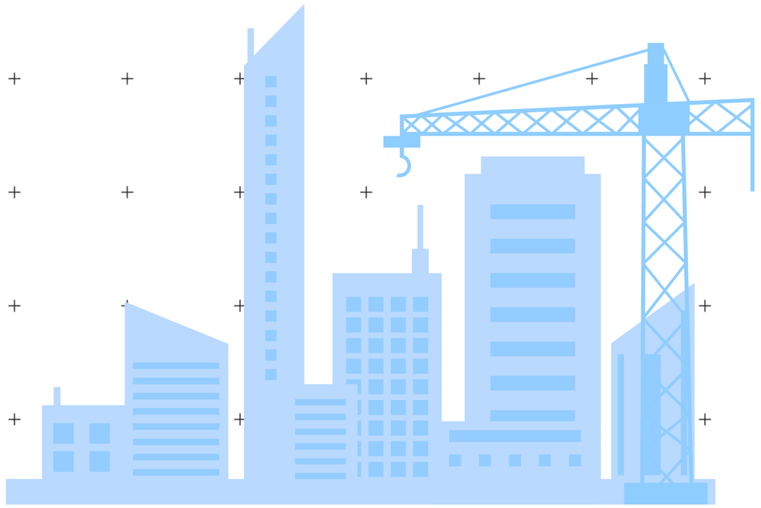
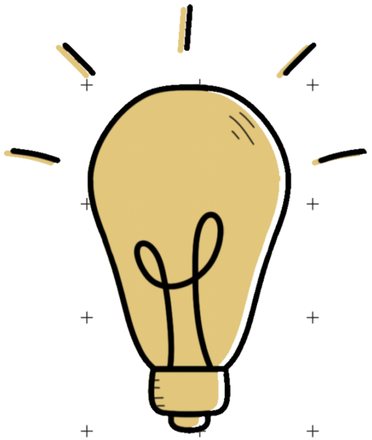
DETECTING ANOMALIES IN INDUSTRIAL CONTROL SYSTEMS





INTRODUCTION

The increasing adoption of the Industrial Internet of Things and integration of operational technology with information technology networks have made industrial control systems (ICS) more vulnerable to cyber-attacks, which can cause severe consequences such as disruption of critical infrastructure, loss of data, and significant financial losses.

To enhance the security and resilience of these systems, anomaly detection in ICS has gained significant attention in recent years.

The generated massive amounts of data require processing to extract valuable insights. A considerable fraction of this data comes from measurement sensor logs distributed throughout the production chain in the form of multivariate time series.

To overcome the limitations of traditional methods, like Statistical Process Control techniques such as CUSUM or EWMA, researchers have increasingly turned to machine learning (ML) based anomaly detection and UEBA for system monitoring and anomaly detection.

RELATED WORK

Pervious works can be typically grouped into

- **Signature-based detection** which is based on a knowledge base of known threats to compare signatures with the current state of the network and its devices.
- **Behavior analytics** which focuses on comparing user and/or entity behavior historically to determine a baseline and detect anomalies against it.

1. Network intrusion detection system for ddos attacks in ICS using deep autoencoders

The use of flow (NetFlow) features to build a network (agnostic) intrusion detection system based on deep autoencoders

2. Deep anomaly detection in packet payload

Introduce a deep learning framework that uses LSTM, Convolutional Neural Networks (CNN), and Multi-head Self Attention Mechanism to detect anomalies in packet payloads.

3. Anomaly detection for industrial control systems using process mining

introduce conformance checking over ICS data logs to detect unusual behaviour and cyberattacks.

4. A Dual-Isolation-Forests Based Attack Detection Framework for ICS

Dual-Isolation-Forests-Based framework is presented, modelling the device data as a tabular input and obtaining state-of-the-art detection performance.

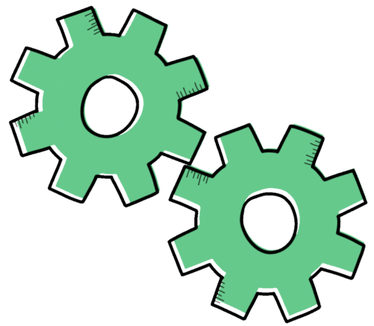
5. Multivariate anomaly detection for time series data with generative adversarial networks

model the sensor measurements as a multivariate time series on which a Generative Adversarial Network (GAN) is trained to identify deviations from the normal behaviour.

