Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning

Najaf Saeed (Corresponding Author)
Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
Email: nnjfali44@gmail.com & Email: SU92-MSSEW-S24-002@superior.edu.pk

Nasir Ayub
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
Email: nasir.ayyub@hotmail.com

Ali Haider
SOPHOS, United States of America (USA) Email: digitaleyeali@yahoo.com

Umair Ghafoor
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: umairghafoor@hotmail.com

Arshad Ali
Faculty of Computer and Information Systems, Islamic University of Madinah, Al Madinah Al Munawarah, 42351, Saudi Arabia Email: a.ali@iu.edu.sa

Abdul Wahab
University of Science and Technology of China, Email: abdulwahab1@mail.ustc.edu.cn

Hamayun Khan
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan Email: hamayun.khan@superior.edu.pk

Muhammad Zunnurain Hussain
Bahria University, Lahore Campus, Email: zunnurain.bulc@bahria.edu.pk

ABSTRACT

Advanced Persistent Threats (APTs) pose a big challenge to today's Computing systems. They use long-term, stealthy, and behaviour-driven attack methods and avoid reusable malware and fixed setups. Traditional detection methods using Indicators of Compromise (IOCs) like IP addresses and file hashes are becoming less effective. This is due to quick changes in infrastructure and the common use of legitimate system tools. As a result, recent research has shifted toward behavior-based and actor-centric detection models. This article focuses on how OpenCTI, MITRE

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

ATT&CK, and machine learning work together. They enhance the detection and attribution of APTs. Stealth Falcon (MITRE ATT&CK) serves as a key case study. A Systematic (SLR) examined recent studies that focused on CTI platforms, behaviour analytics linked to ATT&CK, knowledge graph models, machine learning detection, and simulation-based evaluation. The findings show that OpenCTI's knowledge graph connects actors, campaigns, infrastructure, and TTPs over time. Meanwhile, MITRE ATT&CK offers a standard framework to map adversary actions. Using ATT&CK-aligned TTP sequences in machine-learning models, like Random Forest and XGBoost, improves detection accuracy. It also lowers false positives when compared to IOC-based methods. These models support actor-centric attribution. They find stable behavioural fingerprints. This helps track Stealth Falcon in different campaigns. The review also points out major gaps in current research. These include limited real-world testing, scalability issues, and poor integration with SOC tools. The study shows that using OpenCTI, MITRE ATT&CK, and machine learning creates a strong base for detecting APTs. This approach emphasises behaviour and actors and has a significant shift towards traditional, indicator-driven security models.

Keywords: Advanced Persistent Threats (APTs), Stealth Falcon, MITRE ATT&CK, OpenCTI, Cyber Threat Intelligence (CTI).

Introduction

The global cyber threat landscape has changed greatly in the past twenty years. Early malware outbreaks like Melissa (1999) and ILOVEYOU (2000) were mostly opportunistic. They spread fast, using curiosity to propagate easily [1]. They aimed for disruption or fame, not long-term goals. Modern cyber operations offer a new approach. Intrusions seek long-term access, gather secret intelligence, and can even impact real-world geopolitics. Events like Stuxnet in 2010, the Ukraine power grid attack from 2015 to 2016, and the SolarWinds breach in 2020 show that cyber operations are now crucial for statecraft and espionage. They are now used for strategic leverage, not just as technical breaches [2, 3].

$$r_{XY} = \frac{\sum_i (x_i - \overline{x_i})(y_i - \overline{y_i})}{\sqrt{\sum_i (x_i - \overline{x_i})^2}\sqrt{\sum_i (y_i - \overline{y_i})^2}} \quad \text{Eq (1)}$$

At the core of this evolution is the rise of Advanced Persistent Threats (APTs). APTs differ from commodity malware and many cybercrime campaigns. They focus on long-term engagement, show operational discipline, and have clear strategic goals [4, 5]. These actors often have state support or alignment. Their goals go beyond making money. They include surveillance, espionage, political influence, sabotage, and ongoing infiltration of key institutions. APT operations usually have several stages, including Reconnaissance, Initial compromise, Privilege escalation, Lateral movement, Persistence, Command-and-control (C2), and Data exfiltration. Their sophistication goes beyond technical tools. You can also see it in their patience, stealth, and consistent skills [6, 7]. Modern APT groups intentionally blend into

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

legitimate network activity, making detection exceptionally difficult. They often use "living off the land" methods. This includes built-in admin tools like PowerShell and WMI. It has real credentials, encrypted messages, and modular malware that isn't used the same way each time [8].

$$h^k = f\left(x * w^k + b^k\right)$$ Eq (2)

Defensive models that depend mostly on static signatures or isolated artifacts find it hard to keep up. This change has pushed the cybersecurity community to focus on behaviour-based detection. This is backed by structured behaviour frameworks, graph-based intelligence tools, and increased automation from machine learning [9, 10].

$$y = f\left(\sum_{k=1}^{K} h^k * w^k + c^k\right)$$ Eq (3)

The IOC-Based Detection

For decades, security programs relied on Indicators of Compromise (IOCs). These included file hashes, domains, IP addresses, registry keys, and known malware signatures. These indicators work well for known threats, but they don't suit APTs [11]. A key weakness is timing. IOC-driven intelligence usually reacts after adversaries have adapted. This means indicators are found and shared too late. When defenders use new shared indicators, attackers often change their tactics [12].

$$A(x) = \begin{cases} \alpha x, x \leq 0 \\ x, x > 0 \end{cases}$$ Eq (4)

They rotate infrastructure, modify payloads, or switch delivery methods. This creates a constant gap between how attackers evolve and how defenders respond. A second limitation is that IOCs often lack semantic context.

$$s(x) = \frac{1}{1 + e^{-x}}$$ Eq (5)

A malicious IP address alone rarely reveals who is behind the activity. It doesn't show what stage of the intrusion it represents or how it connects to past campaigns [13]. The lack of context can be risky in today's Security Operations Centers (SOCs). Analysts deal with a high number of alerts.

$$s_A = \frac{TP + TN}{TP + TN + FP + FN}$$ Eq (6)

Alert fatigue causes burnout, missed incidents, and bad prioritisation. This is worse with low-confidence alerts that don't link to attacker intent [14]. APT actors take

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

advantage of this weakness by staying under thresholds. They carry out actions that seem harmless on their own. This includes one PowerShell command, a scheduled task, or a secure HTTPS connection. The harmful signal shows up clearly when these events form a clear behaviour pattern [15]. These limits have led to a shift from "indicator matching" to identifying adversaries by their behaviour. Now, the focus isn't on what the attacker uses, but on how they operate.

$$s_P = \frac{TP}{TP + FP}$$

Eq (7)

Background on MITRE ATT&CK Framework

Behavior-based detection focuses on the idea that infrastructure and malware change quickly. Adversary tradecraft, how attackers gain access, run payloads, stay hidden, move around, and steal data, stays consistent [16]. The main framework behind this shift is MITRE ATT&CK. It stands for Adversarial Tactics, Techniques, and Common Knowledge. ATT&CK provides a clear way to understand how adversaries act, using real campaigns. It breaks down behaviour into tactics and techniques [17, 18]. Tactics are high-level goals like Initial Access, Execution, and Persistence. Techniques and sub-techniques are the specific methods used to reach those goals. ATT&CK techniques stay stable over time. This helps defenders understand enemy behaviour, even when IOCs and malware change [19, 20].

$$s_R = \frac{TP}{TP + FN}$$

Eq (8)

Studies on broader ATT&CK use show how valuable ATT&CK is [21, 22]. It helps to rebuild intrusion chains. It clarifies what attackers want. It also supports detection efforts and improves attribution. Analysts can transform isolated alerts into clear stories. They do this by connecting observed events to ATT&CK techniques [23, 24]. In practice, the difference is clear. Instead of viewing "PowerShell execution" as a broad risk, behavioural modeling can identify if it's used in common attack ways.

$$g^t(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)}$$

Eq (9)

$$S = a_0 = g(0) = \sum_{i=1}^{t} g(i) \prod_{j=1, j \neq i}^{t} \frac{-j}{(i - j)} \, (mod\ p)$$

Eq (10)

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

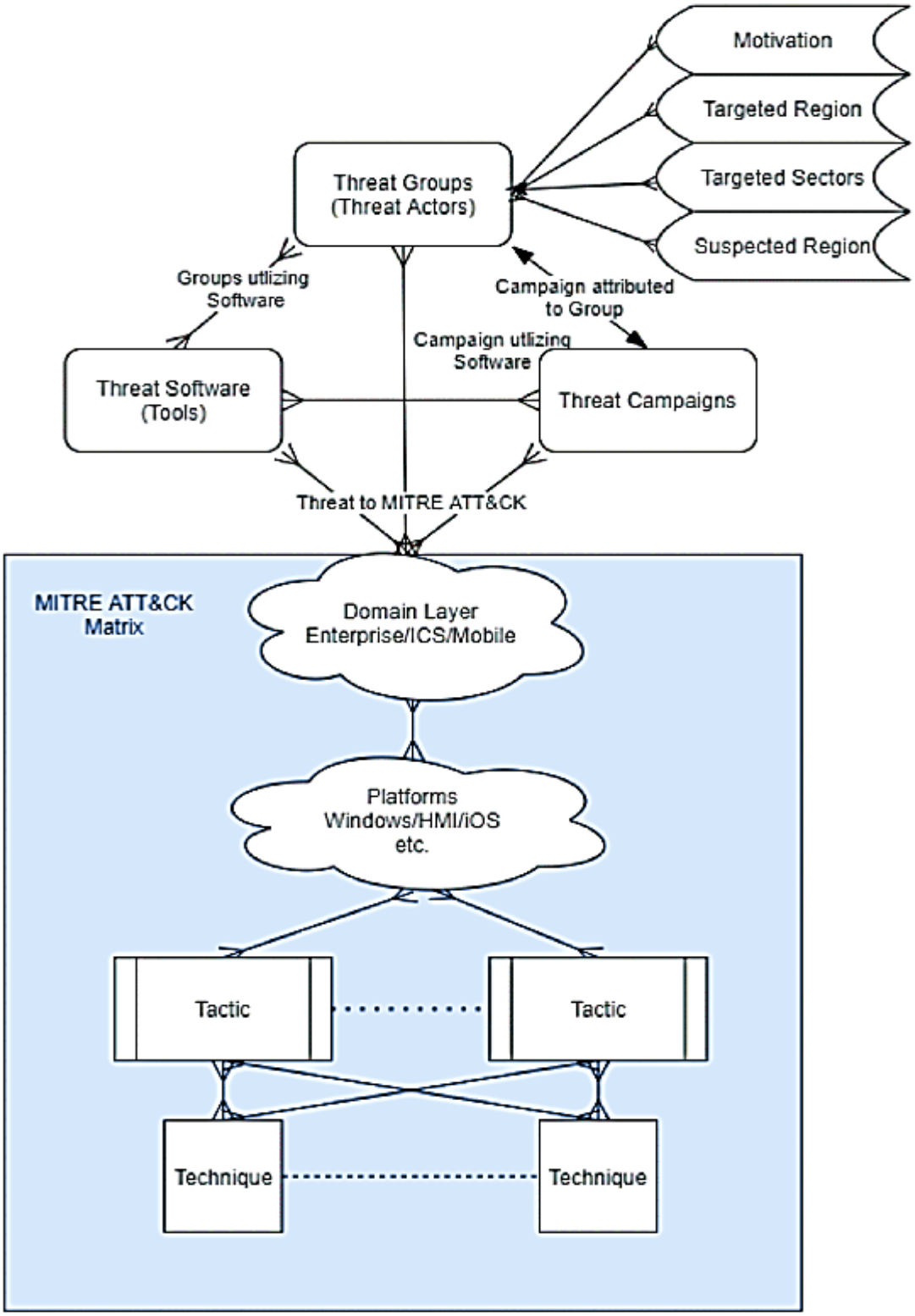


Figure 1. APT Generic conceptual architecture MITRE ATT&CK [25]

