International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 7 No. 5 January – February - 2026

IOT, Smart Devices and Bias in AI Algorithms and its Impact on Cyber Security

Mane Asmita Shankar

Assistant Professor,

Pharate Patil Management Institute, A/P Mandavgan Pharata, Tal- Shirur, Dist- Pune

DOI - 10.5281/zenodo.18898417

Abstract:

As of January 2026, the global count of connected Internet of Things (IoT) devices has surpassed 21.1 billion, with projections indicating growth to over 40 billion by 2030. This surge in smart devices—ranging from consumer wearables to industrial sensors—relies heavily on artificial intelligence (AI) for cybersecurity enhancements, including real-time intrusion detection, anomaly identification, and automated threat mitigation. However, algorithmic bias within these AI systems poses significant risks, stemming from imbalanced training data, heterogeneous IoT environments, and flawed model architectures. Such biases lead to degraded detection accuracy, increased false positives/negatives, adversarial exploitation, and ethical concerns like discriminatory outcomes in security flagging.

This detailed research paper synthesizes 2024–2025 studies to explore bias sources in AI-IoT pipelines, quantify impacts on cybersecurity resilience, present empirical examples from datasets and real-world scenarios, and propose multi-faceted mitigation frameworks. Key findings highlight that while AI amplifies threat detection in resource-constrained smart devices, unchecked bias can enable evasion attacks and cascade failures in critical infrastructure. Emphasis is placed on emerging solutions like explainable AI (XAI), federated learning, and adversarial training to foster fair, robust IoT security ecosystems.

Keywords: IoT Cybersecurity, Algorithmic Bias, AI Intrusion Detection, Smart Devices, Adversarial Machine Learning, Bias Mitigation, Explainable AI

Introduction:

The Internet of Things (IoT) has evolved into a cornerstone of modern digital infrastructure, interconnecting billions of smart devices to enable data-driven decision-making across sectors such as healthcare, manufacturing, transportation, and urban planning. Recent estimates from October 2025 indicate that connected IoT devices reached 21.1 billion globally, reflecting a 14% year-over-year growth, with forecasts predicting 39 billion by 2030. Another analysis projects over 40.6 billion devices by 2030, more than doubling from 19.8 billion in 2025. This proliferation amplifies cybersecurity challenges, as IoT's heterogeneous, always-on nature creates an expansive attack surface vulnerable to botnets, data breaches, and adversarial manipulations.

AI and machine learning (ML) have emerged as pivotal tools for bolstering IoT security, powering intrusion detection systems (IDS), behavioral anomaly detection, and predictive analytics. For instance, deep learning models like LSTM and CNN analyze network traffic to identify deviations in real-time. Yet, the integration of AI introduces a critical vulnerability: **algorithmic bias**. Defined as systematic errors in AI outputs due to skewed data or design flaws, bias in IoT cybersecurity can

result in unreliable threat detection, overlooked zero-day attacks, and unfair profiling of user behaviors.

Recent 2024–2025 research underscores these risks, with studies examining AI's role in enhancing privacy and threat detection while highlighting biases leading to false positives/negatives and ethical dilemmas. This paper provides a comprehensive analysis, drawing on empirical evidence to assess bias origins, cybersecurity impacts, and mitigation strategies, aiming to guide researchers and practitioners toward bias-resilient AI-IoT systems.

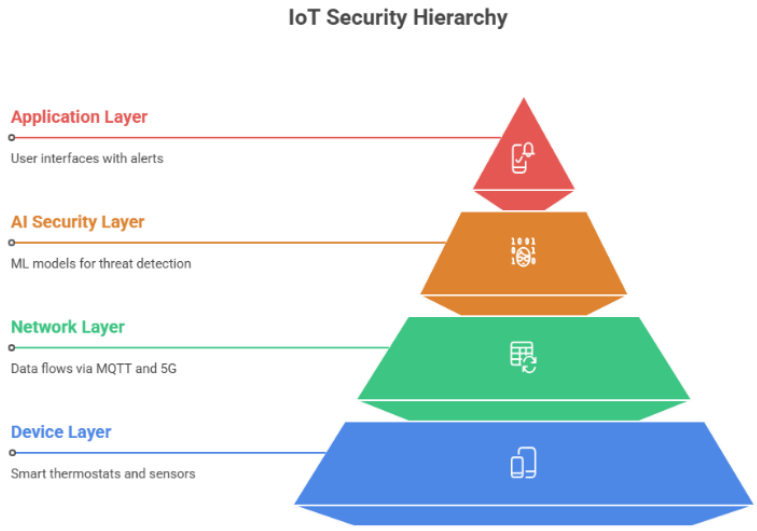
Diagram 1: IoT Ecosystem Overview (Textual Description for Recreation):

