, np} represent the normal behavior dataset. The goal is to model the distribution of normal behaviors, often using statistical methods like the Gaussian distribution.

Detection Equation

$$P(O|N) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(O-\mu)^2}{2\sigma^2}\right)$$

where:

P(O|N) is the probability of observation O under the normal distribution of N.

μ is the mean of normal behaviors, and σ^2 is the variance of normal behaviors.

If the probability of an observation being normal falls below a certain threshold T, it is flagged as anomalous:

If P(O|N) <T, then O is flagged as malicious.

3.4 Behavioral-Based Detection

Behavioral-based detection focuses on analyzing the actions or behaviors of users or processes to detect malicious activity [14]. It identifies deviations in behavior, such as unusual patterns in system or network activity.

Mathematical Representation:

Let B= {b_1, b_2, b_k} represent a set of behavioral patterns, such as file access, system calls, or network activity. A score is calculated for each observation O based on its behavior relative to these patterns.

Detection Equation:

$$H(O,F) = \sum_{i=1}^{k} w_i b_i(O)$$

where:

S(O) is the behavioral score for observation O.

w_i is the weight assigned to the i^{th} behaviour.

bi(O) is the value of the i^{th} behavioural feature for observation O.

An observation is flagged as malicious if the behavioral score exceeds a certain threshold T:

If S(O)≥T, then O is flagged as malicious

3.5 Rule-Based Detection

Rule-based detection uses predefined logical rules to describe potential malicious activities. These rules are generally based on known attack patterns or system vulnerabilities.

Mathematical Representation:

Let R= {r_1, r_2, rq} represent a set of rules, where each rule r_i defines a condition that must be satisfied for an observation O to be considered malicious.

Detection Equation:

$$P(O,R) = \begin{cases} 1 & \text{if O satisfies one or more rules in R} \\ 0 & \text{Otherwise} \end{cases}$$

Where P (O, R) represents the detection result for observation O given the rule set R. If any rule is satisfied by the observation, it is flagged as malicious.

4. EMERGING THREAT DETECTION TRENDS

Emerging threat detection trends focus on addressing the limitations of traditional methods like signature-based and basic anomaly detection [15]. New techniques, such as AI, machine learning, and blockchain, are being integrated to improve detection accuracy, speed, and adaptability. These methods enhance the ability to identify both known and unknown threats. Innovations like behavioral analytics and decentralized systems offer stronger defense mechanisms. Together, these trends promise to better protect against increasingly sophisticated and evolving cyber threats [16].

4.1 Machine Learning and AI in Cybersecurity

Machine learning (ML) and artificial intelligence (AI) are critical components in modern cybersecurity due to their ability to process large amounts of data and adapt to evolving threats [17]. Below is an in-depth discussion of how supervised, unsupervised, and reinforcement learning models enhance threat detection, along with their benefits and challenges.

Types of Machine Learning Models in Cybersecurity:

The main types of machine learning are shown in Figure 1. Main approaches include classification and regression under the supervised learning and clustering under the unsupervised learning. Reinforcement learning enhance the model performance by interacting with environment. Colored dots and triangles represent the training data. Yellow stars represent the new data which can be predicted by the trained model [18].