This is especially true for steps like spear-phishing delivery, using scheduled tasks to

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

stay persistent, and encrypted C2 [25, 26]. However, ATT&CK doesn't solve the problem of handling large amounts of intelligence and data from different tools over time. Defenders now use Cyber Threat Intelligence (CTI) platforms for large-scale behaviour-based detection. These platforms and graph-based architectures can store, relate, and query threat entities clearly [27, 28].

$$Q^{(i)} = \{Q(x_j^{(i)})\}_{j=1}^{m_i},$$

Eq (11)

CTI Platforms and Knowledge Graphs: From Feeds to Context

CTI platforms gather and link details about threat actors, campaigns, malware, infrastructure, and behaviors. Traditional CTI setups often act as indicator stores or feed gatherers. They usually have a limited ability to show relationships or support campaign-level thinking. Modern systems are using graph-based intelligence models more and more. In these models, entities and relationships are important; they can be linked and analyzed [29, 30]. OpenCTI represents a leading example of this direction. OpenCTI uses STIX-based modeling to store threat intelligence. It organises information into connected entities. These include actors, campaigns, malware, tools, infrastructure, observables, and ATT&CK techniques. These entities are linked through semantic relationships. This structure lets analysts explore intelligence as a knowledge graph instead of flat lists.

$$G_B = \sum_{i=1}^{N} W_i \,.\, G_{L_i}$$

Eq (12)

Work such as [31] OpenCTI shows how important it is for attribution support. It helps link new observations to past actor profiles using intelligence. Research on graph-centric threat intelligence, such as threatKG [32], shows that knowledge graphs automate data collection. They also link entities and reconstruct campaigns in large datasets. Graph-based CTI platforms present challenges like high data volume, complex relationships, noise and the need for skilled analysts to interpret and validate intelligence. Human-driven reasoning remains essential, but it is increasingly insufficient on its own. Recent work uses machine learning (ML) to automate tasks. These tasks include correlation, behaviour sequence classification, anomaly detection, and probabilistic attribution support [33, 34].

$$fd_k(x) = \frac{1}{n}\sum_{i}^{n_m} l(p_i, q_i; x)$$

Eq (13)

Machine Learning for APT Detection and Attribution

Machine learning makes threat detection scalable and automatic. It learns patterns from past data and uses them on new information. In APT contexts, ML helps to: Classify events, identify unusual behavior, Cluster campaigns, and Infer likely threat

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

actors based on behavior similarity. Clustering and measuring similarity in CTI-derived technique vectors can group APT activity. This supports distinguishing between different actors. Subgraph matching methods using event logs, ATT&CK-aligned representations, enhance attribution [35]. They do this by matching observed sequences to known campaign structures.

$$minimumfd_k(x) = \sum_{m=1}^{C*M} \frac{1}{n} fd_m(x) \quad \text{Eq (14)}$$

Learning temporal and contextual links from behaviour features, like execution sequences and log signals, surpasses signature-driven models. This is especially true for spotting stealthy, multi-stage intrusions [36, 37]. The paper highlights DeepFake detection, but it also talks about robustness and evaluation. This connects to the larger issue of ensuring that ML-based security detection effectively addresses evolving threats [38]. The literature shows a clear trend: ML is most useful when linked to CTI and behavioural frameworks. It should learn from ATT&CK-aligned features, boosted by CTI context. This allows detection systems to move from basic indicator matching to more thoughtful, actor-aware choices. ELU – E- Linear Unit with $0 < \alpha$ is

$$f(x) = \begin{cases} \alpha(\exp(x) - 1) & \text{for } x < 0 \\ x \text{ for} & x \geq 0 \end{cases} \quad \text{Eq (15)}$$

Stealth Falcon as a Reference Actor for Actor-Centric Detection

This review looks at Stealth Falcon (MITRE ATT&CK) to ground the analysis in a real, documented threat profile. Active since at least 2012, Stealth Falcon is known as a Middle Eastern spy group [39]. It targets journalists, dissidents, human rights organisations, and government-linked entities. The group often uses tactics such as spear-phishing, running PowerShell, scheduling tasks, using encrypted C2, and applying strong obfuscation. Stealth Falcon is great for studying behavioural fingerprinting and actor-centric detection. Its steady behaviour is helpful as tools and infrastructure change [40].

$$\omega = \left\{ \begin{array}{ll} 0; & normal \\ 0 < \omega < 0.25; & Mild \\ 0.25 < \omega, 05; & Moderate \\ 0.5 < \omega < 0.75; & Severe \\ 0.75 < \omega < 1; & Proliferative \end{array} \right\} \quad \text{Eq (16)}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

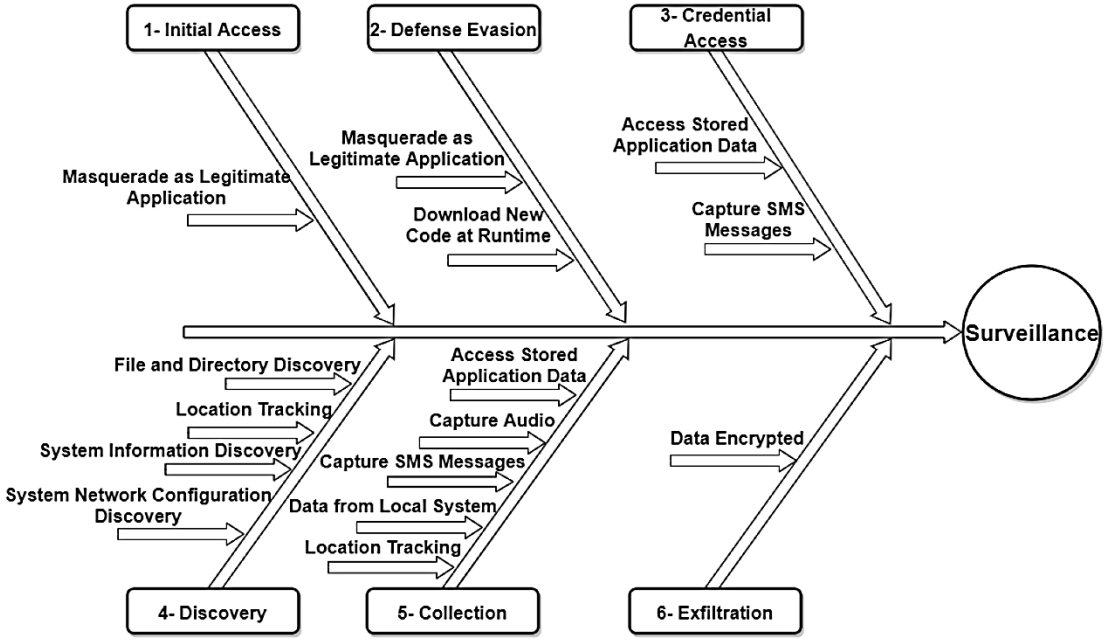


Figure 2. Generic conceptual architecture MITRE Framework [41]

Recent reports on campaigns like the Horus operation show how tradecraft is evolving. They point out the use of fileless or memory-resident execution. They also mention complex delivery chains, particularly with CVE-2025-33053. Even with new loaders or rotated infrastructure, actor tradecraft often remains unchanged. ATT&CK-based modelling and ML-based behavioural classification are key partners for IOC-driven workflows [42].

$$\omega = E_f * \frac{1}{1 + e^{-\theta t_f}} \qquad \text{Eq (17)}$$

Toward an Actor-Centric Detection Paradigm

A key insight in modern cyber defense is that APT behavior is often more stable than artifacts. IOCs change quickly; behavioral sequences change more slowly. Attribution and high-confidence detection improve when based on behavioural fingerprints. These include preferred access methods, scripting environments, persistence methods, C2 styles, and obfuscation patterns.

$$f_{\mathrm{t}} = \mu + \rho GEGR_{\mathrm{it}-1} + \vartheta^{+} EU^{+}_{it-1} \qquad \text{Eq (18)}$$

This notion aligns with work such as [43, 44], which highlights the challenges of attribution. It shows the need to distinguish between actors with similar or hidden techniques. Actor-centric detection reframes the SOC's core question from is this indicator malicious to which adversary is performing this behavior. In this model, OpenCTI offers the relational memory of campaigns and entities. ATT&CK provides the vocabulary for behaviours, while ML allows for automated pattern recognition and classification [45].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

$$C_{\mathrm{t}} = \vartheta^{-} EU^{-}_{it-1} + \emptyset^{+} FD^{+}_{it-1} + \vartheta^{+} EU^{+}_{it-1} \quad \text{Eq (19)}$$

These components help create actor likelihood scores and track campaign correlations over time. They also enable earlier detection from partial playbook execution. Static IOC pipelines and basic rule-based alerts often miss these capabilities [46]. Research has explored CTI platforms, ATT&CK applications, ML-based intrusion detection, and APT attribution. These topics are often explored separately.

$$I_{\mathrm{t}} = \omega^{+} TI^{+}_{it-1} + \omega^{-} TI^{-}_{it-1} \quad \text{Eq (20)}$$

Operational APT detection needs these layers to work as one system. Intelligence must link to telemetry. Behaviour should connect to attribution. Automation needs to fit within a structured threat model. This review therefore, synthesizes four dimensions into one actor-centric narrative: CTI platforms and knowledge-graph architectures (with emphasis on OpenCTI), MITRE ATT&CK–aligned behavioral modeling for detection engineering and threat hunting, and machine learning for behavioral classification and actor attribution. Stealth Falcon as a reference actor for evaluating the stability of tradecraft and actor-centric correlation