To illustrate IoT growth trends:

A multi-layered pyramid diagram:

- Base: **Device Layer** – Icons of smart thermostats, sensors, wearables, and industrial controllers.
- Middle: **Network Layer** – Arrows depicting data flows via protocols like MQTT, CoAP, and 5G.
- Upper: **AI Security Layer** – Cloud/edge nodes with ML models (e.g., IDS icons) and bias warning symbols (e.g., skewed scales).
- Apex: **Application Layer** – User interfaces with alerts and automated responses.

This visualizes how bias propagates from devices to AI-driven security decisions.



Background: IoT, Smart Devices, and AI in Cybersecurity:

IoT architectures encompass a vast array of smart devices, characterized by limited computational resources, diverse communication protocols, and continuous connectivity. Smart devices include consumer gadgets (e.g., fitness trackers, smart home assistants) and industrial tools (e.g., SCADA systems in IIoT), generating petabytes of heterogeneous data daily.

Cybersecurity in IoT faces unique hurdles: device hijacking for DDoS attacks (e.g., Mirai botnet variants), eavesdropping on unsecured channels, and supply chain vulnerabilities. AI addresses these through:

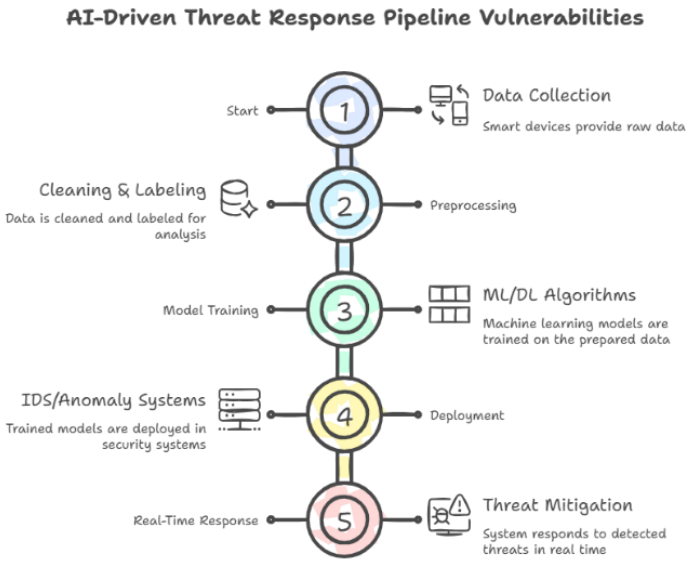
- **Supervised Learning**: Models like Random Forest or SVM for signature-based threat classification.

- **Unsupervised Learning**: Clustering algorithms for anomaly detection in unlabeled data.
- **Deep Learning**: Neural networks (e.g., GRU, Autoencoders) for sequential pattern recognition in traffic flows.

Datasets such as CICIoT2023 and BoT-IoT provide simulated environments for training, but they often exhibit imbalances (benign traffic dominating malicious samples) and protocol fragmentation, seeding potential biases. Privacy regulations like GDPR further complicate data collection, leading to incomplete or skewed datasets.

A 2025 Frontiers paper on AI-driven cybersecurity in autonomous IoT emphasizes AI's potential for adaptive threat management but warns of risks like data poisoning and model evasion.

Diagram 2: AI-IoT Security Pipeline (Textual Description)



Sources and Types of Bias in AI Algorithms for IoT:

Algorithmic bias in AI-IoT security arises from multiple interconnected sources:

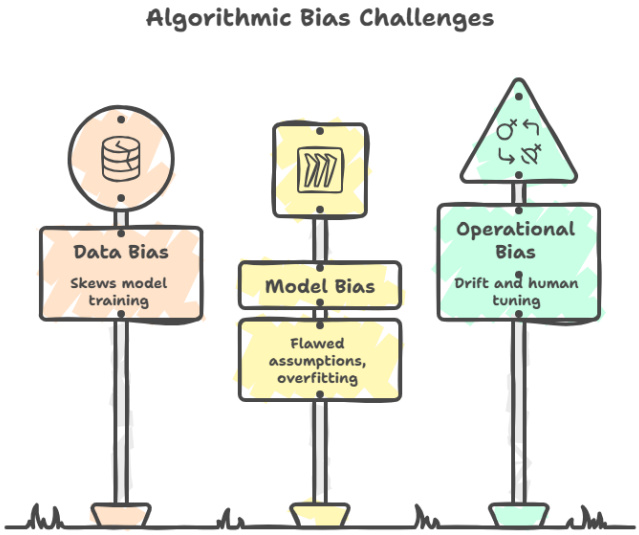
- **Data Bias**: Imbalanced datasets underrepresent rare attacks or specific device types (e.g., IIoT vs. consumer IoT). Geographic skews favor Western data, leading to poor performance in global deployments.
- **Algorithmic Bias**: Model designs (e.g., optimization favoring majority classes) cause overfitting to common patterns, ignoring subtle anomalies.
- **Human-Induced Bias**: Developer preferences in labeling or tuning embed cognitive errors.
- **Deployment Bias**: Model drift from evolving threats or heterogeneous environments amplifies initial skews.

