IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042. Volume 13, Issue 2 (Mar. – Apr. 2026), PP 10-16
www.iosrjournals.org

Going-Over Of The Advanced Persistent Threat (APT) Detection: Challenges Plus Future Research Directions.

Henry Peter Ovili
Department Of Information Systems &Technology
Faculty Of Computing
Southern Delta University, Ozoro

Promise A. Nlerum
Department Of Computer Science And Informatics, Federal University Otuoke (FUO),
Bayelsa State, Nigeria.

Abstract
Advanced Persistent Threats (APTs) represent a sophisticated class of cyberattacks characterized by stealth, persistence plus a targeted tactic aimed at conceding high-value assets. In October 2024, the originators of ChatGPT had publicized the interference of 20 'cyber plus covert influence actions' since the commencement of the year. Mostly, criminal clusters going in non-Western plus non-English speaking provinces can also adventure LLM platforms to yield credible phishing mails, an approach that a current Google Gemini bang has accredited to an Iranian APT cluster. (Abigail & Aryamehr , 2025). Outmoded signature-based intrusion detection systems (IDS) are increasingly unproductive against these embryonic threats. Thus, Artificial Intelligence (AI) have emerged as transformative machineries in behavioral APT detection, allowing systems to recognize anomalies and concealed attack patterns in real time. This paper offers a comprehensive review of recent AI methodologies, their incorporation in APT detection backgrounds and the allied challenges and future research guidelines.
Keywords: *Advanced Persistent Threats, Artificial Intelligence, security frameworks, Anomaly, Detection Analysis.*

Date of Submission: 01-03-2026 Date of Acceptance: 11-03-2026

I. Introduction

In October 2024, the originators of ChatGPT had publicized the interference of 20 'cyber plus covert influence actions' since the commencement of the year. Mostly, criminal clusters going in non-Western plus non-English speaking provinces can also adventure LLM platforms to yield credible phishing mails, an approach that a current Google Gemini bang has accredited to an Iranian APT cluster. (Abigail & Aryamehr , 2025)

The data illustrations that the amount of APTs has mounted progressively during this historical in 2022, this numeral stood at 424, mounting to 504 in 2025, signifying an inclusive growth of 18.9%. Whereas the development has been normally stable, the historical from 2023 to 2024 practiced the chief year-over-year jump, with episodes snowballing by 36 (≈8.0%).(Abigail & Aryamehr , 2025)

The escalation of advanced persistent threats (APTs) has noticeable a momentous cybersecurity contest, characterized by stylish orchestration, stealthy implementation, comprehensive persistence and aiming valuable assets across dissimilar sectors. Advanced Persistent Threats (APT) encompass multiple attack steps over a long period and their examination requires analysis of countless logs to identify their attack steps, which are a set of actions undertaken to run an APT attack. Yet, on a regular basis in an initiative, intrusion detection systems produce numerous threat alerts of suspicious measures (attack symptoms). Cyber analysts must examine such events to govern whether an event is a fragment of an attack. With numerous alerts to examine, cyber analysts often end up with alert lethargy, causing them to snub a large number of alerts and miss true attack events

II. Literature Review

In Yuntao W et al (2024) proposed an competent and robust APT defense structure leveraging provenance charts, comprising a network-level distributed audit prototypical for cost-effective cross attack reconstruction, a trust-oriented APT evasion behavior detection approach and a hidden Markov ideal based adversarial subgraph defense tactic. Through prototype execution and broad experiments, they validated the efficacy of our system and lastly, crucial open research directions are drawn in this emerging field.

Also, Alsaheel A. et al (2021) present ATLAS, a background that paradigms an end-to-end attack story from off-the-shelf audit logs.

By Nur I. et al (2024) highlighted the meaning of integrating multi-stage attack-related behaviors, vulnerability valuation and procedures of visualization for APT detection to improve the overall security of organizations.

Singamaneni & Sukhvinder (2024) stressed on the numerous detection approaches defined by dissimilar researchers along with the limitations of their effort. Data used in this commentary comes from the several annual reports available by security experts, blogs and information unrestricted by the enterprise networks besieged by the attack.

by Vaibhav M. et al (2024) comprehensively analyzed state-of-the-art APT detection procedures and mitigation plans by evaluate the efficiency of many detection approaches, especially network-based, host-based and AI-driven approaches. They equally proposed a multi-layered tactic for APT mitigation, while separate detection performances have specific strengths, a holistic tactic combining multiple approaches yields the most effective defense against APTs..

