The Bioscan AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES 21(2): S.I (2), 660-672, 2026 www.thebioscan.com

Comparative Analysis of Cybersecurity Threats and Privacy Preservation Frameworks in Heterogeneous IoT Ecosystems: A Data-Driven Evaluation Using the CICIoT2023 Dataset

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

[1,2,3,4,5,6,7,8,9]Assistant Professor

[1,2,3,4,5,6,7,8,9]Computer science & Engineering ,Brainware University

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

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, Orcid Id: 0009-0009-6929-7651, 0009-0006-9946-0964,Orcid Id: 0009-0002-3179-227X, Orcid Id: 0009-0003-1950-7530

DOI: https://doi.org/10.63001/tbs.2026.v21.i02.S.I(2).pp660-672

KEYWORDS
Breast Cancer; Computer Aided Diagnosis; Frequent feature-set mining; Classification

Received on:
14-03-2026
Accepted on:
11-04-2026
Published on:
09-05-2026

Abstract

The digital architecture of the twenty-first century has been fundamentally redefined by the rapid expansion of the Internet of Things (IoT), a paradigm that bridges the gap between physical entities and digital networks. By the year 2025, it is estimated that the global deployment of IoT-connected devices will exceed 30.9 billion, a staggering growth rate that underscores the technology's integration into nearly every facet of modern life, from critical healthcare infrastructure and smart city management to industrial automation and consumer electronics.[1] This interconnectedness provides unprecedented operational advantages, including real-time monitoring and autonomous decision-making capabilities. However, this same connectivity introduces a massive and highly distributed cyberattack surface. Unlike traditional computing systems, IoT environments are characterized by an inherent heterogeneity in communication protocols and a pervasive set of resource constraints—including limited processing power, restricted memory, and low battery capacity—that render conventional security mechanisms, such as heavy-duty encryption and centralized firewalling, largely ineffective.

Introduction

The Architectural Vulnerability and Security Challenges of IoT

The structural limitations of IoT devices create a unique set of vulnerabilities that adversaries exploit through increasingly sophisticated methods. Most IoT nodes are designed for specific, low-power tasks, which often precludes the implementation of robust cryptographic suites or complex security kernels. Standard security challenges

include weak default credentials, the lack of secure boot mechanisms, and infrequent or non-existent firmware update cycles, which leave devices vulnerable to long-term exploitation.[1]

The vulnerability of these systems is further exacerbated by the scale of data collection. IoT devices continuously capture sensitive telemetry, including biometric health data, location history, and environmental signatures, which are often transmitted over unencrypted channels or through third-party cloud platforms without adequate oversight.[1] Recent industry reports indicate that nearly 98% of overall IoT traffic is currently unencrypted, and approximately 57% of globally deployed devices possess vulnerabilities ranked at a medium-to-high severity level.[6] This systemic lack of protection has facilitated the rise of large-scale botnet activities, such as the Mirai-family attacks, which weaponize compromised IoT nodes to launch massive Distributed Denial of Service (DDoS) campaigns that can cripple regional and global internet infrastructure.[7]

Comprehensive Taxonomy of Cyber Threats in Smart Environments

To address the complexities of IoT security, it is necessary to categorize the threat landscape into a functional taxonomy. The Canadian Institute for Cybersecurity (CIC) provides a foundational classification system within the CICIoT2023 dataset, which encompasses 33 distinct attack variants categorized into seven high-level classes.[9]

Volumetric and Resource Exhaustion Attacks

DDoS and Denial of Service (DoS) attacks remain the primary threats in the IoT domain due to the collective bandwidth and processing power of unsecured edge nodes. These attacks are characterized by the transmission of massive volumes of traffic intended to overwhelm the target system's resources. Specific variants include ICMP flooding, UDP flooding, and SYN-ACK fragmentation attacks.[1] In the CICIoT2023 benchmark, these volumetric attacks represent a significant portion of the recorded traffic, demonstrating the ease with which synchronized IoT devices can disrupt critical services.[9]

