Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

An Enhanced Mechanism for Advanced Persistent Threat (APT) Detection based on DeepLearning

Najaf Saeed[1]
Department of Software Engineering Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
nnjfali44@gmail.com
Muqaddas Yaqub[2]
Department of Software Engineering Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
muqaddasyaqub67@gmail.com
Ali Haider[3]
DELL SecureWorks. digitaleyeali@yahoo.com
Saman Safdar[4]
Computer Science Department, COMSATS University Islamabad, Lahore Campus. samansafdar@ciitlahore.edu.pk
Hamayun Khan[5]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Abstract

In recent years, Advanced Persistent Threat (APT) attacks on network systems have increased through sophisticated fraud tactics. Traditional Intrusion Detection Systems (IDSs) suffer from low detection accuracy, high false-positive rates, and difficulty identifying unknown attacks such as remote-to-local (R2L) and user-to-root (U2R) attacks. APTs are a big challenge for modern cybersecurity. They are stealthy, persistent, and always evolving. This study reviews the best methods for APT detection and

Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

mitigation. It focuses on machine learning (ML), deep learning (DL), and Explainable AI (XAI). It also covers proactive strategies like Data Backup and Recovery (DBAR). ML and DL methods show high accuracy and adaptability. However, they struggle with evolving threats, dataset biases, and high computational demands. XAI boosts model interpretability, building trust in AI systems. DBAR ensures strong recovery but has strict infrastructure needs. The findings stress the need for dynamic datasets and scalable solutions. They also call for hybrid frameworks that integrate detection, explainability, and mitigation. Fixing these gaps will enable strong, adaptable cybersecurity. It can then combat the rise of APTs. This paper also suggests future research directions to combat evolving threats, paving the way for more effective and reliable cybersecurity solutions. Overall, this paper emphasizes the importance of explainability in enhancing the performance and trustworthiness of cybersecurity systems.

Keywords: Advanced Persistent Threats, Machine Learning, Deep Learning, Explainable AI, Cybersecurity

Introduction

Introduced Advanced Persistent Threats (APTs) are a type of stealthy, long-term cyberattack. They aim to infiltrate targeted networks. APTs differ from conventional attacks. Those aim to disrupt with speed. APTs focus on extracting sensitive data or sabotaging operations over time. These attacks, linked to rich foes like nation-states and cybercriminals, challenge modern cybersecurity [1]. APTs use advanced tactics, techniques, and procedures (TTPs) to evade traditional security measures. These include zero-day exploits, spear phishing, lateral movements, and advanced evasion techniques. Their ability to blend with real traffic

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

makes them hard to detect by static intrusion detection systems (IDS) and firewalls. Undetected APTs can cause data breaches and financial loss. They can damage reputations and threaten national security. So, we must develop smart, dynamic detection systems [2, 3]

Proposed Machine learning (ML) and deep learning (DL) based techniques are widely used tools for APT detection. They help tackle their complexities. ML models, like decision trees and Bayesian networks, excel at finding anomalies in network traffic. However, DL models have outperformed traditional ML techniques, especially in complex cases [4, 5].

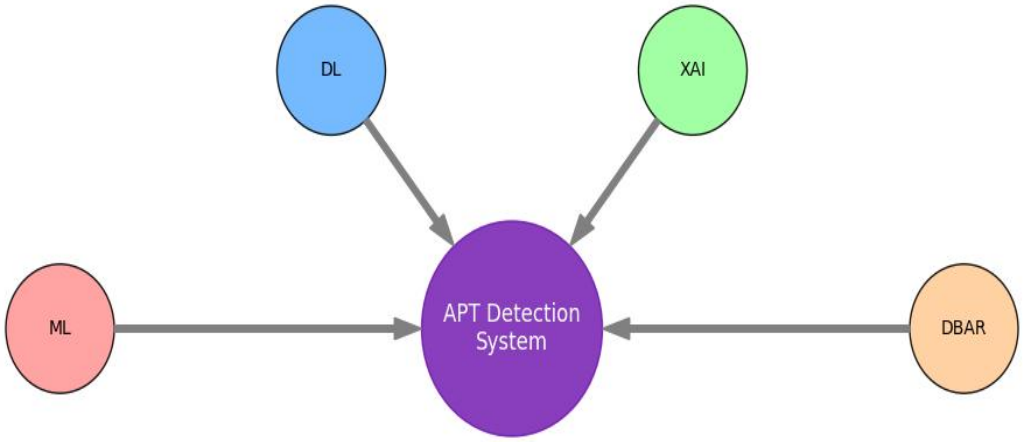


Figure 1. Architecture of APT Detection Systems [6]

