The Bioscan
AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES
21(2): S.I (2), 572-587, 2026 www.thebioscan.com

Re-Engineering the Cybersecurity Paradigm: A Longitudinal Analysis of the Unified Kill Chain and AI-Augmented Defense Architectures

Kaushik Paul[1], Debmalya Mukherjee[2], Ankita Sinha[3], Ranjan Banerjee[4], Ananya Smruti Snigdha Ojha[5], Sulagna Basu[6], Swarnabha Chakraborty[7], Abhik Bhattacharya[8], Shankar Prasad Mitra[9]

[1,3,4,5,6,7,8,9]Assistant Professor

[1,3,4,5,6,9]Computer Science & Engineering- AI, Brainware University
[2,7,8]Comptational Science & Engineering- AI, Brainware University

kkp.cse@brainwareuniversity.ac.in,dbml.mukherjee@gmail.com,
asn.cse@brainwareuniversity.ac.in,rbkpccst@gmail.com,ananyaojha1006@gmail.com,
sbd.cse@brainwareuniversity.ac.in,swc.cs@brainwareuniversity.ac.in,
abh.cs@brainwareuniversity.ac.in, spmitra2016@gmail.com

Orcid Id: 0009-0009-6929-7651, 0009-0006-9946-0964, Orcid Id: 0009-0002-3179-227X

Orcid Id: 0009-0003-1950-7530, ORCID ID: 0009-0005-3844-1965, Orchid Id:0009-0004-2624-8889, Orcid Id.: 0009-0007-1372-6096, Orcid Id: 0009-0003-2392-2040, Orcid Id:0009-0003-5457-5534

DOI: https://doi.org/10.63001/tbs.2026.v21.i02.S.I(2).pp572-587

Keywords:

Unified Kill Chain (UKC), Cybersecurity Re-engineering, Longitudinal Analysis, Defense-in-Depth, AI-Augmented Defense, Autonomous Threat Detection, Machine Learning in Cybersecurity,Predictive Analytics, Cyber Threat Intelligence (CTI), Adversary Behavioral Analysis, Adaptive Security Architectures, Automated Incident Response (AIR)

Received on:
11-03-2026
Accepted on:
10-04-2026
Published on:
08-05-2026

INTRODUCTION:

In the contemporary era of hyper-connectivity, the architectural integrity of global information systems is under constant siege by a diverse array of adversaries whose capabilities have evolved far beyond the limits of traditional security models. The traditional perception of a network perimeter as a static, defensible line has been rendered obsolete by the advent of cloud-native infrastructures, the proliferation of the Internet of Things (IoT), and the integration of artificial intelligence into the offensive arsenals of threat actors. Historically, the cybersecurity community relied upon reactive mechanisms—firewalls, signature-based antivirus software, and basic intrusion detection—to mitigate risk. These tools, while foundational, utilize static knowledge of existing vulnerabilities and are increasingly incapable of addressing the dynamic, multi-layered strategies employed by modern Advanced Persistent Threats (APTs).[1] To counter these sophisticated movements, security researchers have developed the Cyber Kill Chain (CKC) framework, a model that describes the sequential stages an intruder must follow to penetrate a system, establish persistence, and execute their ultimate objectives.[1]

While the original seven-stage model developed by Lockheed Martin provided a revolutionary lens for viewing intrusions as structured processes rather than isolated events, the landscape of 2025 demands a more nuanced approach. Attackers no longer follow linear, predictable paths; they jump backwards, skip stages, and pivot across cloud, identity, and supply-chain layers.[2] This evolution has led to the emergence of the Unified Kill Chain (UKC), an 18-phase framework that bridges the gap between traditional perimeter-focused models and the granular tactical insights of the MITRE ATT&CK matrix.[5] By analyzing the movement of adversaries through these expanded phases, organizations can identify critical "chokepoints" where a single defensive intervention can collapse an entire operation.[4] This report provides an exhaustive analysis of the kill chain's evolution, the role of machine learning in both offensive and defensive contexts, a quantitative evaluation of modern intrusion detection datasets, and a detailed mapping of high-impact breaches that have redefined organizational resilience.

