



विश्वजीवनामृतं ज्ञानम्

ATAL BIHARI VAJPAYEE-INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND  
MANAGEMENT (ABV-IIITM), GWALIOR

**BEHAVIOR-DRIVEN MALICIOUS NODE  
DETECTION AND MITIGATION IN  
IOT NETWORKS USING ENHANCED  
IOTDEVID FRAMEWORK**

# Base research paper

IoTDevID: A Behavior-Based Device  
Identification Method for the IoT by Kahraman Kosta, Mike  
Just and Michael A. Lones  
<https://ieeexplore.ieee.org/document/9832419/>

IEEE Internet of Things Journal  
2022

**PRESENTED BY:**

Swapnil Sontakke

Dr. W Wilfred Godfrey

Prof. Shashikala Tapaswi

**SUBMITTED TO:**

# CONTENTS



1. Background of the Problem
2. Motivation
3. Literatur Survey : Related work
4. Research Gaps
5. Problem Statement
6. Objective
7. Proposed Methodology
8. References

# BACKGROUND OF THE PROBLEM

- The Internet of Things (IoT) ecosystem is rapidly expanding across homes, industries, and critical infrastructure.
- Most IoT devices have limited computational power, heterogeneity nature and weak authentication, making them highly vulnerable to cyber threats.
- Traditional Intrusion Detection Systems (IDS) depend on static signatures, failing to detect behavioral changes or new attacks.
- Existing frameworks like IoTDevID can identify devices but cannot recognize behavioral deviations once a node is compromised.
- This necessitates a dynamic, drift driven adaptive security mechanism that continuously monitors device behavior.

# MOTIVATION

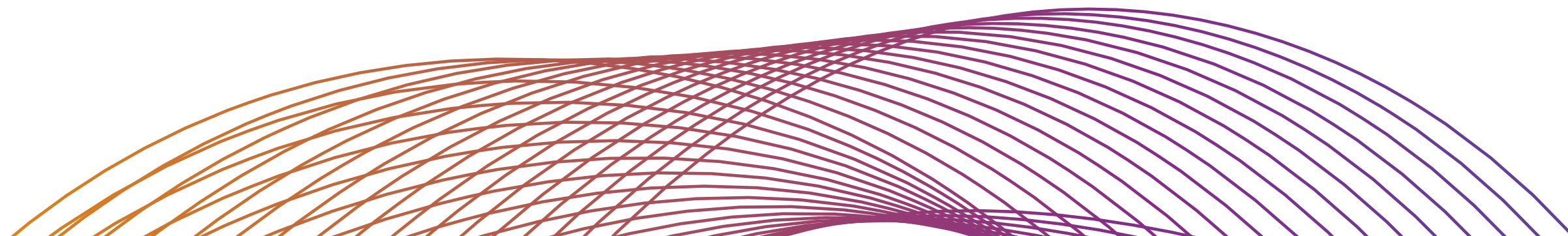
- Increasing IoT attacks (botnets, data tampering, DDoS) highlight the urgent need for proactive defense.
- Static device identification cannot detect changes post-compromise.
- Adaptive, behavior-drift-driven analysis allows detection of early compromise indicators.
- Whale Optimization Algorithm (WOA) offers an efficient way to optimize features in resource-limited environments.
- The goal: design a lightweight, explainable, adaptive malicious node detection and mitigation framework for real-world IoT networks.

# LITERATURE SURVEY

This section reviews related works on:

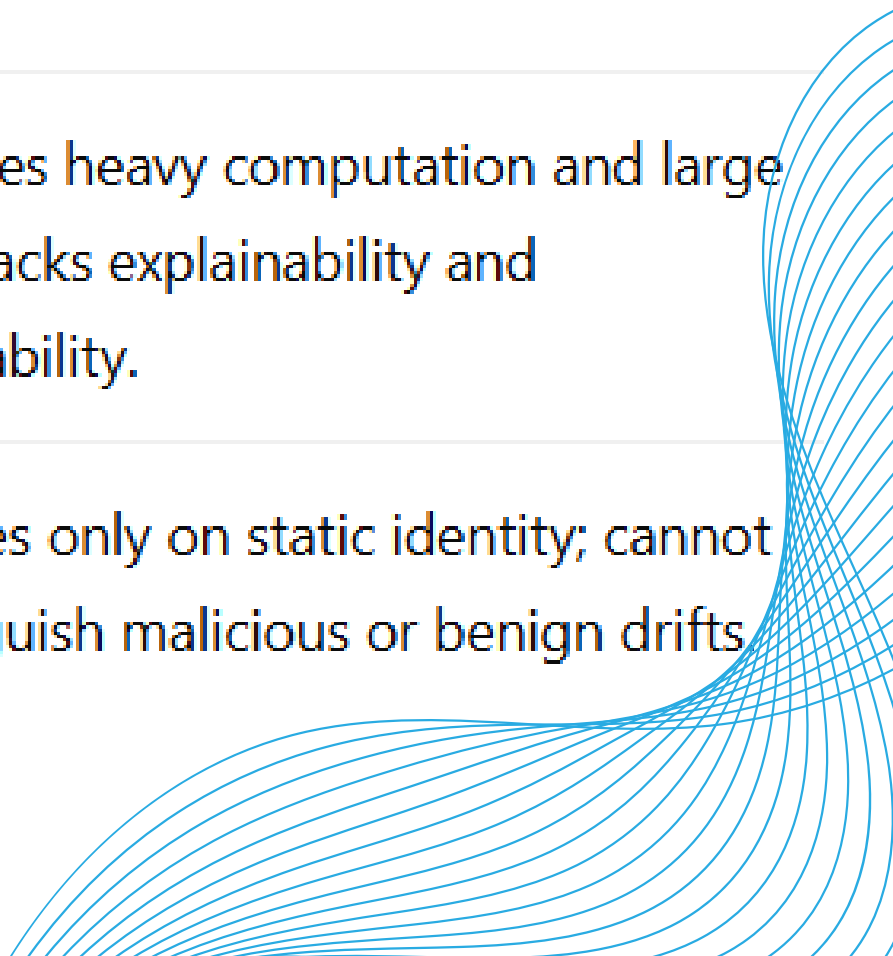
- IoT device identification (IoTDevID, IoTSense)
- Anomaly detection (N-BaIoT, D<sup>2</sup>IoT)
- Optimization algorithms (GA, WOA, GWO)
- Concept drift adaptation (ADWIN, EWMA)