Figure 3 below shows how modern APT detection is shifting. It's shifting from traditional IOC methods to ATT&CK-aligned behaviour analytics. This includes CTI knowledge graphs, machine learning classification, and adversary emulation. Accordingly, this review aims to: (i) analyze how OpenCTI and related CTI systems represent and operationalize threat actors; (ii) examine how ATT&CK enables behavior-based detection and attribution; (iii) evaluate ML approaches that leverage ATT&CK-aligned features; (iv) assess how Stealth Falcon's campaigns are represented in the literature; and (v) identify gaps in real-world validation, integration, scalability, and deployment. By consolidating these strands, the review contributes a structured foundation for designing integrated, ML-enabled, actor-centric APT detection models that move beyond short-lived indicators toward durable behavioral understanding.

$$\delta_h = 60^{\circ} \begin{cases} 0 + \dfrac{(\beta_g - \beta_b)}{(m_x - m_n)}, ifm_x = \beta_r \\ 2 + \dfrac{(\beta_b - \beta_r)}{(m_x - m_n)}, ifm_x = \beta_g \\ 4 + \dfrac{(\beta_r - \beta_g)}{(m_x - m_n)}, ifm_x = \beta_b \end{cases} \quad \text{Eq (21)}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189

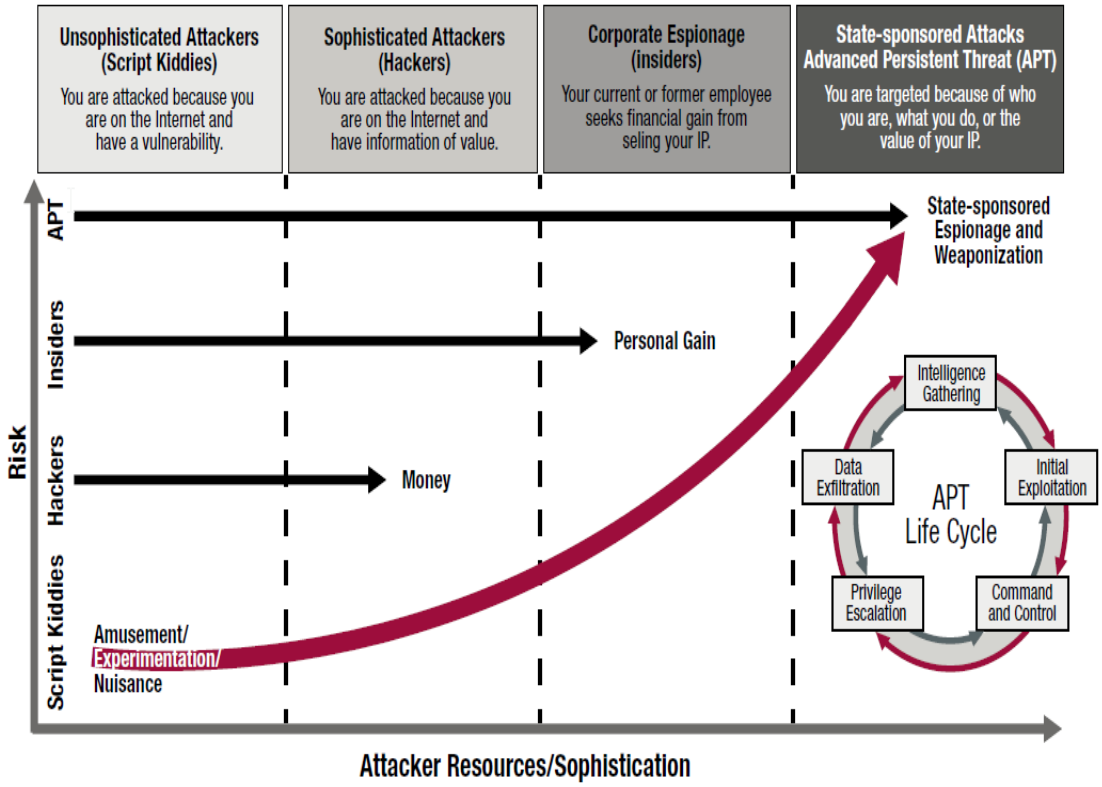


Figure 3. APT Detection evolution [47]

The remainder of this review is organized as follows. Section 2 features the Literature Review. It explores how APT detection has changed. It shifts from IOC-based methods to behavior-focused and MITRE ATTACK-aligned strategies. Next, it explores CTI platforms, knowledge graph-based attribution, and OpenCTI capabilities. It also includes machine-learning methods to classify behaviour and profile threat actors like Stealth Falcon. Additionally, it uses simulation-based validation with MITRE CALDERA. The section concludes with a summary comparing existing studies. Section 3 covers the Methodology. It covers the SLR design, search strategy, inclusion and exclusion criteria, study selection, data extraction and coding, synthesis method, and quality assessment. Section 4 reports the Results of the review. Section 5 discusses the findings and their implications for actor-centric APT detection. Section 6 elaborates limitations, future research directions and Conclusion.

Literature Review

The literature reviewed for this study spans research published between 2012 and 2025, covering Advanced Persistent Threat (APT) detection, adversary behavior modeling, cyber threat intelligence (CTI) systems, MITRE ATTACK–aligned analytics, machine-learning-based classification, knowledge-graph architectures, and simulation-based evaluation methods. The goal of this review is to present a systematic, comprehensive, and multilayered understanding of how academic and industry research has evolved in detecting sophisticated state-aligned threat actors

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

such as Stealth Falcon, and to identify gaps addressed by the proposed OpenCTI–MITRE–ML–CALDERA integrated framework [48, 49].

$$\Delta f_{\mathrm{t_i}} = \sum_{j=1}^{n-1} \alpha j \, \Delta GERG_{it-1} + \sum_{j=0}^{n2} (\pi^{j+} \Delta EU_{it-j}^{+} \quad \text{Eq (22)}$$

The following subsections structure existing literature thematically, as recommended in PRISMA-aligned SLR guidelines: Evolution of APT detection approaches, Behavior-centric detection and MITRE ATTACK, Cyber Threat Intelligence and structured threat modeling, Knowledge graphs for attribution, Machine learning for APT behavior classification, Actor profiling and Stealth Falco, Simulation-based validation and Comparative summary of existing studies The review synthesizes results from cybersecurity journals, threat intelligence reports, conference proceedings, and technical research from security labs such as Citizen Lab, Check Point Research, MITRE Engenuity, and national CERTs.

$$\Delta f_{\mathrm{t_1}} = \sum_{j=0}^{n3} (\tau^{j+} \Delta \mathrm{FD}_{it-j}^{+} + \tau_j^{-} \Delta \mathrm{FD}_{it-j}^{-}) \quad \text{Eq (23)}$$

Evolution of Detection Approaches for APTs: Device Behavioral Sources Used for Attack Detection

Early cybersecurity solutions relied heavily on signature-based detection and rule-driven intrusion detection systems. Research from the early 2010s shows that these methods were effective against commodity malware but consistently failed against APTs, whose hallmark traits include operational stealth, Long-term persistence, Credential misuse, Lateral movement, tailored spear-phishing and Encrypted communication channels. Researchers highlight that APTs rarely reuse malware binaries or fixed infrastructure; instead, they recycle behavioral patterns, making static defenses obsolete [50, 51]. Real-world threat reports further validate this transition. Iranian-backed APT groups, like APT33, APT34 (OilRig), and APT39, still use tactics such as phishing, credential dumping, and file obfuscation. They do this even with modern defenses in place.

$$\Delta f_{\mathrm{t_2}} = \sum_{j=0}^{n3} (\tau^{j+} \Delta \mathrm{FD}_{it-j}^{+} + \tau_j^{-} \Delta \mathrm{FD}_{it-j}^{-}) \quad \text{Eq (24)}$$

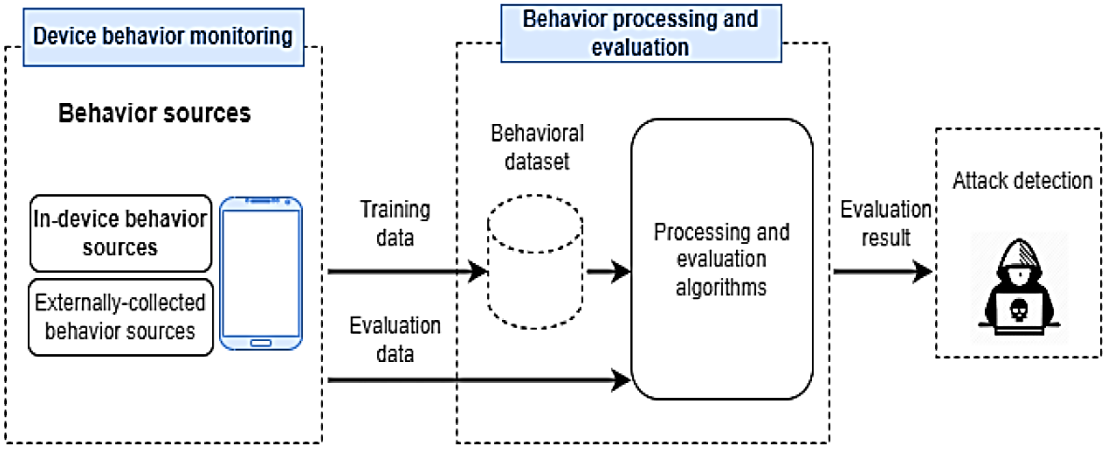


Figure 4. APT Detection evolution: device behavior life cycle [52]

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

The 2020 DHS alert in the report showed that even prepared organisations can be vulnerable. This happens if they rely on static IOCs for detection. The article highlights how quickly adversaries change their tactics. This shows the importance of behaviour-driven detection that aligns with MITRE ATT&CK [53].

Transition Towards Semantic and Behavioral Detection

The second wave of research (2019–2025) shifted toward behavior recognition, focusing not on the malware itself but on how attacks unfold. Studies show that TTP-chain matching can detect APTs even when no signature exists. ATTACK mapping significantly improves triage and attribution [55]. PowerShell behavior models catch 89% of APT scripts undetected by AV [56]. Studies consistently emphasized that APTs exhibit long-term behavioral stability across campaigns, even when tools, infrastructure, and victims change.