They did this by using advanced feature extraction and multi-layered architectures. For instance, DL-based autoencoders are very accurate. They detect APTs in dynamic environments, like cloud systems [7, 8]. Deep reinforcement learning (DRL) boosts APT detection. It attributes malware to specific threat groups. DRL models analyze behavioral data to improve detection accuracy. They show great promise in handling evolving malware patterns but a key challenge of DL models is their lack of interpretability.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

This is often called the "black box" problem. This limits trust in AI-driven decisions, especially in high-stakes environments [9-12]. Explainable AI (XAI) addresses this gap by improving model transparency. Techniques like SHAP and LIME show how features affect detection results. Integrating XAI lets cybersecurity experts understand and improve AI models. This will build trust and collaboration between human analysts and AI. In cybersecurity, explainability is critical. We need actionable insights for a quick response to new threats. The proposed architecture integrates ML, DL, XAI, and DBAR components [13- 16]. In addition to detection, mitigation strategies play a crucial role in APT defense. DBAR mechanisms offer a way to reduce the impact of APTs. They do this by backing up data and recovering it. DBAR automates restoring compromised systems to their pre-attack states. It ensures business continuity and cuts downtime and recovery costs [18, 19].

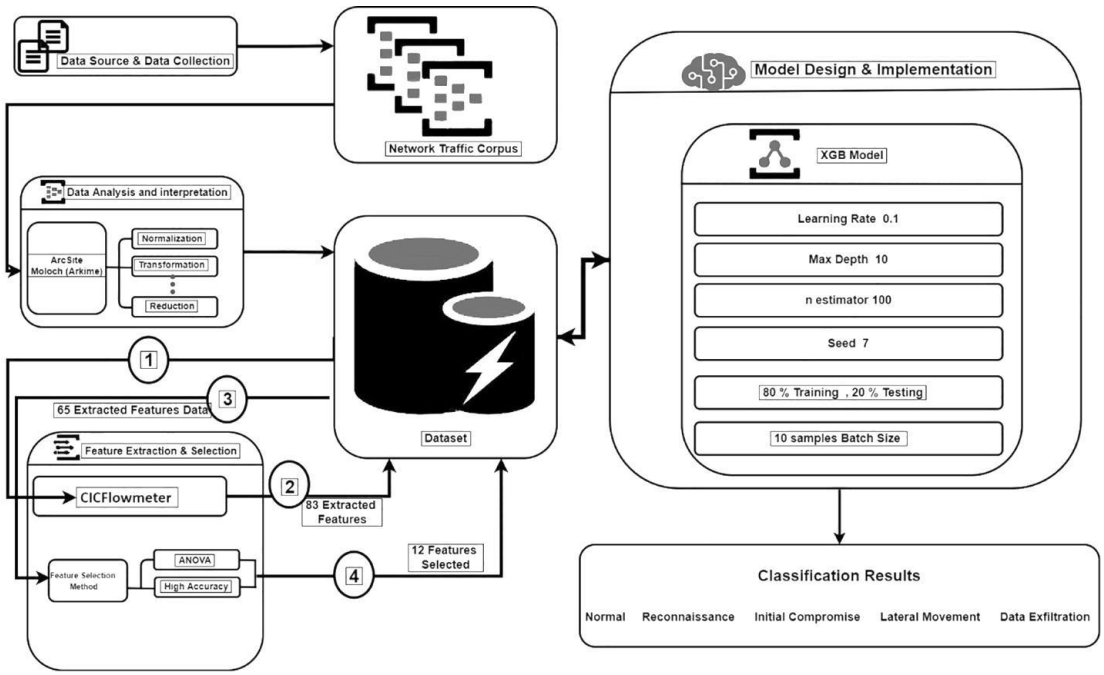


Figure 2: Modern Architectures used for APT Detection [20]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

This review consolidates findings from six key studies. They explore ML, DL, XAI, and advanced frameworks for APT detection and defense. This research aims to provide a full understanding of APT detection technologies. It will highlight their strengths, limits, and uses. It will also inform future research. This paper stresses the need for better detection technology. It also calls for proactive strategies to combat rising cybersecurity threats [21, 23].

