fKPISelect: Fault-Injection Based Automated KPI Selection for Practical Multivariate Anomaly Detection

Xingjian Zhang, Yinqin Zhao, Chang Liu, Long Wang, Xin Yang, Yefei Hou, Zhongwen Lan, Xining Hu, Beibei Miao, Ming Yang, Xiangyi Jing, Sijie Li

Tsinghua University, China Telecom Cloud Technology Co., Ltd., Zhongguancun Laboratory

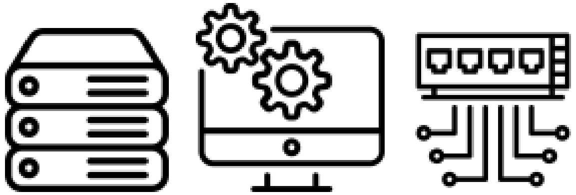
Outline

- Studying the problem of KPI selection for practical KPI-based multivariate anomaly detection in cloud systems
  - KPI-based Multivariate Time Series Anomaly Detection
  - There are a larger number of KPIs in practice than those in datasets and the SOTA model has a detection accuracy loss when the number of KPIs is large
- Proposing fKPISelect, a fault-injection-based automated KPI selection mechanism.

KPI Anomaly Detection

Components on cloud systems

- Software Programs
- Virtual Machines
- Physical Servers
- Network Devices
- …

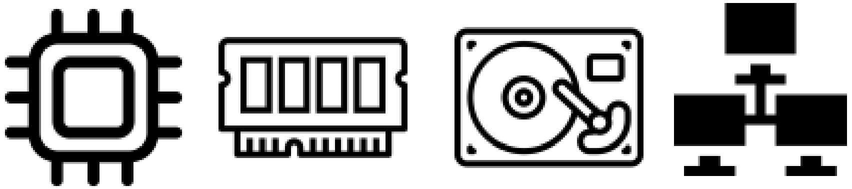


Error Causes Anomaly

Anomaly Indicates Error

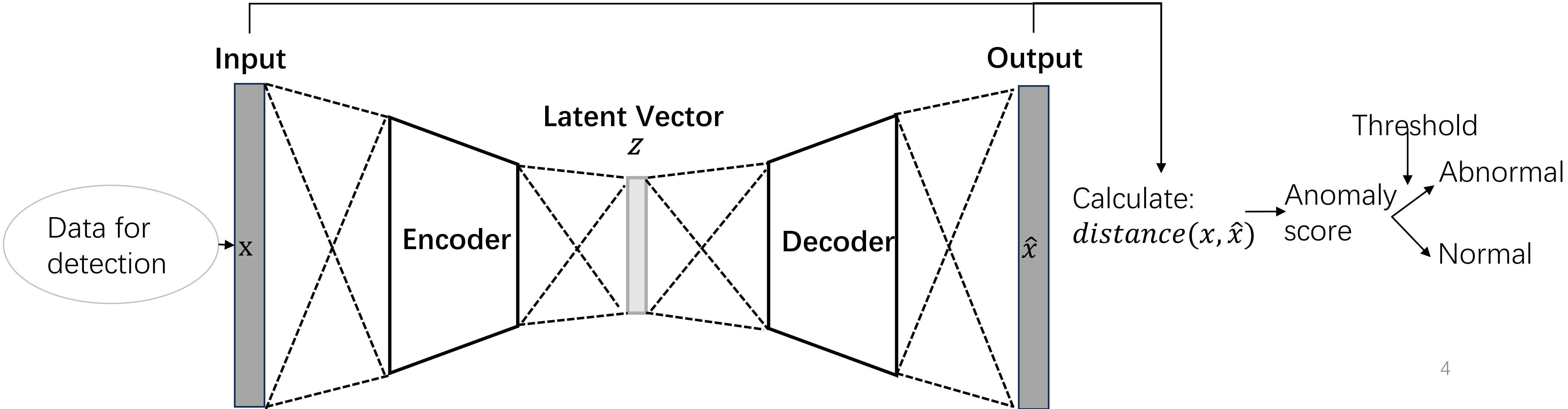
Key Performance Indicators (KPIs) of components

- CPU Utilization
- Memory Utilization
- Disk usage
- Network latency, bandwidth
- Service response time, throughput
- …



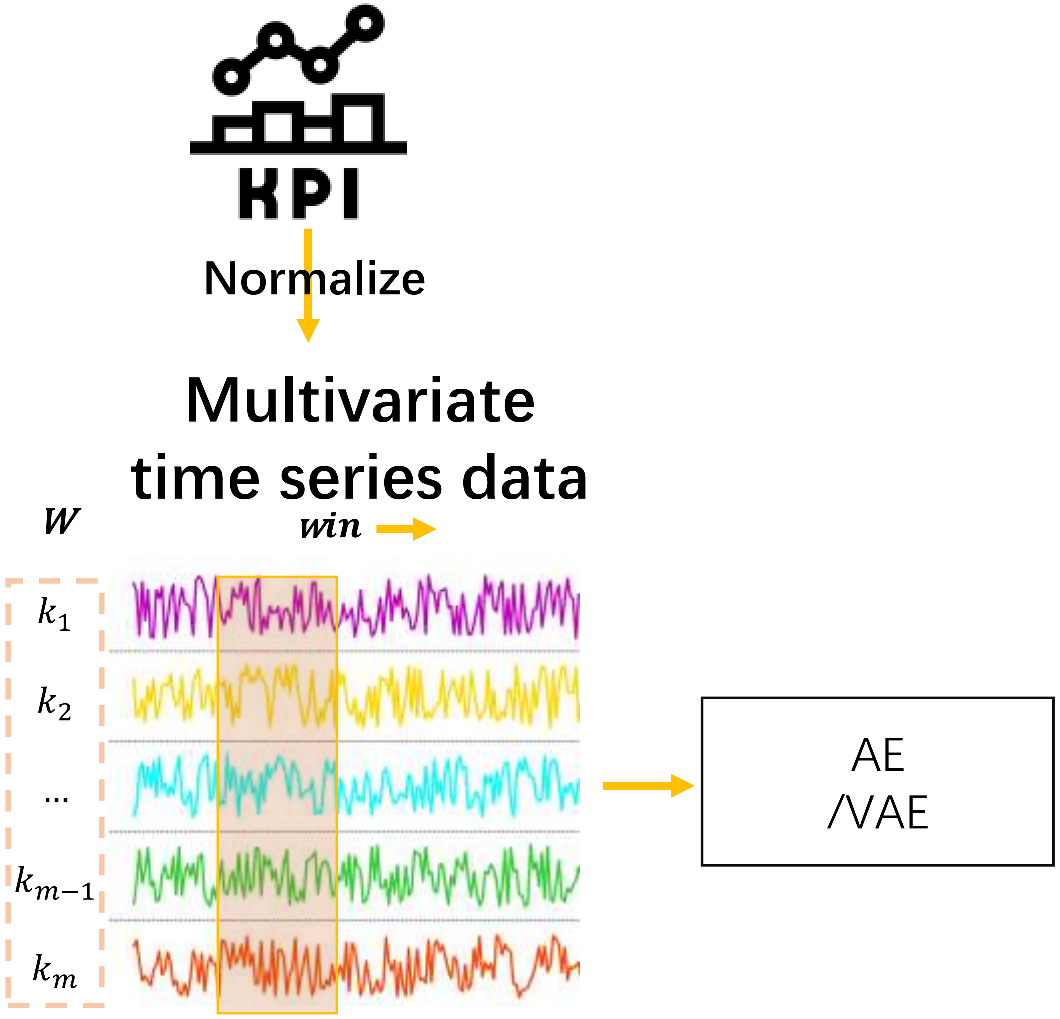
AI-based Anomaly Detection

- Based on Autoencoder (AE)
- Learn representations of normal data patterns
- Encountered data patterns ➡️ Reconstruct well
- Anomalous data patterns ➡️ Reconstruct poorly