Purpose: Identify the limitations and motivate the proposed enhanced framework.



# LITERATURE SURVEY

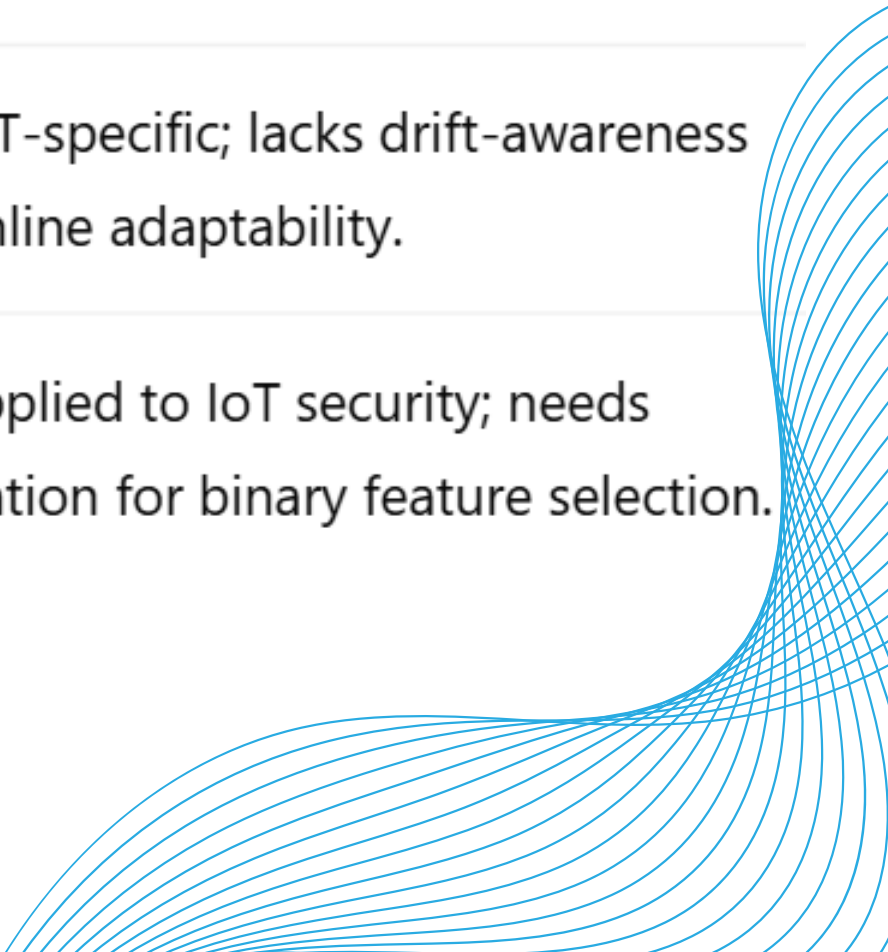
Author & Year	Paper / Approach	Key Contribution	Major Limitation
Kostas et al., 2022	<i>IoTDevID: Behavior-Based Device Identification (IEEE IoT J.)</i>	Introduced packet-level behavioral fingerprinting using Decision Tree for accurate IoT device ID.	Assumes static behavior; cannot detect drift or post-compromise deviation.
Nguyen et al., 2019	<i>DIoT: Federated Self-Learning Anomaly Detection (ICDCS)</i>	Developed a privacy-preserving federated anomaly detection system for IoT gateways.	High computational cost; lacks per-device behavioral profiling.
Meidan et al., 2018	<i>N-BaIoT: Network-Based Botnet Detection (Elsevier)</i>	Used deep autoencoders to detect botnet-infected IoT devices like Mirai.	Requires heavy computation and large data; lacks explainability and adaptability.
Bezawada et al., 2018	<i>IoTSense: Behavioral Fingerprinting (IEEE CNS)</i>	Modeled static traffic patterns for IoT device identification.	Focuses only on static identity; cannot distinguish malicious or benign drifts.