6. Combining user behavioural information at the feature level to enhance continuous authentication systems

present the combination of user behavioural information at the feature level to enhance the performance of continuous authentication systems

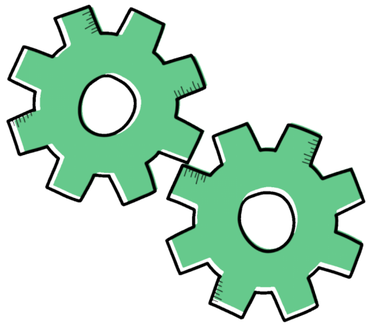
METHODOLOGY



1. **User and Entity Behavior Analytics**

UEBA works by collecting data from various sources, establishing a baseline of normal behavior, and then flagging deviations that could indicate security risks, such as insider threats, compromised credentials, or cyberattack.

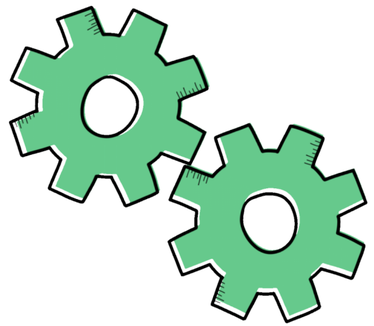
METHODOLOGY



2. **Long Short-Term Memory**

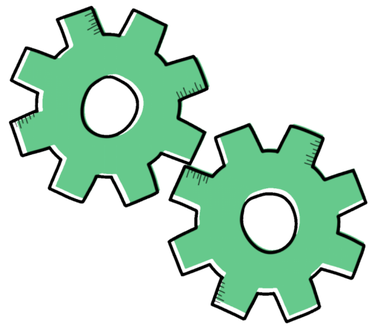
LSTM networks, a type of deep learning method based on Recurrent Neural Networks (RNN), to forecast future sensor measurements for each entity in an industrial facility. The model is trained on historical multivariate data, and predicted values are compared to actual measurements.

METHODOLOGY



A decision threshold, automatically computed over residual error, is used to identify anomalies, providing a reliable method for predicting sensor values and identifying potential anomalies in real-time.

METHODOLOGY



3.System Architecture

The proposed architecture consists of three stages: data preprocessing, model training and validation for threshold computation, and anomaly detection.