Botnet Propagation and Mirai-Family Malware

The Mirai malware represents a watershed moment in IoT security, specifically targeting devices by exploiting weak telnet credentials. Once infected, these devices become part of an autonomous botnet. Modern iterations captured in the benchmark include GREIP floods and UDPPlain variants, which are designed to bypass traditional signature-based detection by varying their traffic signatures and exploiting protocol-level vulnerabilities.[9]

Reconnaissance and Identification Activities

Before launching a full-scale attack, adversaries often engage in reconnaissance to map the network topology and identify vulnerable endpoints. These activities include ping sweeps, port scanning, and OS fingerprinting.[2] While these events do not directly exhaust resources, they are critical precursors to more destructive exploits, making their early detection a priority for

modern Intrusion Detection Systems (IDS).

Brute Force and Web-Based Exploits

As IoT gateways frequently employ web-based interfaces for management, they become targets for traditional web vulnerabilities such as SQL injection, command injection, and cross-site scripting (XSS).[9] Simultaneously, brute-force attacks utilize automated scripts to test millions of credential combinations, exploiting the lack of multi-factor authentication in most consumer IoT devices.[7]

High-Level Attack Category	Exemplary Attack Variants	Core Objective
DDoS	ICMP Flood, UDP Flood, SlowLoris, SYN Flood	Infrastructure Disruption
DoS	TCP Flood, HTTP Flood, UDP Flood (Single Source)	Service Denial
Mirai-Family	GREIP Flood, GREeth Flood, UDPPlain	Botnet Expansion
Reconnaissance	Ping Sweep, Port Scan, Host Discovery	Target Intelligence
Brute-Force	Dictionary-based login, Credential Stuffing	Unauthorized Access
Spoofing	ARP Spoofing, DNS Spoofing	Data Interception

Web-Based	SQL Injection, Backdoor, XSS	Malware Injection

9

Data-Driven Intrusion Detection: Analysis of the CICIoT2023 Dataset

The efficacy of an IDS is fundamentally dependent on the quality of the data used for its training and validation. The CICIoT2023 dataset serves as a modern benchmark, addressing the limitations of earlier datasets by providing large-scale, real-time network traffic from a topology composed of 105 real physical IoT devices.[9]

Dataset Characteristics and Feature Space

The dataset consists of approximately 46.6 million labeled flow samples, offering a realistic representation of both benign activity and malicious traffic.[9] It includes 47 flow features categorized into basic flow information, packet flags, protocol types, and advanced statistical measures such as magnitude, radius, covariance, and variance.[10]

A critical observation from the data analysis is the severe class imbalance present in raw IoT traffic. For instance, the ratio between the most frequent attack (DDoS-ICMP_Flood) and the rarest (Uploading_Attack) is as extreme as 5751:1.[9] This imbalance presents a significant challenge for machine learning models, as standard accuracy metrics tend to favor majority classes, leading to a failure in detecting rare but critical threats.[12]

Machine Learning Methodologies and Performance Evaluation

The study evaluates several machine learning algorithms to determine their suitability for anomaly and attack detection in resource-constrained environments. The models analyzed include conventional classifiers like Decision Trees (DT), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN), alongside advanced ensemble methods such as Random Forest (RF) and XGBoost.[1]

Performance is measured using five key metrics: Accuracy, Precision, Recall, F1-score, and Balanced Accuracy. Given the class imbalance, Balanced Accuracy is the most critical metric, as it accounts for the model's performance on minority classes.[12]

Algorithm	**Overall Accuracy**	**Precision**	**Recall**	**F1-Score**	**Balanced Accuracy**

Decision Tree	96.8%	96.2%	96.5%	96.3%	88.2%
Random Forest	99.1%	99.0%	98.9%	98.9%	91.9%
XGBoost	99.3%	99.2%	99.1%	99.1%	92.1%
SVM	94.6%	94.1%	93.8%	93.9%	87.5%
KNN	95.4%	95.0%	94.7%	94.8%	87.9%
Gradient Boosting	99.6%	99.5%	99.6%	99.6%	92.0%