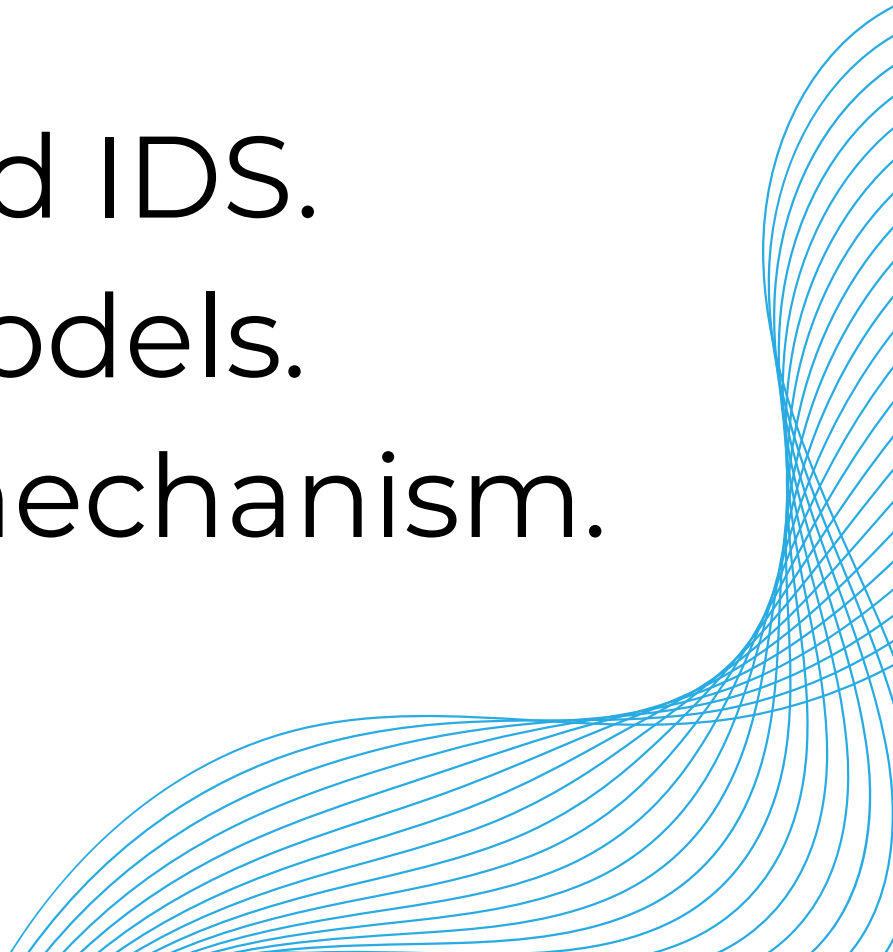
# LITERATURE SURVEY

Author & Year	Paper / Approach	Key Contribution	Major Limitation
Xu et al., 2023	<i>Detecting Compromised IoT Devices (Elsevier Review)</i>	Provided comprehensive survey of compromised device detection methods.	Identified lack of adaptive, lightweight, explainable IDS frameworks.
Xu et al., 2024	<i>Addressing Concept Drift in IoT Anomaly Detection (IEEE)</i>	Integrated ADWIN/EWMA to adapt to evolving IoT data distributions.	Focused only on data drift; ignored context-aware behavioral drift.
Shan et al., 2025	<i>Hybrid WOA–GWO for Intrusion Detection (Nature Sci. Rep.)</i>	Combined WOA and GWO for faster and accurate IDS feature selection.	Not IoT-specific; lacks drift-awareness and online adaptability.
Mirjalili & Lewis, 2016	<i>Whale Optimization Algorithm (Elsevier)</i>	Introduced WOA for efficient global optimization using bubble-net hunting strategy.	Not applied to IoT security; needs adaptation for binary feature selection.





# RESEARCH GAPS

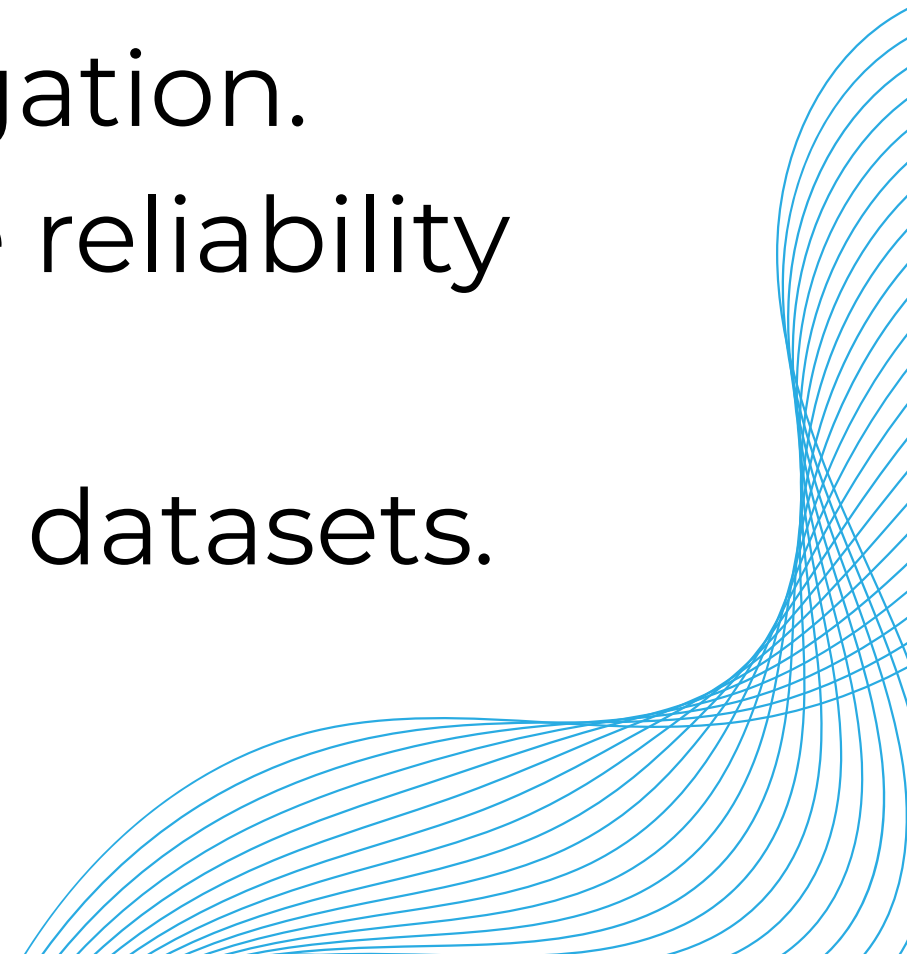
1. No unified adaptive malicious detection and mitigation system combining device ID + anomaly detection.
  2. Static identification fails to track post-compromise drift.
  3. High computational overhead in GA-based feature selection.
  4. Lack of explainability in deep-learning-based IDS.
  5. Absence of lightweight edge-deployable models.
  6. No trust scoring or automated mitigation mechanism.
- 