Behavior Modeling Using MITRE ATTACK

MITRE ATTACK emerged as a turning point in adversary understanding. Literature widely agrees that ATTACK was introduced. A combination of T1566.001 (Spear-phishing) → T1059.001 (PowerShell Execution) → T1053 (Scheduled Tasks) → T1041 (Exfiltration) is strongly linked with Middle Eastern espionage groups, including Stealth Falcon. This alignment shows in the MITRE ATT&CK profile of OilRig (APT34) [56, 57]. It mentions various techniques, including T1059.001 (PowerShell), T1071.004 (DNS tunneling), T1566 (Spear-phishing), and T1555 (Credential Access). These mappings show clear proof that Iranian-aligned APT groups have consistent behaviours. These patterns can be reliably modelled using ATT&CK [58].

$$\Delta f_{t_2} = \sum_{j=0}^{n4}(\sigma^{j+}\Delta TI + \sigma_j^{-}\Delta TI_{it-j}^{-}) + \varepsilon_{it} \qquad \text{Eq (25)}$$

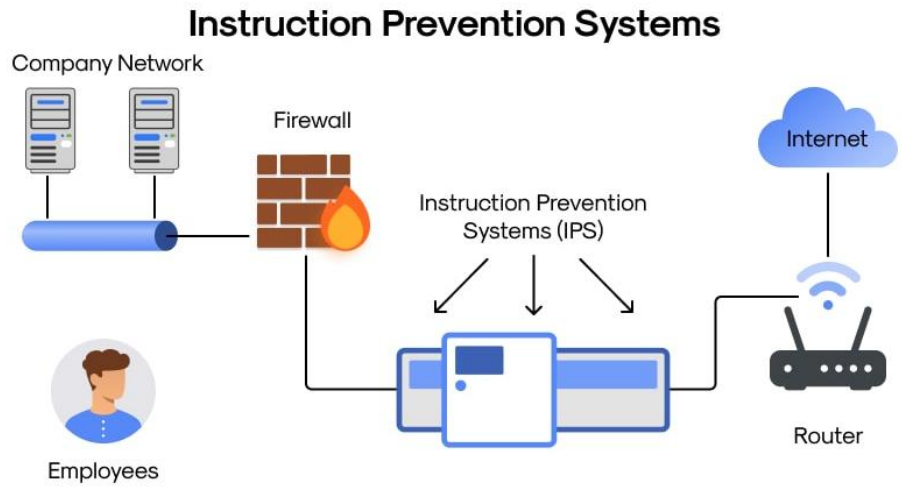


Figure 5. Generalize Intrusion Prevention (IPS) system [59]

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$y = \arg\max \left\{ p\left(y = C_k\right) \prod p\left(x | y = C_k\right) \right\}$$ Eq (26)

Research across 2022–2025 shows ATTACK integrated into: SIEM correlation engines [60], EDR detection policies [61], Behavior scoring algorithms [62], Graph-based threat models [63], Machine-learning training datasets [64], Red-team automation tools atomic Red Team [65], CALDERA [66], Studies like [67] demonstrate that ATTACK-aligned models reduce false positives by correlating events into attack chains, not isolated anomalies.

$$\ln fl_{it}^{+} = \Sigma_{j=0}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=0}^{t} \max(\Delta W^{T}{}_{ij,0}) + \epsilon_{it}$$ Eq (27)

Evolution of Cyber Threat Intelligence (CTI) From Unstructured Reports to Structured Intelligence

Older CTI sources were PDF reports, Vendor advisories, Raw IOC feeds and Blog posts as studies in [68] show these limitations that include CTI analysts manually extracted entities, no automated ATTACK mapping, no graph correlation, no campaign lineage and no actor profiling. Thus, CTI was informational, not operational. You can spot this limit in real public threat reports on Iranian-aligned APT activities. Analyses of APT33, APT34, and APT39 highlight practical defense steps and tactical signs.

$$\ln fl_{it}^{+} = \Sigma_{j=1}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=1}^{t} \max(\Delta W^{T}{}_{ij,1}) + \epsilon_{it}$$ Eq (28)

They are mostly stories, so you need to interpret them manually before taking action [69]. These reports outline adversary methods like credential dumping, spear-phishing, and obfuscated PowerShell use. However, they lack structured ATT&CK mappings and machine-readable entity relationships. This supports wider research showing that traditional CTI outputs boosted awareness and offered basic guidance. They did not succeed in automation and relational modeling. These are key for real-time detection and attribution workflows [70]. Multi-source aggregation [71], Automatic enrichment [72], ATTACK mapping [73], Actor profiling [74], Vulnerability intelligence [75], Knowledge graphs [76].

$$p\left(C_k\right) p\left(x | C_k\right) = p\left(C_k\right) \prod_{i=1}^{n} p\left(x_i | C_k\right)$$ Eq (29)

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189

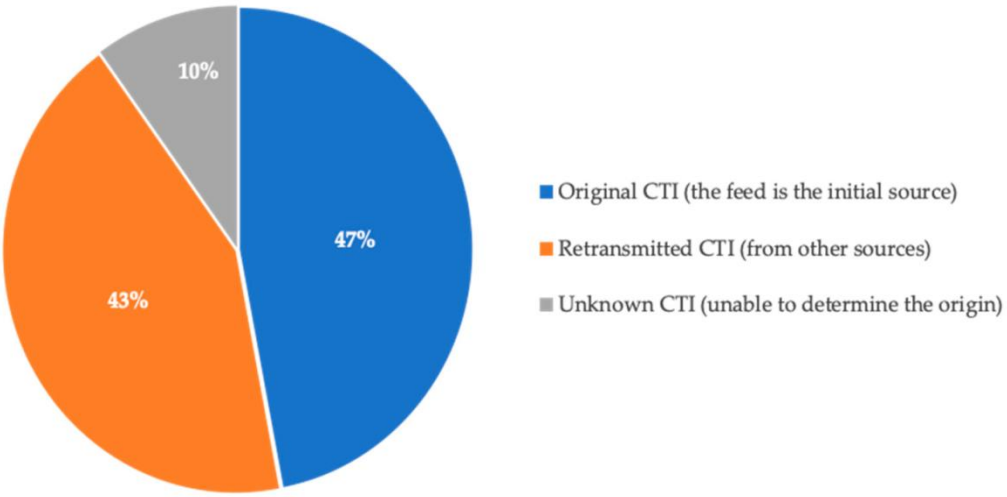


Figure 6. Comparative Analysis of CTI platforms' source originality [77].

Modern CTI aims to move beyond “lists of indicators” to contextual knowledge systems supporting attribution. You can easily spot the difference between unstructured and structured intelligence on platforms like MITRE ATT&CK.

$$G(S,A) = H(A) - \sum_{v \in Values(A)} \frac{|S_v|}{|S|} H(S_v) \quad \text{Eq (30)}$$

The MITRE profile of the OilRig group (APT34) offers a clear, machine-readable map. It details campaigns, tools, techniques, and procedures tied to this specific actor. This report links techniques like spear-phishing, PowerShell execution, credential dumping, and encrypted command-and-control to a persistent threat group over time [78]. Standardised actor profiles show how today’s CTI helps with automated correlation, behavioural fingerprinting, and tracking past campaigns. These features were mostly missing in older, document-based CTI methods [79].

Knowledge Graphs for APT Attribution

Graph-based CTI allows: Linking actors → TTPs → Malware → Infrastructure → Victims. Time-based campaign evolution [80], Multi-hop reasoning [81], Pattern recognition across years [82], Actor fingerprint extraction [83], Studies show that graph-based CTI improves [84], [85], and [86], Attribution accuracy [87], Detection precision [88], TTP clustering [89], Analyst triage and Knowledge graphs are especially effective for APTs because their behavioral chains remain stable. The MITRE ATT&CK OilRig profile provides an ideal dataset for graph-based attribution. It links campaigns (e.g., Juicy Mix, Outer Space) with specific techniques, malware families, and infrastructure, demonstrating how structured TTP knowledge can be converted into knowledge-graph representations similar to those used in OpenCTI [90].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$Gini\,(S) = 1 - \sum_{i=1}^{K} \left(\frac{|C_{i,S}|}{|S|} \right)^2$$ Eq (31)

Datasets like the OilRig [91] ATT&CK profile [92] provide the structured intelligence needed for OpenCTI ingestion [93]. They include technique mappings, campaign timelines, and software associations. This data helps OpenCTI [94] link new observables to past Iranian APT behaviours [95].

Machine Learning Models for Behavior-Centric hased Advanced Persistent Threat (APT) Detection

ML became prominent in APT detection between 2022–2025. Studies propose: Machine learning is a big field that is offered under information technology, statistics, probability, artificial intelligence, psychology, neurobiology and many other disciplines [96]. It is simply possible to solve the problems with machine learning by developing a model that is an adequate model of a chosen dataset. Machine learning has already become a developed field in training computers to imitate the human brain, and has ushered the science of statistics into an extensive science that generates foundations [97]. The learning processes are statistically computed as theories. Machine learning is concerned with generating algorithms that enable the learnability of the computer [98, 99]. Learning is a search for statistical regularities or other patterns of data. The machine learning algorithms [100] are designed to have the capability of representing the human. A strategy of studying a certain activity [101]. Algorithms can also be an insight into these comparably challenging learning in diverse situations. These days, new computing technologies in the sphere of Big Data are being developed [102].

$$r_{XY} = \frac{\sum_i (x_i - \overline{x_i})(y_i - \overline{y_i})}{\sqrt{\sum_i (x_i - \overline{x_i})^2} \sqrt{\sum_i (y_i - \overline{y_i})^2}}$$ Eq (32)

Machine learning is not the same as it used to be in the past. Today, many of the machine learning algorithms have been created [103], upgraded and enhanced and the new feature of machine learning is the automaticity. Subjecting big data to several intricate mathematical computations, which calculates the results much faster. The adaptive programming is highly popular. It is applied in machine learning, in which the applications have the capabilities of identifying patterns and learning by experience. Abstract data informs the new information or streamlines the correctness and effectiveness of its processing. and output. It works with the machine learning techniques [105, 106], as well. multidimensional data that are found in various application areas. Thus, depending on the preferred result of the algorithm, the machine learning algorithms are arranged in the following:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

