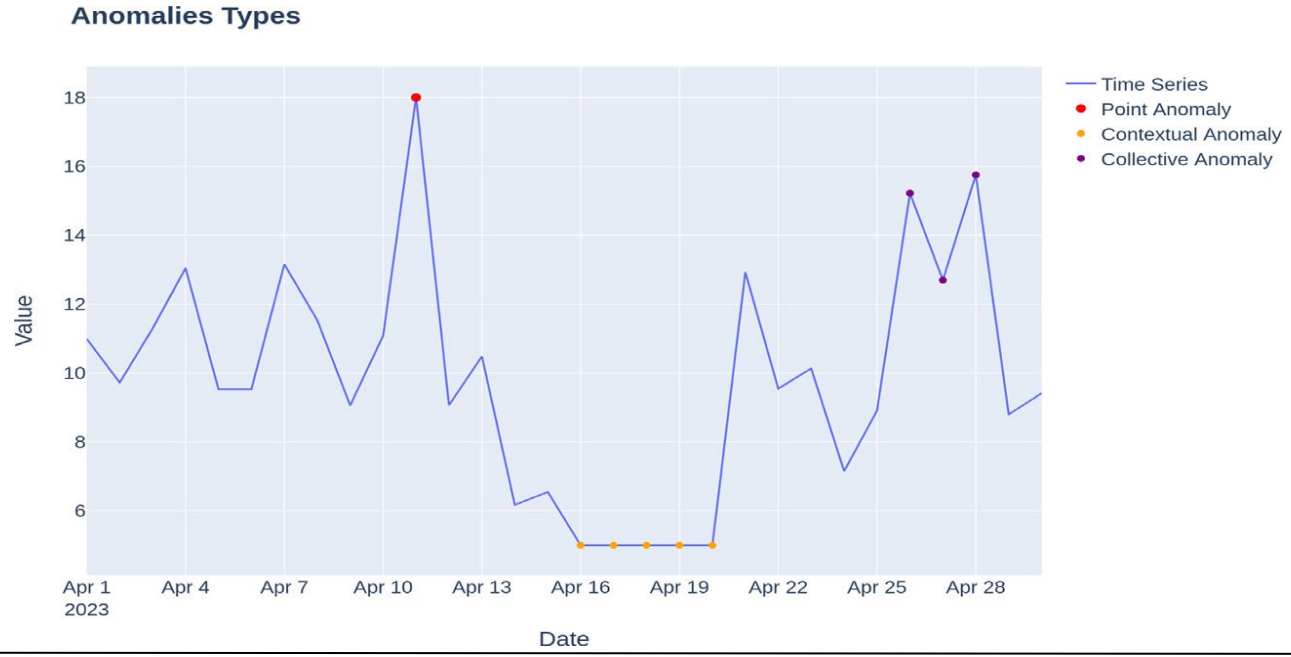
Anomaly Detection

Need for Anomaly Detection

- Network Infrastructure
- Network Management
- Network Flows and Their Types

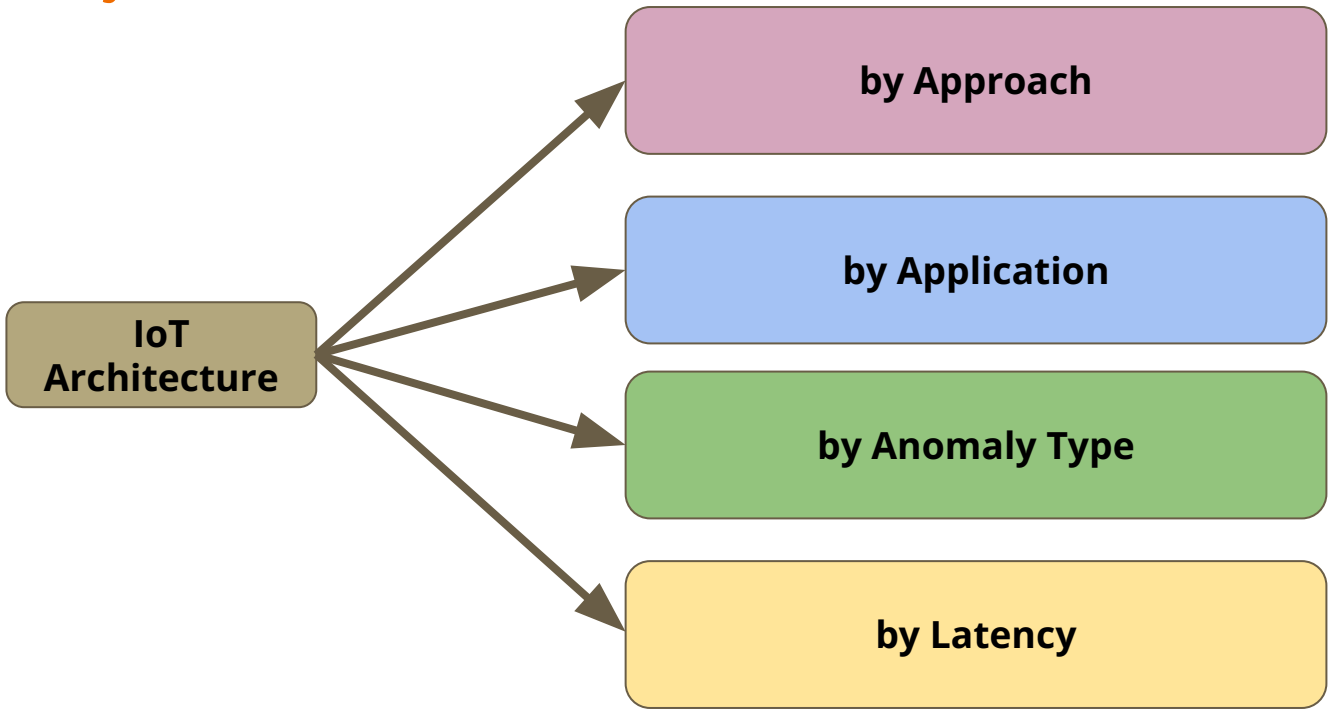
Anomalies (Outliers)

- Definition



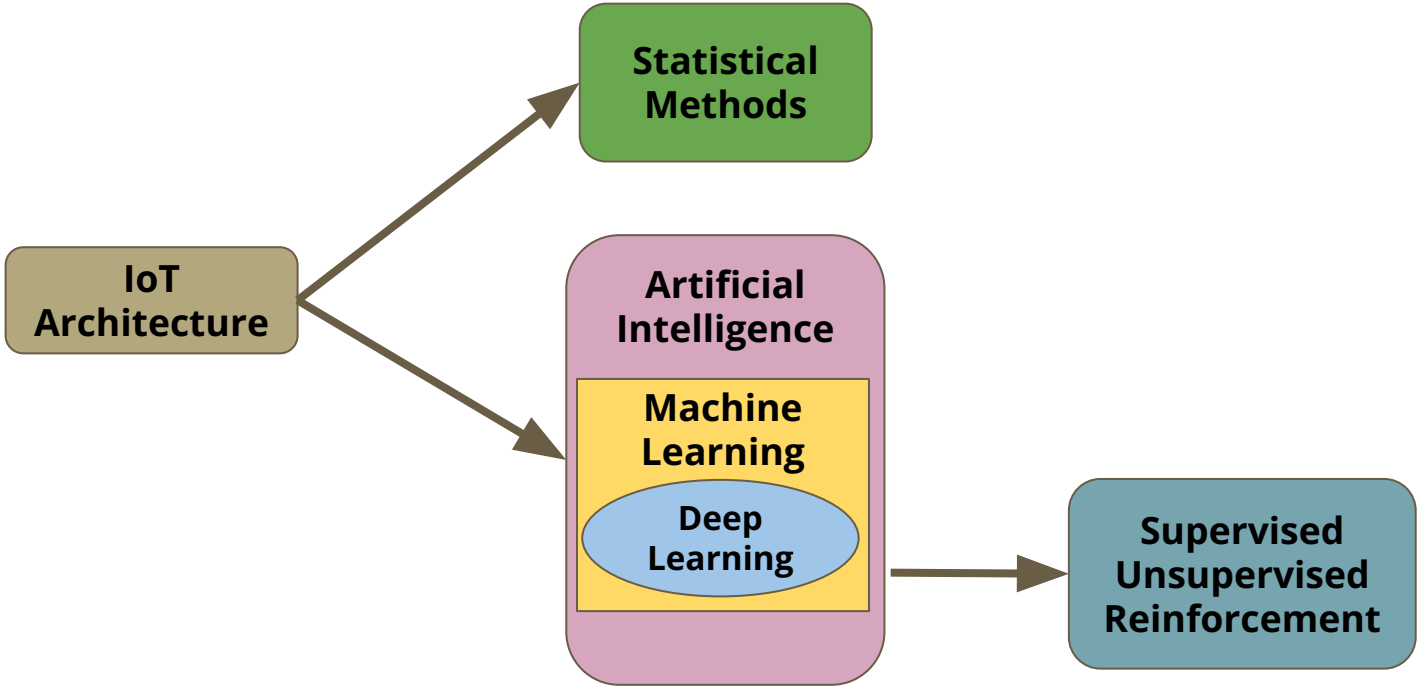
[1] Sergio Trilles, Sahibzada Saadoon Hammad, Ditsuhi Iskandaryan, Anomaly detection based on Artificial Intelligence of Things: A Systematic Literature Mapping, Internet of Things, Volume 25, 2024, 101063, ISSN2542ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101063.