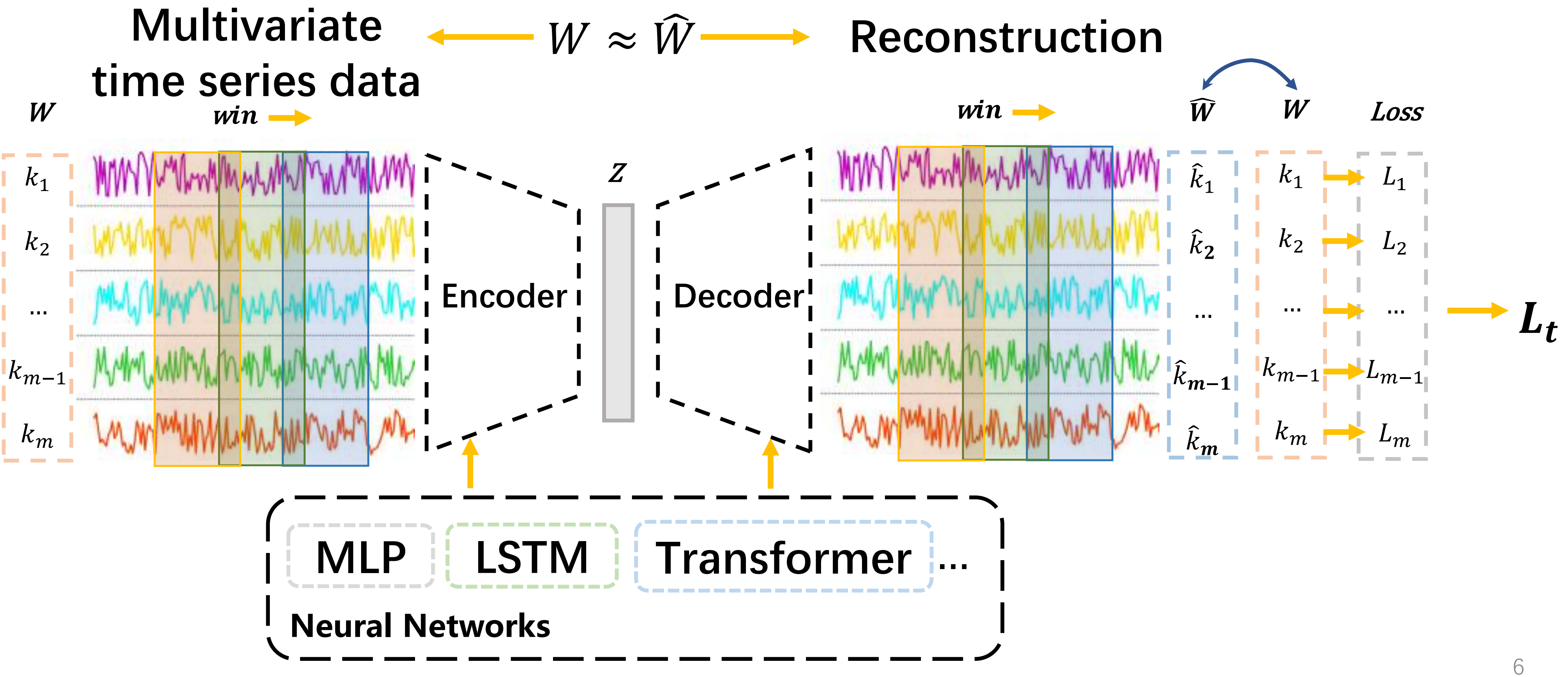


Multivariate Time Series Anomaly Detection

- Sliding windows are used to cut part of the data
- The multiple time series are treated equally with the same weight.
- Anomaly score can be seen as the average reconstruction loss of each time series: $L_t = \frac{1}{m}\sum_{i=1}^{m}\left\|k_{i,t} - \widehat{k_{i,t}}\right\|_2^2$
- Previous models:
  - OmniAnomaly (KDD’19), USAD(KDD’20), AnomalyTransformer(ICLR’22), Uni-AD(ISSRE’22)……



AI-based Multivariate Time Series Anomaly Detection



From experiments to real-world systems

- Models directly applied to real-world systems does not perform as well as reported in experimental datasets.
- There's a gap between existing datasets and data in practice.
- Experimental Datasets
  - Well-preprocessed
  - Limited KPI numbers
  - Lack KPI metadata

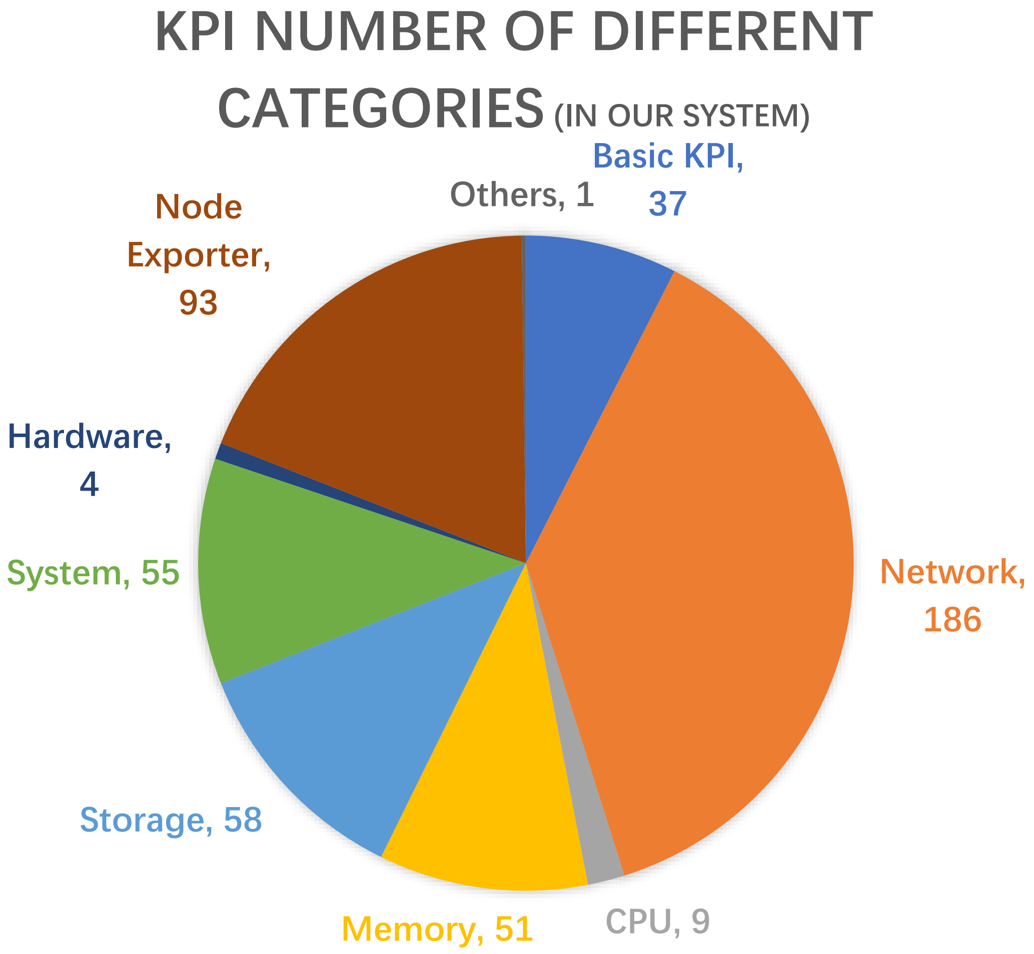
Data	KPI Number	KPI Description in Dataset
SMD (KDD'19)	38	CPU, network and memory usage, etc.
CTF_data (INFOCOM'21)	49	CPU, memory, sockets, UDP, TCP
TC_data (ISSRE'22)	11	CPU usage, memory usage, and network speed, etc
FluxRank (ISSRE'19)	47	CPU, Disk, Memory, Network, and OS kernel