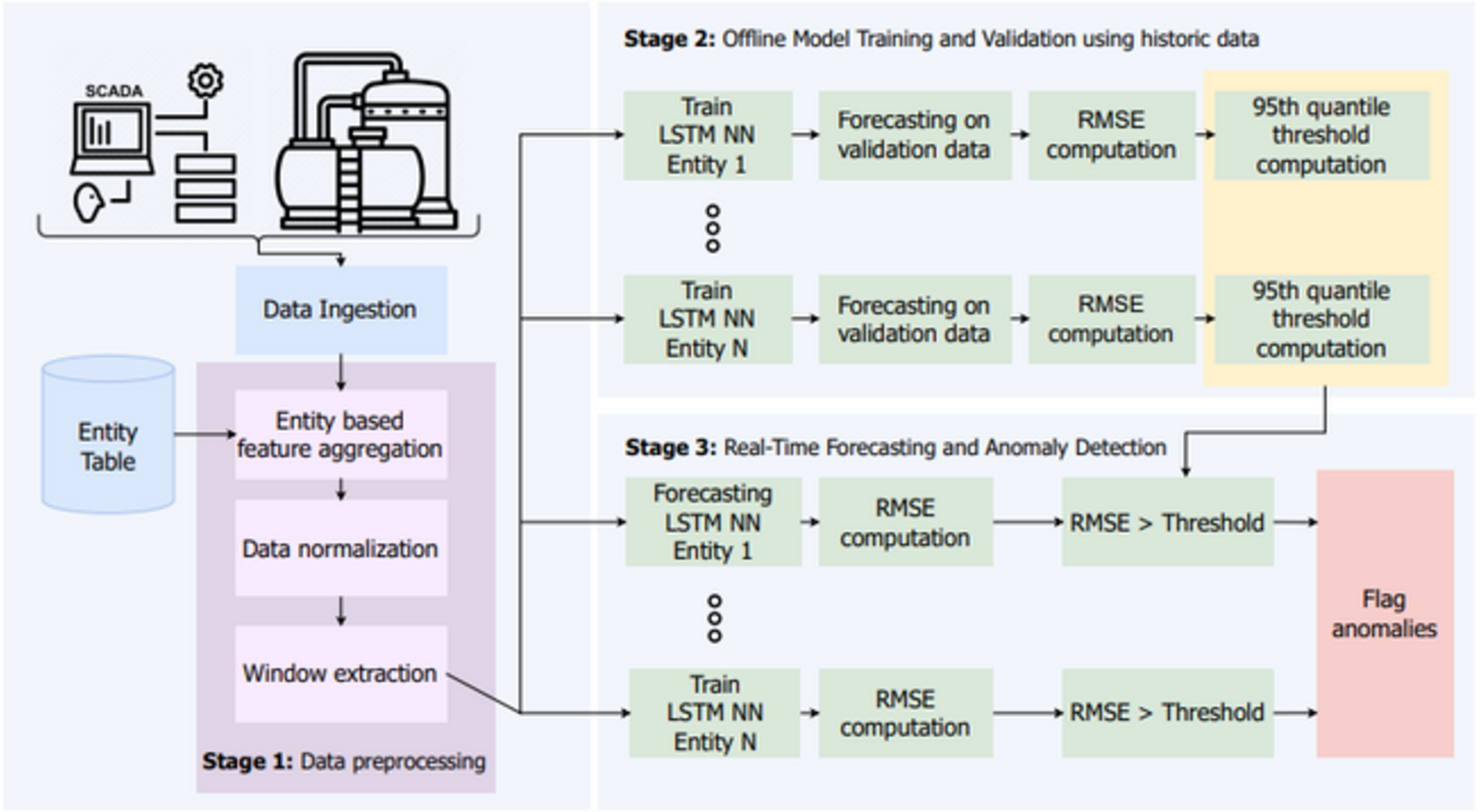
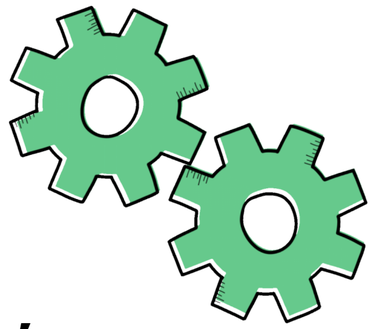


Fig. 3. System architecture

METHODOLOGY



- Data preprocessing

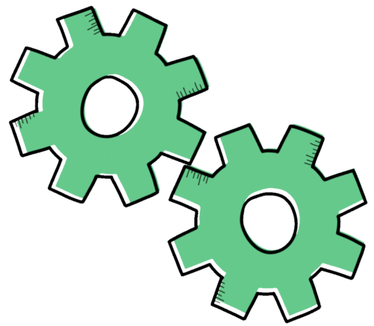
Involves grouping features by entities, normalizing data, and creating input-output pairs for training with fixed window of 60 time steps.
80% of the dataset is used for training.
10% is used for validation and threshold calculation.
10% is reserved for model evaluation (test set).

METHODOLOGY

- Model Training and Validation:

The LSTM model is trained on normal data, with a validation set used to compute a decision threshold for anomaly detection.
-Since the model is trained in normal data only, the model is expected to produce a higher error on anomalies, allowing us to detect them by establishing a decision threshold.

METHODOLOGY



- Real-Time Forecasting and Anomaly Detection:

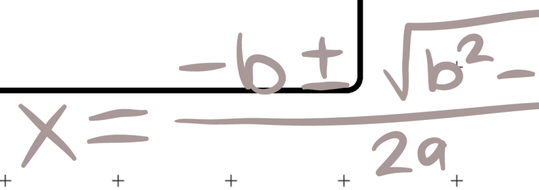
New observations are predicted, and deviations exceeding the threshold are flagged as anomalies.