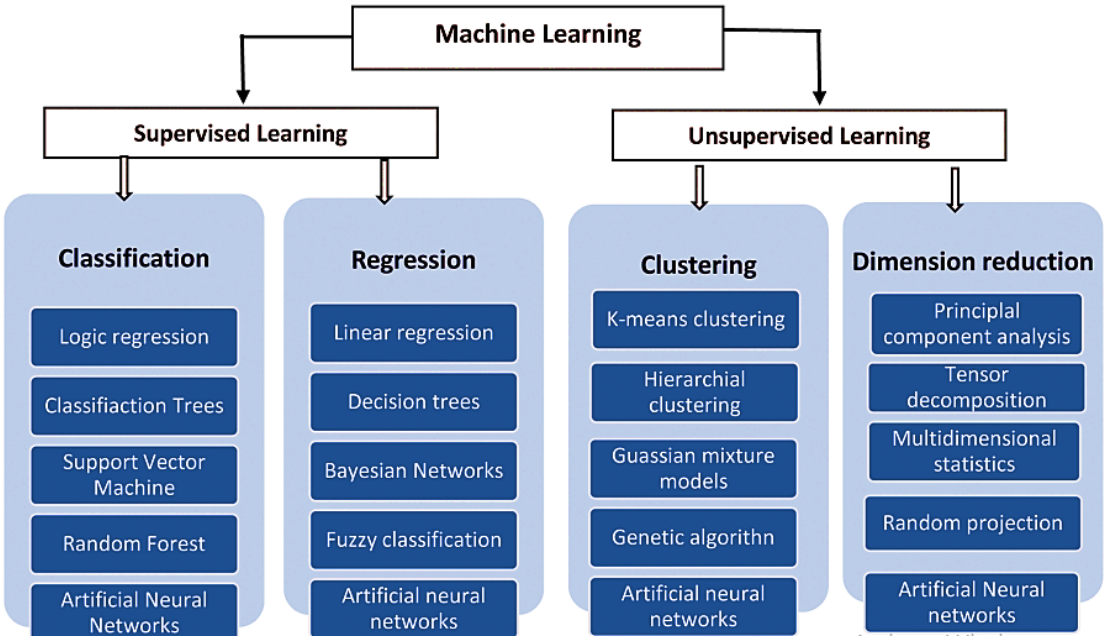


Figure 7. General classification of Machine Learning techniques used for Intrusion Prevention (IPS) system [104]

Supervised and Unsupervised learning - the different algorithms create a function that maps inputs to desired outputs. A single typicalization of supervised learning. task is the type of classification problem: the learner has to study estimate the action of) a function that takes a vector as an input and transforms it into one of from a possibly long list some classes by considering some inputoutput instances of the function and the model includes Random Forest [107], SVM [108], XGBoost [109] and Deep Neural Networks [110] while the Unsupervised learning model includes available DBSCAN [111], K-means [112] and Hierarchical clustering [113].

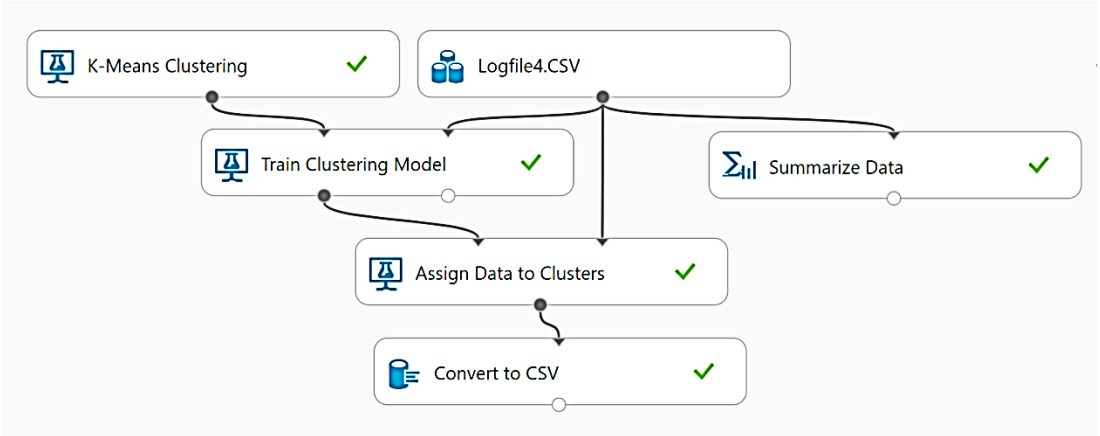


Figure 8. Supervised ML techniques for Intrusion Prevention (IPS) system [114]

Semi-supervised and Reinforcement learning - uses both labeled and unlabeled training examples. produce the right function or a classifier. The policy of operations

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

is learned by the algorithm of how to operate when presented with an observation of the world [115]. No deed does not affect the environment somehow and the environment gives feedback to direct the learning algorithm [116]. On previous experience. In addition to these categories of machine learning algorithms, they are fundamentally separated into two broad categories, supervised and unsupervised learning. The classes are known in advance in supervised algorithms [117]. These classes are created in a way of finite set, characterized by the human, which practically entails that some particular classifications will be put on a segment of data. The task of the machine learning algorithm is to discover patterns and to build mathematical models. These Models are then considered by the predictive ability when compared with measures of variance in the data itself [118]. ML reduces false positives significantly [119], TTP vectors outperform raw IOCs [120], Graph similarity detects actor behavior drift [121], and DNNs accurately classify actor behaviors [122]. ML models need clean, structured CTI data [123]. Recent studies show that agentic and frontier AI systems can automate workflows for cyber threat intelligence. They excel at processing clean, structured data. This helps support proactive and ethical defence strategies in today's SOC environments [124].

$$A(x) = \begin{cases} \alpha x, x \leq 0 \\ x, x > 0 \end{cases} \quad \text{Eq (33)}$$

Practical threat intelligence analyses of Iranian-aligned groups further support these findings. Reports on APT33, APT34, and APT39 show that attackers use consistent methods. They often rely on credential harvesting, spear-phishing, PowerShell execution, and lateral movement. These reports are often stories, but they provide real proof. Enemy behaviour usually follows patterns. When we make these patterns into ATT&CK-aligned features, we can use them in machine-learning models. This helps with automated classification and distinguishing actors, going beyond traditional IOC matching [125, 126].

$$s(x) = \frac{1}{1 + e^{-x}} \quad \text{Eq (34)}$$

Structured machine-learning features add value to actor profiles in MITRE ATT&CK. The OilRig (APT34) knowledge base entry shows clear connections between techniques, campaigns, and tools used over time [127]. Structured representations change raw observations, such as task persistence, PowerShell loaders, and credential dumping, into standard TTP vectors. These vectors can be used directly by supervised and graph-based learning models. They help with clustering, anomaly detection, and attribution tasks. Modern CTI platforms offer high-quality, consistent data. This data is essential for effective ML-driven APT detection [128].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$s_A = \frac{TP + TN}{TP + TN + FP + FN}$$ Eq (35)

Actor Profiling and Attribution of Stealth Falcon

Integrating OpenCTI with MITRE ATT&CK works well for profiling and attributing actors. Actor-specific detection boosts attribution confidence and helps in proactive defence strategies. OpenCTI can now create actor profiles using TTP chains and campaign data. This is a big step forward. Studies like [129] showed that Stealth Falcon's campaigns linked more precisely to past attack patterns. OpenCTI's knowledge graph helped identify actors consistently across campaigns, even as TTPs changed. MITRE ATT&CK mapped TTPs to known adversary behaviours. This gave a clear way to attribute actions to specific actors. Stealth Falcon's regular use of PowerShell, credential dumping, and DNS tunneling made it easier to identify the group. Actor attribution models using this method helped identify actors more quickly and reduced attribution errors.

$$s_P = \frac{TP}{TP + FP}$$ Eq (36)

This was better than older signature-based methods. The mix of behaviour patterns and actor-specific detection helped spot Stealth Falcon's tactics in real-time, even as their attack methods changed. This review mainly looks at Stealth Falcon (G0038). However, related Iranian-aligned groups like OilRig (APT34) and APT33 show similar operational patterns. These groups use similar tactics, like spear-phishing, credential misuse, and obfuscation. This shows that the OpenCTI–ATT&CK–ML framework applies not only to Stealth Falcon but also to the broader Iranian APT ecosystem [130].

Simulation-Based Validation with MITRE CALDERA

Simulation is crucial for validating APT detection models. CALDERA reliably emulates ATTACK techniques. Simulations reveal detection blind spots. Emulation validates model performance and SOC teams use simulation for readiness tests [131]. Actor-specific simulation results are not fed back into CTI systems. Few models integrate ML + CTI + ATTACK simultaneously. Practical validation through adversary emulation is also emphasized in industry literature. [132] recommends using MITRE CALDERA to check how ready organizations are against Iranian APT techniques. He highlights that simulation-driven evaluation is key in supporting CTI and ML-based detection. This review adopts a Systematic Literature Review (SLR) methodology to examine how OpenCTI, MITRE ATTACK, and machine-learning–based behavioral models contribute to the detection and attribution of Advanced Persistent Threats (APTs), with a focused lens on Stealth Falcon as a representative actor. The methodology follows established SLR guidelines (Kitchenham, 2007; PRISMA, 2020) to ensure accuracy, transparency, and repeatability. The review is

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

structured to address two guiding research questions:

RQ1: How can we improve APT detection by combining OpenCTI, MITRE ATT&CK, and machine learning? How does this help us understand how we view threat actors like Stealth Falcon?

RQ2: To what extent do existing studies demonstrate improvements in detection performance (accuracy, precision, false-positives) when using behavioral or ATTACK-aligned models, compared to IOC-based approaches, and how adaptable are these approaches across different APT groups?

Review Design and Methodology Strategy

We chose a systematic review approach. Research on APT detection covers several areas: cybersecurity, machine learning, CTI, and threat-actor profiling. The SLR method ensures: Comprehensive coverage of ATTACK-aligned behavior modeling. Cross-comparison of CTI platforms (OpenCTI, MISP, ThreatKG) and Evaluation of ML-driven APT classification models, Actor-centric interpretation relevant to Stealth Falcon.

Search Strategy: Inclusion and Exclusion Criteria

A multi-database search was performed from 2016 to 2025, covering both academic and intelligence research sources. Databases Searched: IEEE Xplore, ACM Digital Library, Springer Link, Elsevier ScienceDirect, MITRE ATTACK knowledge base, Citizen Lab reports (Stealth Falcon archives), ESET & Check Point APT intelligence reports, Threat intelligence repositories (MISP, GitHub OSINT collections). Search Keywords are Boolean search strings that were used to ensure coverage: "Advanced Persistent Threat" OR "APT detection" AND "MITRE ATTACK" OR "OpenCTI" OR "CTI platform" OR "Machine Learning" AND "Stealth Falcon". Studies were included if they: Discussed APT detection, attribution, or behavioral modeling; utilized MITRE ATTACK, CTI platforms, or ML-based classification; or focused on actor behaviour, campaign analysis, or TTP correlation. Were peer-reviewed OR published by reputable cybersecurity entities, published between 2016–2026. Studies were excluded if they: Focused solely on commodity malware (not APT), Lacked methodological detail, Provided only high-level descriptive summaries, Were duplicates across databases, or Were opinion articles with no empirical or conceptual contribution.

Data Synthesis and Data Extraction Assessment

A narrative synthesis combined with comparative table analysis was used.