Gap Between Existing Datasets and Data in Practice

- Data in Practice
  - Complex & Diverse
- Example: Node Exporter Data
  - Collected by Prometheus
  - Visualized by Grafana

Data	KPI Number	KPI Description in Dataset
SMD (KDD'19)	38	CPU, network and memory usage, etc.
CTF_data (INFOCOM'21)	49	CPU, memory, sockets, UDP, TCP
TC_data (ISSRE'22)	11	CPU usage, memory usage, and network speed, etc
FluxRank (ISSRE'19)	47	CPU, Disk, Memory, Network, and OS kernel
Node Exporter	**493**	**All KPIs provided by node exporter**

Gap Between Existing Datasets and Data in Practice

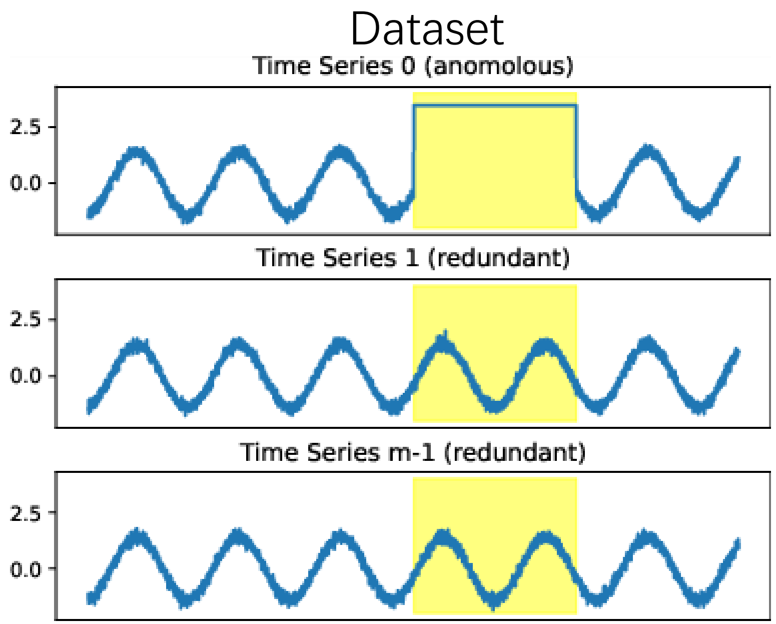


The figure is from Grafana

Accuracy loss of TSAD: Experiment

Phenomenon: Current multivariate TSAD models have a detection accuracy loss when there are a huge number of KPIs.

- Synthetic datasets
  - With various KPI numbers
  - Partial KPIs are affected by errors, other KPIs remain normal
- SOTA Model: AnomalyTransformer (ICLR’22)

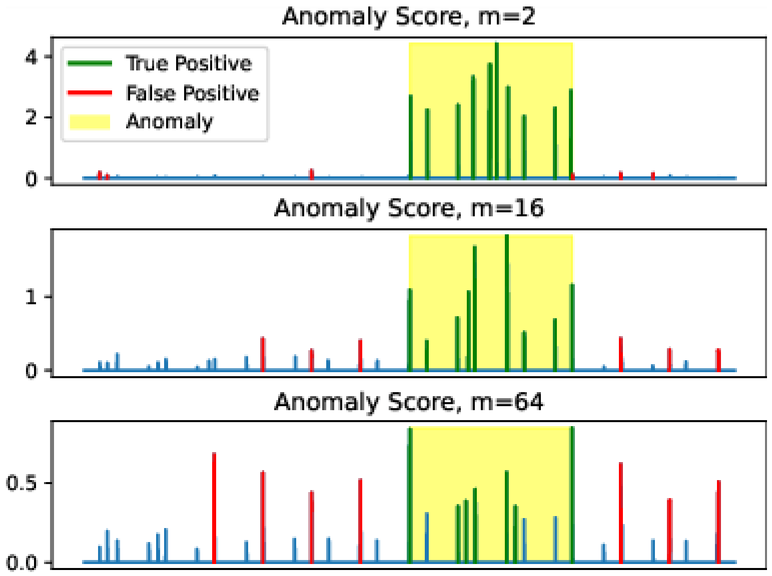


Performance loss of TSAD: Experiment

Phenomenon: Current multivariate TSAD models have a detection accuracy loss when there are a huge number of KPIs.

- Result
  - When the number of KPIs increases, the anomaly scores during the error-present period become not so outstanding, causing more false positives.

Anomaly score & Prediction Results



KPI number is m

Performance loss of TSAD: Explanation

Phenomenon: Current multivariate TSAD models have a detection accuracy loss when there are a huge number of KPIs.

Unsupervised learning: Anomaly scores can only be calculated as the averages of the reconstruction loss values of all KPIs.

$$L_t = \frac{1}{m} L_{i,t}$$

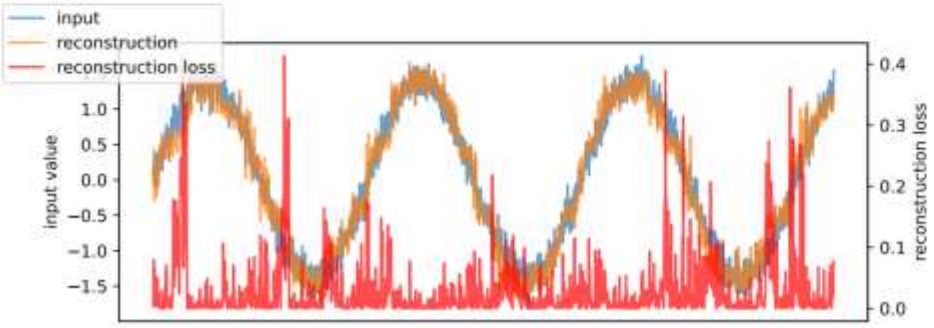
Imprecise Reconstruction: Deviation exists in the reconstruction loss of each KPI due to noises.

$$n_i \sim N(\mu_i, \sigma_i)$$

Deviation accumulates:

$$n = \sum_{i=0}^{m} n_i \sim N\left(\sum_{i=0}^{m} \mu_i, \sum_{i=0}^{m} \sigma_i^2\right)$$