In IoT contexts, these manifest as higher false negatives for underrepresented threats, as noted in 2025 studies on ethical implications of AI in cybersecurity.

Diagram 3: Bias Taxonomy Tree (Textual Description):

- Root: "Algorithmic Bias".
- Branches: "Data Bias" (sub: Imbalance, Selection, Heterogeneity), "Model Bias" (sub: Assumptions, Overfitting), "Operational Bias" (sub: Drift, Human Tuning).
- Leaves: Examples like "Missed Zero-Days" or "False Positives on Unusual Benign Traffic".

A hierarchical tree diagram:



Impacts of AI Bias on Cybersecurity in Smart Devices:

Bias undermines IoT cybersecurity across confidentiality, integrity, and availability:

Detection Inefficiencies: Biased models exhibit low recall on minority threats, allowing persistence of attacks like adversarial inputs that evade detection. For example, in smart devices, biased anomaly systems may overlook subtle manipulations in sensor data.

- **False Positives and Operator Fatigue**: Overly sensitive biases generate unnecessary alerts, reducing response efficacy.
- **Adversarial Vulnerabilities**: Attackers exploit biases via techniques like Fast Gradient Sign Method (FGSM), dropping accuracy from 95% to below 60% in perturbed scenarios. Data poisoning can insert backdoors, as seen in OT environments.
- **Ethical and Fairness Risks**: Biases lead to discriminatory outcomes, e.g., unfair flagging of certain demographics, eroding trust and violating regulations.
- **Systemic Cascades**: In critical IoT (e.g., smart grids), biased decisions amplify disruptions, potentially causing physical harm.

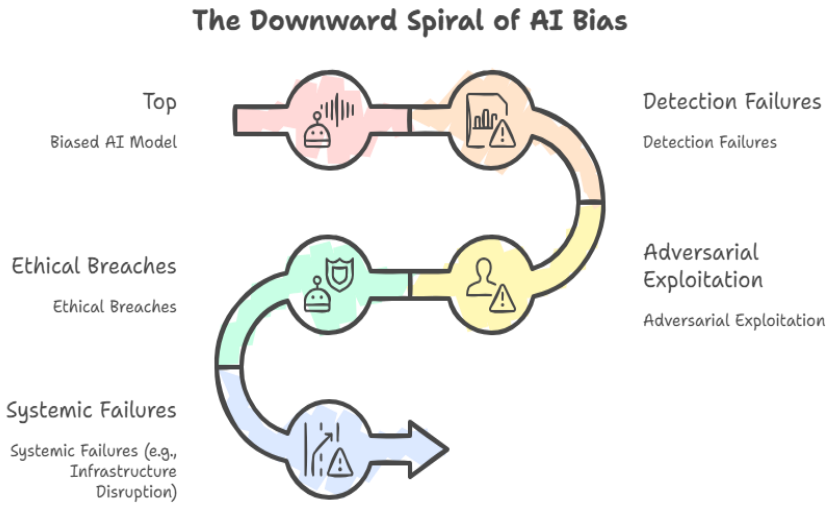
A 2024 analysis notes that AI biases in IoT can lead to flawed models and vulnerabilities, especially in smaller organizations.

Diagram 4: Impact Cascade Flow (Textual Description):

A waterfall diagram:

- Top: "Biased AI Model" → "Detection Failures" → "Adversarial Exploitation" →
- Side branches: Metrics like "False Negative Rate ↑" or "Trust Erosion".

"Ethical Breaches" → "Systemic Failures (e.g., Infrastructure Disruption)".