Three synthesis layers were applied: Grouping findings into five themes: ATTACK-based detection, CTI-driven actor profiling, Knowledge-graph modeling, ML-based TTP classification, Simulation/validation gaps, while Cross-Study Comparison is a structured table compared: publication year, method type, data source, ATTACK usage ML method strengths & limitations. Each study was rated using a 5-point evaluation scale adapted from Kitchenham (2007). Each paper was coded according to nine analytical dimensions as mentioned below:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Table 1: Data Extraction Dimensions for APT Detection

Dimension	Description
D1: Artifact Type	CTI reports, ATTACK mappings, telemetry logs, knowledge graphs
D2: Detection Method	signature-based, behavior-based, ATTACK-aligned, ML-driven
D3: Use of MITRE ATTACK	Technique mapping, kill-chain reconstruction, actor profiling
D4: Use of CTI Platform	OpenCTI, MISP, ThreatKG, custom graph systems
D5: ML Integration	supervised/unsupervised models, feature engineering
D6: Actor Attribution Detail	how strongly the study supports linking campaigns to APTs
D7: Evaluation Metrics	accuracy, precision, false positives, correlation strength

This coding allowed comparison across very different research traditions (CTI, ML, ATTACK engineering). All reviewed material was publicly available. No intrusive experiments, datasets, or live systems were accessed. Threat intelligence reports used were legally published by MITRE, Citizen Lab, ESET, and Check Point. This section combines findings from the reviewed literature. Using OpenCTI, MITRE ATT&CK, and machine learning improves how we detect and attribute APT campaigns like Stealth Falcon. The findings are categorized according to the research questions (RQ1 and RQ2).

Integration of Open CTI, MITRE ATTACK, and ML in APT Detection

OpenCTI, MITRE ATT&CK, and machine learning (ML) have greatly improved APT detection. Studies showed that when these platforms work together, they boost actor-centric behaviour detection. This helps in attributing advanced persistent threats (APTs), such as Stealth Falcon. OpenCTI offers a graph-based model. It helps map actor behaviours and identify TTPs (Tactics, Techniques, and Procedures) over time. For instance, [133], it was shown how OpenCTI's knowledge graph could effectively map the repeated actions of Stealth Falcon. This includes spear-phishing and PowerShell execution tied to its past attack campaigns. MITRE ATT&CK lets us map TTPs in a standard way. This helps us link Stealth Falcon's attack methods to known adversary tactics. It was noted that using ATTACK's framework improved the detection and attribution of advanced attacks. It did this by connecting observed actions to known APT behaviours [134]. Machine learning (ML) enhanced this model by classifying TTP sequences and automating detection. XGBoost [135] and Random Forest [136] worked well to classify Stealth Falcon's attack patterns. They used ATTACK-based TTP vectors as features, as shown by [137]. The ML models could spot subtle differences in attack patterns. This made them better at detection than traditional IOC-based methods.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Traditional IOC-Based Detection Approaches

Comparing behaviour-based detection with OpenCTI and MITRE ATT&CK highlights the advantages of using behavioural models alongside traditional IOC methods. IOC-based methods work well for spotting known attacks. However, they struggle to adapt to the changing nature of APTs like Stealth Falcon. IOC-based detection primarily relies on static indicators such as IP addresses, file hashes, and URLs. These indicators quickly become obsolete as APT actors change tactics. For example, it was argued that by the time IOCs are spread widely, APT actors have already changed their infrastructure. This makes this method useless against shifting threat actors [138]. In contrast, behaviour-based detection uses MITRE ATT&CK and OpenCTI. It looks at patterns of attack behaviours, like lateral movement and data exfiltration. This helps in spotting new attack methods, even if the actor changes its tools or infrastructure. It was shown that behavioural models could spot Stealth Falcon's activities [139]. They did this by recognising patterns, even when new IOCs were added. ML models trained on TTP vectors also showed improved performance over traditional methods. XGBoost and Deep Neural Networks (DNNs) cut down false positives. They also detected Stealth Falcon's attacks more accurately than static IOC-based models. These models quickly adapted to new attack methods. They learned from past TTP data and real-time CTI feeds [140].

Gaps and Limitations in Current Research

Even with advances in behaviour-based detection through OpenCTI, MITRE ATT&CK, and machine learning, there are still research gaps. Real-World Validation: Many of the studies reviewed lacked real-world validation of their models. MITRE CALDERA and simulated datasets were used in some studies. However, the real use of these models in live operations is still limited. Using real-world datasets from live systems can improve models' applicability and generalization [144]. Actor-Specific Profiling: Actor-specific models look promising. However, there's still limited work on detecting multiple APT groups focused on individual actors. Most studies focused on Stealth Falcon, with limited cross-comparison to other APTs like APT28 and APT33. This limits how well actor-centric models apply to other threat groups with similar TTP patterns. Scalability and Adaptability: Machine learning models did a good job classifying Stealth Falcon's TTPs. However, they faced scalability issues with larger datasets. ML-based models still face challenges in real-time operations, especially for large organisations. The Discussion section looks at the findings from the Results chapter. It links them to the research questions and looks at the strengths, limitations, and implications of the findings. This study shows that using OpenCTI, MITRE ATT&CK, and machine learning to detect and attribute Advanced Persistent Threats (APTs) from the Stealth Falcon group works well. However, several important aspects require further exploration and refinement. This section looks at the importance of these findings and highlights key areas for future research.

RQ1: **How can the integration of OpenCTI, MITRE ATTACK, and machine learning improve APT detection and support actor-centric behavioral attribution for threat actors such as Stealth Falcon**

The findings show that using OpenCTI, MITRE ATT&CK, and machine learning

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

together boosts APT detection. This approach builds a complete, behaviour-based framework. OpenCTI maps Stealth Falcon's tactics and techniques. This creates a dynamic knowledge graph for actor-specific detection across campaigns. MITRE ATT&CK uses a clear structure to connect behaviours to known tactics, techniques, and procedures (TTPs). Machine learning boosts detection by automating attack pattern classification. This cuts down false positives and improves accuracy. This combination helps detect threats in real time. It also profiles actors, making it easier to attribute and distinguish Stealth Falcon's attack patterns from other APT groups. Behavior-Based Detection: OpenCTI and MITRE ATT&CK worked together to boost the detection of Stealth Falcon's actions. This includes spear-phishing, PowerShell use, and DNS tunneling. OpenCTI used graph-based analysis to link activities across many campaigns. This method helps in continuously detecting and mapping ongoing behaviours over time. Machine Learning in Detection: XGBoost and Random Forest models classified TTP sequences from Stealth Falcon's campaigns effectively. These models demonstrated higher accuracy compared to traditional IOC-based detection systems. ML models manage complex, high-dimensional data well. They also automate behaviour classification, which helps them adapt to changing APT tactics.

RQ2: **To what extent do existing studies demonstrate improvements in detection performance (accuracy, precision, false positives) when using behavioral or ATTACK-aligned models, compared to IOC-based approaches, and how adaptable are these approaches across different APT groups**

Linking behaviour-based detection models to MITRE ATT&CK has boosted detection performance significantly. Machine learning models using TTP sequences from ATTACK techniques outperformed traditional IOC-based methods. They showed better accuracy and precision. Accuracy & Precision: The XGBoost model showed the highest detection accuracy. It was particularly good at distinguishing Stealth Falcon's attack patterns from those of other APT groups. This was especially true when compared to IOC-based methods. Those methods rely on static indicators that quickly become outdated. Using MITRE ATT&CK mappings with machine learning helps models adapt to new APT behaviours more efficiently. False Positives: Machine learning models greatly cut down on false positives. This was a big problem for traditional IOC-based systems. These systems often raise alerts for harmless actions, like PowerShell use during updates. In contrast, ML-based models can tell apart malicious activities from benign ones by analysing TTP patterns. Adaptability to Other APT Groups: A major benefit of the ATTACK-aligned machine learning method is that it can adapt to various APT groups. The methods used on Stealth Falcon can also apply to other groups like APT28, APT33, and Lazarus Group, if enough TTP data is available. [145] highlighted how ATTACK-based models can adapt to various APT behaviours. Future research should also validate these models against a wider range of adversaries.

Limitations and Future Directions

While the findings provide valuable insights, this study is subject to several limitations: Real-World Validation: The research primarily utilized historical threat intelligence and simulated data. The findings have not been tested in a live,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

operational environment. Real-world validation is key. It helps us see how well the proposed models work in changing and uncertain conditions. Cross-APT Generalizability: The study centred on Stealth Falcon. The model showed it could work well, but more research is needed. We must explore how this approach scales and applies to other APT groups and threat types. Tool Integration Challenges: The integration of OpenCTI and machine learning models with existing SIEM (Security Information and Event Management) systems and SOAR (Security Orchestration, Automation, and Response) platforms is not yet fully explored. Operational integration presents several challenges that require further investigation. Model Interpretability: Machine learning models can classify data accurately. It's still tough to see how they make decisions, especially deep neural networks. This is crucial for cybersecurity teams to trust and act upon the model's predictions effectively. Several avenues for future research emerge from this study: Future research should explore the OpenCTI, MITRE ATT&CK, and Machine Learning framework in real-world situations. This would give useful insights into how the model detects things in real time and performs. Expansion to Other APT Groups: This study focused on Stealth Falcon, but it would help to expand the framework. Covering more APT groups would improve cross-group adaptability. This could help check how well the model works with different APT tactics. Integration with SOC Tools: Future efforts should focus on smoothly connecting the framework to SIEM and SOAR systems. This would automate threat detection and response tasks. It reduces manual work and boosts efficiency. Enhanced Actor Profiling: Future research could improve actor profiling. This can be done by adding data sources like social media activity, language analysis, and political context. These could boost the accuracy of actor attribution and help us better anticipate enemy actions. You can check out new methods like unsupervised learning and reinforcement learning. These can help improve how we classify behaviour. These techniques might find new threats and help models adapt to changing enemy behaviours. Simulation and Emulation Enhancements in the MITRE CALDERA simulation provide a secure environment to test detection models. Advancements in adversary emulation will help us understand detection gaps and system weaknesses. They will also show how well detection models handle more complex APT tactics.