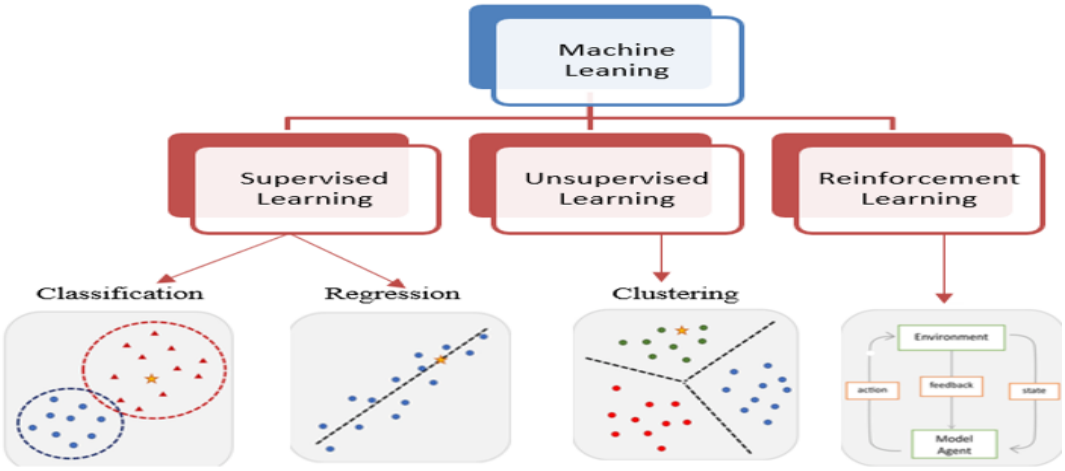

Figure 1: Types of Machine Learning

- Supervised Learning: This model is trained with labelled data (e.g., known attack patterns and normal behaviour) to classify new data as either benign or malicious. Algorithms like Random Forest, Support Vector Machines (SVM), and Neural Networks etc.

- Unsupervised Learning: This approach uses unlabelled data to identify hidden patterns and outliers, making it useful for detecting unknown threats. Effective at identifying zero-day vulnerabilities and novel attacks not previously seen. Clustering methods like K-means, Hierarchical Clustering, and anomaly detection techniques.

- Reinforcement Learning: The system learns by interacting with the environment and adjusting its actions based on rewards or penalties [19]. Used to develop adaptive security systems that continuously improve their responses to evolving threats. Techniques such as Q-learning, Deep Q Networks (DQN), and Policy Gradient methods.

4.2 Behavioral Analytics in Cybersecurity

Behavioral analytics focuses on examining the actions and patterns of users and systems to identify anomalies that might indicate security threats shown in figure2.

- User and Entity Behavior Analytics (UEBA): UEBA tools track users' behaviors and create a baseline of what is considered normal activity. Any deviation from this baseline can trigger alerts for potential threats.

- Insider Threat Detection: Analyzing patterns such as unusual access to sensitive data or abnormal login times can help identify insider threats that might otherwise go undetected.

4.3. Threat Intelligence Sharing

Threat intelligence sharing refers to the exchange of threat data between organizations and cybersecurity providers to enhance detection and improve response times [20].

Four categories of Cyber Threat Intelligence (CTI) shown in figure3.

- Strategic: Intelligence gathered from public or open sources to provide a high-level view of threats.

- Operational: Focuses on specific cyber attacks, events, or campaigns.

- Tactical: Provides details on the tactics, techniques, and procedures (TTPs) used by threat actors.

- Technical: Derived from internal resources, offering specific technical indicators like IP addresses or malware signatures.

4.4 Blockchain for Cybersecurity

Blockchain, the technology behind cryptocurrencies, is gaining attention for its potential to bolster cybersecurity by enhancing data integrity and transaction security.

Cybersecurity Improvement in Blockchain:

- Immutable Ledgers: Once data is recorded on a blockchain, it cannot be altered, preventing tampering, and ensuring the integrity of transaction logs.
- Transparent Audit Trails: Blockchain allows for an immutable, transparent record of all transactions, which aids in detecting unauthorized activities and providing accountability.
- Secure Transactions: Blockchain's cryptographic techniques ensure secure communication and transactions, minimizing risks such as data breaches.

5. COMPARISON OF THREAT DETECTION TECHNIQUES

The Performance summary of traditional threat detection methods based on different parameters is represented graphically as shown in figure 2.