APTs are the top most cybersecurity trepidations in organization networks. In historical era, APT attack clashes like Ghostnet in 2009, Stuxnet in 2010 and Deep Panda in 2015 rose in large-scale data breaches such as stealthy data exfiltration throughout weeks or months, system impurity, integrity humiliation, denial-of-service plus damage to cyber-physical systems (D. Kushner.2013)

Najah Kalifah Almazmomi (2025) forwarded an optimized deep learning tactic that pools a Convolutional Neural Network - Long Short-Term Memory (CNN-LSTM) design by the lime mold algorithm (SMA) for better APT detection. Throughout the training, the SMA balances investigation and utilization fit, leading to faster merging and better enactment.

The surveyed paper delivered awareness about APT attacks and their indispensable steps that will generate clear evidence about the APT attack procedure and the countless detection approaches defined by dissimilar researchers alongside with the restrictions of the work. Data recycled in this artefact arises from the numerous yearly reports printed by security authorities and blogs and sign limitless by the initiative networks embattled by the attack. (Singamaneni & Sukhvinder, 2019)

Hope N, et al (2019) searched the use of Artificial Immune System (AIS) and Recurrent Neural Networks (RNNs) modifications for APT detection and the variants recommended algorithms that run not only detection competence, but can too categorize hateful data traffic with respect to the type of APT attacks. In the assessment Metrics, The true positive rate (TPR) plus false positive rate (FPR) endured used to evaluate the effectiveness of LSTM-RNN model:

✓True Positive (TP): abnormal cases correctly forecasted as abnormal.
✓True Negative (TN): normal cases correctly forecasted as normal
✓False Positive (FP): normal cases falsely predicted as abnormal
✓False Negative (FN): abnormal cases falsely predicted as normal

Manish K et al (2025) projected background leverages AI-driven behavioral analytics for initial anomaly detection, incorporating Zero-Trust philosophies to limit cross movement inside networks and underlines the significance of adaptive, multi-layered fortifications in fighting the developing APT background and bids legal awareness for edges looking for vigorous cybersecurity results.

Henry P, et al (2026) pondered on the efficacy of countless booth dealings, containing FIDO2/U2F hardware proofs and app-based authentication and user education creativities. By reviewing the style on both the threats plus the fortifications, they also targeted to proposal a clear unselfish of the lively interplay between phishing attacks plus 2FA structures.

Henry & Promise (2026) Pinned that XDR is considered as a functioning requirement, retaining AI and machine learning to unify telemetry over endpoints, networks desirable cloud atmospheres to shape a common attack chronicle and constitute rapid, liberal threat neutralization. They also determined that the integration of ZTA's exacting entry controls, Deception Technology's energetic counter-intelligence plus XDR's joint detection plus response bids a robust, adaptable plus multi-layered defense significant for battling the persistent background of radical cyber adversaries.

Advanced Persistent Threats (APTs)

It is a stealthy and unstoppable cyberattack that intruder gain unauthorized access over a network even while undetected for a given period of time which is normally accomplished by trained adversaries, arranged group of crime with a common goal of data theft, espionage and disruption of activities.

The features of APTs include:

i. Advanced: intruder uses sophisticated procedures especially the use of zero-day exploits, customer malware to jump traditional security measures

ii. Persistent: APTs include continuous effort to maintain access and not readily one time attack in order to achieve the objective over a month or even years.
iii. Targeted: government agencies, critical infrastructures of huge companies using social engineering tricks especially spear phishing to gain early access is their main goal and focus.

Attack Lifecycle

The lifecycle of an APT attack classically follows numerous phases:

1. Early access: phishing emails and exploiting vulnerabilities in software are mainly entry points of attackers or intruders.
2. Launching presence: they create backdoors as soon as access is gained and maintain it while mapping the network to identify valuable data
3. Cross drive: intruders move with the gained network to gather credentials and access sensitive data and information.
4. Data exfiltration: its main objective is to steal and disrupt activities without any detection

Detection and Avoidance

Detecting APTs can be challenging owing to their stealthy nature.
Establishments can gadget numerous approaches to mitigate the menace of APTs: such as

1. Multilayered security: bringing or introducing a combination of firewalls, intrusion detection system and also endpoint protection approaches helps identify and block APT activities
2. Staff Training: frequent training on spotting phishing attempts and of her social engineering tricks may reduce the probability of successful early trials to gain access.
3. Threat brainpower: being informed about the latest threat and vulnerabilities will actually help establishments prepare and respond effectively against any attack by the intruders.