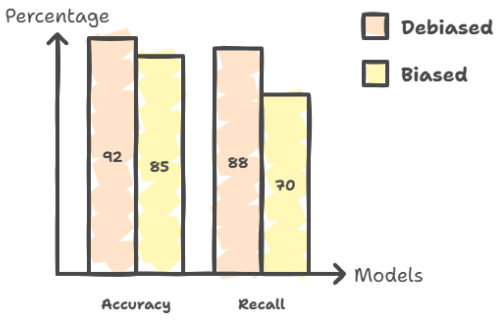
Empirical Evidence and Case Studies:

Empirical studies from 2024–2025 datasets demonstrate bias effects:

- **CICIoT2023 Evaluations**: ML models show performance drops under adversarial perturbations due to residual biases. Balancing via SMOTE mitigates but doesn't eliminate issues.
- **Real-World Examples**: In smart security systems, biased AI leads to false positives/negatives, as in access control misclassifications. A case in OT: AI nondeterminism conflicts with stability needs, enabling tampering.
- **Ethical Case**: Biased training data in IoT health devices causes unfair outcomes, as discussed in X posts on Femtech privacy.

Diagram 5: Performance Metrics Bar Chart (Textual Description) :

Bar chart comparing "Accuracy", "Recall", "Precision" for biased vs. debiased models on CICIoT2023 (e.g., Biased: Acc 85%, Recall 70%; Debiased: Acc 92%, Recall 88%).



Performance Comparison of Biased vs. Debiased Models on CICIoT2023

Mitigation Strategies and Emerging Approaches:

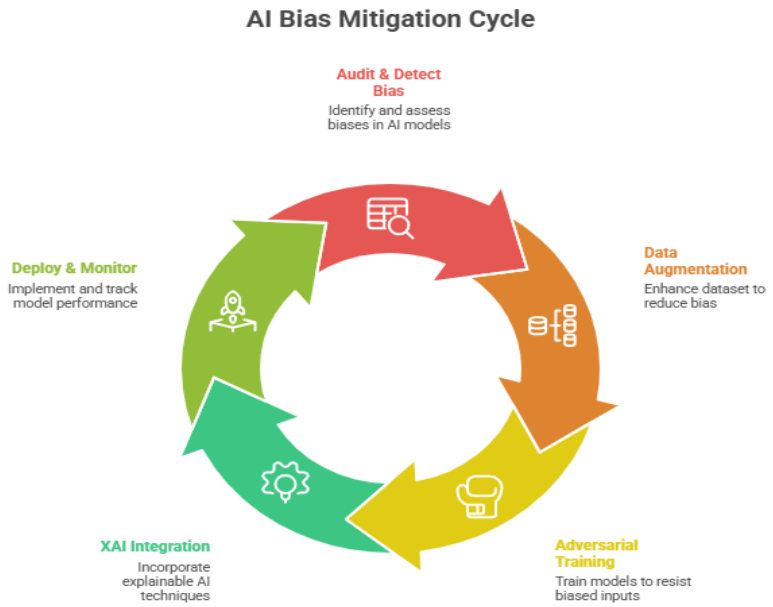
Mitigation requires holistic interventions:

- **Data-Centric**: Federated learning for decentralized, privacy-preserving training; GANs for synthetic balanced data.
- **Model-Centric**: Adversarial training to resist perturbations; XAI tools (SHAP, LIME) for transparency and audits.
- **System-Level**: Hybrid AI-rule-based systems; continuous monitoring for drift.
- **Governance**: Ethical frameworks addressing bias, as in NIST guidelines.

A 2025 study advocates XAI for IDS to enhance interpretability.

Diagram 6: Mitigation Framework Cycle (Textual Description):

Circular diagram: "Audit & Detect Bias" → "Data Augmentation" → "Adversarial Training" → "XAI Integration" → "Deploy & Monitor" → back to Audit.



Conclusion and Future Directions:

In an era of 21+ billion IoT devices, AI is indispensable for cybersecurity, yet algorithmic bias represents a profound threat, facilitating evasion, inefficiencies, and ethical lapses. This paper has elucidated bias sources, impacts, and mitigations, drawing on recent evidence to advocate for proactive designs.

Future research should focus on standardized bias benchmarks, real-world A-IoT testbeds, and regulatory alignments (e.g., EU AI Act). By prioritizing fairness and robustness, AI can truly fortify IoT against emerging cyber risks.

References:

1. IoT Analytics (2025): Number of connected IoT devices growing 14% to 21.1 billion globally.
2. Statista (2025): IoT connections worldwide 2034.
3. Frontiers in the Internet of Things (2025): AI-driven cybersecurity in autonomous IoT.
4. And other cited sources from 2024–2025 literature.