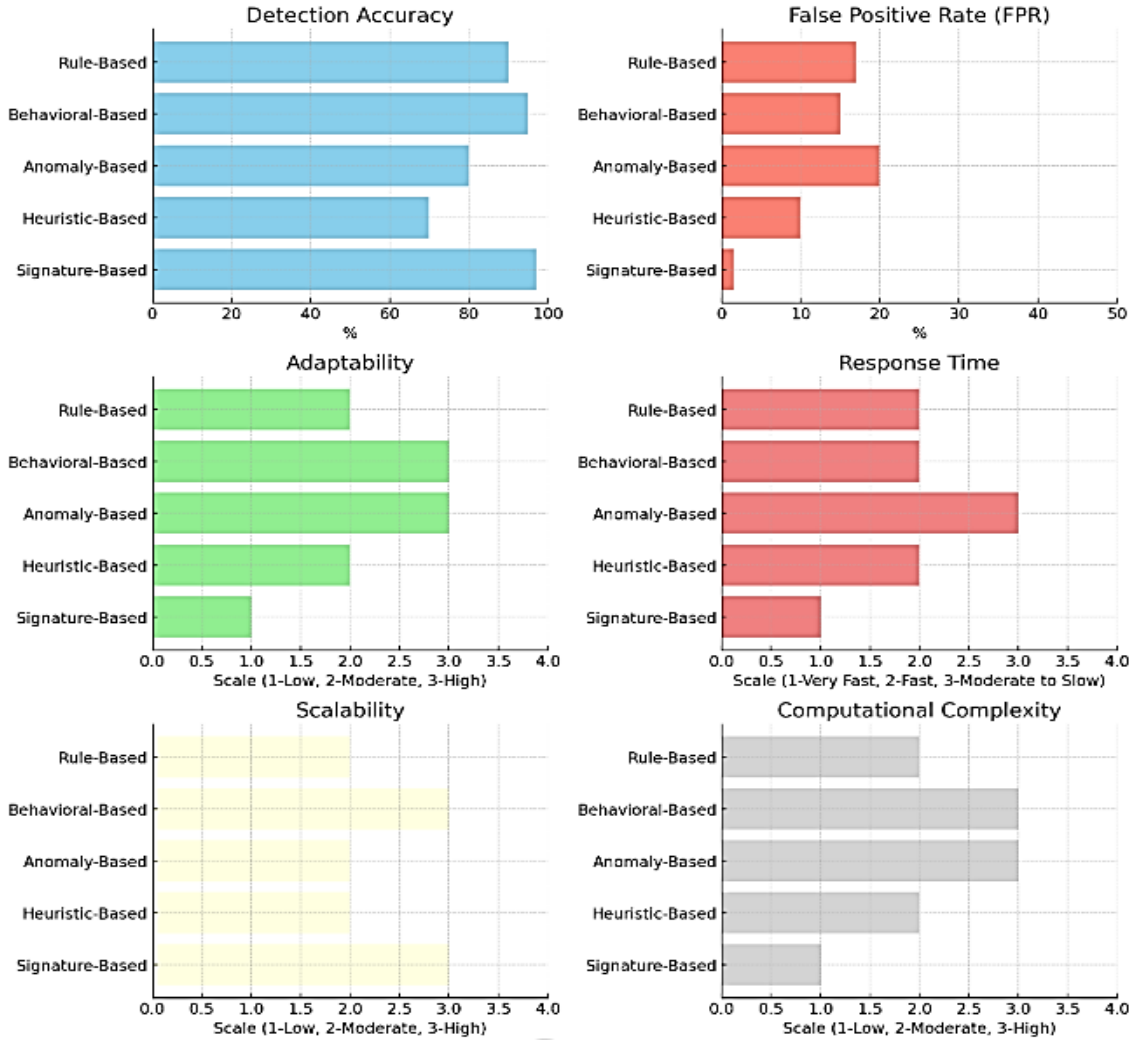

Figure 2: Graphical representation of traditional threat detection methods

The performance summary of emerging threat detection trends based on different parameters is shown in figure3.