Anomaly Detection



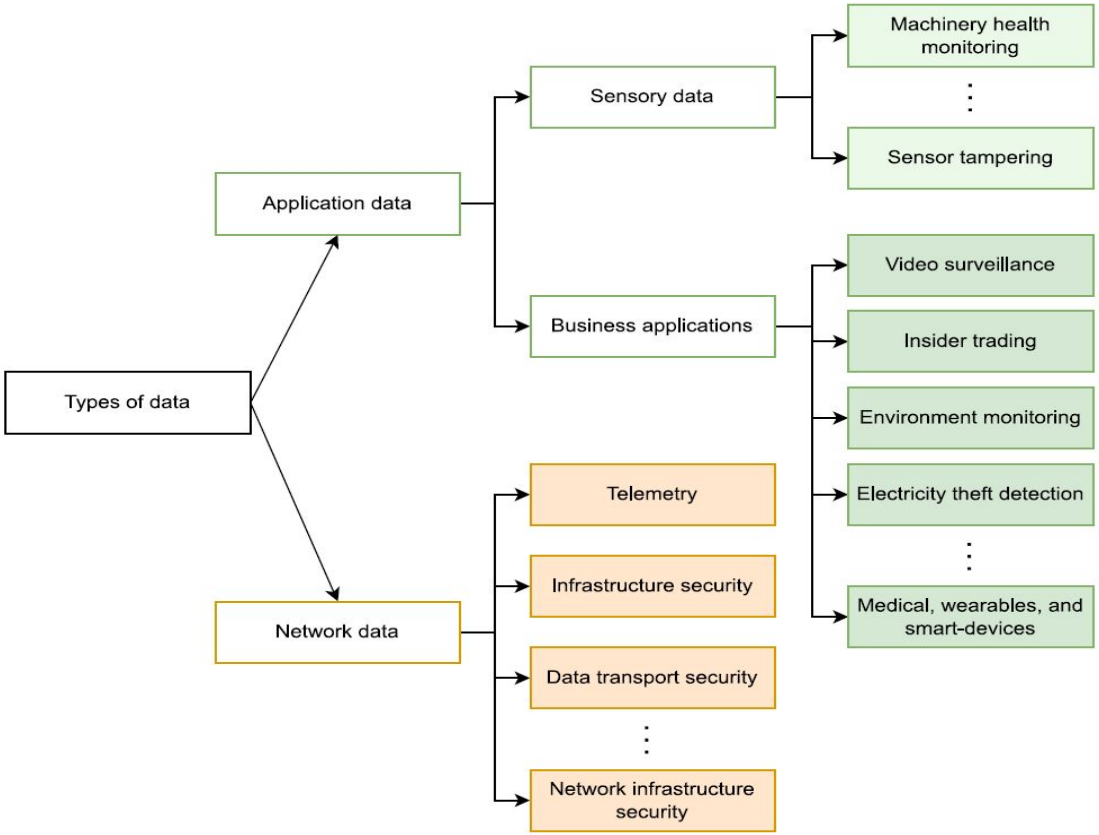
[2] Ayan Chatterjee, Bestoun S. Ahmed, IoT anomaly detection methods and applications: A survey, Internet of Things, Volume 19, 2022, 100568, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100568.