# PROBLEM STATEMENT

- Existing IoT identification systems are static and cannot detect malicious behavior once a legitimate device is compromised.
- There is a need for an adaptive, lightweight, behavior-driven IoT device monitoring framework that detects and mitigates compromised nodes efficiently.

# OBJECTIVES

1. Replace Genetic Algorithm (GA) with Whale Optimization Algorithm (WOA) for robust and efficient feature selection .
2. Integrate Decision Tree + Drift Detection Layer (ADWIN/EWMA) for adaptive monitoring.
3. Continuously track behavioral deviations in IoT devices for anomaly and malicious nide detection and mitigation.
4. Develop a trust scoring mechanism for real-time reliability assessment.
5. Validate performance using Aalto and UNSW IoT datasets.





# PROPOSED METHODOLOGY - OVERVIEW

Enhanced IoTDevID Framework :

- Combines WOA-based feature optimization, Decision Tree classification, and drift detection.
- Implements trust-based mitigation (e.g., isolation or throttling).
- Designed for edge gateway deployment.

## System architecture

Modules:

### 1.Feature Selection (WOA)

Selects optimal subset using fitness score.

### 2. Device Classification (DT)

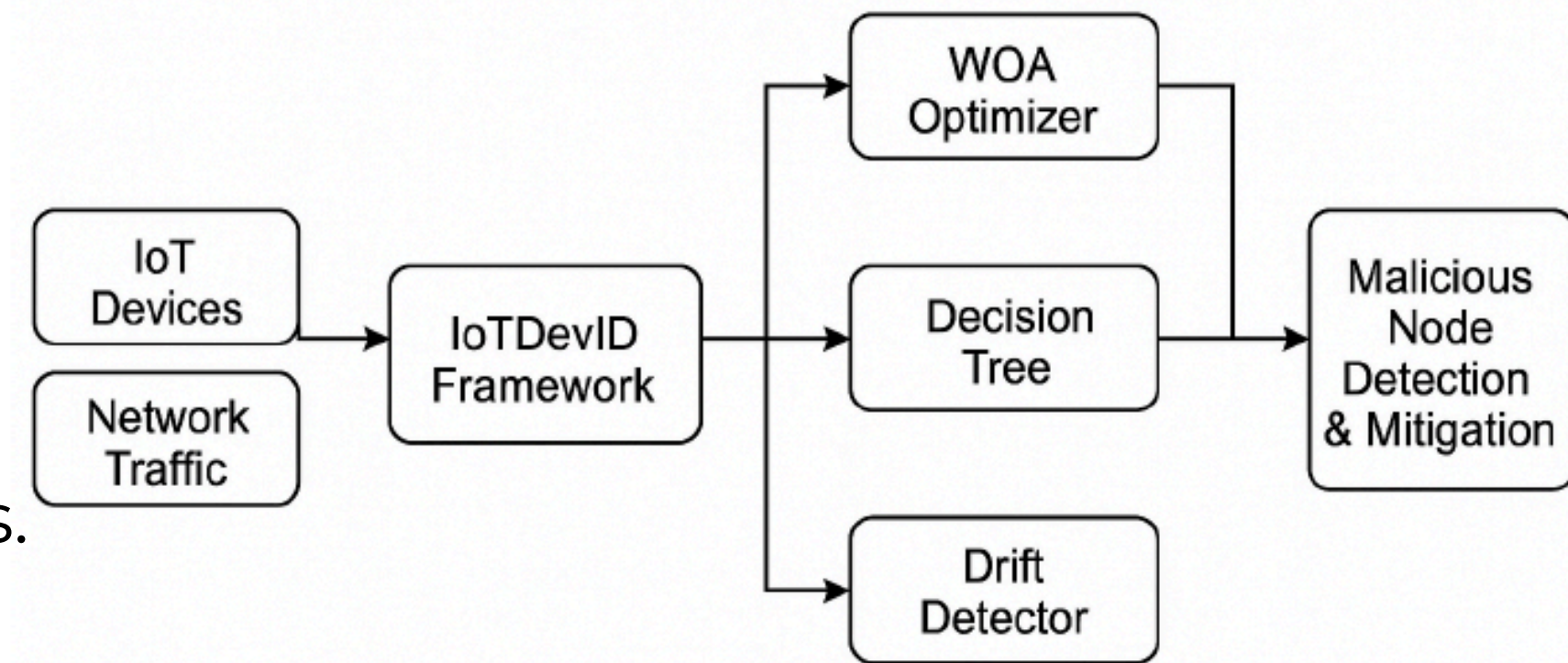
Identifies device type using behavioral features.