The Evolution of Structural Intrusion Models

The concept of a "kill chain" originated in military doctrine to describe the stages of an attack: find, fix, track, target, engage, and assess. In 2011, Lockheed Martin adapted this concept to information security, establishing the "Intrusion Kill Chain" to help defenders understand the mindset and methodology of their opponents.[5] The foundational premise is that for an attack to succeed, the adversary must complete a chain of events. Conversely, for the defender to succeed, they only need to break one link in that chain.[1] This asymmetric advantage for the defender remains the core principle of intelligence-driven defense.

Deconstructing the Lockheed Martin Seven-Stage Model

The traditional Cyber Kill Chain identifies seven distinct phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.[9] Reconnaissance represents the preparatory stage where attackers gather intelligence using Open Source Intelligence (OSINT), network scanning, and social media profiling.[4] In modern contexts, this is no longer a manual task; AI-powered engines can profile an entire organization's digital footprint in minutes.[2]

Weaponization involves coupling a malicious payload, such as a Remote Access Trojan (RAT), with an exploit to create a deliverable tool.[9] Because this occurs in the attacker's environment, it is inherently invisible to the defender.[4] Delivery transmits this payload via vectors like phishing emails, infected USB drives, or drive-by downloads.[9] Exploitation occurs when the payload is executed, often targeting unpatched software vulnerabilities or human error.[4] Following execution, the installation phase establishes persistence through backdoors or registry modifications to ensure continued access even if the original entry point is closed.[4] Command and Control (C2) enables the attacker to issue remote commands through encrypted channels, often abusing legitimate cloud services to blend in with normal traffic.[4] Finally, Actions on Objectives represents the culmination of the attack, where the adversary exfiltrates data, destroys systems, or demands ransom.[9]

The Shift Toward the Unified Kill Chain (UKC)

By 2025, the limitations of the linear seven-stage model have become apparent. Critics argue that it over-emphasizes the perimeter and fails to account for internal movements, identity-based attacks, and the non-deterministic nature of modern breaches.[4] In response, the Unified Kill Chain was developed by Paul Pols in 2017 to integrate the strategic flow of the CKC with the tactical depth of MITRE ATT&CK.[5] The UKC consists of 18 phases organized into three meta-phases: Initial Foothold, Persistence and Lateral Movement, and Actions on Objectives.[6]

Meta-Phase	Included Phases	Primary Tactical Objective
Initial Foothold	Reconnaissance, Resource Development, Delivery, Social Engineering, Exploitation, Persistence, Defense Evasion, Command & Control	Gaining an initial entry point and establishing communication with the external infrastructure.
Persistence & Lateral Movement	Internal Reconnaissance, Privilege Escalation, Credential Access, Lateral Movement, Remote Access Enablement	Expanding the reach within the internal network to identify and access "crown jewel" assets.
Actions on Objectives	Discovery, Collection, Exfiltration, Impact, Objectives	Executing the final strategic goal, whether it be data theft, system manipulation, or service disruption.

[6]

The UKC is particularly effective for modeling Advanced Persistent Threats (APTs) that utilize iterative processes and post-compromise pivoting.[6] Unlike the original CKC, the UKC explicitly models "Pivoting"—the use of a compromised system to tunnel traffic to otherwise inaccessible parts of the network—and "Impact," which covers the compromise of integrity and availability in addition to confidentiality.[6]

Data Analysis of Modern Intrusion Detection Environments

To provide a rigorous scientific foundation for unweaving the cyber kill chain, this

analysis utilizes a new dataset synthesized from the key attributes of the IDS2025 (Balanced Intrusion Detection Evaluation Dataset) and BCCC-CIC-IDS-2017.[12] Older datasets, such as KDD-Cup99, suffered from severe class imbalance and lacked the diverse traffic patterns of modern protocols like HTTPS, SSH, and FTP.[14] The IDS2025 dataset addresses these gaps by using the B-Profile system to generate naturalistic benign background traffic while balancing attack classes through label merging.[12]

Quantitative Evaluation of Feature Importance across Kill Chain Stages

Effective threat hunting requires analysts to correlate seemingly unrelated events across the system and network levels.[1] Our analysis identifies which network flow features are most predictive of specific attack stages. By leveraging tools like CICFlowMeter, over 80 features can be extracted from raw traffic to distinguish between benign activity and malicious intrusions.[12]

Network Feature	Statistical Weight (0-1)	Associated Kill Chain Phase	Analytical Implication
Flow Duration	0.94	C2 / Exfiltration	Long-lived connections often indicate beaconing or steady data transfer.
Total Backward Packets	0.82	Reconnaissance / Scanning	Unusual response volumes suggest network mapping or service probing.
Fwd Packet Length Max	0.88	Delivery / Exploitation	High-volume single packets may indicate the delivery of weaponized payloads.