Anomaly Detection



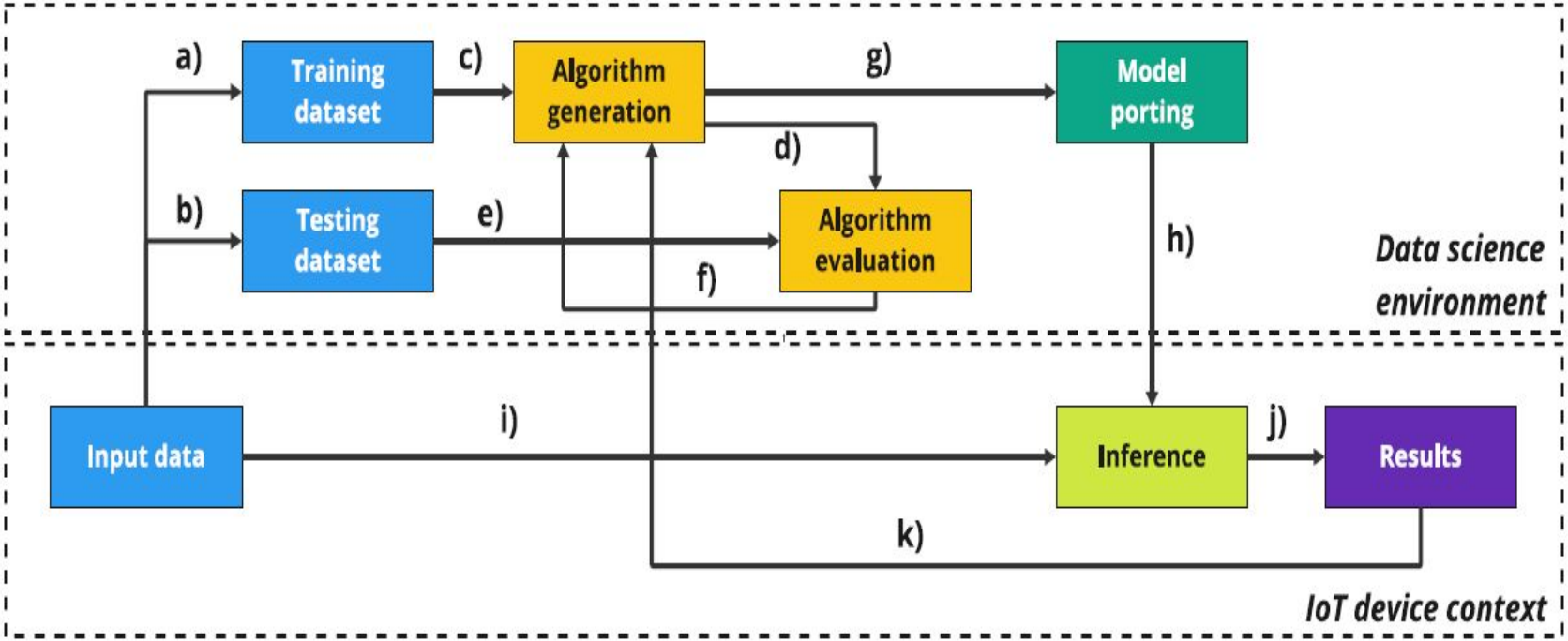
[1] Sergio Trilles, Sahibzada Saadoon Hammad, Ditsuhi Iskandaryan, Anomaly detection based on Artificial Intelligence of Things: A Systematic Literature Mapping, Internet of Things, Volume 25, 2024, 101063, ISSN2542ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101063.