### 3.Drift Detection (ADWIN/EWMA)

Detects behavioral deviations over time and adapt to network changes.

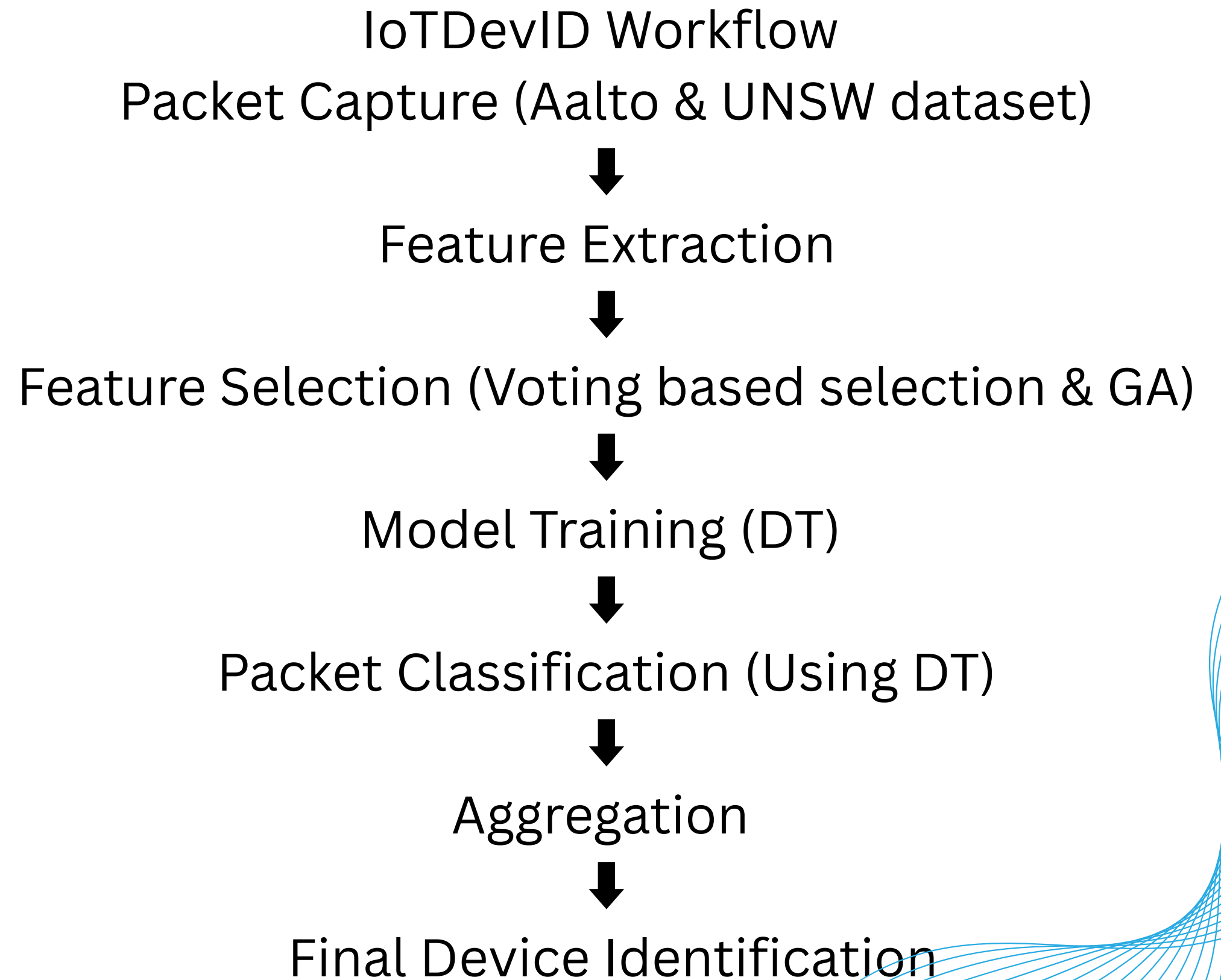
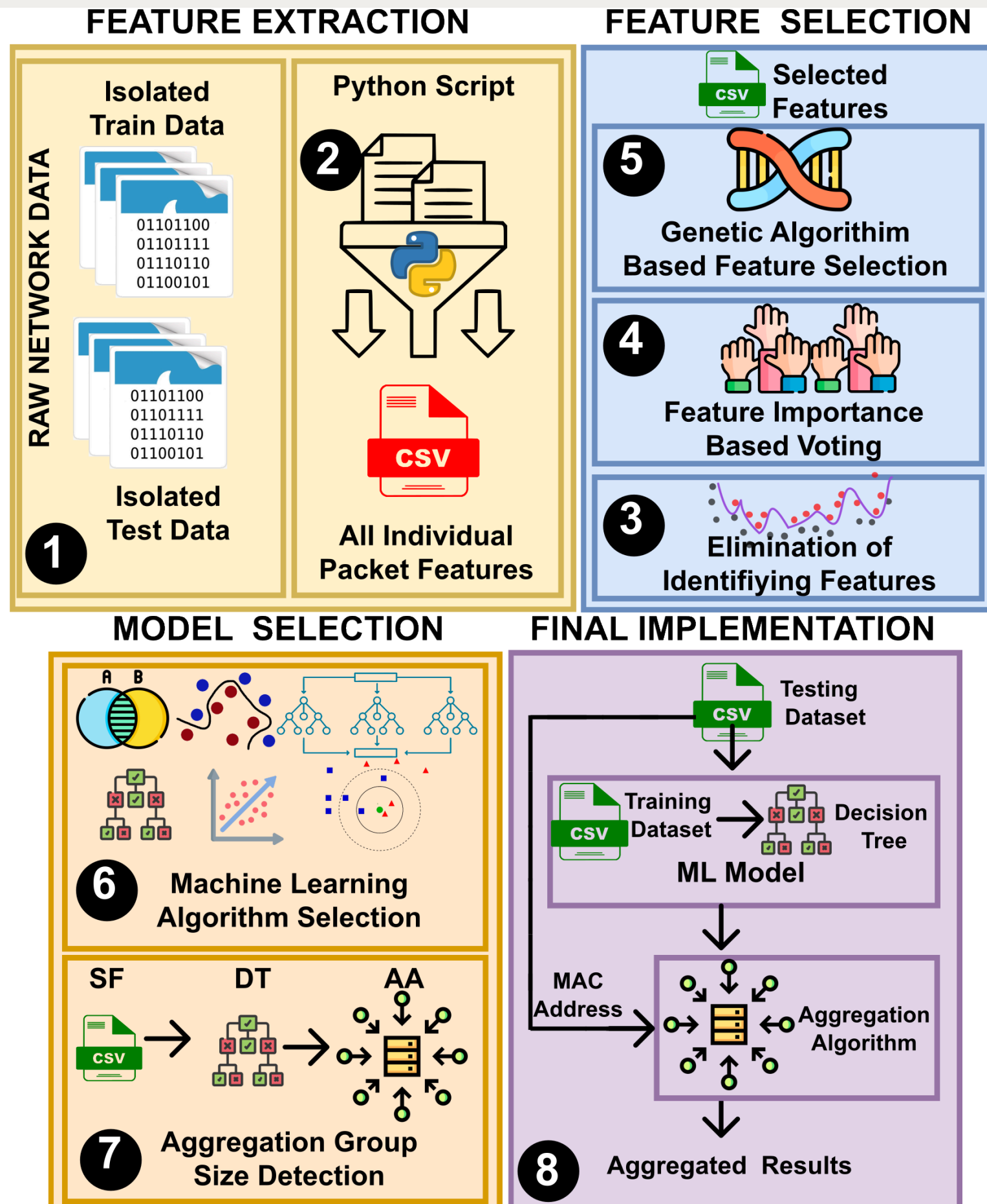
### 4.Trust Scoring Engine