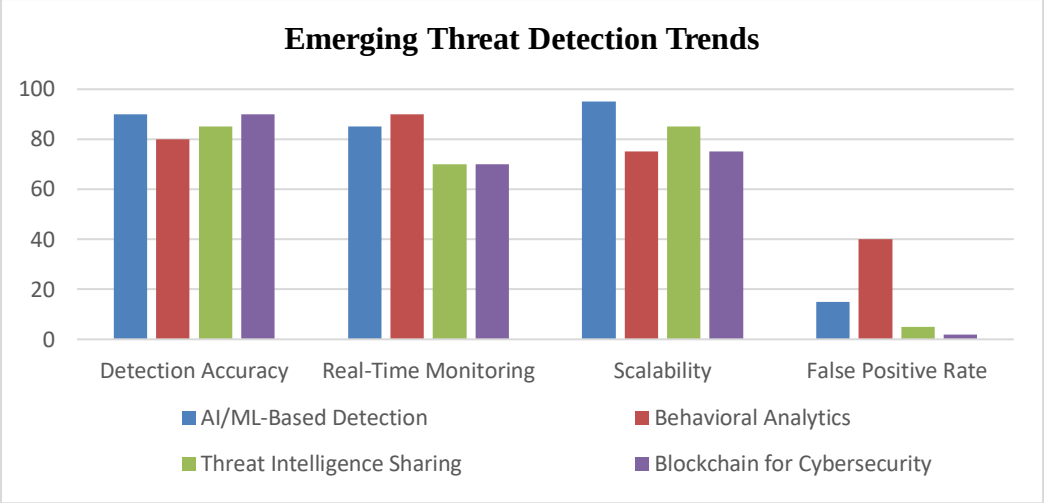

Figure 3: Graphical representation of emerging threat detection trends

6. CHALLENGES AND FUTURE DIRECTIONS

As cybersecurity threats become increasingly complex, organizations must address several challenges to maintain effective protection. This section explores the major obstacles in improving threat detection methods, while also highlighting the future trends that may shape the field.

6.1 Threat Detection Challenges

Changing Nature of Cyber Threats

- **Advanced Persistent Threats (APTs):** APTs are particularly challenging due to their covert, long-term nature, often exploiting vulnerabilities that are not immediately detectable. This requires adaptive detection systems and constant monitoring.
- **Insider Threats:** Identifying malicious insiders who misuse their privileges remains difficult, as traditional perimeter defenses do not account for internal risks. Advanced behavioral analysis and anomaly detection are needed to address this challenge.
- **Ransomware and Fileless Malware:** The rise of fileless malware, which operates solely in memory, and ransomware attacks complicate detection systems that rely on traditional signatures.

Limitations of Conventional Detection Methods

- **Signature-Based Detection:** While effective against known threats, signature-based detection

struggles with unknown attacks and polymorphic malware. This method requires regular updates to databases, and there is often a delay in detecting threats in real-time.

- **Heuristic and Behavioral Detection:** Though more advanced than signature methods, heuristic and behavioral analysis often suffer from high false-positive rates and the challenge of balancing accuracy and performance.

Data-Related Challenges

- **Overwhelming Data Volume:** The vast amount of cybersecurity data, such as network traffic logs and user behavior data, can overwhelm traditional security systems. Big data analytics and machine learning may help, but they demand significant computational resources and fine-tuning.
- **Data Privacy Concerns:** The need to collect and analyze more user and network data raises concerns about data privacy and regulatory compliance. Ensuring an appropriate balance between effective detection and privacy protection is crucial.

Adapting to Emerging Technologies

- **IoT and Edge Computing:** The increasing number of IoT devices and edge computing systems creates

new security challenges, including protecting devices with limited resources and mitigating large-scale DDoS attacks.

- **Cloud Security:** As more organizations move to the cloud, securing cloud infrastructures from new types of threats, such as misconfigurations and multi-cloud attacks, remains difficult. Detection systems must evolve to monitor dynamic cloud environments.

- **5G Networks and SDN (Software-Defined Networking):** The expansion of 5G and SDN introduces both opportunities and challenges for cybersecurity. Although 5G offers increased speeds, it also broadens the attack surface, and SDN requires new detection and response strategies for virtualized systems.