Conclusion

This study explores how to merge OpenCTI, MITRE ATT&CK, and machine learning to spot Advanced Persistent Threats (APTs). It uses Stealth Falcon as a case study. This research shows major progress in detecting APTs and identifying actors. It brings together cyber threat intelligence (CTI) platforms, ATTACK-based behaviour modelling, and machine learning classification. The integration of OpenCTI and MITRE ATT&CK enhances actor-centric detection. It links TTPs (Tactics, Techniques, and Procedures) to known threat actors like Stealth Falcon. Machine learning models effectively classified Stealth Falcon's TTPs. They achieved better accuracy and precision than traditional IOC-based methods. Actor-centric attribution uses consistent behaviour patterns to track APT activities across campaigns. This method is a powerful tool for incident response and threat intelligence. This study adds to the field of behavioural APT detection. It provides useful insights for future

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

research and practical cybersecurity use. This study adds to research on APT attribution by showing how well OpenCTI, MITRE ATTACK, and machine learning work together. Key strengths of the study include: Comprehensive Coverage: The SLR gave a clear view of current research. It showed how various CTI platforms, ATTACK frameworks, and ML methods are used in APT detection. It brings together findings from different sources. This gives a clear view of the current state of APT detection methods. Real-Time Detection: The use of OpenCTI and MITRE ATTACK enabled tracking of Stealth Falcon's behaviour in real time. This is key for adapting to the ever-changing threat landscape of APT campaigns. Actor-Centric Detection: OpenCTI's actor-specific profiling, along with ATTACK mappings, boosts attribution accuracy. This is especially true for APTs like Stealth Falcon, which use advanced evasion techniques. This study provides helpful insights, but it has some limitations for future research to consider: Real-World Validation: The study showed that OpenCTI, MITRE ATT&CK, and machine learning work well in controlled settings. However, they still need real-world validation. Threat intelligence platforms and machine learning models must be tested in live networks. This helps us see how well they work in changing environments and against real APT actors. Scalability: The machine learning models classified Stealth Falcon's TTPs well. However, we still question how they'll scale in larger, enterprise-level settings. Future research should focus on testing these models on larger datasets and in distributed networks. Cross-APT Group Adaptability: The methods showed promise for Stealth Falcon, but more studies are needed. We must find out how well these models apply to other APT groups with different TTPs. We need to broaden the research. This includes studying various APT campaigns and testing the detection models against more types of adversaries. The results of this study have several practical implications for cybersecurity: Enhanced Detection Systems: Organisations should adopt a behaviour-based detection framework. This should integrate CTI platforms and MITRE ATT&CK to better detect APT groups. Machine learning models using TTP chains provide a flexible and scalable way for real-time detection. Proactive Threat Attribution: This actor-focused model gives a more accurate and proactive method to identify APTs. Linking observed behaviours to known APT groups helps defenders identify adversaries quickly. This way, they can also anticipate the next steps, improving incident response. Tool Integration: Connecting platforms like OpenCTI with SIEMs and SOAR will help organisations automate detection and attribution.

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

have given their consent.

References

Abbas, G., Ali, A., Mushtaq, Z., Rehman, A. U., Hussen, S., & Hamam, H. (2025). Advancing wind energy potential estimation through multidistribution wind speed analysis in coastal Pakistan. Scientific Reports, 15(1), 18297.

Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016, October). Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 755-766).

Tariq, S., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2025). Alert fatigue in security operations centres: Research challenges and opportunities. ACM Computing Surveys, 57(9), 1-38.

Al-Sada, B. M. (2024). Threat Profiles Analysis Based on MITRE ATTACK Knowledge Base (Doctoral dissertation, Hamad Bin Khalifa University (Qatar)).

Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L. T. H., Lim, H. W., & Sikdar, B. (2025). MITRE ATTACK Applications in Cybersecurity and The Way Forward. arXiv preprint arXiv:2502.10825.

Ruohonen, S., Kirichenko, A., Komashinskiy, D., & Pogosova, M. (2024). Instrumenting OpenCTI with a capability for attack attribution support. Forensic Sciences, 4(1), 12-23.

Gao, P., Liu, X., Choi, E., Ma, S., Yang, X., Ji, Z., ... & Song, D. (2022). Threatkg: A threat knowledge graph for automated open-source cyber threat intelligence gathering and management. arXiv preprint arXiv:2212.10388.

Chen, Z. S., Vaitheeshwari, R., Wu, E. H. K., Lin, Y. D., Hwang, R. H., Lin, P. C., ... & Ali, A. (2024). Clustering apt groups through cyber threat intelligence by weighted similarity measurement. IEEE Access.

Huang, Y. T., Guo, Y. R., Wong, G. W., & Chen, M. C. (2024). A Cascade Approach for APT Campaign Attribution in System Event Logs: Technique Hunting and Subgraph Matching. arXiv preprint arXiv:2410.22602.

Saeed, Najaf, et al. "An enhanced mechanism for advanced persistent threat (APT) detection based on deep learning." Spectrum of engineering sciences (2025): 118-142.

Saeed, Najaf, et al. "Improving DeepFake Detection: A Comprehensive Review of Adversarial Robustness, Real-Time Processing and Evaluation Metrics." Journal of Computing & Biomedical Informatics 7.02 (2024).

The MITRE Corporation. (2025, April 25). Stealth Falcon (G0038). MITRE ATT&CK. https://attack.mitre.org/groups/G0038/Check Point Research. (2025). CVE-2025-33053, Stealth Falcon and Horus: A saga of Middle Eastern cyber espionage. Check Point Software Technologies Ltd. https://research.checkpoint.com/2025/stealth-falcon-zero-day/

Rani, N., Saha, B., & Shukla, S. K. (2024). A comprehensive survey of advanced persistent threat attribution: Taxonomy, methods, challenges and open research problems. arXiv preprint arXiv:2409.11415.

Khan, I. U., Ali, A., Taylor, C. J., & Ma, X. (2025). Data-driven insights: Boosting

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

algorithms to uncover electricity theft patterns in ami. IEEE Transactions on Instrumentation and Measurement.

Khan, W., Ishrat, M., Ahmed, M. N., Abidin, S., Husain, M., Izhar, M., ... & Ali, A. (2025). Enhancing anomaly detection in attributed networks using proximity preservation and advanced embedding techniques. IEEE Access.

Abbas, G., Ali, A., Othman, M. T. B., Nawaz, M. W., Rehman, A. U., & Hamam, H. (2025). A novel energy pattern factor-based optimized approach for assessing Weibull parameters for wind power applications. Scientific Reports, 15(1), 37.

Liaquat, S., Hussain, T., Kassab, F. A., Ali, A., Celik, B., Fourney, R., & Hansen, T. M. (2025). An Integrated Two-Stage Hybrid P2P-DR Transactive Energy Trading Platform Using Iterative Distributed-Mixed Integer Linear Optimisation. IET Smart Grid, 8(1), e70027.

.

A. Zadeh, R. Zellers, E. Pincus, and L.-P. Morency, "Multimodal sentiment intensity analysis in videos: Facial gestures and verbal messages," IEEE Intelligent Systems, vol. 31, no. 6, pp. 82-88, 2016.

V. Perez-Rosas, R. Mihalcea, and L.-P. Morency, "Utterance-level multimodal sentiment analysis," in Proc. 51st Annu. Meeting Assoc. Comput. Linguistics (ACL), 2013, pp. 973-982.

M. Wöllmer, A. Metallinou, F. Eyben, B. Schuller, and S. Narayanan, "Context-sensitive multimodal emotion recognition from speech and facial expression using bidirectional LSTM modeling," in Interspeech, 2013, pp. 2362-2366.

V. Rozgic, S. Anershan, and G. Mulholland, "Ensemble of SVM trees for multimodal emotion recognition," in Proc. APSIPA Annu. Summit Conf., 2012, pp. 1-4.

N. Majumder, D. Hazarika, A. Gelbukh, and E. Cambria, "Multimodal sentiment analysis using hierarchical fusion with context modeling," Knowledge-Based Systems, vol. 161, pp. 124-133, 2018.

D. Ghosal, M. S. Akhtar, D. Chauhan, S. Poria, A. Ekbal, and P. Bhattacharyya, "Contextual inter-modal attention for multi-modal sentiment analysis," in Proc. EMNLP, 2018, pp. 3454-3466.

D. Hazarika, S. Poria, R. Mihalcea, E. Cambria, and R. Zimmermann, "ICON: Interactive conversational memory network for multimodal emotion detection," in Proc. EMNLP, 2018, pp. 2594-2604.

H. Pham, P. P. Liang, T. Manzini, L.-P. Morency, and B. Póczos, "Found in translation: Learning robust joint representations by cyclic translations between modalities," in Proc. AAAI, 2019, pp. 7521-7528.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Ali, G., Shahbaz, H., Hassan, M. A., Ahmad, M., & Waleed, M. (2024). An Enhanced Approach of Exploring Digital Economy Using Modern Computer

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Networks. Spectrum of Engineering Sciences, 2(4), 292-312.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Blockchain-based Privacy Preservation Framework for IoT-Based Information Systems. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-7). IEEE, 2022

Y. Wang, Z. Liu, X. Qiu, and M. Zhang, "Gated fusion for efficient multimodal sentiment analysis," IEEE Transactions on Multimedia, vol. 24, pp. 230-241, 2022.

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Ayub, N., Yaseen, A., Amin, M. N., Rizwan, S. M., Farooq, I., & Hussain, M. Z. (2025). Reliable Federated Learning (Rdl) Assisted Intrusion Detection And Classifications Approach Using (Ssl/Tls) For Network Security. Annual Methodological Archive Research Review, 3(7), 376-400.

M. Chen, Q. Jin, and S. Wang, "Multimodal sentiment analysis with attention-based fusion on social media data," IEEE Access, vol. 9, pp. 45123-45132, 2021.

D. Guo, H. Wang, Y. Zhang, and R. Xu, "Deep multimodal representation learning for sentiment analysis," IEEE Access, vol. 7, pp. 102345-102354, 2019.

N. Majumder, S. Poria, A. Gelbukh, and E. Cambria, "DialogueRNN: An attentive RNN for emotion detection in conversations," in AAAI, 2019, pp. 6818-6825.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

D. Ghosal, N. Majumder, S. Poria, R. Mihalcea, and A. Gelbukh, "DialogueGCN: A graph convolutional neural network for emotion recognition in conversation," in EMNLP, 2019, pp. 154-164.

Ali, M., Khan, H., & Rehman, S. U. (2023). Edge Computing for Low-Latency IoT Applications. International journal of advanced sciences and computing, 38-

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

49Malik, A., Khan, H., Ali, A., Nawaz, A., & Ahmad, S. The Impact of Climatic Parameters on the Streamflows & Future Sustainable Hydro-Energy Generation Predicting Streamflows for the 21st Century Under Climate Change Scenarios.

Y. Shen et al., "DialogXL: All-in-one XLNet for multi-party conversation emotion recognition," in AAAI, 2020, pp. 8835-8842.

Ali, M., Khan, H., Din, I. U., Tariq, M. I., & Javed, A. Design and Implementation Role of Middleware in Shared Network Environments: A Systematic Review. Securing the Digital Realm, 229-243.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

G. Hu, Z. Xu, Y. Li, and J. Luo, "MM-GCN: Multi-modal graph convolutional network for personalized micro-video recommendation," IEEE Transactions on Multimedia, vol. 24, pp. 451-462, 2022.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

G. Abbas, A. Ali, M. Zubair, Z. Mushtaq, U. Farooq and I. A. Khan, "Identifying Appropriate Probability Density Function for Wind Speed Profiles of Two Coastal Cities in Pakistan for Better Wind Power Assessment," 2024 3rd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE), Lahore, Pakistan, 2024, pp. 1-5, doi: 10.1109/ETECTE63967.2024.10823896.