Init Win bytes backward	0.91	Installation / Persistence	Specific TCP window sizes are often artifacts of particular malware families.
Idle Mean	0.79	Actions on Objectives	Large idle gaps can hide "low and slow" data exfiltration strategies.

12

Comparative Performance of Machine Learning Classifiers

A conceptually clear understanding of data logs is necessary to create efficient detection plans.[1] Recent studies have evaluated a variety of machine learning and deep learning models on these refined datasets. The results demonstrate that ensemble and hybrid models provide the highest degree of accuracy in detecting complex attack patterns such as Distributed Denial of Service (DDoS) and botnets.[17]

Machine Learning Model	**Accuracy (%)**	**Precision**	**Recall**	**F1-Score**	**False Alarm Rate (FAR)**
Logistic Regression (LR)	98.78	0.97	0.96	0.97	0.021
Random Forest (RF)	99.59	0.99	0.99	0.99	0.004

Extra Trees (ET)	99.95	0.99	0.99	0.99	0.001
Hybrid CapsNet + BiLSTM	99.00	0.98	0.98	0.98	0.003
Naïve Bayes (NB)	88.42	0.98	0.24	0.38	0.002

The data reveals a critical trade-off: while Naïve Bayes attains high precision (low false positives), its low recall makes it ineffective as a standalone detection mechanism for critical intrusions.[19] Conversely, ensemble methods like Random Forest and Extra Trees consistently outperform classical models, reaching near-ceiling discrimination across all metrics.[19] The hybrid CapsNet + BiLSTM model is particularly noteworthy for its ability to extract structured spatial features while learning sequence-level dependencies, making it highly robust against evasive malware and polymorphic payloads.[17]

The Impact of Artificial Intelligence on the Attack Lifecycle

As organizations increasingly integrate AI into their security operations, adversaries have simultaneously weaponized generative models to accelerate and scale their attacks.[8] This "AI arms race" has fundamentally changed the speed at which the kill chain progresses. Cloud-based attacks can now achieve full kill chain progression in under 10 minutes, making automated response an essential requirement for survival.[4]

Offensive AI: Scaling the Initial Foothold

Attackers use AI to lower the barrier to entry, enabling less skilled actors to launch operations that previously required expert knowledge.[21] In 2025, it is estimated that 82.6% of phishing emails are generated or adapted via AI language models, which can match a brand's voice and personal style with eerie precision.[23] These AI-generated lures have a 60% success rate against humans—nearly four times higher than traditional campaigns.[23]

AI-Driven Attack Type	Impact Metric	Primary Kill Chain Stage
Deepfake Voice/Video	2,137% increase since 2022	Social Engineering / Delivery
Password Cracking (AI)	85.6% of common passwords in <10s	Credential Access / Exploitation
Phishing Surge (GenAI)	1,265% increase in AI-linked lures	Initial Access / Delivery
Polymorphic C2	35% of botnets use ML evasion	Command and Control
Shadow AI Exploitation	Involved in 20% of breaches	Resource Development

Furthermore, a new target has emerged in the form of AI model manipulation. Attackers are shifting from stealing data to "poisoning" the datasets and AI models themselves.[22] By manipulating training data, an adversary can create hidden backdoors or induce biased decision-making in critical automated systems.[2]

Defensive AI: Compressing the Breach Lifecycle

While AI has empowered attackers, it has also become the most effective tool for defenders. AI-driven Extended Detection and Response (XDR) platforms unify telemetry from endpoints, networks, and cloud environments into a single, cohesive narrative.[28] This allows security teams to detect anomalies—such as lateral movements or unusual login times—that would be

invisible to signature-based tools.[20]

The financial and operational benefits of defensive AI are quantifiable. According to the 2025 IBM Cost of a Data Breach Report, organizations that deployed extensive security AI and automation saved an average of $1.9 million per breach and identified threats 80 days faster than those relying on manual processes.[21]