Challenges in APT Detection and Explanation by Vaibhav M. et al (2024)

Detecting and Explanation of APTs present exceptional challenges due to their stylish nature:

1. Stealth Procedures: APTs practice cutting-edge evasion strategies, making them hard to detect with outmoded security measures.
2. Persistence: The long-term environment of APTs means that even after detection, comprehensive extinction is routine.
3. Adaptive Performance: APT players repeatedly develop their strategies in reply to improved fortifications.
4. Resource Strength: Active APT defense entails weighty resources in both technology and skilled workforces.
5. False Positives: The weakness of APT activities can lead to extraordinary rates of false positives in detection schemes, hypothetically awesome security crews.
6. Data Volume: The absolute volume of data in current networks makes recognizing subtle APT deeds similar to discovery an indicator in a haystack.
7. Supply Chain Weaknesses: As established by assaults like SolarWinds, APTs can abuse trust in genuine software plus updates, sidestepping countless outmoded security controls.

Thoughtful of these challenges is vital for emerging and executing active detection techniques and modification approaches. (Vaibhav M. et al, 2024)

APT Detection Techniques

Active APT detection needs a multi-layered tactic, combining several techniques to recognize subtle indicators of concession across dissimilar aspects of an establishment's IT infrastructure. This segment investigates key detection approaches, their strengths plus limitations.

A. Network-based Detection Approaches

Network-based detection emphases on recognizing APT activities by examining network traffic patterns plus behaviors.

1)Traffic Examination plus Anomaly Detection: it encompasses establishing a baseline of normal network behavior and identifying eccentricities that may show APT activity
Strengths: Can detect novel threats and subtle behavioral changes.
Limitations: High false-positive rates; requires significant tuning.
2)Deep Packet Inspection (DPI): DPI observes the content of network packets, looking for signatures of known malware or suspicious patterns
Strengths: Can identify specific malware or attack techniques.
Limitations: Resource-intensive; less effective alongside encrypted traffic.

3)NetFlow Examination: NetFlow data offers a high-level opinion of network traffic, permitting for the identification of unfamiliar communication patterns
Strengths: Accessible; can perceive command-and-control (C2) communications.
Limitations: Lacks full content examination; may miss low-volume exfiltration.

B. Host-based Detection Approaches
Host-based detection emphases on recognizing APT activities on distinct endpoints within the network.
1. Endpoint Detection and Response (EDR): EDR answers display endpoint activities, gathering and examining data to detect plus respond to extortions
Strengths: Offers full visibility into endpoint behavior; allows quick response.
Limitations: Needs deployment plus controlling on all endpoints; potential routine impact.
2. User and Entity Behavior Analytics (UEBA): UEBA systems launch baselines of normal user behavior and recognize anomalies that may show compromise
Strengths: Can spot insider threats and bargained accounts.
Limitations: Needs time to form precise baselines; privacy worries.
3. File Reliability Monitoring: This procedure includes monitoring dangerous system files and configurations for unauthorized modifications
Strengths: Can spot subtle system alterations made by APTs.
Limitations: High capacity of alerts in dynamic situations; needs careful configuration.

C. Log-based Detection Approaches
Log-based detection includes the collection and examination of logs from numerous sources to recognize indicators of APT action.
1)Security Information and Event Management (SIEM): SIEM systems combined and compare logs from multiple frameworks to detect security incidents
Strengths: Offers a centralized observation of security events; allows multifaceted link rules.
Limitations: Needs important setup and tuning; can be overcome by data capacity.
2)Log Correlation and Examination: This includes examining logs from dissimilar frameworks to recognize patterns or series of events that may show APT activity
Strengths: it spot multifaceted attack patterns bridging multiple systems.
Limitations: Needs watchful rule formation; can be computationally exhaustive.

D. AI-based Detection
AI procedures are progressively being realistic to APT detection, posing the likely to recognize subtle patterns and unique threats.
1)Supervised Learning Techniques: They use labeled datasets to train models to classify known APT practices and behaviors
Strengths: Can precisely detect known attack designs.
Limitations: Needs big, precisely labeled datasets; may struggle with unique attacks.
2)Unsupervised Learning for Anomaly Discovery: They recognize strange patterns or behaviors without preceding labeling, hypothetically detecting unique APT activities
Strengths: Can spot hitherto unidentified threats; adapts to altering backgrounds.
Limitations: High false-positive rates; results can be problematic to deduce.
3)Deep Learning Prototypes for APT Discovery: Deep learning tactics like Recurrent Neural Networks (RNNs) plus Convolutional Neural Networks (CNNs), are being smeared to APT discovery, chiefly for examining successive data like network traffic
Strengths: Can identify complex patterns in large datasets.
Limitations: Needs important computational assets; absence of explainability.