1

The results demonstrate the clear superiority of ensemble learning. XGBoost and Random Forest consistently achieve F1-scores above 99%, indicating a robust capability to differentiate between complex attack patterns.[12] However, the analysis also reveals a significant trade-off between detection accuracy and computational efficiency. Ensemble methods like Gradient Boosting require substantial training time—over 53,000 seconds on large-scale subsets—whereas linear classifiers using Stochastic Gradient Descent (SGD) offer training speeds 200 to 600 times faster, making them more appropriate for real-time edge deployment where latency is a primary concern.[12]

Mathematical Underpinnings of Top-Performing Classifiers

The success of XGBoost in this domain is attributed to its gradient-boosted decision tree framework, which iteratively improves model performance by minimizing a regularized loss function. Mathematically, the objective function $Obj(\Theta)$ at iteration t is defined as:

$$Obj(\Theta) = \sum_{i=1}^{n} L(y_i, \hat{y}_i^{(t-$$

where L is a differentiable loss function, $\hat{y}_i^{(t-1)}$ is the prediction from the previous round, f_t is the new tree added to the ensemble, and Ω represents the regularization term that penalizes tree complexity.[16] This structure allows XGBoost to efficiently capture non-linear relationships in high-dimensional network traffic while avoiding the pitfalls of overfitting.[16]

Random Forest, conversely, utilizes the bagging technique to construct a multitude of independent decision trees. Each tree is trained on a bootstrap sample of the dataset, and the final classification is determined by majority voting. The computational complexity for training a forest with t trees, m features, and n samples is $O(t \times m \times n \log n)$, while the inference time is $O(t \times d)$, where d is the tree depth.[15] This parallelizable nature makes Random Forest highly effective for processing the large volumes of data generated in IoT networks.

Feature Engineering and the AFAM Pipeline

The dimensionality of the IoT feature space necessitates effective feature selection to reduce computational overhead without compromising accuracy. The Attack-aware Feature Aggregation Model (AFAM) has been proposed as a specialized pipeline to address the distortions caused by class imbalance.[14]

AFAM operates by partitioning training data into specific attack domains and applying feature selection (using RF or XGBoost) within these partitions. By aggregating these localized rankings using a maximum operator, the system can identify critical predictors for rare attacks—such as Uploading_Attack and Recon-PingSweep—that would typically be overshadowed in a global feature ranking.[14] Implementing AFAM with the top-30 aggregated features has been shown to increase the F1-score for minority attacks from 11.4% to 67.2% while maintaining near-perfect accuracy for majority classes like DDoS.[14]

Privacy Preservation Paradigms in Connected Ecosystems

The security of an IoT network is inextricably linked to the privacy of its users. Privacy concerns in smart environments are categorized by the risks of data collection, behavioral profiling, and unauthorized data sharing.[1]

Cryptographic and Statistical Protections

Given the resource constraints of edge devices, traditional cryptography such as RSA is often replaced with Elliptic Curve Cryptography (ECC), which provides equivalent security with smaller key sizes

and lower energy consumption.[4] Beyond encryption, data-oriented strategies such as Differential Privacy (DP) have gained traction. DP involves the injection of controlled random noise into aggregated datasets, ensuring that individual records cannot be inferred while still allowing for meaningful statistical analysis.[4]

Decentralized Intelligence through Federated Learning

To mitigate the risks associated with centralized data storage, Federated Learning (FL) has emerged as a privacy-preserving alternative for training machine learning models. In an FL framework, IoT devices train models locally on their own data and only share the resulting model weights with an aggregator.[17] This decentralized approach ensures that raw, sensitive data never leaves the device, thereby aligning with regulatory requirements like the EU's GDPR.[8]

Recent studies have evaluated FL-based IDS models, demonstrating a detection accuracy of over 95.2% in simulated supply chain environments while maintaining data privacy across 50 simulated devices.[18] However, FL remains susceptible to model poisoning and gradient inversion attacks, where adversaries attempt to reconstruct raw data from shared weight updates.[8]