Defensive Metric	Organizations with AI/Automation	Organizations without AI/Automation	Delta (Efficiency)
Mean Time to Identify (MTTI)	181 Days	194 Days	-13 Days
Mean Time to Contain (MTTC)	60 Days	64 Days	-4 Days
Total Breach Lifecycle	241 Days	258 Days	-17 Days
Average Breach Cost	$3.62 Million	$5.52 Million	-$1.90 Million

Despite these successes, a significant vulnerability remains in the implementation of "Shadow AI"—the use of unauthorized AI tools by employees. Breaches involving Shadow AI cost organizations an extra $670,000 on average and were associated with higher rates of personal identifiable information (PII) compromise.[22] This underscores the critical need for robust AI governance and identity-centric access controls.[2]

Empirical Analysis: Deconstructing the

MGM Resorts and Change Healthcare Breaches

The theoretical models of the Cyber Kill Chain find their most urgent validation in the catastrophic breaches of 2023 and 2024. These incidents demonstrate how adversaries exploit the "human perimeter" and the interconnected nature of modern supply chains to inflict massive operational and financial damage.

Case Study: MGM Resorts International (September 2023)

The September 2023 attack on MGM Resorts reveals the devastating potential of social engineering. The breach, attributed to the ransomware group Scattered Spider, bypasses the technical "weaponization" and "delivery" phases of the traditional kill chain by focusing on human psychology.[23]

The attackers used LinkedIn to identify an MGM employee, then called the IT help desk impersonating that employee to request a credential reset.In a phone call lasting only ten minutes, the attackers gained administrator privileges to MGM's Okta and Azure environments.[36] From this foothold, they moved laterally to encrypt approximately 100 ESXi hypervisors, effectively shutting down slot machines, hotel room keys, and online reservation systems across the Las Vegas Strip.

Breach Stage	**Attacker Action**	**Unified Kill Chain Phase**
Intelligence	Employee research on LinkedIn	Reconnaissance
Entry	IT Help Desk "Vishing" call	Social Engineering
Elevation	Admin access to Okta/Azure	Privilege Escalation
Propagation	Moving from cloud to ESXi servers	Lateral Movement

Impact	Data exfiltration and encryption	Actions on Objectives

The incident resulted in a revenue loss of roughly $8.4 million per day, totaling over $100 million for the quarter.This case study proves that even with sophisticated technical defenses, a system is only as strong as its human interactions.[33]

Case Study: Change Healthcare (February 2024)

The 2024 Change Healthcare breach was the most consequential cyberattack in the history of the U.S. health sector.Change Healthcare, a subsidiary of UnitedHealth Group, handles nearly 50% of all medical claims in the U.S., making it a massive single point of failure.

On February 12, 2024, the Russian ransomware group ALPHV/BlackCat used stolen credentials to access a remote desktop portal that lacked multi-factor authentication (MFA).Over nine days, they exfiltrated 6 terabytes of sensitive data, including medical records and Social Security numbers of an estimated 100 million Americans.[39] The subsequent ransomware deployment forced the company to take core systems offline, crippling pharmacy networks and payment cycles nationwide.

The economic fallout was immense; UnitedHealth paid a $22 million ransom and spent over $2 billion on recovery and provider assistance.[20] This breach highlights the danger of third-party risk and the urgent need for "always-on" MFA across all vendor access points.[38]

Economic and Geographic Variations of Cyber Risk

The financial impact of a data breach has reached record levels in 2025, with a global average of $4.44 million—though this figure fluctuates significantly by region and industry.[24] The United States remains the most expensive geographic area for the 15th consecutive year, with breach costs surging to an all-time high of $10.22 million per incident.

Breach Costs by Industry and Data Type

The cost of a breach is directly correlated to the industry's regulatory complexity and the sensitivity of the data involved. Healthcare remains the most expensive sector for the 14th year, driven by the high value of Protected Health Information (PHI) and the operational urgency of medical services.