E. Threat Intelligence Incorporation
Incorporating threat intelligence into detection manners can improve an establishment's ability to recognize and contextualize APT actions.
1. Indicators of Compromise (IoCs): IoCs are explicit items or remarks that specify a latent security incident. Incorporating up-to-date IoCs into detection schemes can help recognize branded APT tools and practices
Strengths: Delivers unlawful intelligence for detecting recognized threats.
Limitations: IoCs can develop swiftly outmoded; over-reliance can lead to alert weariness.
2. Threat Forages and Information Sharing: Contributing in threat intelligence sharing groups and incorporating threat forages can offer wider visibility into evolving APT tactics
Strengths: Improves detection competences with outer intelligence.
Limitations: Needs watchful examining of frameworks; can present racket into detection developments.

III. Steps For Advanced Persistent Threats Detection

To detect and respond to Advanced Persistent Threats (APTs), follow these steps:

1. Gadget advanced threat detection system: make adequate use of security information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA) to track and monitor the activities and identify anomalies in the network.
2. Employ Threat brainpower: subscribe to threat brainpower feeds and integrate them with SIEM and some security tools to improve detection abilities.
3. Establish frequent network audit: anomalies like unexpected data flow or argument with known malicious IP addresses should be tracked and analyzed in the network traffic frequently
4. Threat chasing: always be active for signs of APT activity across your network by focusing on Indicators of Compromise (IoCs).
5. Multilayered tactic: numerous methods like network-based, host-based and AI methods to create a widespread defense against APTs must be combined.
6. Continuous monitoring: to ensure the efficacy of your defense tactic, frequent exercises and engagements must be adopted for regular detection abilities to be achieved.

IV. Application Of AI In Advanced Persistent Threats Detection

Well-tuned IDSs in initiative atmospheres can produce thousands of warnings per second, building real-time physical review infeasible. The measure of alerts rest on on the quantity of observed endpoints and the intricacy of the network. Hence, alert clustering is engaged to reduce racket by grouping correlated alerts into consistent incidents. (Pedro, 2025)

Similarly, Pedro Ramos Brandao (2025), User and Entity Behavior Analytics (UEBA) foils IDS by detecting anomalies in user conduct that may not contest recognized attack signatures. UEBA schemes are vital for APT detection that comprises dormant and unintended compromise phases, necessitating background and historic behavior modeling. A computerized design learns from ancient alerts and incident data to advance APT detection. It allocates trust scores to novel alerts, then customs these scores to arrange and knot alerts into credible APT incidents. The scheme must mix IDS and UEBA productions, apply statistical prototypes and endlessly adapt to emerging threat designs. In fact they depicted a transformative design that redefines exactly how alerts are controlled in cybersecurity actions. Instead of devastating experts with an overflow of raw signals, it functions as a clever arbitrator cleaning, contextualizing and humanizing the input stream into a controllable set of high-quality yields. By incorporating data preprocessing, behavioral modeling, anomaly detection, clustering plus scoring, the scheme greatly decreases noise, increases interpretability, and eventually improves managerial resilience against Advanced Persistent Threats.

Explanation of each phase:

1) Raw Alerts from IDS/UEBA: High-volume, shapeless data from detection schemes.
2) Alert Preprocessing: Racket filtering, reduplication, plus timestamp standardization.
3) Behavioral Sketching: Builds user/device activity baselines from past logs.
4) Anomaly Detection plus Trust Scoring: Allots confidence echelons to each alert using statistical/ML models.
5) Alert Clustering Machine: Clusters alerts built on entity, time and action resemblance.
6) Incident Construction: Procedures structured incidents demonstrating a suspected APT phase.
7) Incident Scoring and Prioritization: Grades incidents centered on risk level, novelty plus dependence metrics.
8) Absolute Incident Reports: Ranked incidents offered to human analysts for triage plus response.