AI and Reinforcement Learning in Cybersecurity

- **AI and Machine Learning:** AI-driven solutions, particularly those using machine learning and deep learning, have shown promise in detecting complex and emerging threats [21]. However, challenges remain in obtaining diverse training datasets, protecting AI models from adversarial attacks, and ensuring transparency in AI decisions.

- **Reinforcement Learning (RL):** RL has the potential to enhance cybersecurity by allowing systems to learn from interactions with their environment. However, challenges include the need for safe, simulated environments for testing and the high computational cost of training RL models.

Threat Intelligence Integration

- **Sharing Threat Intelligence:** Effective threat intelligence sharing across organizations and sectors is vital for collective defense. However, concerns over the security and privacy of shared data, as well as legal and regulatory issues, pose obstacles.

- **Real-time Threat Intelligence:** Integrating real-time threat intelligence into detection systems can significantly improve response times and accuracy. The challenge lies in effectively correlating and analyzing data from diverse sources.

Human Factors in Cybersecurity

- **Shortage of Skilled Professionals:** The cybersecurity industry faces a significant shortage of skilled workers, limiting the ability to deploy and manage advanced detection systems effectively. Continuous training and education in emerging technologies, such as AI, ML, and cloud security, are essential.

- **Human Behavior and Awareness:** Despite technological advancements, human error continues

to be a major contributor to cybersecurity breaches. Enhancing user education and incorporating

user behavior analytics into detection systems can help mitigate this risk.

6.2 Future Directions

- **Quantum Computing:** As quantum computing advances, it will not only present new threats, such as breaking existing encryption techniques, but also offer opportunities to develop more secure cryptographic systems and advanced detection methods.

- **Zero Trust Architectures:** The shift to Zero Trust models, which assume no user or device is inherently trustworthy, will likely play a central role in the future of threat detection. These models continuously verify the trustworthiness of users and devices, reducing the attack surface.

- **Decentralized Security Systems:** The use of blockchain and distributed ledger technologies could lead to more secure, transparent methods of tracking cyber threats, particularly in areas like supply

chain security and authentication.

- **Predictive and Behavioural Analytics:** Combining historical data with predictive analytics will

enable more proactive detection of emerging threats by identifying unusual patterns before they lead to major damage.

7. RESULTS AND DISCUSSION

The effectiveness of the presented model is validated using several performance measures and it is associated with some existing datasets such as Network Attack Dataset, an IoT-specific attack dataset (Rt-IoT), and the UNSW-NB15 to estimate its effectiveness in categorizing various network traffic.

Performance Evaluation

The proposed network attack detection system performance was assessed using numerous key metrics like accuracy, precision, recall, specificity and F1-Score. These metrics offer a complete understanding of the replica's capability to categorize network traffic accurately and efficiently. Thus, the results obtained through simulation are exposed in the following table2 and 3. The graphical representation is shown in figure 4 and 5.

Table 2: Types of attacks obtained from the datasets based on different parameters

Parameters /Attack Types	Accuracy	Precision	Recall	Specificity	F1-Score
Blackhole	95.136778	93.939394	90.2913	97.345133	92.0792
Diversion	95.136778	91.25	89.0244	97.165992	90.1235
Port Scan	97.568389	95.333333	99.3056	96.216216	97.2789
Arp_Poisioning	99.985635	99.872041	99.936	99.989649	99.904
Dos_Syn_Hping	99.995212	99.994713	100	99.94929	99.9974
Nmap_Xmas_Tree_Scan	99.990423	100	99.5122	100	99.7555
Dos	93.222956	52.774632	55.5423	96.145313	54.1231
Exploits	91.464356	76.89312	79.4013	94.330608	78.1271
Fuzzers	96.697263	88.099467	79.8069	98.713271	83.7484
Normal	100	100	100	100	100