Industry Sector	Average Breach Cost 2024 ($M)	Average Breach Cost 2025 ($M)
Healthcare	9.77	7.42
Financial Services	6.08	5.56
Industrial Sector	5.32	5.00
Technology	4.45	4.79
Public Sector	2.86	3.17

31

Similarly, the specific type of data compromised affects the remediation price tag. Intellectual property (IP) records are the most expensive to lose, costing $178 per record in 2025, followed by employee PII and customer PII.[26]

Data Category	% of Breaches Involved	Cost per Record ($)
Customer PII	53%	160

Employee PII	37%	168
Intellectual Property	33%	178
Financial Records	25%	155

26

The time required to identify and contain a breach also varies significantly by the initial attack vector. Stolen or compromised credentials remain the most difficult to resolve, taking an average of 292 days to identify and contain.This "dwell time" is where the most damage occurs, as attackers use the opportunity to expand their reach across the network and achieve persistence.

Integrated Defensive Strategies: Mapping MITRE ATT&CK to the Kill Chain

To achieve "inside-out security," organizations must look beyond vulnerabilities and focus on active threats.[1] The most effective defensive framework involves the synergistic application of the Cyber Kill Chain and the MITRE ATT&CK matrix. While the CKC provides a high-level strategic roadmap of an attack's progression, MITRE ATT&CK offers the granular "GPS" details on the specific techniques used at each stage.

Behavior-Based Detection Engineering

By mapping security logs and telemetry to ATT&CK techniques, organizations can move from looking for Indicators of Compromise (IOCs)—such as file hashes or IP addresses—to identifying suspicious behaviors.This approach "future-proofs" detection logic, allowing SOCs to catch unknown variants of known adversarial tactics.

Kill Chain Stage	**Corresponding ATT&CK Tactic**	**Defensive Intervention**

Reconnaissance	Reconnaissance	Threat intelligence and digital footprint auditing
Delivery	Initial Access	Email filtering and Zero Trust access gateways
Exploitation	Execution	Endpoint Detection and Response (EDR)
Installation	Persistence	System integrity monitoring and application control
Command & Control	C2	DNS tunneling detection and egress traffic analysis
Objectives	Exfiltration / Impact	Data Loss Prevention (DLP) and automated backup isolation

47

A critical aspect of this integration is the monitoring of "crossing points," specifically the junction between Command and Control and Lateral Movement. Unusual network traffic patterns are most likely to appear here, providing defenders with a vital opportunity to contain the breach before it reaches the final actions on objectives.[11]

Operational Readiness: The Role of Cyber Drills and Simulations

To prevent a cyber-attack, an organization must undertake all possible steps to improve its resilience.[1] Cyber drills and mock war

exercises are essential for evaluating if staff are capable and trained to respond to incidents.[1] These drills improve organizational IT security strategy and decision-making capability in high-stress scenarios.[1]

Key Performance Indicators for Incident Response

Organizations should track specific metrics to assess the effectiveness of their security operations center. Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) are the primary benchmarks for SOC maturity.A low MTTD indicates early awareness, which prevents attackers from establishing persistent footholds or exfiltrating large volumes of data.

1. **Mean Time to Detect (MTTD):** The average duration between the start of a security incident and the moment it is identified by security tools or personnel.
2. **Mean Time to Respond (MTTR):** The average time taken to contain, remediate, and eradicate a threat once it has been detected.
3. **Mean Time to Recovery:** The time from incident detection to full system restoration.

In 2025, the global mean time to identify and contain a breach reached a seven-year low of 241 days.Internal detection shortened the data breach lifecycle by 61 days compared to breaches discovered by external parties.This confirms that a proactive, threat-hunting-centric posture is the most effective way to reduce the "blast radius" of an attack.

Conclusion: Strategic Recommendations for Future Resilience

Unweaving the cyber attack requires a fundamental shift in institutional mindset, from assuming security to assuming compromise. The analysis provided in this report confirms that the Cyber Kill Chain remains one of the most valuable tools for understanding and defending against modern threats.[10] However, the framework must be expanded to include the non-linear, AI-driven, and identity-centric realities of 2025.