V. Algorithms For Advanced Persistent Threats Detection

The SMA-optimized CNN-LSTM was assessed on the unknotted dataset, a standard for network intrusion detection, with 94.3% accuracy and precision, remember, and F1 scores of 92.8%, 93.5%, and 93.1%, respectively. Also, the model took a false positive rate of 2% and a false negative rate of 3% besides was extra intelligent to detect. Scalability examinations established the model's competence at handling high traffic, with dispersed training handling 50,000 proceedings per seconds and decreasing training period by 35% over single-node systems. These outcomes show that linking novel optimization methods with deep learning is an active routine for APT detection and the projected framework was healthy, scalable, well-organized and it considerably advances real-time APT detection and advances the resilience of dangerous cybersecurity foundations. (Najah, 2025)

A routine module was executed to calculate evaluation metrics whereas restraining memory usage animatedly. The lively ROC adder stored negligible test state, allowing evaluation on large-scale datasets with Python healthy routine (where single top P percentile of alerts per the chief anomaly scores are painstaking). This method supports scalability for utilization in initiative Security Operation Centers (SOCs). (Pedro Ramos Brandao, 2025)

VI.Advanced Persistent Threat (APT) Detection: Challenges And Future Research Directions

Challenges in APT Detection

Notwithstanding momentous advances in cybersecurity know-hows, perceiving Advanced Persistent Threats (APTs) rests a multifaceted and embryonic challenge. One of the principal hitches lies in the sneaky and long-duration environment of APT operations, which are intentionally considered to evade conformist security controls and balance into standard system behavior. Attackers repeatedly employ low-and-slow tactics, making malicious goings-on difficult to differentiate from genuine procedures.

Alternative chief challenge is the unsuccessfulness of signature-based detection devices against zero-day adventures and polymorphic attack performances usually used in APTs. These schemes rely on recognized attack designs and therefore fail to detect formerly unseen or vigorously embryonic threats.

The claim of Artificial Intelligence (AI) to APT detection presents supplementary challenges. Data quality plus availability remain important anxieties, as real-world APT datasets are rare, exceedingly imbalanced and frequently comprehend noisy or incomplete information. This imbalance can prejudice learning simulations and damage detection enactment. Also, high false-positive rates formed by anomaly-based detection schemes can overpower security analysts and lessen operational competence.

Scalability plus performance issues also ascend when installing AI-based APT detection in large-scale or heterogeneous atmospheres such as cloud, hybrid and Internet of Things (IoT) infrastructures. Besides, the nonexistence of explainability and transparency in numerous deep learning mockups limits their implementation, as security squads need interpretable results to support incident response plus forensic examination.

Future Research Directions

Future research in APT detection should prioritize the development of explainable AI (XAI) techniques that offer clear insights into detection verdicts, allowing security analysts to improved and realize, validate plus belief AI-generated alerts. Enhancing interpretability that will support narrow compliance plus advance human–machine collaboration.

A new favorable direction is the plan of hybrid and ensemble detection structures that incorporate AI-driven behavioral examination with outmoded rule-based plus signature-based approaches. Such tactics can advance detection truth while sinking false positives plus improving robustness against evasion strategies.

Research focuses on adaptive and incessant learning models proficient of embryonic beside attacker plans. Combining wired learning, reinforcement learning and threat intelligence response circles can help schemes endure effective against developing APT techniques.

Talking the shortage of labeled APT datasets is precarious. Future studies ought to search collaborative data-sharing tools, privacy-preserving learning approaches (e.g., federated learning), and realistic fake data cohort to improve model training while shielding sensitive information.

Lastly, countless attention should be specified to real-world authentication and utilization of APT detection methods. Weighing models in a working-environments, across numerous domains and beneath adversarial circumstances will be vital to safeguard scalability, resilience plus applied efficacy in shielding alongside advanced persistent threats.

VII. Conclusion

Advanced Persistent Threats (APTs) endure to fake a weighty challenge to fashionable cybersecurity owing to their stealthy, adaptive and long-term landscape. Outmoded signature-based intrusion detection schemes are progressively insufficient in recognizing such cultured attacks, mainly when adversaries pay innovative or complicated practices. This review has tinted the growing role of Artificial Intelligence, driven tactics in enhancing behavioral APT detection by permitting the empathy of anomalies, unseen attack forms and embryonic threat behaviors in close real time.

The study scrutinized topical AI methodologies pragmatic to APT detection, counting machine learning and deep learning replicas and argued their incorporation within current security frameworks. While these tactics determine substantial promise in refining detection accuracy and decreasing response time, numerous challenges endure. These comprise data imbalance, model explainability, high false-positive rates, scalability subjects plus the exertion of deploying AI models in dynamic, real-world environments. Overall, the findings indicate that AI-based APT detection signifies a dangerous advancement in cyber defense, but its efficacy depends on cautious design, robust datasets plus unbroken assimilation with prevailing security structures.

