دانشگاه اصفهان

دانشگاه فردوسی مشهد

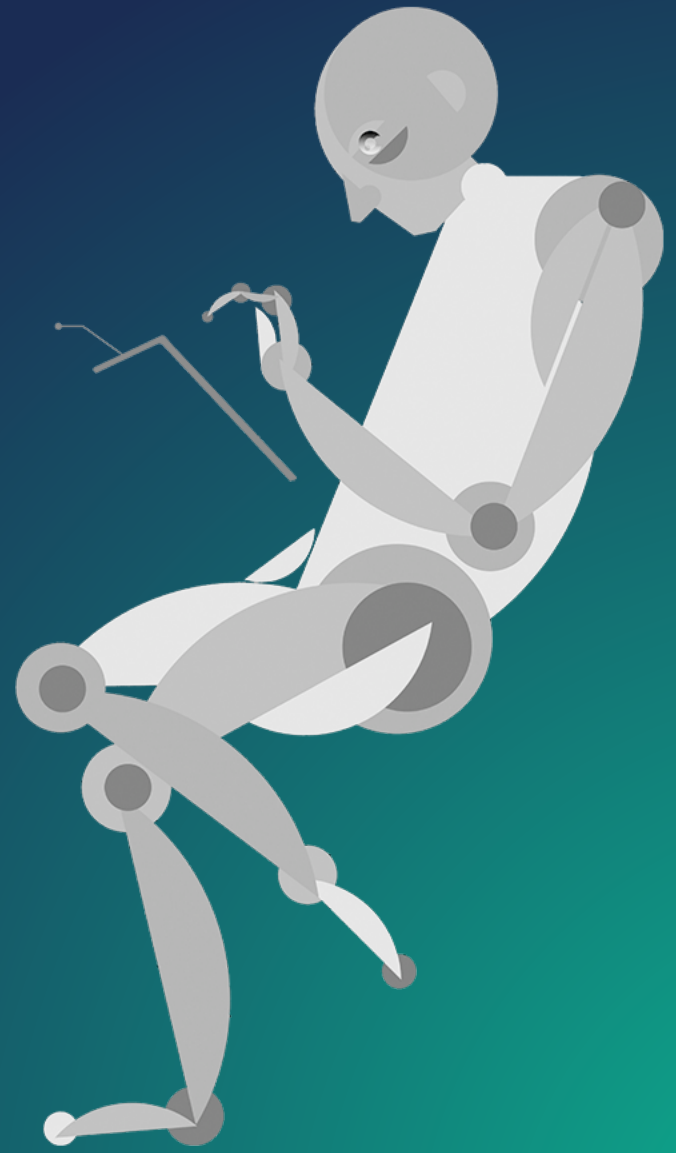
9TH

INTERNATIONAL CONFERENCE ON

INTERNET OF THINGS AND ITS APPLICATIONS

نهمین کنفرانس بین المللی

اینترنت اشیاء و کاربردها



دانشکده مهندسی کامپیوتر دانشگاه اصفهان

۷ و ۸ آبان ماه ۱۴۰۴

ITRC

سازمان نظام مهندسی رایانه‌ای کشور
استان اصفهان

کارشناسی نیروگاه آبی
SNOWATEC

ریاست جمهوری
معاونت علمی، فناوری و اقتصاد دانش‌بنیان

IEEE
IRAN SECTION

دانشگاه صنعتی امیرکبیر

مرکز تحصیلات تکمیلی دانشگاه اصفهان
University of Isfahan CERT Center

دانشگاه فناوری‌های نوین شهری

Privacy-Preserving Data Anonymization for IoT: A Strategy Selection Framework

Dr. Alireza Sadeghi-Nasab

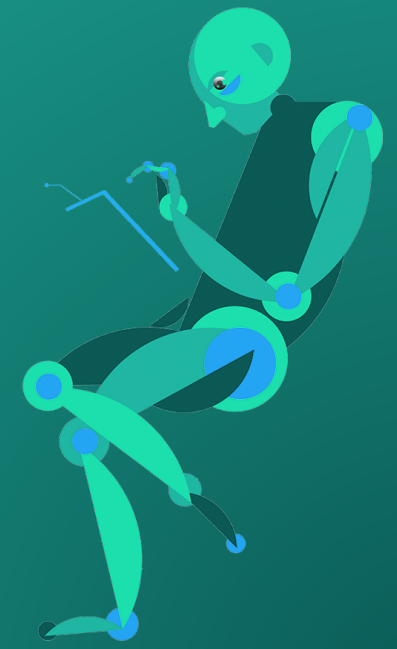
Arak University

s39913161002@araku.ac.ir

Dr. Mohsen Rahmani

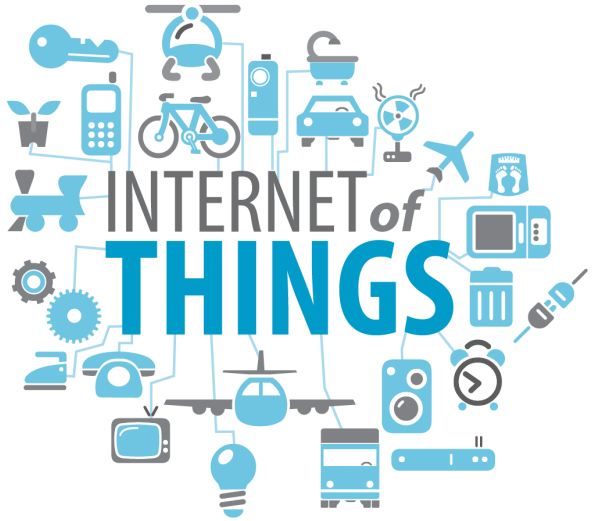
Associate Professor,
Arak University

m-rahmani@araku.ac.ir



Motivation and Problem Statement