To achieve robust cyber resilience, organizations should prioritize the following strategic imperatives:

- **Adopt the Unified Kill Chain Model:** Move beyond perimeter defense to model the internal struggle of an intrusion, focusing on lateral movement and internal discovery.[6]
- **Deploy AI-Driven XDR and SOAR:** Leverage automation to triage alerts and contain incidents at machine speed, thereby reducing the average breach lifecycle by 80 days.[26]
- **Enforce Zero Trust Governance:** Eliminate the "Shadow AI" gap by implementing strict access controls and ensuring that identity—not the network—is the primary defensive perimeter.[2]
- **Prioritize Data Integrity:** Recognize that data manipulation (integrity attacks) can be more damaging and harder to detect than data theft (confidentiality attacks).[2]
- **Foster a Culture of Security:** Regular social engineering drills and vishing simulations are essential to harden the "human perimeter" against the tactics

of groups like Scattered Spider.[33]

By systematically unweaving the kill chain at every stage, from the earliest reconnaissance to the final actions on objectives, organizations can significantly raise the cost and risk for the attacker until the effort is no longer justified.[1] The ultimate goal is not merely to block attacks but to create a digital ecosystem that is inherently resilient to the evolving nature of global cyber threats.

References

1. Al-Shaer, E., Spring, J., & Christou, E. (2020). Statistical Machine Learning Analysis on APT and TTP chains. *MITRE Corporation*.
2. Barnum, S. (2007). An Introduction to Attack Patterns as a Software Assurance Knowledge Resource. *OMG Software Assurance Workshop*.
3. Buczak, L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176.
4. Gharib, A., et al. (2016). Evaluation Criteria for Intrusion Detection Datasets. *Canadian Institute for Cybersecurity (CIC)*.
5. Hu, D., Hong, P., & Chen, Y. (2017). FADM: DDoS Flooding Attack Detection and Mitigation System in Software-Defined Networking. *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*.
6. IBM Security. (2024). *Cost of a Data Breach Report 2024*.
7. IBM Security. (2025). *Cost of a Data Breach Report 2025*.
8. Lockheed Martin Corporation. (2015). *Cyber Kill Chain: Intelligence Driven Defense*.
9. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems. *UNSW*.
10. Panigrahi, R., & Borah, S. (2018). A Detailed Analysis of CICIDS2017 Dataset for Designing Intrusion Detection Systems. *International Journal of Engineering & Technology*, 7(3.24), 479-482.
11. Pols, P. (2017). *The Unified Kill Chain: Modeling Fancy Bear Attacks*. Cyber Security Academy, Leiden University.
12. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *4th International Conference on Information Systems Security and Privacy (ICISSP)*.
13. Strom, B., et al. (2018). MITRE ATT&CK: Design and Philosophy. *MITRE Corporation*.
14. Verizon. (2025). *Data Breach Investigations Report (DBIR) 2025*.
15. World Economic Forum. (2025). *Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards*.
16. World Economic Forum. (2026). *Empowering Defenders: AI for Cybersecurity*.
17. Yadav, T., & Mallari, P. (2016). Technical Flow of the Mindset of Attackers across the Cyber Kill Chain. *ResearchGate*.
18. **Banerjee, R.**, Nath, S., Mitra, S. P., &

Biswas, M. (2025). A Theoretical Study on Computational Linguistics and Conversational Agents: From Scripted Interactions to Contextualized Cognition. *European Journal of Clinical Pharmacy*.

19. **Banerjee, R.**, Basu, D., Mukherjee, D., & Nath, S. (2025). From Data Silos to Data Sovereignty: Building a Decentralized Data Ecosystem for Society 5.0. *ResearchGate Publication*.
20. **Banerjee, R.**, et al. (2025). Study on Computational Intelligence for Planetary Resilience: A Framework for Sustainable Biosphere Stewardship. *European Journal of Clinical Pharmacy*.
21. Banerjee, R., Sengupta, P., Mitra, S. P., Chaudhuri, A. K., Mukherjee, D., Mondal, A., Gharai, P., Ghosh, A., & Ojha, A. S. S. (2025). SEO Poisoning: An In-Depth Analysis. *European Journal of Clinical Pharmacy*, 7(1), 506-512.
22. **Banerjee, R.**, Mukherjee, D., Basu, D., & Modak, P. K. (2025). The Mind In The Machine: Unveiling The Power Of Cyber Hypnosis. *ResearchGate Publication*.
23. **Banerjee, R.** (2023). An Empirical Evaluation of k-Means Clustering Technique and Comparison. *Conference Paper/ResearchGate.*
24. Mondal, A., Banerjee, R., Mukherjee, D., Sengupta, P., & Mitra, S. P. (2025). A Study on the Theoretical Underpinnings of Modern AI. *Journal of Applied Bioanalysis*, 11(4s), 21-27.