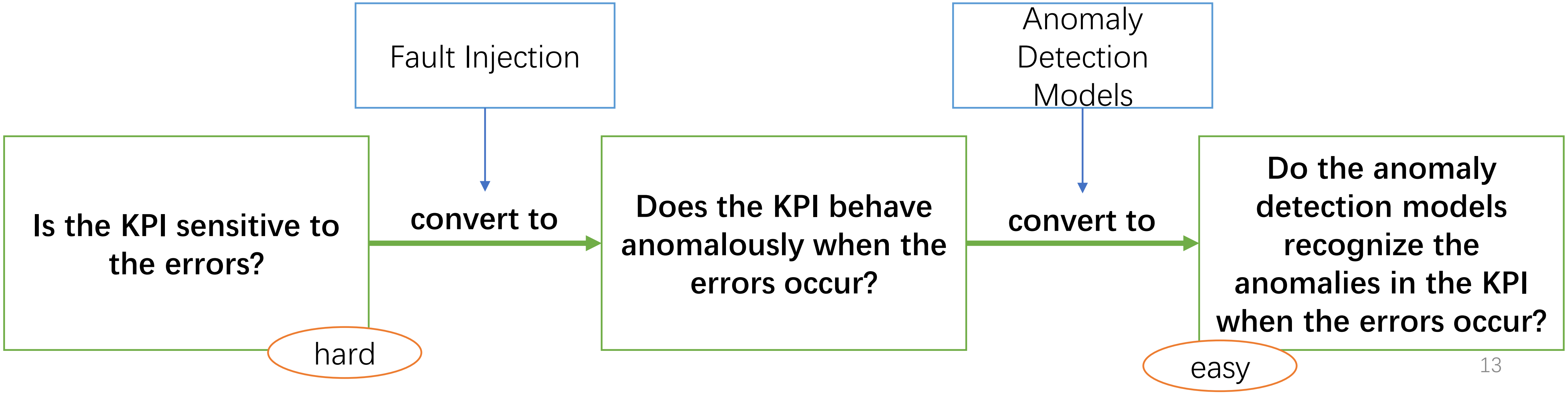
(assume the deviations are in normal distribution)



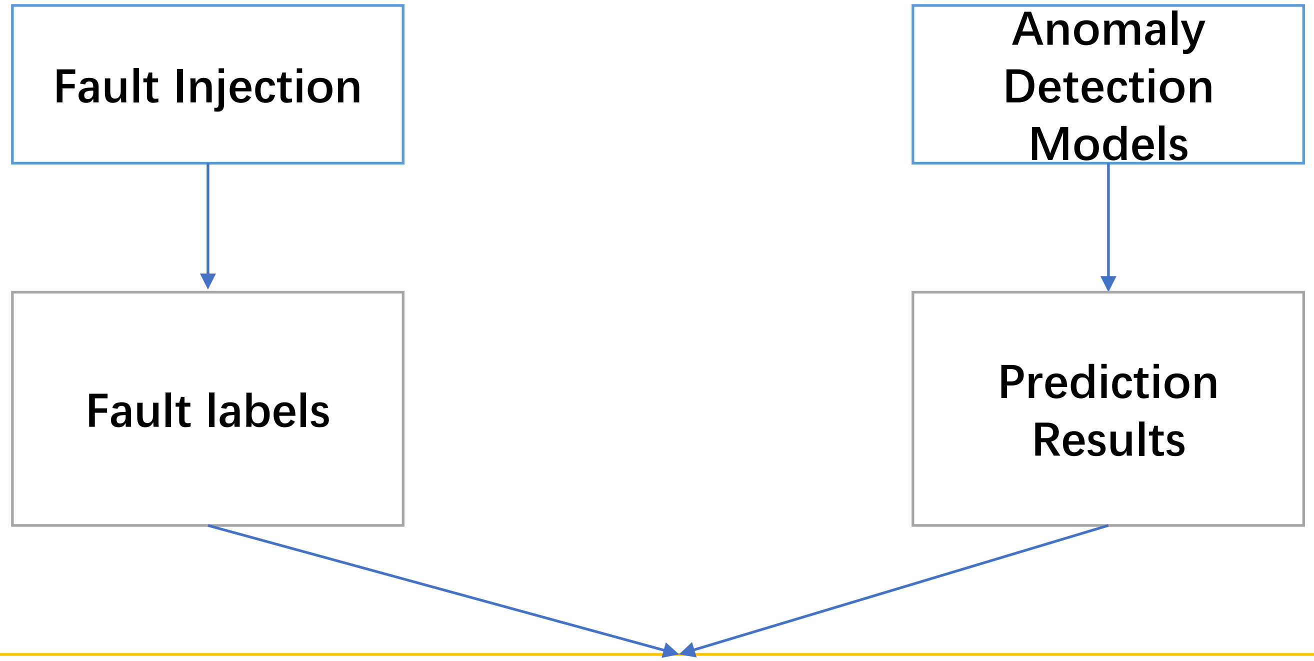
fKPISelect: Fault Injection-Based KPI Selection

- **Problem: KPI selection for practical KPI-based multivariate anomaly detection in cloud systems**
- Solution:

For each KPI, consider:



fKPISelect: Fault Injection-Based KPI Selection

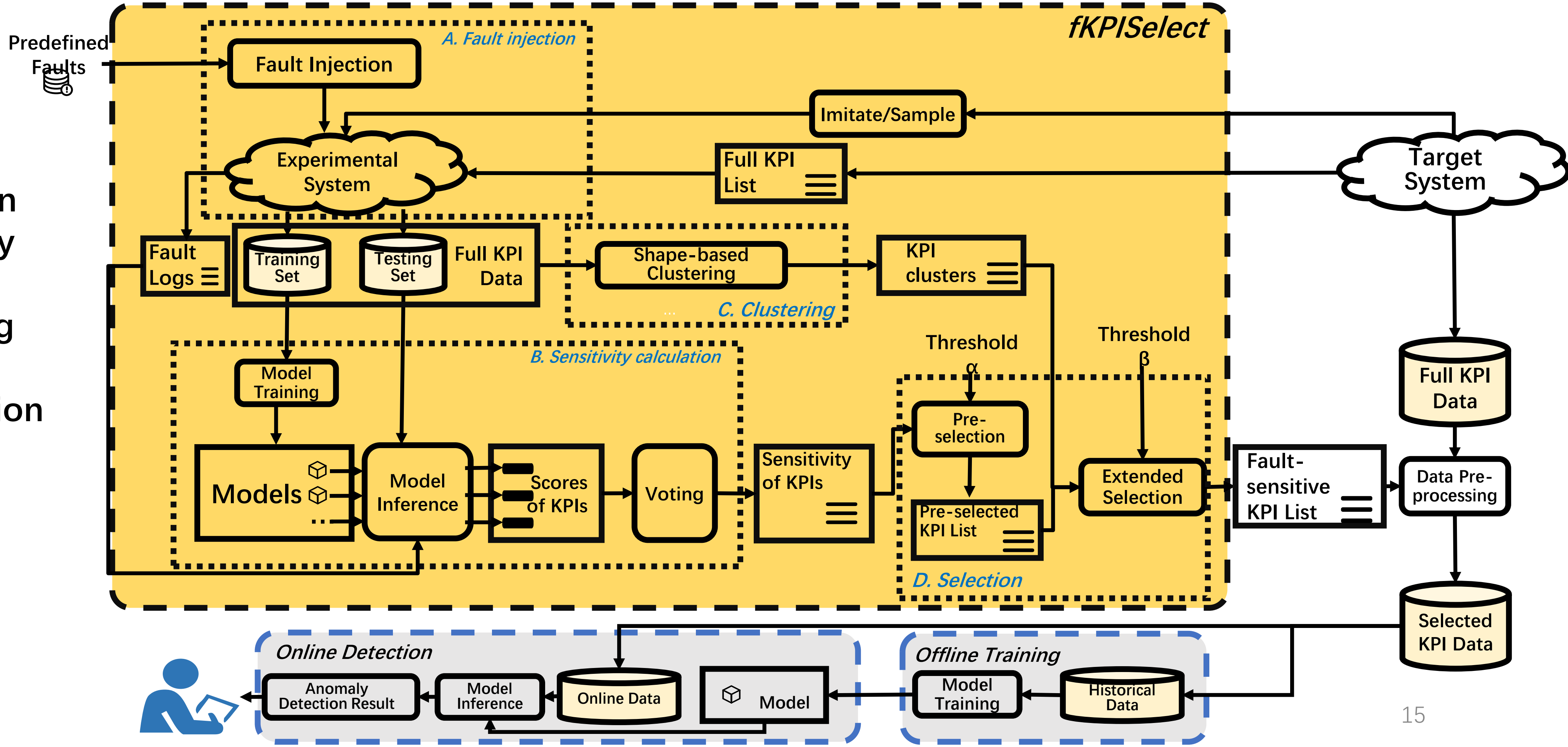


quantitative criterion of KPI's Sensitivity to Errors:

$$\text{sensitivity of KPI i} = \frac{\textit{The number of errors correcly predicted by the model with KPI i}}{\textit{The total number of injected errors}}$$

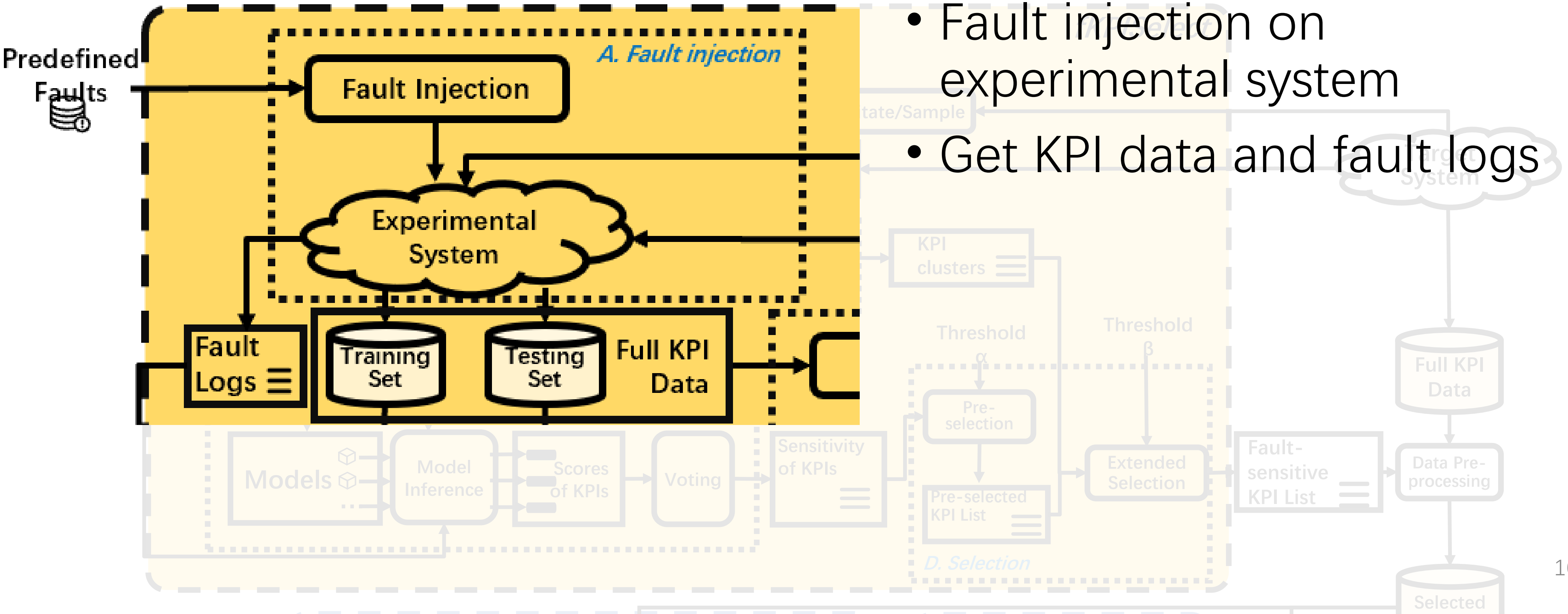
fKPISelect: Fault Injection-Based KPI Selection

(1) Fault Injection
(2) KPI Sensitivity Calculation
(3) KPI Clustering
(4) KPI Selection
Anomaly Detection



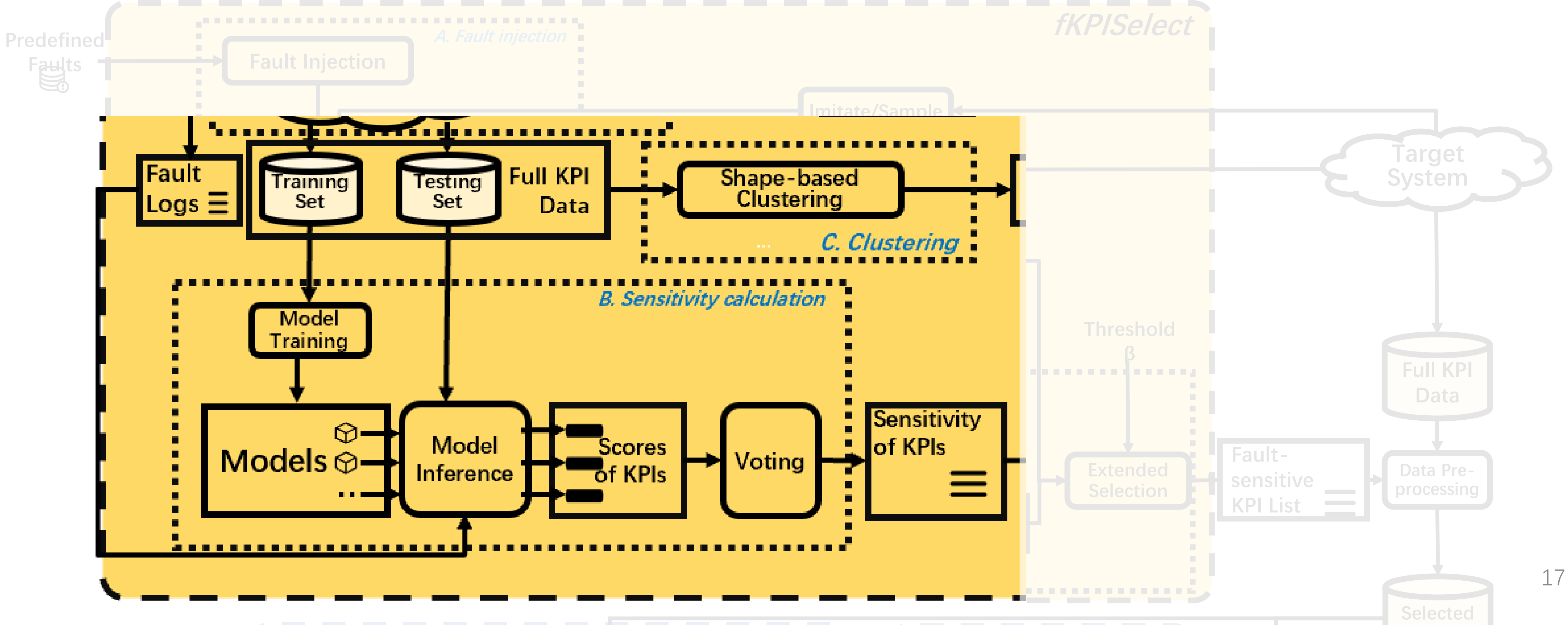
fKPISelect: (1) Fault Injection

- Define fault types and plan fault injection configurations in detail
- Fault injection on experimental system
- Get KPI data and fault logs