Literature Review

APTs are a major threat to modern cybersecurity. They are very sophisticated and stealthy. To address these challenges, researchers have explored various methods. They incorporate machine learning (ML), deep learning (DL), and Explainable AI (XAI). This section reviews the key contributions of these technologies. It focuses on their applications, strengths, and limits in APT detection and mitigation [25, 26]. Introduced Machine learning (ML) and deep learning (DL) based techniques like decision trees and Bayesian networks excel at spotting known threats. They offer high accuracy and work in real-time. However, their reliance on labeled datasets limits them and this makes them less effective for identifying novel attacks [27, 28]. DL methods, like autoencoders and reinforcement learning, address this gap. They analyze complex and evolving attack patterns. Autoencoders, for example, excel at feature extraction and reducing dimensions. They detect APTs with high accuracy in dynamic cloud environments. Deep reinforcement learning (DRL) can adapt to evolving malware. It can also link malware to specific APT groups. These approaches are powerful but their high computational demands and reliance on large datasets pose challenges [29, 30]. Explainable AI (XAI) improves the interpretability of ML and DL models. It addresses the "black box"

Vol. 3 No. 1 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

problem. Techniques like SHAP and LIME show feature importance. They help analysts trust AI decisions. This transparency is crucial in high-stakes scenarios where actionable insights are essential. However, XAI frameworks often increase system complexity and costs. This makes deployment in resource-constrained environments challenging [31].

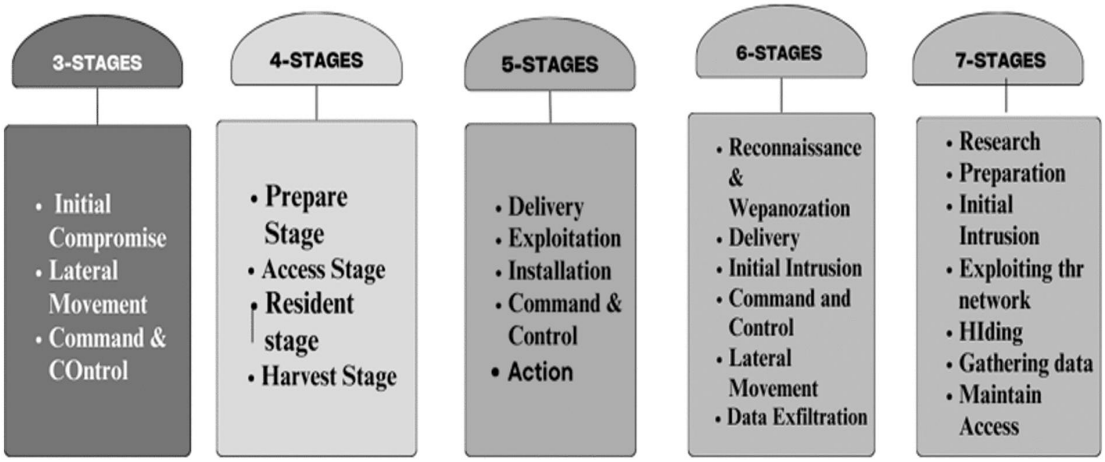


Figure 3: APT lifecycle [32]

Proactive measures, like DBAR, reduce the impact of successful APTs. They do this by complementing detection mechanisms. DBAR automates the recovery process, restoring systems to pre-attack states and eliminating backdoors. Proposed DBAR strategies. They used SDN for better recovery and lower costs. These strategies are effective. But, they need advanced infrastructure. This limits their use in legacy systems [33]. A unified framework that combines ML, DL, XAI, and DBAR gives a complete approach to APT defense. Such frameworks combine the strengths of individual methods. They ensure robust detection, interpretability, and recovery. We must solve compatibility issues and trade-offs to integrate [34].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 1: Comparative Analysis on XAI based APT detection [35]