Integration of Blockchain for Immutable Trust and Logging

The integration of blockchain technology addresses the "single point of failure" and trust deficits inherent in centralized FL and traditional IoT architectures. Blockchain provides a decentralized, immutable ledger for recording security events, authentication logs, and model updates.[1]

Lightweight Consensus for Edge Environments

The traditional Proof of Work (PoW) consensus is unsuitable for IoT due to its extreme computational requirements. Instead, lightweight protocols such as Proof of Authority (PoA) and Delegated Proof of Accessibility (DPoAC) are utilized.[5] For instance, the DPoAC protocol leverages Shamir secret sharing and randomized selection to achieve 90% less consensus delay compared to standard protocols, making it viable for power-constrained IIoT scenarios.[21]

Component	Role in Integrated Framework	Benefit
FL Engine	Decentralized model training	Data Privacy

Blockchain	Immutable recording of alerts/updates	Traceability & Trust
Smart Contracts	Automated access control/authentication	Decentralized Management
LWC (AES/ECC)	Secure end-to-end communication	Confidentiality

4

Socio-Economic Impact and Sectoral Vulnerabilities: Case Studies of 2024–2025

The theoretical vulnerabilities of IoT have manifested in significant real-world breaches, highlighting the urgent need for a shift in defensive strategy.

The 2025 Smart Healthcare Breach

In February 2025, a systemic failure in healthcare cybersecurity led to the exposure of over 1 million medical IoT devices across multiple hospital networks.[3] This breach resulted in the leak of 16.6 million patient documents, including MRI scans and biometric results, which were found in unencrypted, publicly accessible directories.[3] The investigation revealed that many devices were directly connected to the internet with no authentication, demonstrating a complete lack of Zero Trust implementation in medical environments.[24] The average cost of such a breach in the healthcare sector is estimated at $7 million, factoring in regulatory fines and legal remediation.[24]

Industrial IoT and Smart Infrastructure

The industrial sector faced similar challenges in 2024, with retailers losing over $20 billion to IoT-related cyberattacks targeting POS terminals and supply chain trackers.[7] In smart city infrastructure, attacks on connected surveillance and traffic management systems jumped by 50% year-over-year, illustrating the risks of using centralized cloud architectures to manage critical public safety systems.[7]

The Horizon of 2025: Quantum Safety and Zero Trust

As we approach the latter half of the decade, two paradigms are set to dominate the IoT security discourse: Post-Quantum Cryptography (PQC) and the Zero Trust

architecture.

NIST Standards and the Transition to PQC

The rapid advancement of quantum computing threatens the foundations of modern encryption, as Shor's algorithm could theoretically break RSA and ECC standards. To counter this, NIST finalized its first set of PQC standards in August 2024, including CRYSTALS-Kyber for general encryption and CRYSTALS-Dilithium for digital signatures.[26] By December 2025, organizations are required to begin adopting these quantum-resistant algorithms to future-proof their data security.[27] For IoT, the challenge lies in the larger key sizes and higher computational load of lattice-based cryptography, which requires further optimization for 8-bit and 16-bit microcontrollers.[26]

Zero Trust as a Fundamental Posture

The traditional perimeter-based security model is no longer viable in the decentralized IoT landscape. The Zero Trust model operates on the principle of "never trust, always verify," requiring every device—whether internal or external to the network—to be authenticated and authorized for every interaction.[7] Implementing Zero Trust reduces the risk of lateral movement by attackers and has been shown to reduce breach costs by up to 35% when combined with effective network segmentation.[7]

Comprehensive Evaluation of Security Metrics and Computational Cost

The implementation of advanced security frameworks in IoT is a balancing act between safety and resource preservation. The data analysis from the comparative study highlights these trade-offs through detailed metrics.