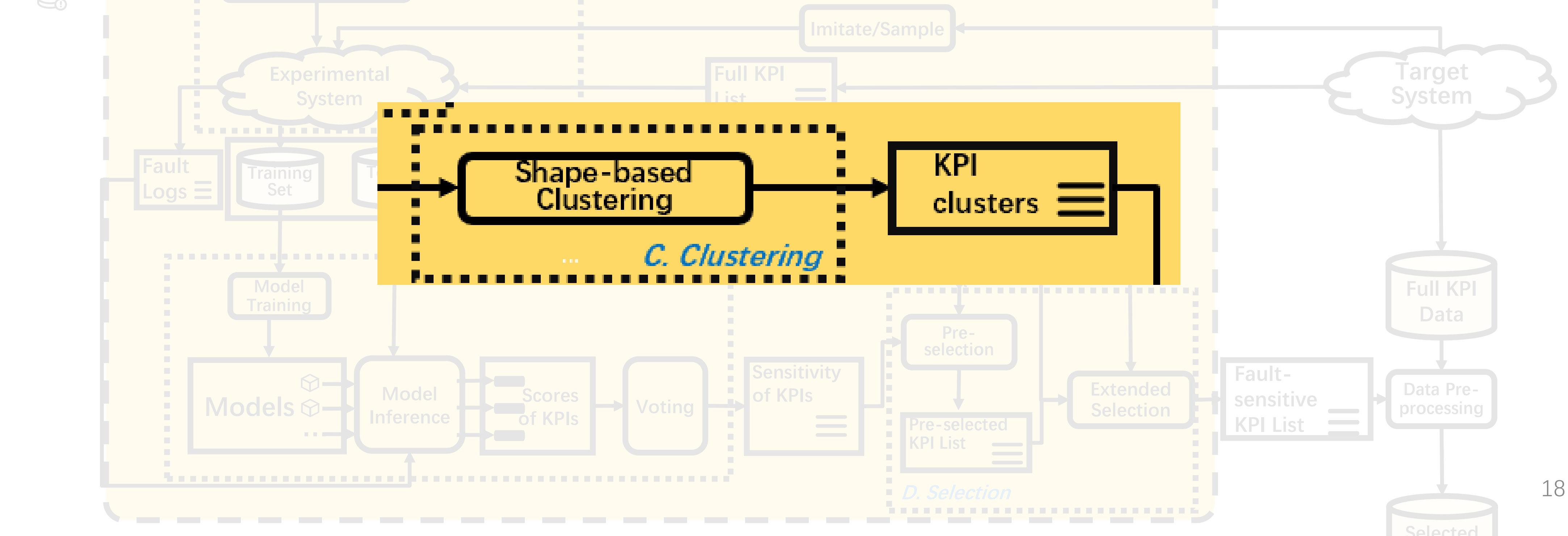
fKPISelect: (2) KPI Sensitivity Calculation

- Use the detection results for injected faults to calculate sensitivity
- Voting mechanism by multiple models to improve accuracy



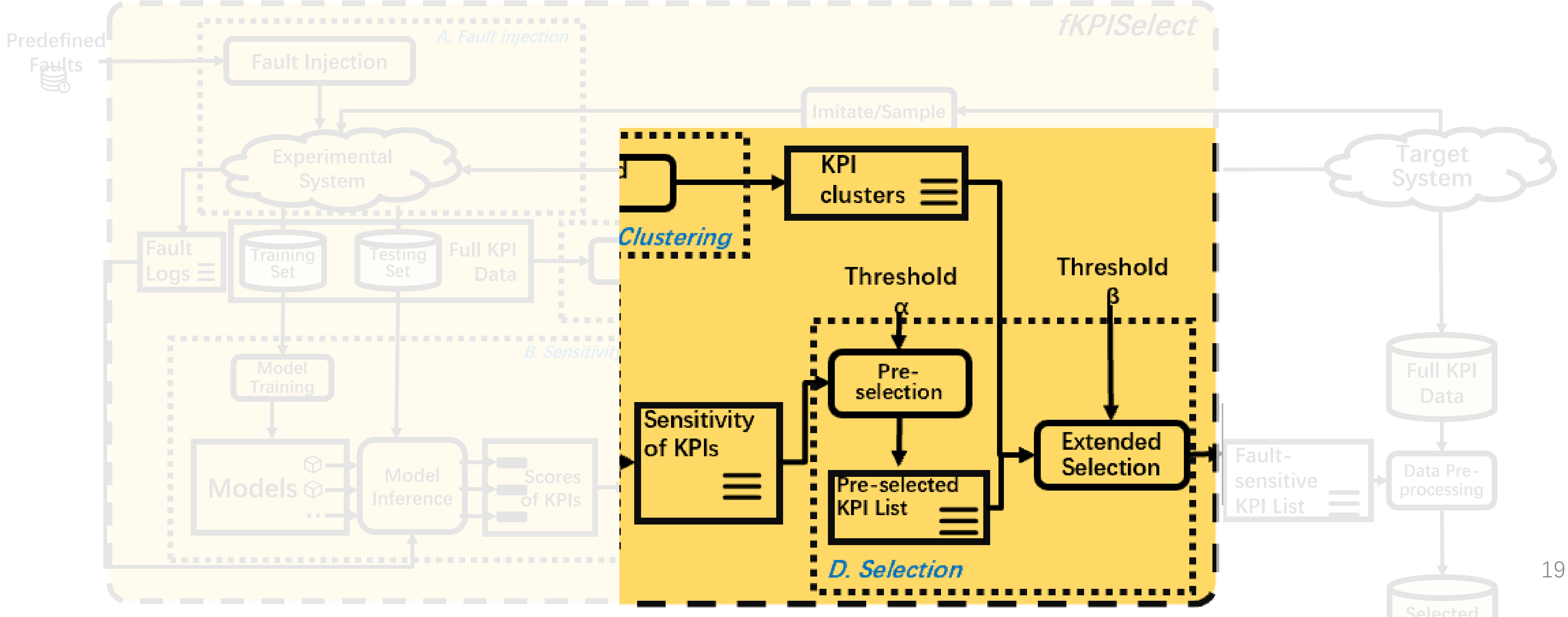
fKPISelect: (3) KPI Clustering

- Solve the problem of the false ignorance of error-sensitive KPIs due to the limitation of fault injections
- Cluster the KPIs with similar properties for extended KPI selection