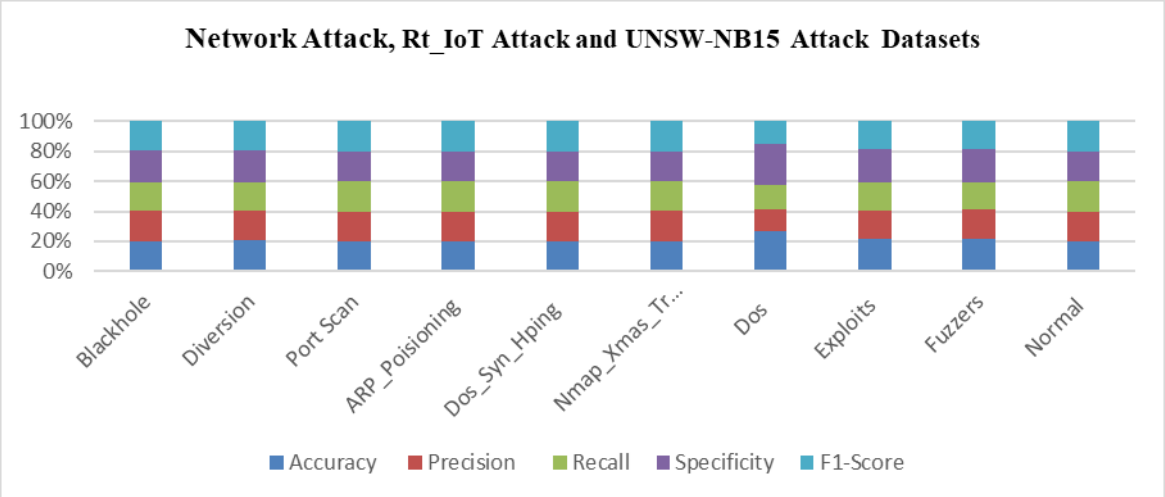

Figure 4: Graphical representation of types of attacks obtained from the datasets

Table 3: Performance comparison across various datasets with proposed system

Parameters	**Accuracy**	**Precision**	**Recall**	**Specificity**	**F1-Score**
Proposed System	99.938776	99.787794	99.7857	99.964276	99.786
Network	95.947315	93.507576	92.8737	96.909114	93.1605
Rt-IoT	99.990423	99.955585	99.8161	99.979646	99.8856
UNSW_NB15	95.346144	79.441805	78.6876	97.297298	78.9996

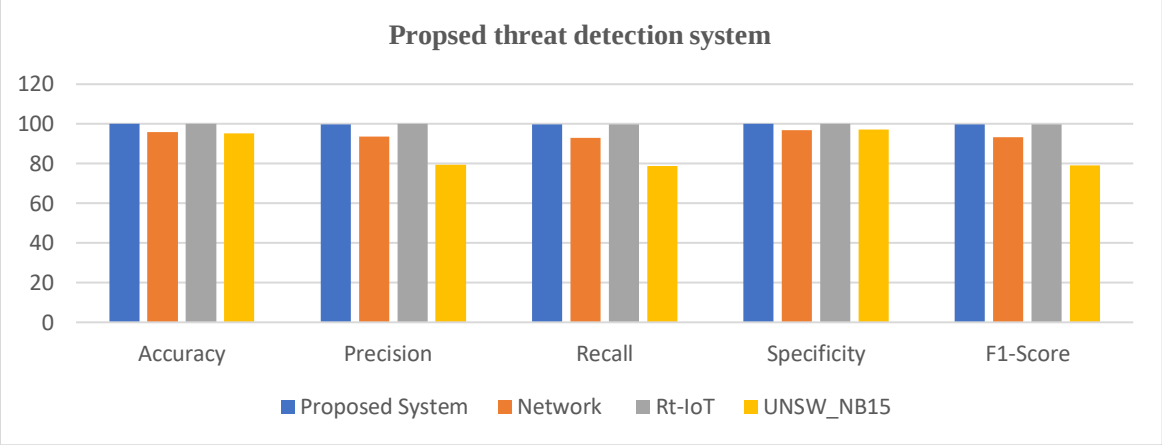

Figure 5: Overall performance comparison across various datasets with proposed system