Metric	Decision Tree	Random Forest	XGBoost	SVM	Gradient Boosting
Training Time (sec)	18	95	102	220	53,476
FPR (False Positive Rate)	14.2%	13.8%	13.2%	16.5%	13.4%

Specificity (Benign Class)	84.1%	85.9%	86.4%	81.2%	86.6%
Total Memory Load (MB)	Low	Medium	Medium	High	High

[1]

Gradient Boosting exhibits the highest specificity (86.6%), correctly identifying about six out of seven benign samples, which is critical for reducing "alert fatigue" in Security Operations Centers (SOCs).[12] However, its training time makes it unsuitable for frequent retraining on edge gateways. Decision Trees remain the most lightweight option, though their lack of robustness against adversarial noise makes them less suitable for high-risk environments like industrial controllers.[1]

Conclusions and Strategic Recommendations for IoT Deployment

The comparative analysis of IoT security threats and privacy preservation techniques indicates that the current defensive posture is insufficient to address the scale of the 30.9 billion device landscape of 2025.

1. **Adoption of Ensemble Methods:** For network-level intrusion detection, XGBoost and Random Forest should be prioritized due to their superior handling of high-dimensional flow data and imbalanced attack classes.
2. **Shift to Decentralized Frameworks:** The integration of Blockchain-enabled Federated Learning is essential for privacy-sensitive sectors such as healthcare and smart cities. By keeping data local and logs immutable, these systems provide a "secure-by-design" foundation.
3. **Mandatory Firmware and Credential Policies:** As 60% of breaches stem from unpatched firmware and default passwords, automated lifecycle management tools should be integrated into the deployment pipeline to enforce regular updates and unique credentialing.
4. **Quantum Readiness and Migration:** Organizations must immediately audit their cryptographic inventories to identify RSA and ECC dependencies, establishing a roadmap for transitioning to NIST's PQC standards

before quantum capabilities become a reality.

5. **Zero Trust Implementation:** Network segmentation and continuous authentication are no longer optional. Isolating IoT devices on dedicated VLANs can prevent an unsecured smart thermostat from becoming a point of entry into a corporate server network.

The future of secure IoT ecosystems lies in the convergence of lightweight AI-driven detection, decentralized trust architectures, and adaptive, context-aware privacy preservation. Only by integrating these technologies into a unified framework can we protect the integrity of the digital transformation that underpins modern society.

References

1. Advanced Ensemble Techniques for IoT Cybersecurity: A Performance Comparison on the CICIoT2023 Dataset, accessed May 9, 2026, https://www.mii.lt/damss/files/posters_2024/id_I-1.pdf
2. Impact of IoT Security on Different Industries in 2025, accessed May 9, 2026, https://www.iotforall.com/IoT-security-industry-overview
3. Privacy Preservation And Data Security In Iot-Based ... - RJ Wave, accessed May 9, 2026, https://rjwave.org/ijedr/papers/IJEDR2504147.pdf
4. An Efficient Lightweight Blockchain for Decentralized IoT - arXiv, accessed May 9, 2026, https://arxiv.org/html/2508.19219v1
5. Privacy and Security Best Practices for IoT Solutions - UniCA IRIS, accessed May 9, 2026, https://iris.unica.it/retrieve/7be33d82-0813-4e0b-878d-88248de8bf5c/2023-11%20Access%20-%20Privacy%20and%20Security%20Best%20Practices%20for%20IoT%20Solutions.pdf
6. IoT Security Risks: Stats and Trends to Know in 2025 - JumpCloud, accessed May 9, 2026, https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025
7. A Survey on Privacy Preservation Techniques in IoT Systems - MDPI, accessed May 9, 2026, https://www.mdpi.com/1424-8220/25/22/6967
8. CICIoT2023 Dataset - Emergent Mind, accessed May 9, 2026, https://www.emergentmind.com/topics/ciciot2023-dataset
9. CIC IoT dataset 2023 - University of New Brunswick, accessed May 9, 2026, https://www.unb.ca/cic/datasets/iotdataset-2023.html
10. Class distribution of CICIoT 2023 dataset | Download Scientific Diagram - ResearchGate, accessed May 9, 2026, https://www.researchgate.net/figure/Class-distribution-of-CICIoT-2023-dataset_fig1_372858798
11. Comparative Analysis of Machine Learning Algorithms for Anomaly ..., accessed May 9, 2026, https://infocomp.dcc.ufla.br/index.php/infocomp/article/view/5342/644
12. Feature Importance Study on the CICIoT2023 - Kaggle, accessed May 9, 2026, https://www.kaggle.com/code/shreyaan10/feature-importance-study-on-the-ciciot2023
13. Enhancing IoT Security Using Ensemble Based Feature Selection,