Anomaly Detection



[2] Ayan Chatterjee, Bestoun S. Ahmed, IoT anomaly detection methods and applications: A survey, Internet of Things, Volume 19, 2022, 100568, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100568.

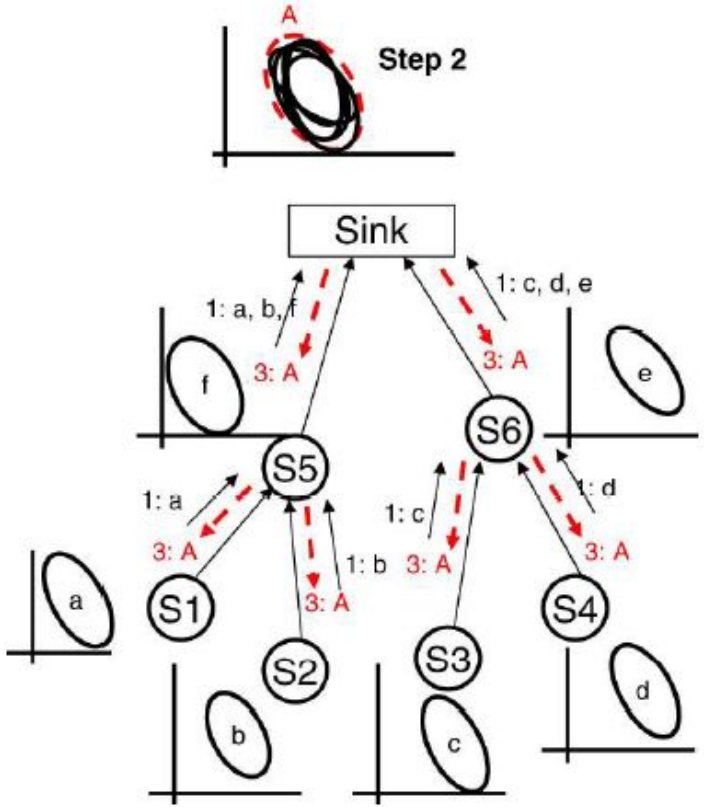
Anomaly Detection



[1] Sergio Trilles, Sahibzada Saadoon Hammad, Ditsuhi Iskandaryan, Anomaly detection based on Artificial Intelligence of Things: A Systematic Literature Mapping, Internet of Things, Volume 25, 2024, 101063, ISSN2542ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101063.

Distributed Anomaly Detection

Diagram Reference: From the Textbook "Internet of Things: Principles and Paradigms" By Rajkumar Buyya, Amir Vahid Dastjerdi, Elsevier, 2016.