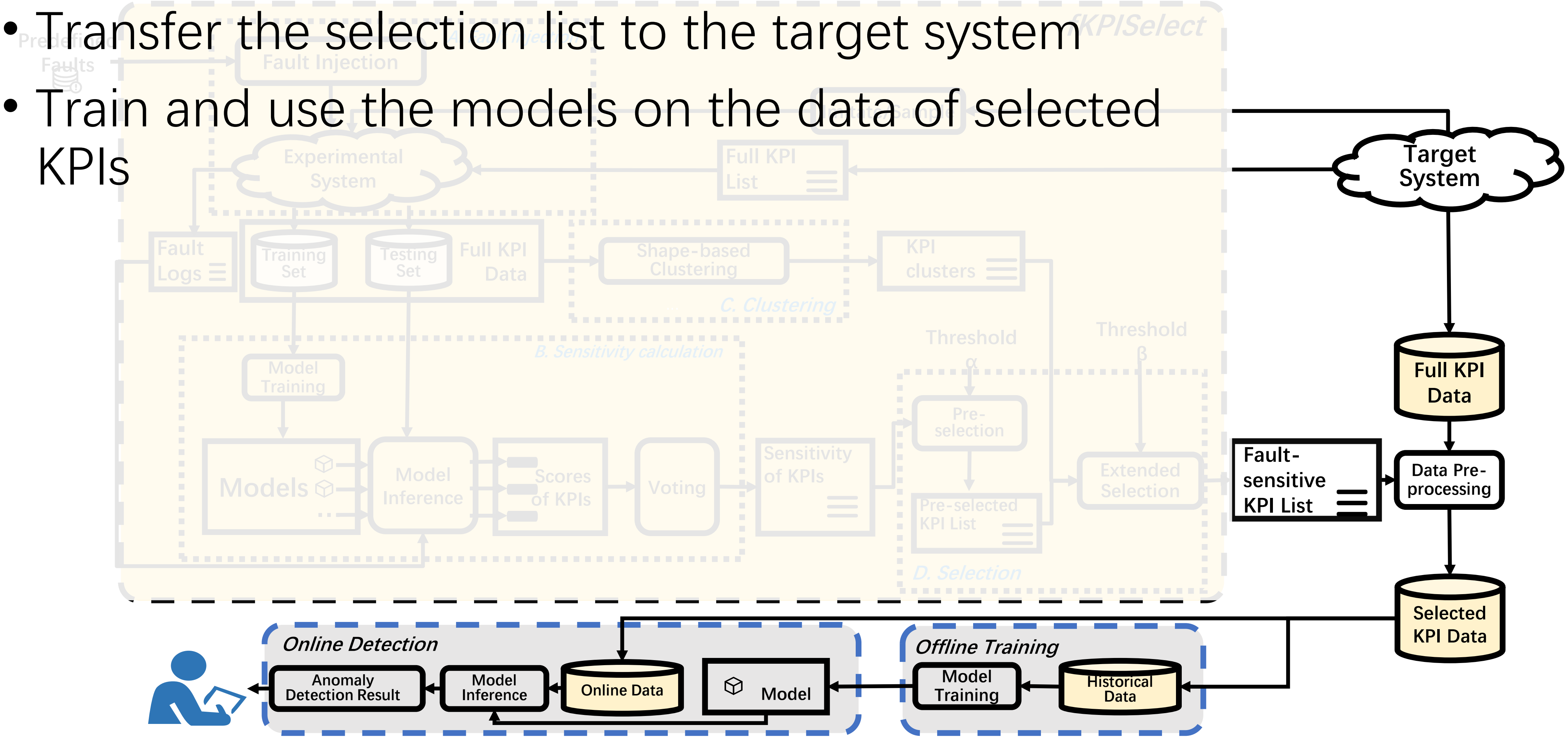
fKPISelect: (4) KPI Selection

- Threshold of KPI sensitivity (step 2)
- Threshold of cluster selecting ratio (step 3)



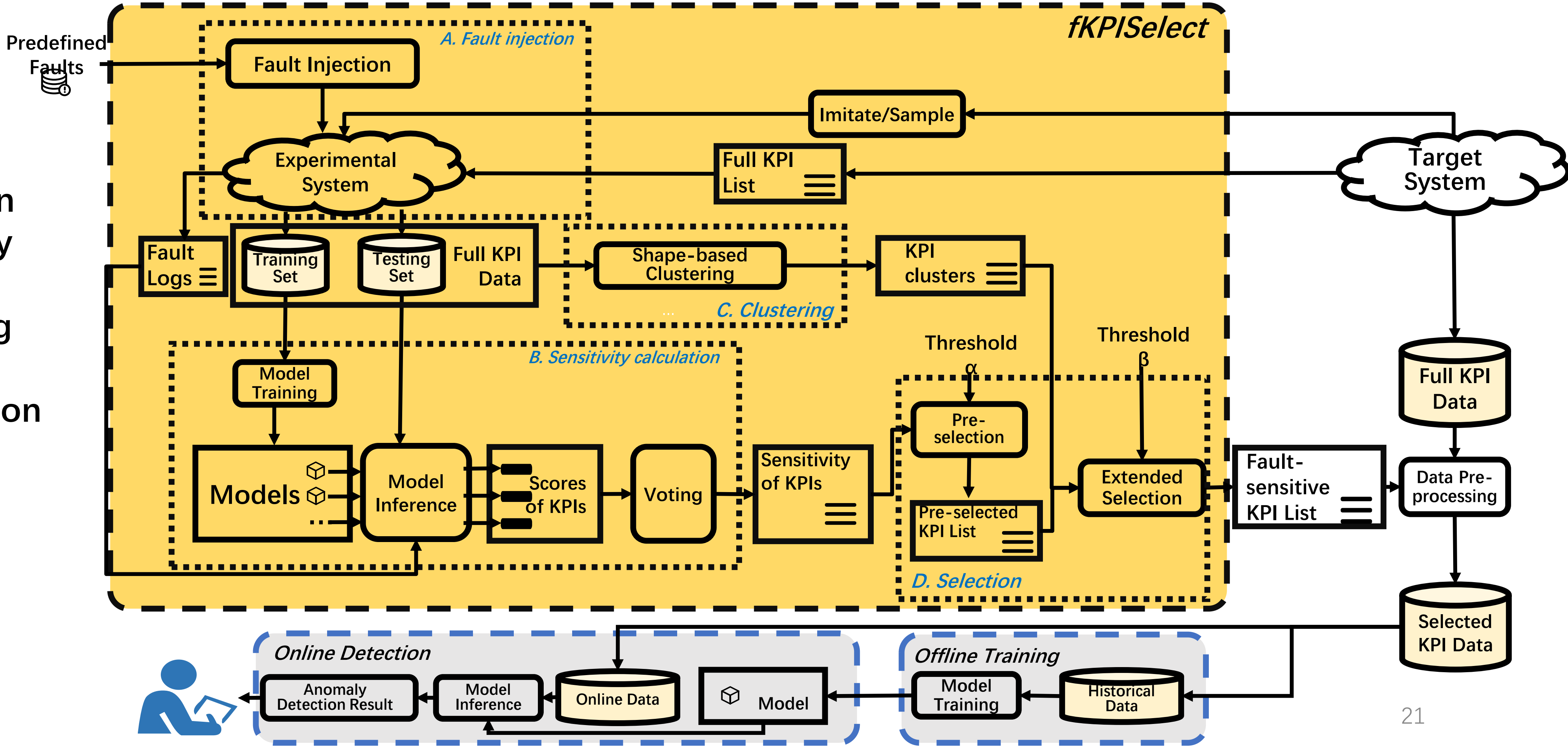
fKPISelect: Anomaly Detection on Target System

- Transfer the selection list to the target system
- Train and use the models on the data of selected KPIs



fKPISelect: Fault Injection-Based KPI Selection

(1) Fault Injection
(2) KPI Sensitivity Calculation
(3) KPI Clustering
(4) KPI Selection
Anomaly Detection



Evaluation

- Compare performance with
  - All KPIs
  - Manual Selection
- Dataset replicating practical scenario: Node_data
  - Experimental System: 5-node Kubernetes cluster
  - Fault Injection on nodes
    - Network Anomalies
    - High CPU consumption
    - Memory Leaks
    - Anomalous number of disk access
- Also performed simplified experiments on public datasets