accessed May 9, 2026, https://www.oajaiml.com/uploads/archivepdf/288861271.pdf
14. Intrusion Detection Framework for Internet of Things with Rule Induction for Model Explanation - MDPI, accessed May 9, 2026, https://www.mdpi.com/1424-8220/25/6/1845
15. Network Intrusion Detection with XGBoost - Distributed, Parallel and Secure Systems - INESC-ID, accessed May 9, 2026, http://www.gsd.inesc-id.pt/~mpc/pubs/XGBoost_chapter.pdf
16. IoT threat detection moves to transparent, decentralized AI systems - Devdiscourse, accessed May 9, 2026, https://www.devdiscourse.com/article/technology/3895722-iot-threat-detection-moves-to-transparent-decentralized-ai-systems
17. A Federated Learning–Based Intrusion Detection ... - Cureus Journals, accessed May 9, 2026, https://www.cureusjournals.com/articles/12961-a-federated-learning-based-intrusion-detection-framework-for-blockchain-enabled-internet-of-things-iot-supply-chains.pdf
18. Blockchain Empowered Federated Learning Ecosystem for Securing Consumer IoT Features Analysis - MDPI, accessed May 9, 2026, https://www.mdpi.com/1424-8220/22/18/6786
19. Federated Learning and Blockchain Integration for Privacy Protection in the Internet of Things: Challenges and Solutions - Semantic Scholar, accessed May 9, 2026, https://pdfs.semanticscholar.org/c267/81af739bef194c3c4c418bcc87da488edf88.pdf
20. Manpreet Kaur Shikha Gupta - PERFORMANCE EVALUATION OF A ..., accessed May 9, 2026, https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-e9abb5c9-d720-4018-988c-893949c709e5/c/CS_2025_26_1_Kaur.pdf
21. An Efficient Lightweight Blockchain for Decentralized IoT - arXiv, accessed May 9, 2026, https://arxiv.org/pdf/2508.19219
22. Efficient Lightweight Blockchain with Hybridized Consensus Algorithm for IoT Networks, accessed May 9, 2026, https://www.semanticscholar.org/paper/fe7c9a7fbc36e9afe70613a3f35757ca7904d982
23. Healthcare IoT Security Breach 2025: Why Over 1 Million Devices Were Exposed, accessed May 9, 2026, https://deviceauthority.com/healthcare-iot-security-breach-2025-why-over-1-million-devices-were-exposed/
24. 40 IoT Applications & Use Cases - AIMultiple, accessed May 9, 2026, https://aimultiple.com/iot-applications
25. NIST PQC Standards Explained: The Path to Quantum-Safe Encryption, accessed May 9, 2026, https://www.ssh.com/academy/nist-pqc-standards-explained-path-to-quantum-safe-encryption
26. Post-quantum cryptography | NIST - National Institute of Standards and Technology, accessed May 9, 2026, https://www.nist.gov/pqc
27. Product Categories for Technologies That Use Post-Quantum Cryptography Standards, accessed May 9, 2026, https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards
28. Migration to Post-Quantum Cryptography - NCCoE, accessed May 9, 2026, https://www.nccoe.nist.gov/applied-

cryptography/migration-to-pqc

29. **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*.
30. **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*.
31. **Banerjee, R.**, et al. (2025). Study on Computational Intelligence for Planetary Resilience: A Framework for Sustainable Biosphere Stewardship. *European Journal of Clinical Pharmacy*.
32. 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.
33. **Banerjee, R.**, Mukherjee, D., Basu, D., & Modak, P. K. (2025). The Mind In The Machine: Unveiling The Power Of Cyber Hypnosis. *ResearchGate Publication*.
34. **Banerjee, R.** (2023). An Empirical Evaluation of k-Means Clustering Technique and Comparison. *Conference Paper/ResearchGate.*
35. 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.