- Rapid IoT growth produces vast data
- Data often sensitive and personal
- Privacy and utility often conflict
- Traditional methods over-generalize data
- IoT data is noisy, high-dimensional
- Need adaptive anonymization for IoT

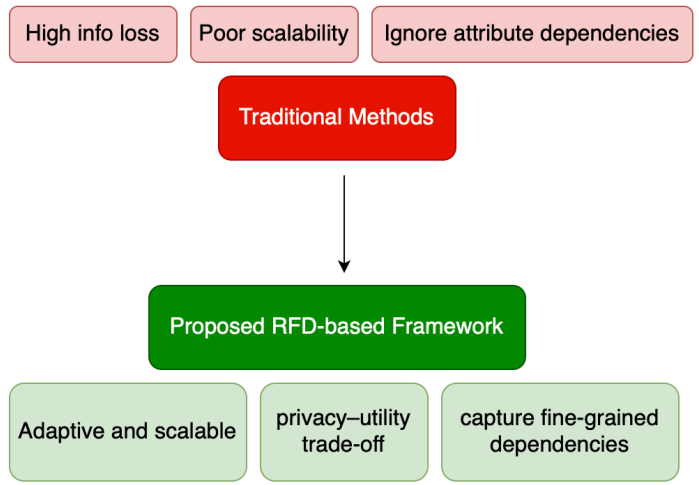


Limitations of Existing Methods

- k-anonymity, l-diversity, t-closeness widely used
- Apply uniform transformations to data
- Cause excessive generalization, high info loss
- Struggle with large IoT datasets
- Ignore inter-attribute dependencies
- Lack adaptive, data-aware behavior

Research Objective and Contribution

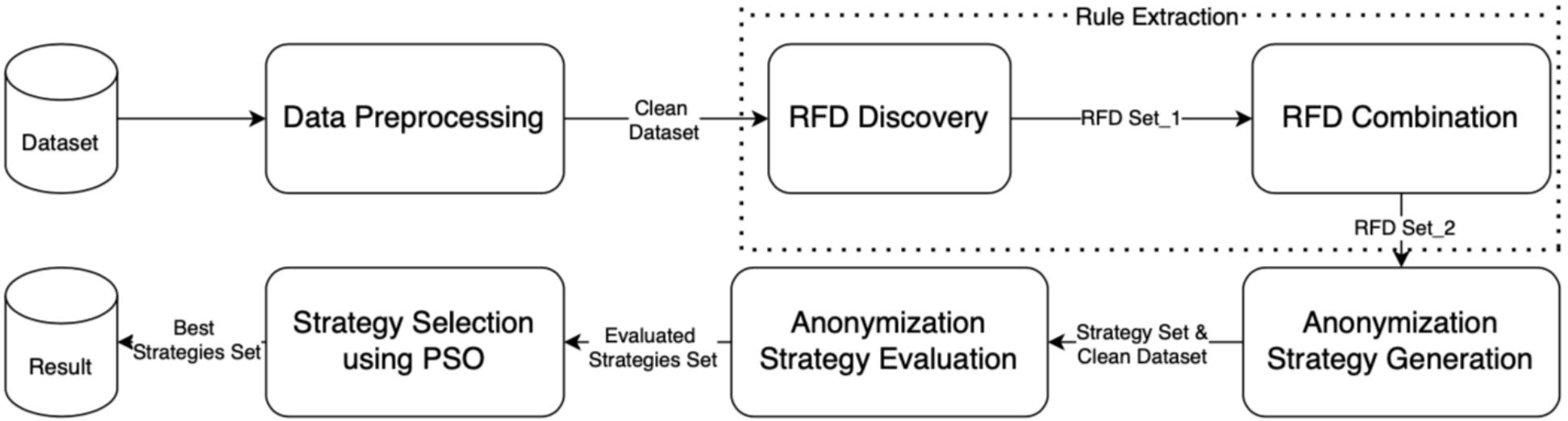
- Introduce RFD-based anonymization framework
- Capture attribute relations via RFDs
- Optimize strategy selection using PSO
- Balance privacy and data utility
- Scalable and adaptive for IoT data
- Validated on Bot-IoT dataset