Quantifies reliability; triggers mitigation.



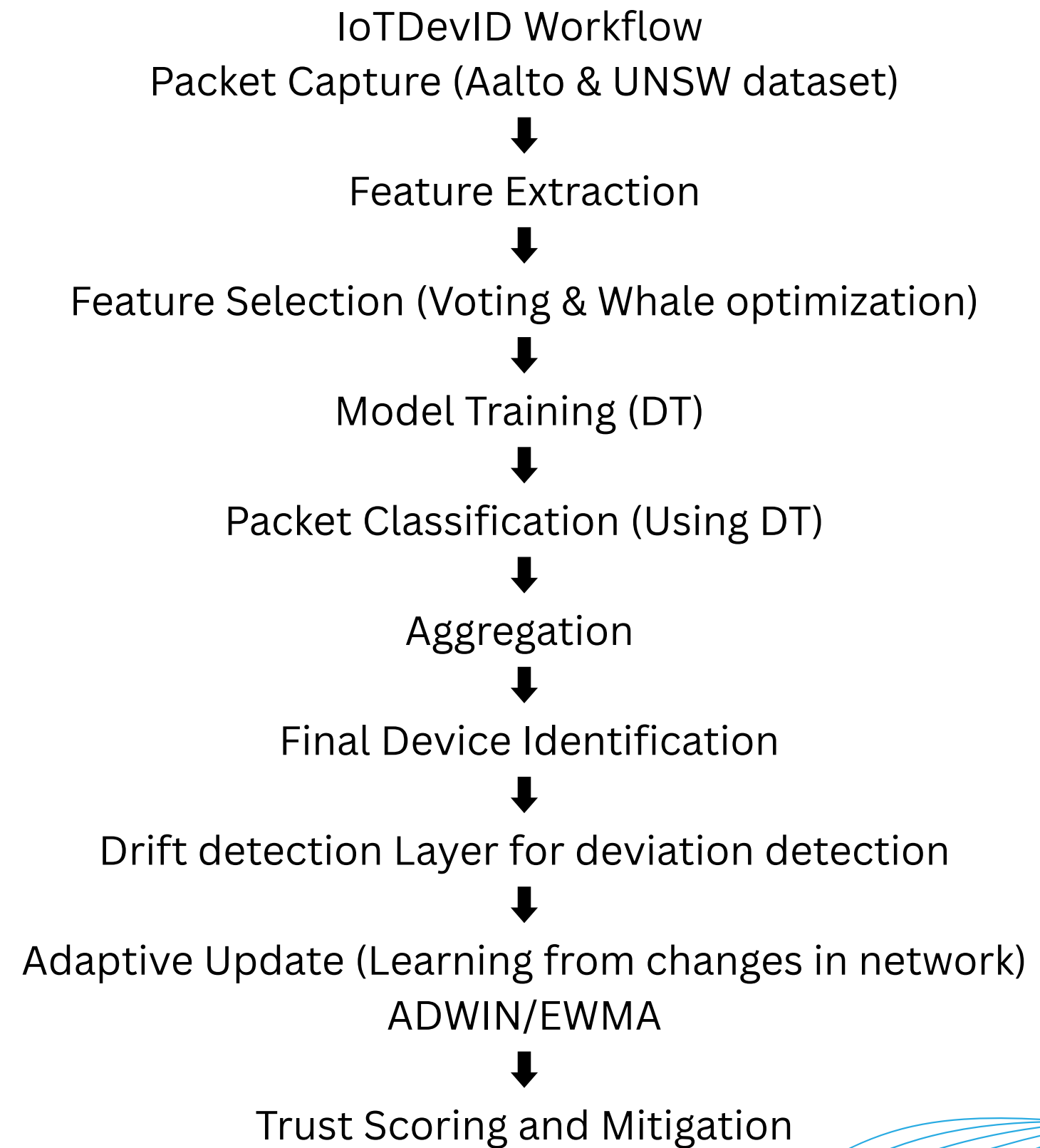
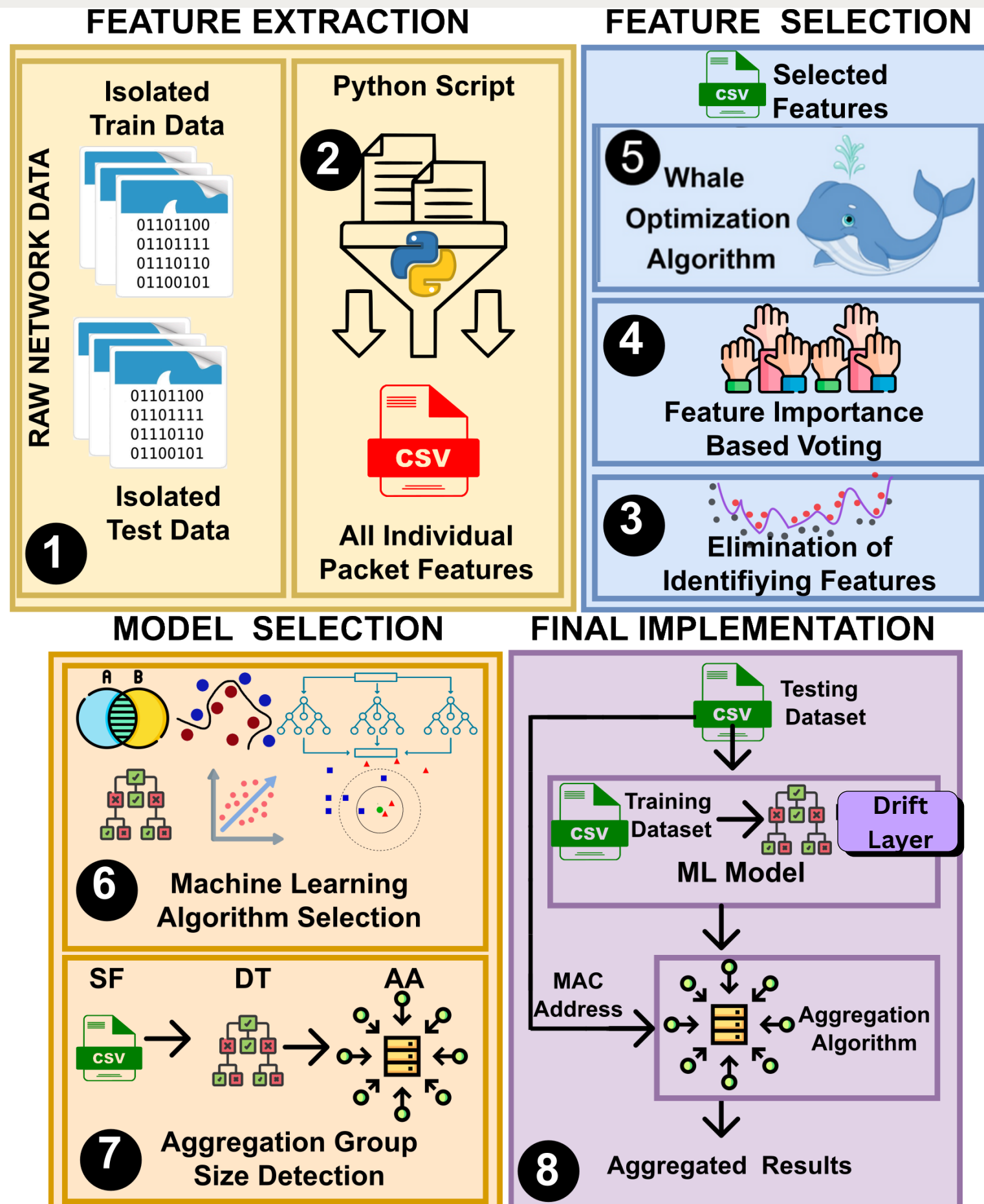
Behavior-Driven Malicious Node Detection and Mitigation in IoT Networks using enhanced IoTDevID framework