Year	Objective	Motivation
2024	Provide an extensive analysis of XAI based cybersecurity modeling in digital twin (DT) environments, focusing on the methods, taxonomy, challenges, and prospects.	The industrial transformation heavily relies on AI, including machine learning and data-driven technologies, to enable tasks such as self-monitoring, investigation, diagnosis, future prediction, and decision-making.
2023	Examined the different approaches used to detect APT attacks directed at the network system in terms of approach and assessment metrics	Traditional cyber defense mechanisms often fail to detect APTs due to their sophisticated nature and the rapid evolution of attack patterns. This detection failure underscores the need for more advanced and adaptive detection techniques.
2022	Analyzed APT defense mechanisms were presented as a systematic literature review (SLR).	Limited resources, along with minimal storage capacity, limited computing power as well as specific energy resources, make smartphones lack built-in security and privacy protection.
2021	Discussed the feature representations, extraction techniques and ML models used in the reviewed studies.	To deal with limitations of dataset availability, lack of (1) devices, (2) security, and (3) software standards, model complexity, evasion methods, and others.
2020	Analyzed datasets and descriptions utilized in the APT detection literature and feature extraction techniques employed in APT detection-related literature.	Advanced threats are very complex. This makes it hard to create models of attacks for training and testing.
2024	This review aims to identify deep learning techniques integrated with XAI, assess the interpretability of existing research, and pinpoint the specific XAI methods utilized in the cybersecurity domain to enhance explainability and transparency.	To enhance the effectiveness and transparency of APT detection systems. As APTs become increasingly sophisticated, traditional detection methods often fall short in terms of accuracy, interpretability, and the ability to identify novel or early-stage attacks.

Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

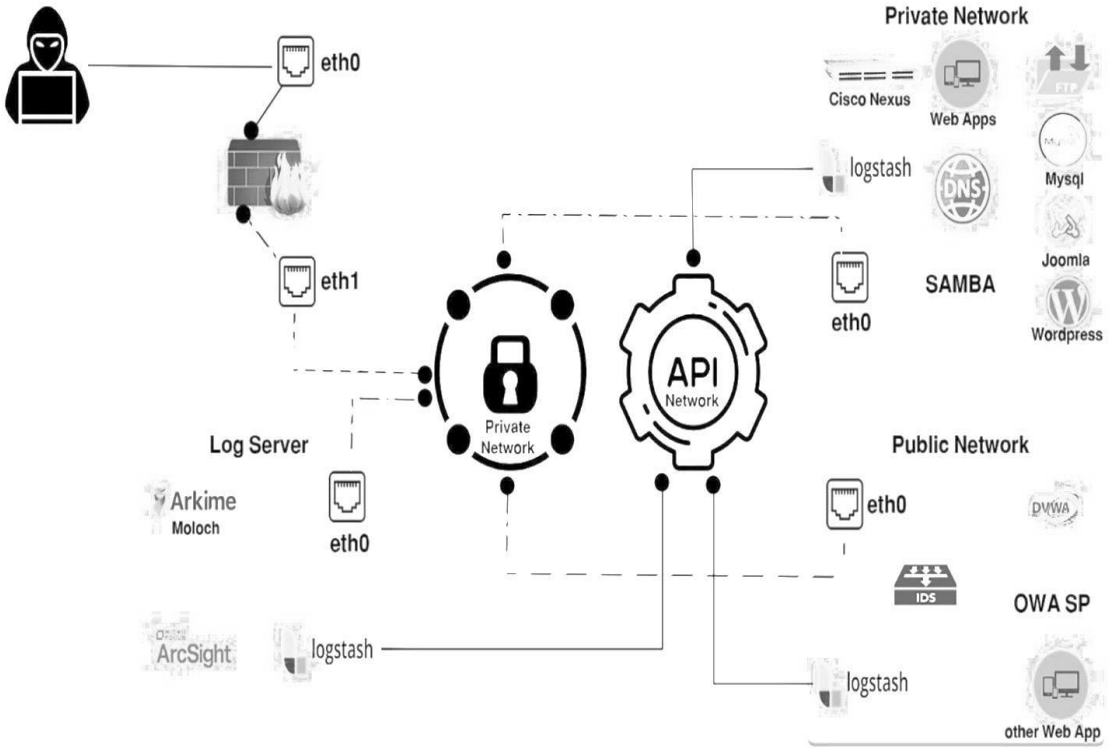


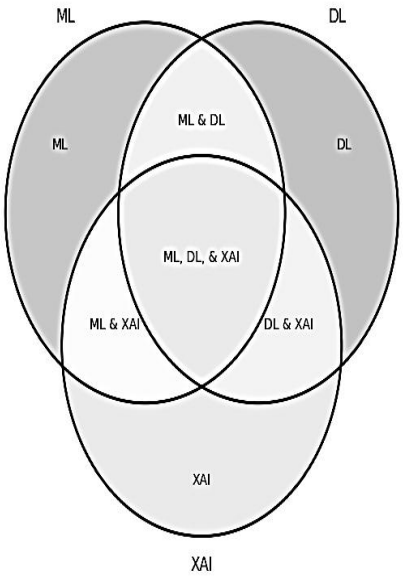
Figure 3: Widely Used Data Collection mechanism for APT Detection [36]