Proposed Framework Overview

- Four main stages:
  1. Data preprocessing
  2. RFD discovery & combination
  3. Strategy generation & evaluation
  4. PSO-based optimization
- Ensures data consistency and scalability
- Supports IoT data characteristics

Proposed Framework Overview



Relaxed Functional Dependencies (RFDs)

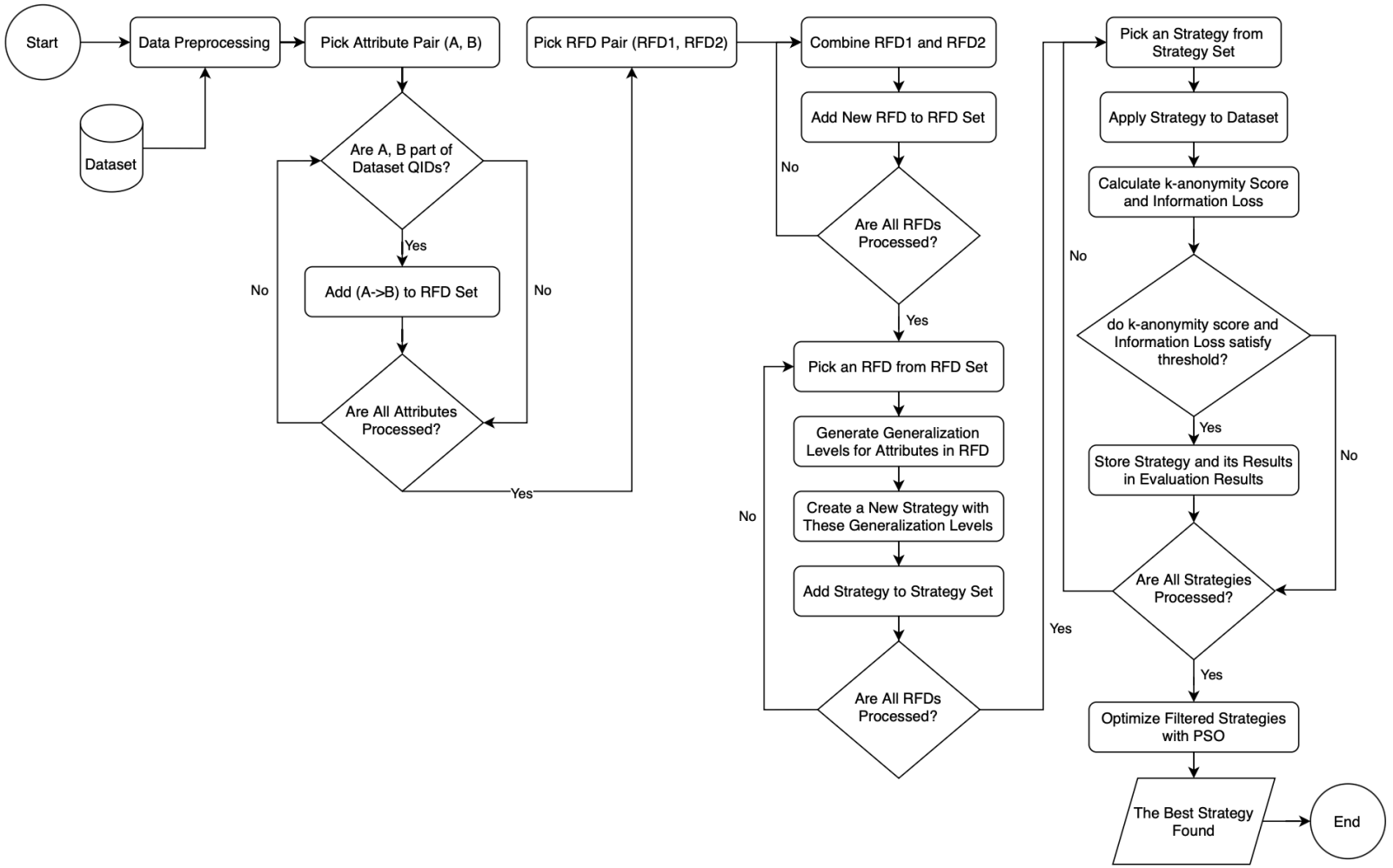
- Extend functional dependencies with tolerance
- Capture approximate attribute relationships
- Applied as roll-up dependencies
- Relax via generalization in DGHs
- Enable fine-grained, context-aware anonymization
- Form basis for candidate strategies

$$\texttt{age}_{\leq 3},\ \texttt{fnlwgt}_{\leq 2} \rightarrow \texttt{classes}_{\leq 0}$$