The comparative analysis highlights that while traditional threat detection methods provide robust solutions for known threats, they are increasingly inadequate for new and sophisticated attacks. Anomaly-based methods are valuable for detecting unknown threats but suffer from high false positives and computational demands. Heuristic-based methods offer a balanced approach but are limited by static rules and maintenance needs. Hybrid methods integrate various techniques to offer comprehensive detection but face challenges related to complexity and resource requirements.

Emerging trends such as machine learning integration and synthetic data generation present promising solutions for addressing the limitations of current methods. Future research should focus on leveraging these advancements to develop more adaptive, scalable, and efficient cybersecurity threat detection systems.

8. CONCLUSION

The growing sophistication and frequency of cyber threats necessitate advanced and adaptive cybersecurity solutions that surpass traditional signature-based and rule-based detection methods. This study underscores the importance of AI-driven approaches, particularly machine learning and deep learning, in strengthening threat detection capabilities. By evaluating the proposed Intrusion Detection System (IDS) across multiple datasets—including the Network Attack Dataset, Rt-IoT, and UNSW-NB15—the system demonstrated notable improvements in accuracy, precision, recall, and F1-score, achieving up to 99.99% accuracy for IoT-specific attacks. These results highlight the effectiveness of AI-based IDS models in identifying and mitigating cyber threats across diverse network environments.

However, challenges such as scalability, adaptability to evolving attack strategies, and efficient handling of diverse datasets persist. Future research should focus on enhancing the resilience and adaptability of AI-powered IDS solutions to proactively counter emerging cyber threats. Addressing these issues will

contribute to the development of more robust and real-time security mechanisms, ensuring stronger protection in an increasingly digital landscape.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

Data availability

None.

Author's contribution statement

Rakhi Kalantri: Conceptualization, investigation, writing–review and editing.

Dr. Rajesh Bansode: Conceptualization, investigation, and supervision.

References

[1] S. Sibi Chakkaravarthya, D. Sangeethab, M. Venkata Rathnamb , K. Srinithib and V. Vaidehi, "Futuristic cyber-attacks," International Journal of Knowledge-based and Intelligent Engineering Systems ISSN 1327-2314,2018 DOI 10.3233/KES-180384.

[2] Jitendra Jain and Dr. Parashu Ram Pal, "A Recent Study Over Cyber Security and its Elements," International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017.

[3] Branka Stojanovic, Katharina Hofer-Schmitz and Ulrike Kleb, "APT Datasets and Attack Modeling for Automated Detection Methods: A Review," Computers & Security,2020, https://doi.org/10.1016/j.cose.2020.101734.

[4] Nektaria Kaloudi and Jingyue Li, "The AI-Based Cyber Threat Landscape: A Survey," ACM Computing Surveys, Vol. 53, No. 1, Article 20. February 2020.

[5] Afsheen Ahmed, Rabia Latif, Seemab Latif, Haider Abbas & Farrukh Aslam Khan, "Malicious insiders attack in IoT based multi-Cloud e-Healthcare environment: A Systematic Literature Review," Multimed Tools Appl, Springer,January 2020, https://doi.org/10.1007/s11042-017-5540-x.

[6] Yingzhou Lu, Minjie Shen, Huazheng Wang, Xiao Wang§ , Capucine van Rechem , Wenqi Wei ," Machine Learning for Synthetic Data Generation: A Review", Journal of Latex Class Files, Vol. 14, No. 8, August 2021.

[7] Nektaria Kaloudi and Jingyue Li, "Deep learning approaches for detecting DDoS attacks: a systematic review," Soft Computing, Springer ,2020, https://doi.org/10.1007/s00500- 021-06608-1.