Table 2: Comparison of approaches [37]

Approach	Strengths	Limitations	Ref
Machine Learning	High accuracy, real-time detection	Dataset biases	[38]
Deep Reinforcement Learning	Adaptability to evolving threats	High computational demands	[38]
Explainable AI	Improved trust and interpretability	Complexity in implementation	[39]
DBAR Mechanism	Automated recovery, cost-effectiveness	Requires SDN integration	[40]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Approach	Strengths	Limitations	Ref
API Security Framework	Minimized false negatives, scalability	Dataset quality issues	[41]
Auto encoder Models	High accuracy, feature extraction	Limited real-time adaptability	[42]



Technique	Key Attributes
ML	High Accuracy, Real-Time Detection
DL	Dynamic Analysis, Novel Attack Detection
XAI	Interpretability, Actionable Insights
ML & DL	Novel Attack Detection
ML & XAI	Improved Trust, Actionable Insights
DL & XAI	Feature Analysis, Interpretability
ML, DL, & XAI	Comprehensive Detection, Transparency

Figure 4: Contributions of ML, DL, and XAI in APT Defense [42]

Figure 4 summarizes the contributions of ML, DL, and XAI in addressing APT detection. It shows their strengths, overlaps, and potential to build strong cybersecurity systems.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 3: Comparison of Approaches [43]

Application	Method	Dataset	Accuracy%	Precision%
Network Intrusion Detection	Gradient descent-based flow filtering, autoencoders, 1D-CNN	Virtual Network Traffic Artifacts, KDD99	98.9 and 99.97	-
Biomedical Data Security	Threat-vector database, improved SRU network	Various healthcare datasets	-	-
Malware Detection	XAI methods (SHAP, LIME, LRP, Attention)	Diverse datasets	99.43	95.69
APT Threat Detection	Boosting-based ML, XGBoost with SHAP	SCVIC-APT-2021	97	97
Cybersecurity	TRUST XAI, multimodal Gaussian distributions	WUSTL-IIoT, NSL-KDD, UNSW	97.77–99.98	-
Cyber Threat Discovery in IIoT Networks	Autoencoder, convolutional, recurrent networks	ToN_IoT	98	-
Cybersecurity in IoMT	Bidirectional SRU, XSRU-IoMT	ToN_IoT	99.38	99.39

Method & Materials

This study uses a systematic literature review (SLR). It reviews the latest deep learning methods. They detect and reduce Advanced Persistent Threats (APTs). The SLR framework ensures a complete and unbiased review of relevant studies. It focuses on key advancements, methods, and challenges in this field. The following research questions (RQs) guide this review:

- RQ1: What are the main machine learning and deep learning techniques for APT detection?
- RQ2: How do XAI methods improve the trust and understanding of APT detection models?
- RQ3: What proactive strategies exist for mitigating APT impacts, like DBAR?
- RQ4: What are the limits of current methods? How can future research address them?

We used various search phrases and keywords to avoid bias and ensure coverage. Researchers used Boolean operators, such as AND, OR, and NOT, to improve the search for studies. The search terms used included combinations such as:

- “Advanced Persistent Threat” AND

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

- "Deep Learning" OR
- "Explainable AI" AND
- "Machine Learning" OR
- "Data Backup and Recovery" AND
- "Cybersecurity"

The search strategy involved querying several academic databases. These were IEEE Xplore, SpringerLink, ACM Digital Library, and ScienceDirect. This approach ensured that researchers considered a wide range of studies.