Optimization Using PSO

- Each particle = anonymization strategy
- Fitness combines privacy (P) and utility (U)
- P from normalized k-anonymity
- U = 1 – Information Loss
- PSO finds optimal balance between both
- Reduces manual parameter tuning

Proposed Framework - Flowchart

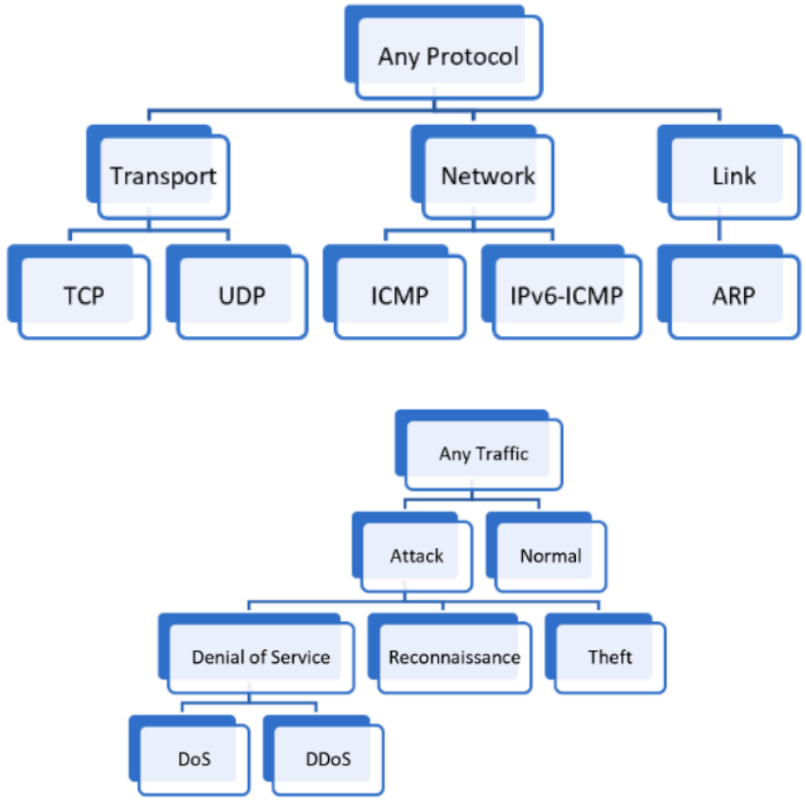


Experimental Setup

- Dataset: Bot-IoT benchmark
- 5% stratified subset used for testing
- Metrics: k-anonymity and information loss
- Thresholds: k = 5, IL = 0.7
- Compared with traditional anonymization methods
- Implemented in Python on IoT data

Experimental Setup

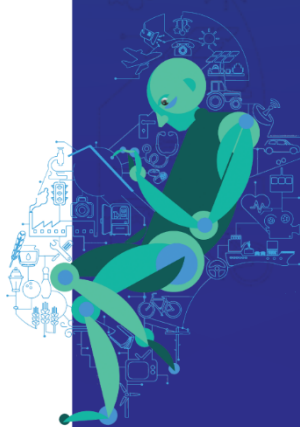
Attribute Name	Type	Range	
		Min	Max
sport	Numeric	1	9999
dport	Numeric	1	9999
seq	Numeric	1	262212
		Hierarchy Tree	
		Height	Nodes
proto	Categorical	3	9
category	Categorical	4	8



Results and Discussion

- Higher k-anonymity, lower information loss
- Outperforms classical and optimization methods
- RFDs guide precise generalizations
- PSO ensures adaptive optimization
- Scalable to large IoT datasets

Methods	k-anonymity	Information loss
Hybrid Optimization Algorithm	6	0.68
Decision-Support Framework	6	0.65
Genetic Chimp Optimization	6	0.63
Adaptive Whale Optimization	7	0.72
Proposed framework	8	0.63



Conclusion and Future Work

- RFD + PSO = adaptive anonymization
- Achieves strong privacy with low loss
- Effective for IoT and structured data
- Future: parallel RFD discovery
- Extend to l-diversity, differential privacy

Thanks for your attention!

9th international Conference on Internet of Thing and Its Applications

University of Isfahan, Isfahan, Iran

Contact: iot@res.ui.ac.ir