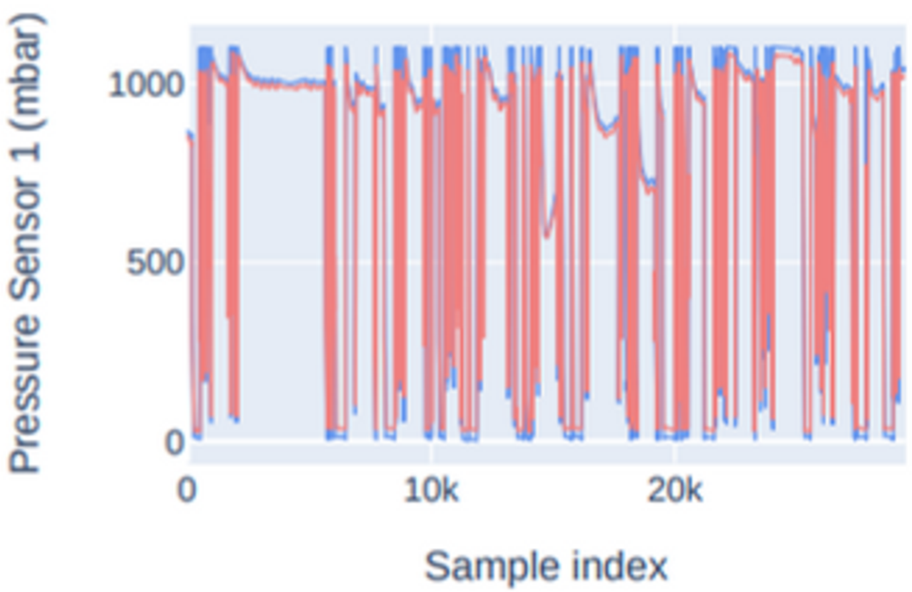
PRELIMINARY RESULTS

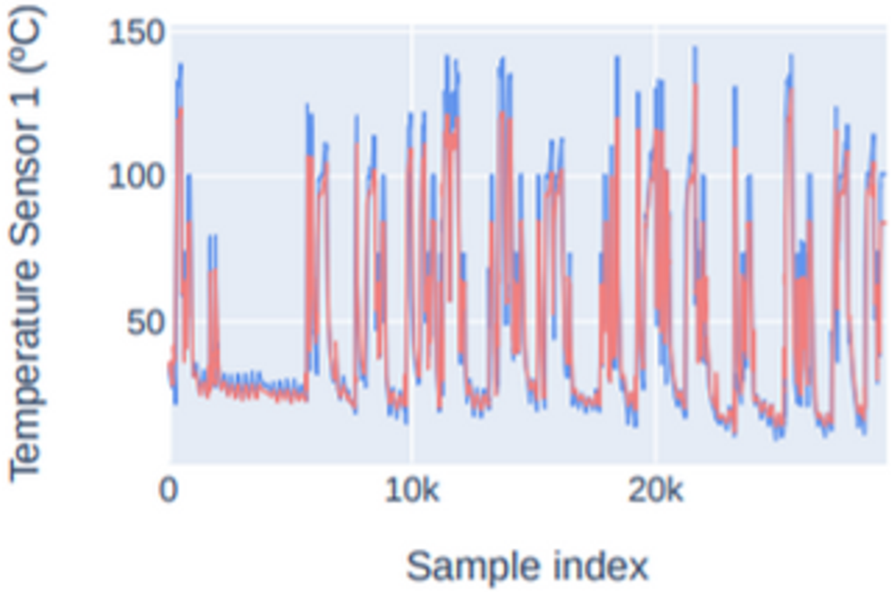
The methodology was evaluated against a dataset collected from a chemical plant, comprising 12 features over three years. The LSTM model was trained to predict sensor values, achieving Normalized Root Mean Squared Error (NRMSE) values between 4.32% and 8.14% for different sensors.