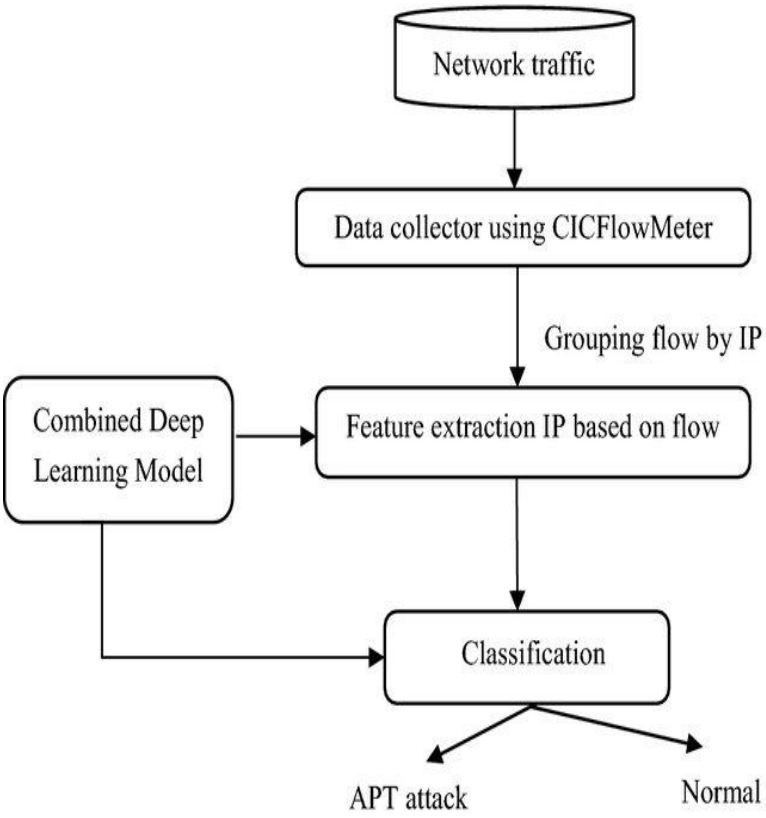


Figure 5: APT attack detection model using deep learning

Inclusion and Exclusion Criteria

To identify the most relevant studies, the following criteria were applied:

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Inclusion Criteria

- Studies published in peer-reviewed journals or conferences.
- Research focusing on APT detection and mitigation using ML, DL, or XAI.
- Papers published between 2020 and 2024 to ensure the inclusion of recent advancements.
- Availability of full-text articles in English.

Exclusion Criteria

- Studies without a clear focus on APT detection or mitigation.
- Duplicate publications across databases.
- Non-English articles or those without accessible full text.

We assessed each selected study's quality using a set of criteria. This included the research design, the results' validity, and the findings' relevance. We included studies that met these criteria in the final synthesis. This ensured the systematic review's reliability and validity. This section answers the study's research questions. It analyses key methods for detecting and mitigating Advanced Persistent Threats (APTs). It discusses their strengths and weaknesses.

RQ1: What are the main machine learning and deep learning techniques for APT detection?

Modern APT detection systems rely on ML and DL techniques. ML models, like decision trees and Bayesian networks, are popular for detecting network traffic anomalies. They are efficient and scalable. For instance, reported high accuracy using these models in real-time network intrusion detection scenarios. Their reliance on labeled datasets limits their effectiveness against zero-day threats. They cannot generalize to new attack patterns.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Deep learning models, like autoencoders and reinforcement learning frameworks, overcome these limits. They use neural networks to analyze complex, evolving attack behaviors. Showed that autoencoders can reduce data dimensionality and extract features in cloud environments. They achieved a 98.32% detection accuracy. Deep reinforcement learning to attribute malware to specific APT groups. It showed adaptability to evolving attack patterns. These advanced techniques, however, require significant computational resources and extensive training datasets.

RQ2: How do XAI methods improve the trust and understanding of APT detection models?

Deep learning models are accurate. But their "black-box" nature limits their acceptance among cybersecurity experts. Explainable AI (XAI) addresses this limitation by making model decisions interpretable and transparent. Techniques such as SHAP and LIME. This helps analysts trust and improve AI-driven detections. XAI bridges the gap between automated systems and human analysts. It ensures that AI-generated alerts are actionable and credible. This interpretability is vital in high-stakes settings. Clear reasoning is key to timely decisions. However, integrating XAI increases the complexity of system design and deployment.

RQ3: What proactive strategies exist for mitigating APT impacts, like DBAR?

Detection alone is insufficient for handling APTs; robust mitigation strategies are also essential. Data Backup and Recovery (DBAR) mechanisms, proposed by [38] provide a proactive defense by automating system recovery processes. DBAR restores hacked systems to their pre-attack state. It removes backdoors and cuts downtime. This approach works well in software-defined

Vol. 3 No. 1 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

networking (SDN) environments. Central management can optimize recovery operations to cut costs. DBAR's reliance on SDN integration may limit its use in legacy networks, despite its benefits.