References

[1]. Yuntao Wang, Han Liu, Zhendong Li, Zhou Su, Jiliang Li (2024) Combating Advanced Persistent Threats: Challenges And Solutions; IEEE Network, Volume 38, Issue 6 Pages 324 – 333. Https://Doi.Org/10.1109/MNET.2024.3389734

[2]. Alsaheel Et Al., "ATLAS: A Sequence-Based Learning Approach For Attack Investigation," In Proc. USENIX Security, 2021, Pp. 3005–3022. Https //Www.Usenix.Org/System/Files/Sec21-Alsaheel.Pdf

[3]. Nur Ilzam Che Mat, Norziana Jamil, Yunus Yusoff, Miss Laiha Mat Kiah (2024) A Systematic Literature Review On Advanced Persistent Threat Behaviors And Its Detection Strategy Open Access. Journal Of Cybersecurity, Volume 10, Issue 1, 2024, Https://Doi.Org/10.1093/Cybsec/Tyad023
[4]. Singamaneni Krishnapriya & Sukhvinder Singh (2024) A Comprehensive Survey On Advanced Persistent Threat (APT) Detection Techniques; Computers, Materials And Continua. Volume 80, Issue 2, 15 August 2024, Pages 2675-2719. Https://Doi.Org/10.32604/Cmc.2024.052447
[5]. Vaibhav Malik, Anirudh Khanna, Nandan Sharma And Suryaprakash Nalluri (2024) Advanced Persistent Threats (Apts): Detection Techniques And Mitigation Strategies DOI10.21428/E90189c8.91e89a3e
[6]. Pedro Ramos Brandao (2025) Exploring The Role Of Artificial Intelligence In Detecting Advanced Persistent Threats; ICT Infrastructures For Cybersecurity 14(7), 245; Https://Doi.Org/10.3390/Computers14070245.
[7]. D. Kushner (2013) The Real Story Of Stuxnet, IEEE Spectrum, And Feb. 26, 2013. Available: Https://Spectrum.Ieee.Org/Telecom/Security/The-Real-Story-Of-Stuxnet.
[8]. Najah Kalifah Almazmomi (2025) Advanced Persistent Threat Detection Using Optimized And Hybrid Deep Learning Approach. Willey Online Library; Volume8, Issue2; Https://Doi.Org/10.1002/Spy2.70011
[9]. Singamaneni Krishnapriya, Sukhvinder Singh (2019) A Comprehensive Survey On Advanced Persistent Threat (APT) Detection Techniques; Science Direct; Volume 80, Issue 2, Pages 2675-2719; Https://Doi.Org/10.32604/Cmc.2024.052447
[10]. Manish Khule, Deepak Motwani & Dipti Chauhan (2025) A Layered And Integrative Framework For Advance Persistent Threat Detection And Mitigation: Combining AI, Zero-Trust, And Advanced Threat Intelligence; Springer Nature Link; Volume 28, Article Number 740, Https//Link.Springer.Com/Article/10.1007/S10586-025-05561-0
[11]. Henry & Promise (2026) Embryonic Apt Alteration Tools: A Criticism Of Successive Knot Defensive Mechanisms; Journal JENER Journal Of Empirical And Non-Empirical Research; Volume 2, Issue 2, Page 296-300 | Article No. 35 DOI: 10.4898/Jener.V2i2.A35 ISSN: 7895-9216
[12]. Henry P, Et Al (2026) The Interplay Of 2FA And Phishing: A Review Of Attack Routes And Booth Dealings; International Journal Of Engineering Research & Technology (IJERT.ORG); Volume 15, Issue 02 (February 2026); DOI : Https://Doi.Org/10.5281/Zenodo.18546985
[13]. Matthew Walsh, Clarence Worrell, Thomas Scanlon (2024) Toward The Use Of Artificial Intelligence (AI) For Advanced Persistent Threat Detection; TECHNICAL REPORT CMU/SEI-2024-TR-001 DOI: 10.1184/R1/25282333; Http://Www.Sei.Cmu.Edu
[14]. Abigail Darwish And Aryamehr Fattahi (2025) Apts Global Review 2022–2025: Trends, Regions And Forecast, Diplomacy And Securitytechnology. Https://Bisi.Org.Uk/Reports/Apts-Global-Review-2022-2025-Trends-Regions-Forecast