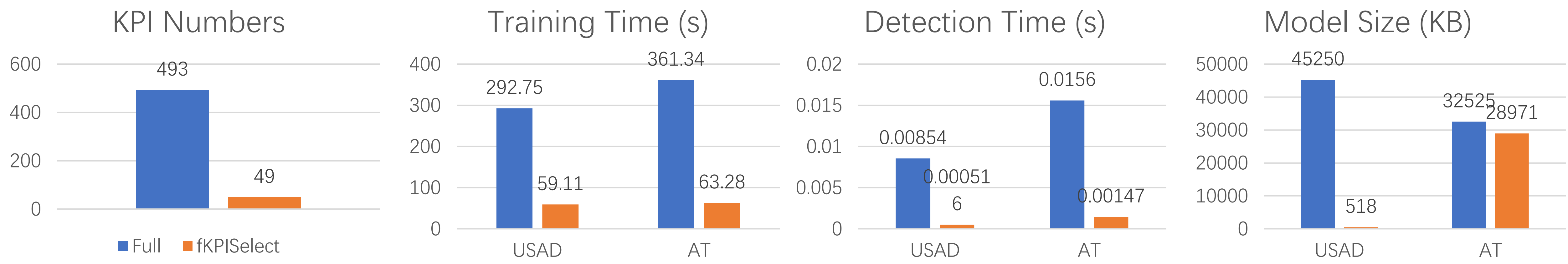
Evaluation

- The detection performance improved
  - F1 score increased from 0.68 to **0.91** (for AnomalyTransformer) in Node_data

Dataset	Preprocess	USAD Precision	USAD Recall	USAD F1 score	AnomalyTransformer Precision	AnomalyTransformer Recall	AnomalyTransformer F1 score
Node_data	Full	0.3847	0.4088	0.2756	0.5625	0.8571	0.6792
	Manual	0.4610	0.7976	0.5843	0.6296	0.9285	0.7504
	fKPISelect	**0.4702**	**0.8069**	**0.5942**	**0.8461**	**0.9897**	**0.9123**
SMD	Full	0.6509	0.6533	0.6521	0.9414	0.8901	0.9151
	Manual	**0.6800**	0.7100	0.6946	**0.9424**	0.8354	0.8856
	fKPISelect	0.6082	**0.8110**	**0.6951**	0.9421	**0.9247**	**0.9338**
CTF	Full	0.2976	0.3439	0.3190	0.9047	1.0000	0.9500
	Manual	0.2976	0.3440	0.3191	0.9051	1.0000	0.9502
	fKPISelect	**0.4534**	**0.5598**	**0.5010**	**0.9070**	**1.0000**	**0.9646**

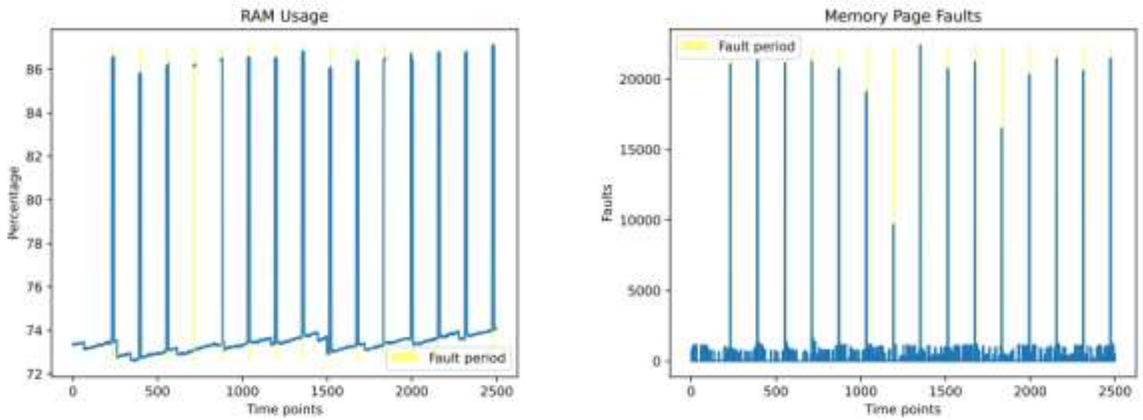
Evaluation

- Time & Space cost are reduced



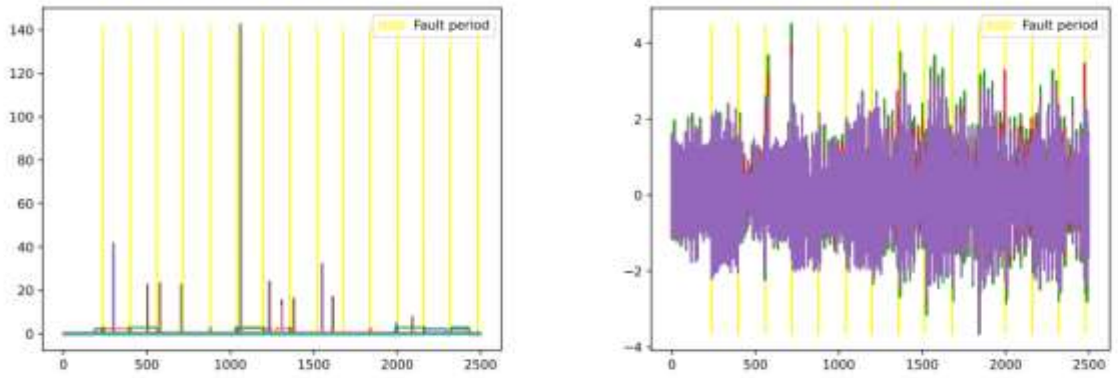
Evaluation

- Selected KPIs



RAM Usage & Memory Page Faults are sensitive to memory errors

- Unselected KPIs



2 groups of Unselected KPIs

Summary

- Focus on the issue of KPI selection in multivariate time series anomaly detection.
- Investigate the performance loss issue of multivariate TSAD models with experiments.
- Propose fKPISelect, a fault-injection-based automated KPI selection mechanism.
- Code and dataset are available at https://github.com/THUzxj/fKPISelect

References

- Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun, and D. Pei, “Robust anomaly detection for multivariate time series through stochastic recurrent neural network,” in Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining, 2019, pp. 2828–2837.
- N. Authors, “Netmanaiops/ctf data: Data of paper ”ctf: Anomaly detection in high-dimensional time series with coarse-to-fine model transfer”,” 2021, accessed: 2021-12- 14. [Online]. Available: https://github.com/NetManAIOps/ CTF data
- Z. He, P. Chen, and T. Huang, “Share or not share? towards the practicability of deep models for unsupervised anomaly detection in modern online systems,” in 2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE). IEEE, 2022, pp. 25–35.
- P. Liu, Y. Chen, X. Nie, J. Zhu, S. Zhang, K. Sui, M. Zhang, and D. Pei, “FluxRank: A Widely-Deployable Framework to Automatically Localizing Root Cause Machines for Software Service Failure Mitigation,” in 2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE), pp. 35–46.
- J. Audibert, P. Michiardi, F. Guyard, S. Marti, and M. A. Zuluaga, “USAD: UnSupervised Anomaly Detection on Multivariate Time Series,” in Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, ser. KDD ’20. New York, NY, USA: Association for Computing Machinery, Aug. 2020, pp. 3395– 3404.

Thank you!