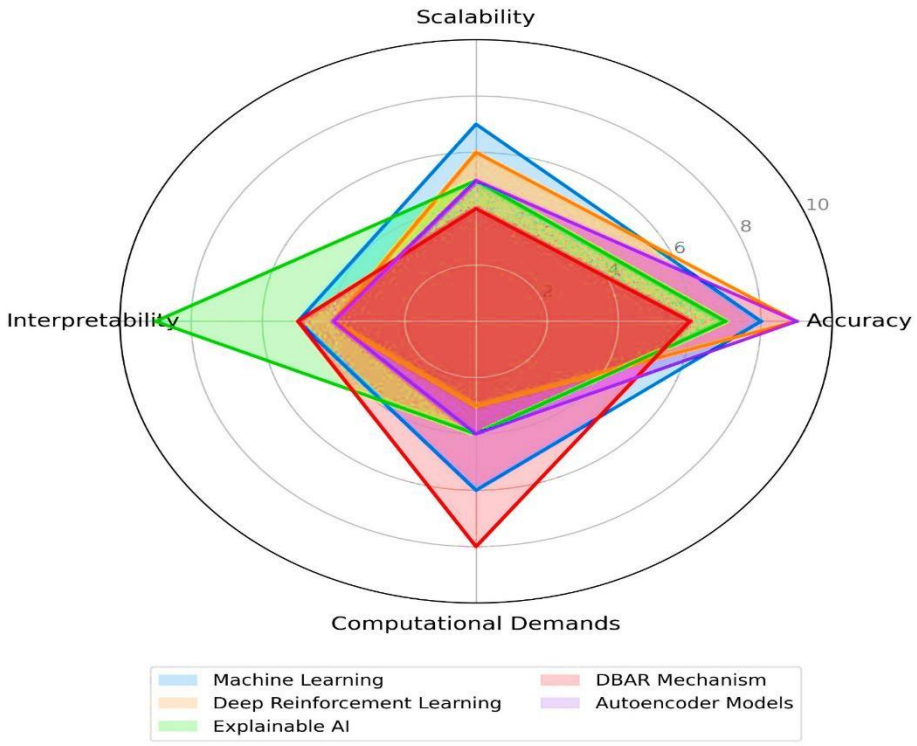


Figure 6: Comparison of approaches in APT detection [39]

Together, these methodologies underscore the need for a multi-layered defense strategy that combines detection, interpretability, and recovery to address the evolving landscape of APTs effectively.

RQ4: What are the limits of current methods? How can future research address them?

While ML and DL techniques excel in accuracy and adaptability, several challenges remain. ML models often suffer from dataset biases and struggle with zero-day threats. DL models can handle evolving attack patterns. However they need vast resources and large datasets for training. Additionally, the real-time adaptability of autoencoder models in dynamic environments remains a

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

limitation. Explainable AI improves interpretability. But it adds complexity to system design. This makes it hard to deploy in resource-constrained settings. Proactive strategies like DBAR are effective. But they need advanced networks, like SDN. Not all organizations can access them. Also, API security frameworks struggle with dataset quality and real-time use which limits their scalability. The comparative analysis highlights the diversity and complementarity of the reviewed approaches. Machine learning techniques are effective for real-time detection of known threats but are limited in handling novel attacks. Deep reinforcement learning and autoencoders provide adaptability and accuracy for complex threat detection but at the cost of computational efficiency. Explainable AI enhances decision-making by improving trust and transparency, while DBAR mechanisms ensure robust post-attack recovery. API frameworks and ML models are highly scalable but require improved datasets and real-time implementation capabilities.

Research Gaps

Current APT detection and mitigation methods have strengths in some areas. However, issues with adaptability, dataset quality, and efficiency limit them. They also lack interpretability, scalability, and integration. Addressing these gaps requires:

Developing real-time adaptive models that are capable of handling evolving threats.

- Creating dynamic and representative datasets for training robust models.
- Enhancing XAI frameworks to balance interpretability with scalability.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

- Adapting proactive strategies like DBAR for broader applicability.
- Integrating detection, explainability, and mitigation into unified frameworks.
- Optimizing computational efficiency for resource-constrained environments.

Bridging these gaps will enable better, more resilient cybersecurity. It will help combat evolving APTs with greater effectiveness. The findings stress the need to combine ML, DL, XAI, and proactive methods. This will improve APT detection and mitigation. ML excels at the real-time detection of known threats. DL adapts to new attacks. But limitations remain. They include dataset biases, high computing demands, and poor scalability. XAI improves AI system trust by making them easier to understand. However its complex implementation limits scalability. Proactive measures like DBAR can recover data well. But they need an SDN infrastructure. Fixing these gaps can result in significant improvements to cybersecurity. Use dynamic datasets, adaptive models, lightweight XAI, and scalable DBAR. Future research should focus on hybrid frameworks and federated learning for adaptability. It should also seek resource-efficient, accessible solutions for SMEs. We must collaborate with the industry to develop datasets and technologies. This is key to advancing the fight against APTs.