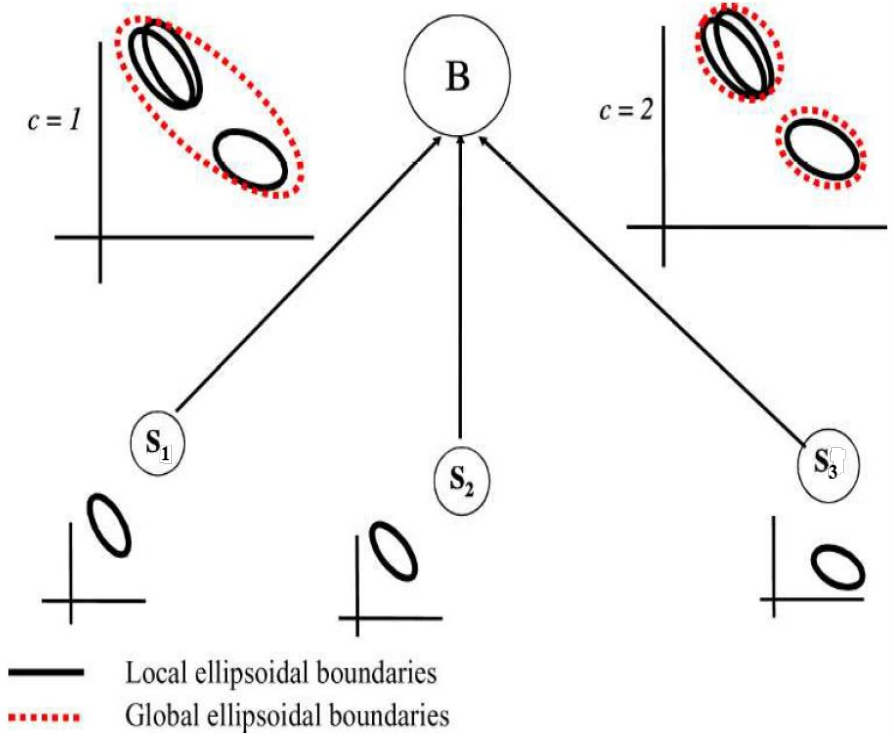
node i (where $i = 1, 2, \ldots, N$)

$$\mu_i = \frac{1}{M_i} \sum_{j=1}^{M_i} x_{i,j} \quad \textbf{(1)}$$

$$\Sigma_i = \frac{1}{M_i - 1} \sum_{j=1}^{M_i} (x_{i,j} - \mu_i)(x_{i,j} - \mu_i)^T \quad \textbf{(2)}$$

Distributed Anomaly Detection

Diagram Reference: From the Textbook "Internet of Things: Principles and Paradigms" By Rajkumar Buyya, Amir Vahid Dastjerdi, Elsevier, 2016.



$$\mu_{\text{combined}} = \frac{M_i\mu_i + M_k\mu_k}{M_i + M_k} \quad (4)$$

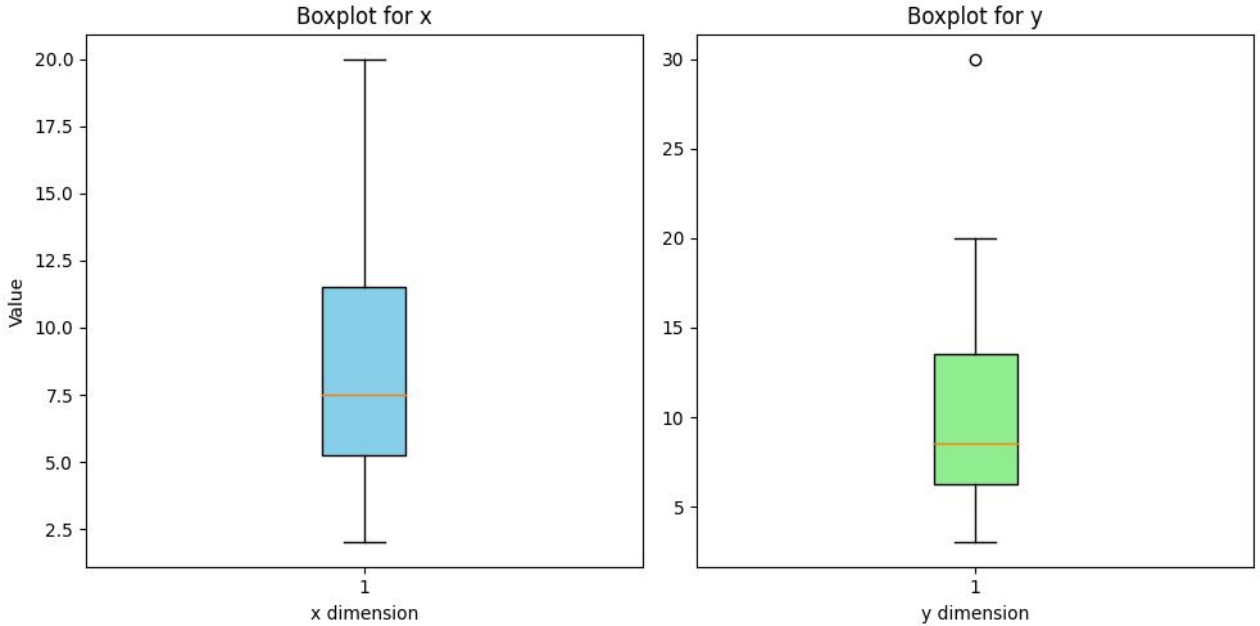
$$\Sigma_{\text{combined}} = \frac{M_i\Sigma_i + M_k\Sigma_k}{M_i + M_k} + \frac{M_iM_k}{(M_i + M_k)^2}(\mu_i - \mu_k)(\mu_i - \mu_k)^T \quad (5)$$