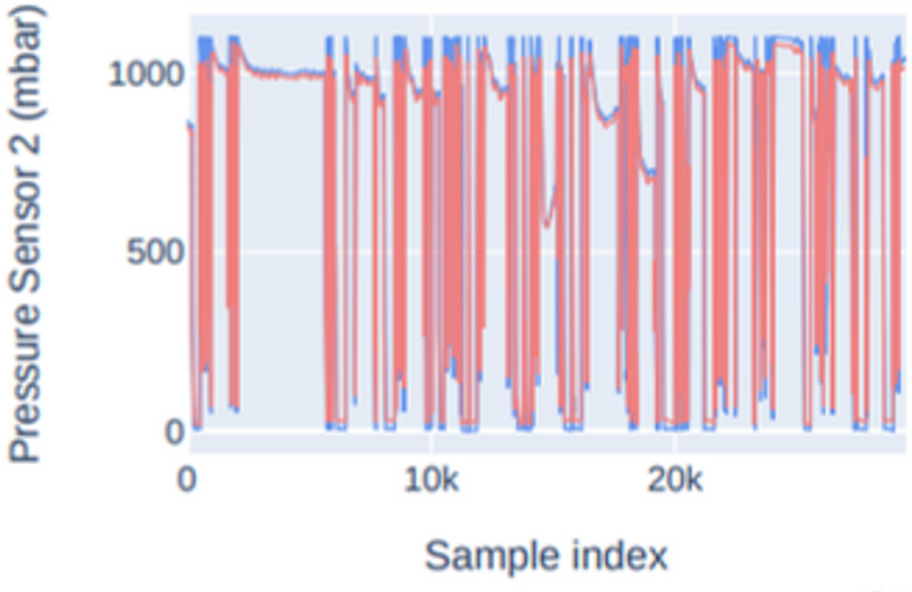
TABLE II
DETAILED EXPERIMENTAL RESULTS WITH THE PROPOSED LSTM MODEL

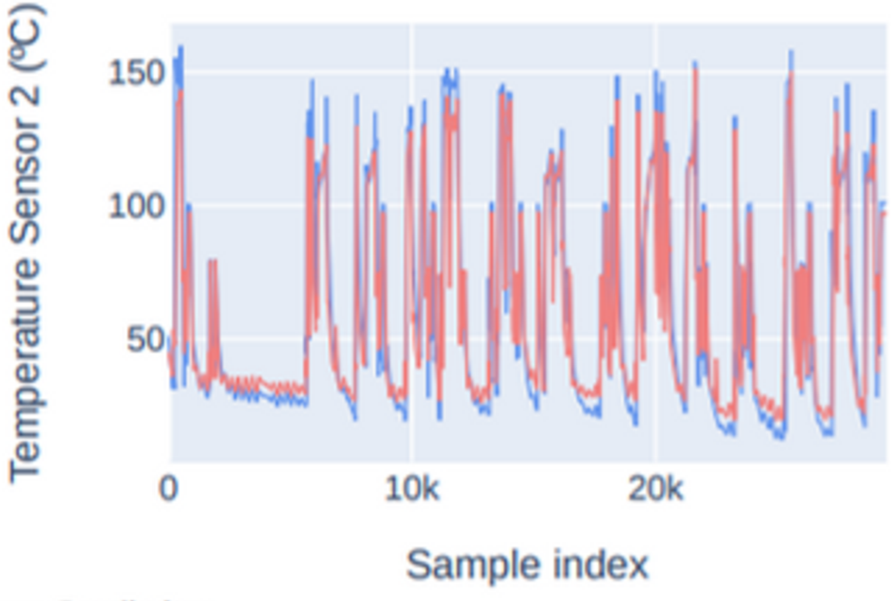
Metric	Result
TN	22997
FP	4983
TP	1419
FN	54
Precision	0.222
Recall	0.963
TPR	0.963
TNR	0.822
G-Mean	0.890
F1-Score	0.360
AUC-ROC	0.893
AUC-PR	0.593











Real Prediction

PRELIMINARY RESULTS

In order to validate the proposed anomaly detection framework, we generate synthetic anomalies in the data.

The main drawback of our current implementation is the high number of false positives, which implies a low precision and subsequent low F1-Score and AUC-PR results.

$$x = \frac{-b \pm \sqrt{b^2 -}}{2a}$$

CONCLUSIONS AND FUTURE WORK

Future work will focus on addressing the high false positive rate, validating the methodology with established datasets, and exploring more robust LSTM architectures, such as Bidirectional LSTM (Bi-LSTM) networks and attention mechanisms, to improve the accuracy and efficiency of anomaly detection.