Limitations and Future Directions

Despite significant advancements, current methodologies for APT detection and mitigation face several limitations:

Dataset Constraints: Most models use static or simulated datasets. They do not reflect the dynamic nature of real-world attacks.

High Computational Demands: Deep learning models are

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

effective. But, they need vast computing power and large datasets. This makes them impractical for smaller organizations.

Complexity of Explainable AI: Adding XAI makes detection systems more complex. It may reduce their scalability.

Limited Scalability of Proactive Measures: Strategies like DBAR rely on advanced tech, such as SDN. This limits their use in legacy systems and low-resource environments.

Future Directions

To address these limitations, future research should focus on:

Dynamic and Representative Datasets: Developing real-time, large-scale datasets that capture diverse attack scenarios. Collaborative efforts between academia and industry can enhance dataset quality and availability.

Adaptive Models: Create models that can adapt to changing attack patterns. They should not need frequent retraining. We should explore techniques like federated learning and self-learning frameworks.

Simplified XAI Frameworks: Build lightweight, scalable XAI models. They must balance interpretability with efficiency.

Scalable Proactive Strategies: Expand DBAR mechanisms to work with non-SDN infrastructures. This will make them accessible to SMEs and legacy networks.

Hybrid Defense Systems: They integrate detection, explainability, and recovery into a unified framework. This provides a complete defense against APTs.

Resource Optimization: Developing low-computation models to enable effective deployment in resource-constrained environments.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Future work can improve APT detection and mitigation systems. It should boost their resilience and scalability to meet changing cybersecurity demands.

Conclusion

This study highlights the critical role of integrating machine learning, deep learning, Explainable AI, and proactive strategies in addressing the challenges posed by APTs. ML and DL models excel in accuracy and adaptability but are hindered by dataset biases, high computational demands, and real-time adaptability constraints. XAI bridges the gap between performance and interpretability, while DBAR mechanisms complement detection systems by ensuring post-attack recovery. The research underscores the need for dynamic, real-time datasets and hybrid defense frameworks that unify detection, explainability, and mitigation strategies. Future efforts should focus on developing resource-efficient models, scalable proactive measures, and adaptive learning techniques to address evolving threats effectively. Collaboration between academia, industry, and government agencies will be essential to create robust, scalable, and real-world applicable solutions. These advancements are critical for safeguarding critical infrastructure and sensitive data against the growing complexity of APTs.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.

[2] Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access, 8, 186125-186137.

[3] Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 55(5), 1-37.

[4] Mutalib, Noor Hazlina Abdul, et al. "Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review." Artificial Intelligence Review 57.11 (2024): 1-47.

[5] Yang, Lu-Xing, et al. "Defense against advanced persistent threat through data backup and recovery." IEEE Transactions on Network Science and Engineering 8.3 (2020): 2001-2013.

[6] Joloudari, Javad Hassannataj, et al. "Early detection of the advanced persistent threat attack using performance analysis of deep learning." IEEE Access 8 (2020): 186125-186137.

[7] Abdullayeva, Fargana J. "Advanced persistent threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm." Array 10 (2021): 100067.

[8] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[9] Ranjan, Piyush, and Sumit Dahiya. "Advanced threat detection in api security: Leveraging machine learning

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

algorithms." International Journal of Communication Networks and Information Security 13.1 (2021).

[10] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[11] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[12] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[13] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[14] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[15] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[16] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[17] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[18] Khan, A. Ali, S. Alshmrany, "Enery-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[19] Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

[20] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[21] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[22] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[23] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[24] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[25] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[26] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[27] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[28] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[29] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering siences, 2(3), 528-586.

[30] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 201

[31] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[32] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[33] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[34] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[35] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[36] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[37] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[38] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[39] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[40] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[41] Imran, M., Siddiqui, H. U. R., Raza, A., Raza, M. A., Rustam, F., & Ashraf, I. (2023). A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems. Computers & Security, 134, 103445.

[42] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[43] Maddireddy, B. R., & Maddireddy, B. R. (2023). Adaptive Cyber Defense: Using Machine Learning to Counter Advanced Persistent Threats. International Journal of Advanced Engineering Technologies and Innovations, 1(03), 305-324.