$$(x - \mu_{\text{combined}})^T\Sigma_{\text{combined}}^{-1}(x - \mu_{\text{combined}}) \leq 1 \quad (6)$$

$$D_M(i,k) = \sqrt{(\mu_i - \mu_k)^T\left(\frac{\Sigma_i + \Sigma_k}{2}\right)^{-1}(\mu_i - \mu_k)} \quad (7)$$

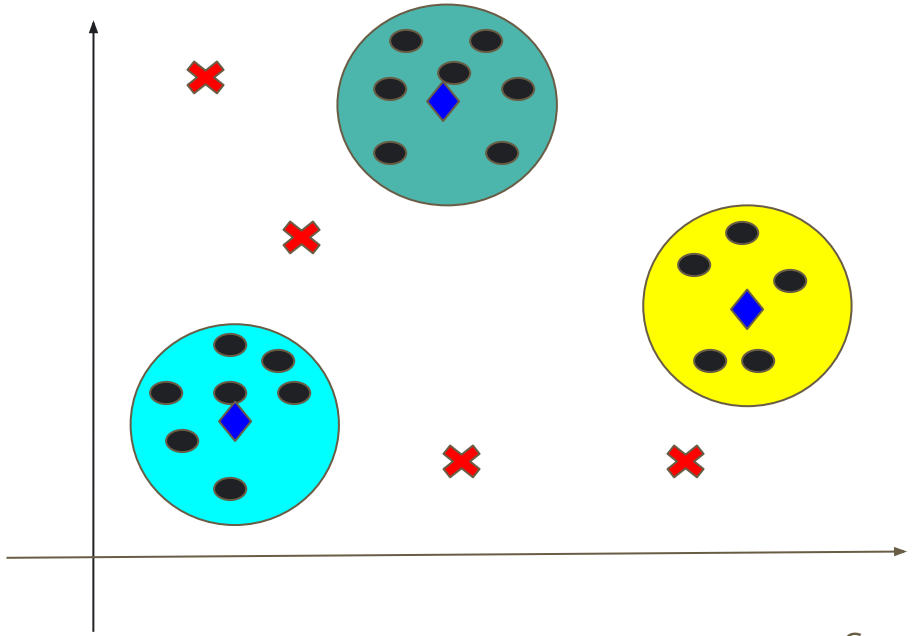
Distributed Anomaly Detection

- Other Methods
  - IQR



Distributed Anomaly Detection

- Other Methods
  - Distance Based



Distributed Anomaly Detection

Problem 1 :

Data = {(2,3), (4,5), (5,8), (6,6), (7,7), (8,9), (10,12), (12,14), (13,20), (20,30)}

Problem 2 :

Node 1 Samples: {(1,2),(2,3),(3,4)}

Node 2 Samples: {(5,5),(6,6),(7,7)}

Problem 3 :

Node 1 Samples: {(1,2),(2,1),(1,1)}

Node 2 Samples: {(4,5),(5,4),(4,4)}

Node 3 Samples: {(7,8),(8,7),(7,7)}

Node 4 Samples: {(10,10),(10,9),(9,10)}

Node 5 Samples: {(13,14),(14,13),(13,13)}

Test the Point : (3,3)

THANK YOU