# IOTDEVID : CURRENT APPROACH





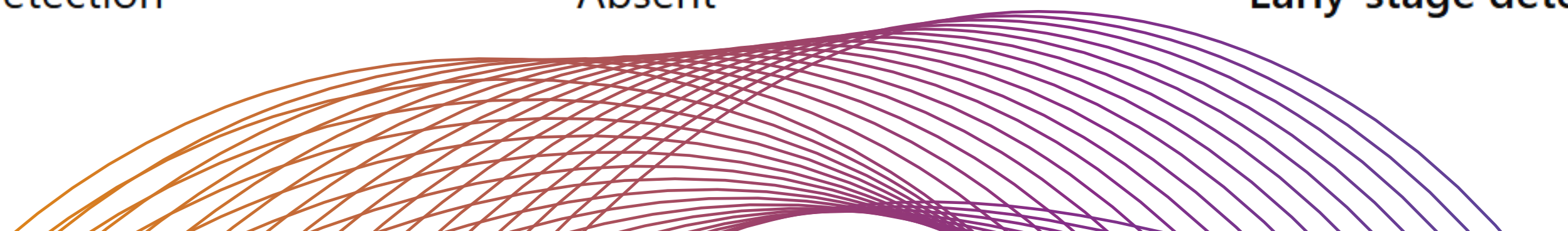
# IOTDEVID : PROPOSED APPROACH





# ADVANTAGES OVER EXISTING WORK

Aspect	Existing Models	Enhanced IoTDevID
Feature Optimization	GA/manual	WOA (stable, fast)
Adaptivity	Static	Drift-aware (ADWIN/EWMA)
Interpretability	Partial	Fully explainable DT
Resource Use	High	Lightweight (Edge-ready)
Compromise Detection	Absent	Early-stage detection

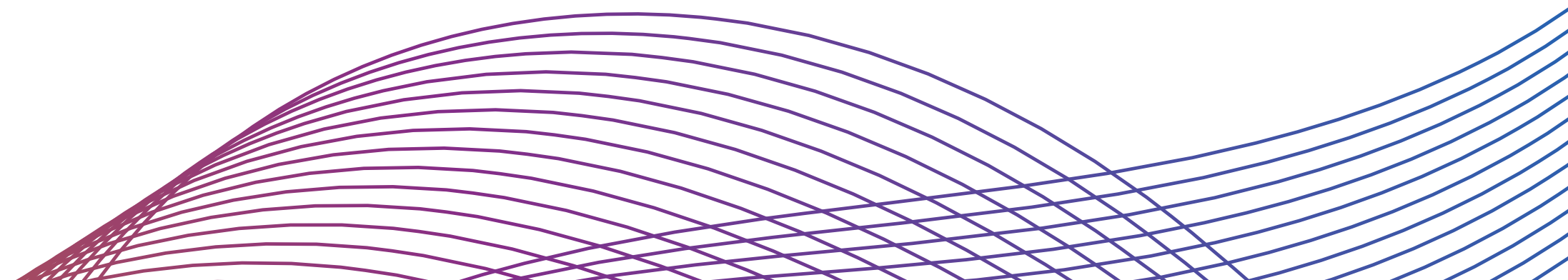


# ADDRESSING RESEARCH GAPS


Gap	Solution
Lack of adaptive detection	Integrated DT + Drift Detection Layer
High GA overhead	WOA-based optimization
Disjoint identity & anomaly detection	Unified IoTDevDrift pipeline
Weak early compromise response	Dynamic trust scoring + mitigation
Edge unsuitability	Lightweight architecture
No mitigation	Automated firewall/SDN actions

# METHODOLOGY : EXPECTED OUTCOMES & AIM

- +2% improvement in identification accuracy over IoTDevID
- 30–40% faster convergence in feature selection
- 45 vs 52 features (reduced set)
- Early compromise detection
- <1% false positives, <2 ms inference delay
- Suitable for real-time IoT edge deployment



# REFERENCES

- Kostas et al., IoTDevID: Behavior-Based Device Identification, IEEE IoT Journal, 2022.
  - Nguyen et al., DIoT: Federated Self-Learning Anomaly Detection, ICDCS, 2019.
  - Meidan et al., N-BalIoT, Elsevier, 2018.
  - Xu et al., Addressing Concept Drift in IoT Anomaly Detection, IEEE TNSM, 2024.
  - Mirjalili & Lewis, Whale Optimization Algorithm, Elsevier, 2016.
  - Shan et al., Hybrid WOA–GWO for IDS, Nature Sci. Rep., 2025.
  - Bezawada et al., IoTSense, IEEE CNS, 2018.
  - Xu et al., Detecting Compromised IoT Devices, Elsevier, 2023.
- 



The background features a series of flowing, wavy lines in shades of blue, purple, and orange. These lines are composed of many thin, parallel strokes that create a sense of movement and depth. The lines are arranged in a way that they seem to flow from the top left towards the bottom right, with some lines curving back towards the left. The colors transition smoothly from blue on the left to purple in the center to orange on the right.

THANK YOU! ✦