[8] Iqbal H. Sarker, Md Hasan Furhad and Raza Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," SN Computer Science, Springer Nature, ,2021, 2:173 https://doi.org/10.1007/s42979-021-00557-0.

[9] Haonan Yan, Xiaoguang Li, Wenjing Zhang, Rui Wang, Hui Li, Xingwen Zhao, Fenghua Li and Xiaodong Lin, "Automatic Evasion of Machine Learning-Based Network Intrusion Detection Systems," IEEE Transactions on Dependable and Secure Computing,2023, DOI 10.1109/TDSC.2023.3247585.

[10] Yuming Feng, Weizhe Zhang, Shujun Yin, Hao Tang, Yang Xiang and Yu Zhang, "A Collaborative Stealthy DDoS Detection Method based on Reinforcement Learning at the Edge of the Internet of Things," IEEE, Internet of things journal,2023, DOI 10.1109/JIOT.2023.3279615.

[11] Singh, A. & SharmaV., "Machine Learning Techniques for Anomaly Detection in Cybersecurity," IEEE Transactions on Information Forensics and Security, 18(1), 23-35,2023.

[12] Zhang, Y. & Lee J., "A Hybrid Intrusion Detection System Using Signature and Anomaly-Based Techniques," In Proceedings of the IEEE International Conference on Cybersecurity (pp. 102-110). 2022.

[13] Kim, H. & Park S., "Reinforcement Learning for Adaptive Cyber Defense," ACM Computing Surveys, 54(3), 45-78,2021.

[14] Jiang, M. & Zhai F., "A Review of Real-Time Threat Intelligence for Cybersecurity," Journal of Cybersecurity, 10(2), 78-95,2022.

[15] Cheng, X. & Li Y., "Scalable and Decentralized Collaborative Threat Detection in IoT Networks," IEEE Internet of Things Journal, 8(5), 2334-2349,2021.

[16] Alam, S. & Khan N., "Synthetic Data Generation for Cybersecurity: A GAN-Based Approach," Cybersecurity and

Privacy, 2(1), 17-30,2023.
[17] Pinto, A. & Gupta R., “Federated Learning in Cybersecurity: A New Paradigm for Distributed Threat Detection,” Journal of Information Security and Applications, 58, 102701,2021.
[18] Sarker, I. H. “AI-Driven Cybersecurity: An Overview of AI Applications for Cyber Defense,” IEEE Access, 10, 71442-71466,2022.
[19] Xu, W. & Feng Y., “Anomaly Detection in IoT Using Reinforcement Learning: Challenges and Solutions,” Future Generation Computer Systems, 115, 494-505,2021.
[20] Cui, L., & Liu, F., “Adaptive Intrusion Detection Systems Based on Reinforcement Learning: A Comprehensive Review." Computers & Security, 96, 101901,2020.
[21] Seymour, E. & O’Donnell M., “Using Natural Language Processing to Extract Real-Time Threat Intelligence,” Journal of Cybersecurity Research, 5(2), 88-101,2021.

Rakhi A. Kalantri is a Research Scholar in Department of Information Technology, Thakur College of Engineering and Technology, Mumbai and Assistant Professor in Computer Engineering at Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai. She has completed her M.E. Computer Engineering in 2013. She has more than 22 years’ experience in the field of academics. She has published around 36 papers in International Conferences and Journals. Her research area includes Cyber security, Artificial Intelligence, Robotics, IOT etc.

Email: rakhi.kalantri@fcrit.ac.in

Dr. Rajesh Bansode, is a Professor and Head of Department of Information Technology, Thakur College of Engineering and Technology, Mumbai. He received B.Tech in Electronics and Communication from J.N.T.U Hyderabad in 1999. He received his MTech from DAVV Indore.in 2001. He received his Ph.D. in Information Technology from SGBAU Amaravati in 2016.His research interest include Network Security, Wireless Communication in MIMO OFDM, Light Weight Cryptography.

Email: rajesh.bansode@thakureducation.org