Ali, A., Khan, L., Javaid, N., Bouk, S. H., Aldegheishem, A., & Alrajeh, N. (2025). Mitigating anomalous electricity consumption in smart cities using an AI-based stacked-generalization technique. IET Renewable Power Generation, 19(1), e12785.

Abbas, G., Ali, A., Rashid, F., Ashraf, N., Mushtaq, Z., & Zubair, M. (2024). An optimal approach for assessing Weibull parameters and wind power potential for six coastal cities in Pakistan. IEEE Access, 13, 2503-2517.

Ali, A., Farquad, M. A. H., Atheeq, C., & Altaf, C. (2024). A quantum encryption algorithm based on the rail fence mechanism to provide data integrity. Engineering, Technology & Applied Science Research, 14(6), 18818-18823.

Alharthi, A. I., Khalid, A., Ahmad, P., Ali, A., Saleem, S., & Munir, M. A. (2025). A study on the role of moderate optical band gap energy in dielectric properties of NiFe 2 O 4 nanoparticles by Ce ion doping for electronic device applications: the effect of doping concentration. Physical Chemistry Chemical Physics, 27(23), 12405-12415.

Ali, A., Hansen, T. M., Liaquat, S., & Hussain, T. (2025, June). Energy-constrained

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

critical load aware post-disaster home energy management. In 2025 IEEE Kiel PowerTech (pp. 1-6). IEEE.

Patidar, K., Jain, S., Husain, M., Muqeem, M., Ahmed, M. N., Khan, A. N., ... & Mushtaque, N. (2025). Blockchain Based Decentralized Identity Management System for Authentication and Authorization in IoT Networks. Informatica, 49(34).

Jain, A., Muqeem, M., Uzair, M., Madina, M., Arabia, S., Ahmed, M., ... & Ali, A. (2025). Integrating UAV Networks and Edge Computing for Smart Cities: Architecture, Techniques, and Future Trends. International Arab Journal of Information Technology (IAJIT), 22(6).

Ali, Arshad. "Coarse Classification of Terrain Image Information by Using Sobel Edge Detection Technique." International Journal of Computer Network and Information Security 18 (2018): 149-154.

Ali, A., & Alsaawvy, Y. (2019). Un-Interrupted Glucose Monitoring and Prediction by Using Smart Sensor System. IJCSNS, 19(4), 211.

Ali, A., Fakhar, M. S., Kashif, S. A. R., Abbas, G., Khan, I. A., Rasool, A., & Ullah, N. (2022). Optimal scheduling of neural network-based estimated renewable energy nanogrid. Energies, 15(23), 8933.

Ali, A., Khan, L., Javaid, N., Bouk, S. H., Aldegheishem, A., & Alrajeh, N. (2025). Mitigating anomalous electricity consumption in smart cities using an AI-based stacked-generalization technique. IET Renewable Power Generation, 19(1), e12785.

Ali, A. (2022). A framework for air pollution monitoring in smart cities by using IoT and smart sensors. Informatica, 46(5).

Ali, Arshad. "Images classification and feature extraction by using unmanned aerial vehicles (uav's)." International Journal of Applied Engineering Research 12.24 (2017): 15432-15437

J. Wei, Z. Lin, J. Li, and Y. Zhang, "EmoBERTa: Speaker-aware emotion recognition in conversation with pre-trained neural networks," arXiv preprint arXiv:2009.08458, 2020.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242

W. Li, Z. Yang, J. Yu, and C. Zhang, "Align and prompt: Video-and-language pre-training with entity prompts," in CVPR, 2022, pp. 4953-4963.

Ayub, N., Uzair, M., Din, I., Ali, A., Khan, H., Yuldashev, F., & Makhmudov, S. (2025). An Efficient Human Activity Recognition (HAR) Model Based on Convolutional Neural Networks for Computing Devices Aiming to Reduce Latency and Tackle the Inactivity of Gadgets. Engineering, Technology & Applied Science Research, 15(6), 28885-28890.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

T. Fu, X. Li, Y. Zhang, and J. Gao, "VIOLET: End-to-end video-language transformers with masked visual-token modeling," arXiv preprint arXiv:2111.12681, 2021.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

L. Zhu, Y. Yang, P. Hsieh, and S.-F. Chang, "ActBERT: Learning global-local video-text representations," in CVPR, 2020, pp. 8746-8755.

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

H. Luo et al., "UniVL: A unified video and language pre-training model for multimodal understanding and generation," arXiv preprint arXiv:2002.06353, 2020.

Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," arXiv preprint arXiv:1503.02531, 2015.

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

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

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.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

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

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

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

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

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.

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

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, Oct. 2018

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

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

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

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

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.

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

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. 2018

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.

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

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... &

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

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

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

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

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.

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

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

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

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

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

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

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

, G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

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

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

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.

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

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Hardware and Software Security, Communication, and Forensics, 126.

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). 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, 14(4), 442-452.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Impact of adopting robots as teachers: a review study. In 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC) (pp. 1-9). IEEE.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

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

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Hashmi, U., & ZeeshanNajam, S. A. (2023). 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, 14(4), 442-452.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ...

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

& Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

Khan, A. K., Ghafoor, U., Ayub, N., Ali, A., Abdullah, M. M., & Khan, H. (2026). AI and Machine Learning Assisted Customer Aware Queries: A Comprehensive Analysis to improve User experience based on Natural Language Processing (NLP), Databricks, and Oracle APEX. The Asian Bulletin of Big Data Management, 6(1), 94-118.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Y. Zhang, S. Wang, and R. Li, "Multimodal sentiment analysis with dynamic fusion graph," Information Fusion, vol. 91, pp. 142-153, 2023.

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

Z. Sun, P. Sarma, W. Sethares, and Y. Liang, "Self-supervised learning for multimodal sentiment analysis," arXiv preprint arXiv:2011.09673, 2020.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

L. Li, H. Yin, Y. He, and X. Wang, "Oscar: Object-semantics aligned pre-training for vision-language tasks," in ECCV, 2020, pp. 421-437.

Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

P. Zhang et al., "VinVL: Revisiting visual representations in vision-language models," in CVPR, 2021, pp. 5579-5588.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

Z. Dou et al., "An empirical study of training end-to-end vision-and-language transformers," in CVPR, 2021, pp. 18166-18176.

Ali, H., Ayub, N., Irfan, A., Fayyaz, S., Masood, H., Ahmad, A., ... & Khan, H. (2025). A Unified AI-powered Social Media Platform for Intelligent Scheduling and Data Driven Analytics Using Multi-Layered Artificial Neural Networks (ANNs): https://doi. org/10.5281/zenodo. 17572988. Annual Methodological Archive Research Review, 3(11), 94-134.

Z. Wang et al., "SimVLM: Simple visual language model pretraining with weak supervision," in ICLR, 2021.

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

J.-B. Alayrac et al., "Flamingo: a visual language model for few-shot learning," in NeurIPS, 2022, pp. 23716-23736.

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.

J. Li, D. Li, C. Xiong, and S. Hoi, "BLIP: Bootstrapping language-image pretraining for unified vision-language understanding and generation," in ICML, 2022, pp. 12888-12900.

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

H. Akbari et al., "VATT: Transformers for multimodal self-supervised learning from raw video, audio and text," in NeurIPS, 2021, pp. 24206-24221.

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

V. Gabeur, C. Sun, J.-B. Alayrac, and C. Schmid, "Multi-modal transformer for video retrieval," in ECCV, 2020, pp. 214-229.

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

J. Lei et al., "Less is more: ClipBERT for video-and-language learning," in CVPR, 2021, pp. 13571-13581.

Hamayun Khan,Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland

Muhammad Anas,Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Farooq, I., Ghafoor, U., Umer, S., Ali, A., Shahid, A. K., & Khan, H. (2025). An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud. The Asian Bulletin of Big Data Management, 5(4), 231-258.

Hassan, A., Hadullo, K., & Tole, K. (2025). Advances in Cybersecurity: A Literature Review. International Journal of Computer Applications Technology and Research.

Tahir. (2024, December 8). The rise of Iran-backed APT groups APT 33, 34, and 39: 5 steps to secure your network. Medium. https://medium.com/@tahirbalarabe2/the-rise-of-iran-backed-apt-groups-apt-33-34-and-39-5-steps-to-secure-your-network-d755b9d18239

Ghura, B. S. (2023). Scaling & Automating Cyber Threat Intelligence (CTI) Operations with Free and Open-source Software (FOSS).

Park, N. E., Lee, Y. R., Joo, S., Kim, S. Y., Kim, S. H., Park, J. Y., ... & Lee, I. G. (2023). Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks. Computers and Electrical Engineering, 105, 108548.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
https://doi.org/10.5281/zenodo.19240257

Online ISSN 3007-3197
Print ISSN 3007-3189

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys & Tutorials, 25(3), 1748-1774.

Guarascio, M., Cassavia, N., Pisani, F. S., & Manco, G. (2022). Boosting cyber-threat intelligence via collaborative intrusion detection. Future Generation Computer Systems, 135, 30-43.

Thilakarathne, N. N., Bakar, M. S. A., Abas, P. E., & Yassin, H. (2025). A novel cyber threat intelligence platform for evaluating the risk associated with smart agriculture. Scientific Reports, 15(1), 3904.

MITRE ATT&CK. (2025). OilRig (G0049): Threat Group Profile. MITRE Corporation. https://attack.mitre.org/groups/G0049

Rastogi, N., & Alam, M. T. (2023). Cyber Threat Intelligence for SOC Analysts.

González, F. S., Pastor-Galindo, J., & Ruipérez-Valiente, J. A. (2025). Toward interoperable representation and sharing of disinformation incidents in cyber threat intelligence. arXiv preprint arXiv:2502.20997.

Zhuwankinyu, E. K., Mupa, M. N., & Tafirenyika, S. (2025). Graph-based security models for AI-driven data storage: A novel approach to protecting classified documents.

Mohamed, I., Hefny, H. A., & Darwish, N. R. (2024). Enhancing cybersecurity defenses: a multicriteria decision-making approach to MITRE ATTACK mitigation strategy. arXiv preprint arXiv:2407.19222.

Tallam, Krti. "Transforming Cyber Defense: Harnessing Agentic and Frontier AI for Proactive, Ethical Threat Intelligence." arXiv preprint arXiv:2503.00164 (2025).