Attack detection in

Water Distribution System

Part of

Safeguarding Supervisory Control and Data Acquisition(SCADA)

By

Mr.Sukkarin Ruensukont

G6538138

**Introduction**

SCADA, which stands for Supervisory Control and Data Acquisition, is a system used in various industries to monitor and control processes. It typically involves a combination of hardware and software components that collect and analyze real-time data. SCADA systems are crucial in managing and controlling complex industrial processes such as manufacturing, energy distribution, and water treatment.

In the context of a water distribution system, SCADA plays a pivotal role in ensuring the efficient and reliable operation of the system. It allows operators to remotely monitor and control various components such as pumps, valves, tanks, and sensors. By providing real-time insights and control capabilities, SCADA enables water utilities to optimize their operations, respond to emergencies, and ensure the delivery of safe and reliable water to consumers.

The war between Ukraine and Israel that occurred in 2023 witnessed SCADA attacks with military objectives. Therefore, knowledge and understanding of the system, attack methods, and defense mechanisms are crucial. The Singaporean government, in collaboration with iTrust - the Center for Research in Cyber Security at Singapore University, has been organizing the Continuous Learning Program on Critical Information Infrastructure Security (CISS) since 2016. The program aims to study, comprehend attacks, and devise protection measures. The systems under consideration include water systems, electrical systems, and gas systems. More information on CISS at <https://itrust.sutd.edu.sg/ciss-2023/#ed>

Awareness of the importance of understanding SCADA attacks and defenses has continuously increased. In 2024, the first International Conference on the Design of Cyber-Secure Water Plants, DCS-Water'24, will be held on April 23-24, 2024, at The Water Tower, Buford, Georgia, USA. For more details, more information at <https://itrust.sutd.edu.sg/first-international-conference-on-the-design-of-cyber-secure-water-plants-dcs-water24/programme-dcs-water24/>.



Fig1. First International Conference on the Design of Cyber-Secure Water Plants

“Water is life, and clean water means health.”

– Audrey Hepburn

**Problem and Objective**

**Objective:**

Detect 2 classes, attack and no attack in Water distribution system

**Dataset:**

Individual need to request for dataset. iTRUST will provide the link to shared google drive, include labeled dataset. iTRUST hold Central Infrastructure Security Showdown (CISS) which is sponsored by the Cyber Security Agency of Singapore and co-organised with the Ministry of Defence, Singapore. CISS competition began in 2016. They cover Secure Water Distribution, Electric power, gas distribution. We focus on Secure water distribution.

Main Dataset:

Water Distribution 2019(WADI2019)

Use for machine learning and attack detection purpose.

<https://drive.google.com/drive/folders/12mqpuejSSjq2Wa_0muVjcoQuLN0H6vZt>

Additional Dataset:

Battle of the Attack Detection Algorithms(BATADAL2017)

Use to add more understanding of important between features

https://drive.google.com/drive/folders/12-nEv4WaPlgj6SYb-vc7tBFrwxNSWjaV

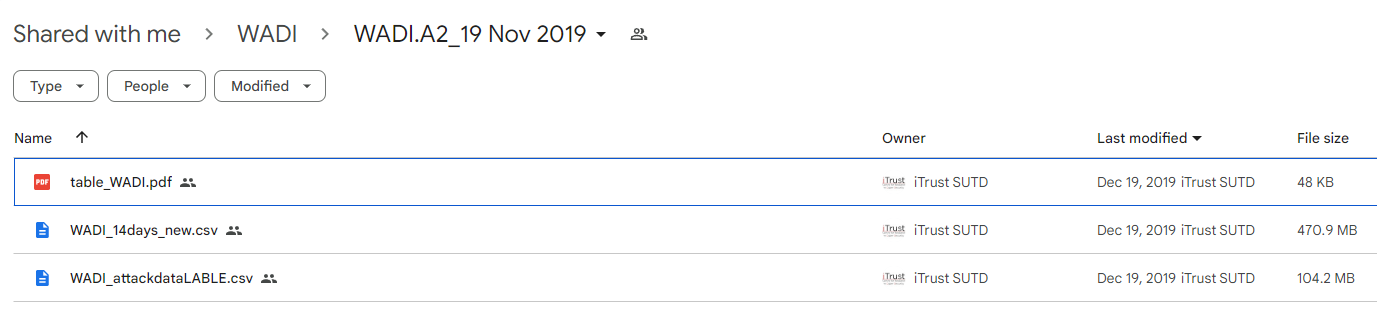


Fig2. WADI2019

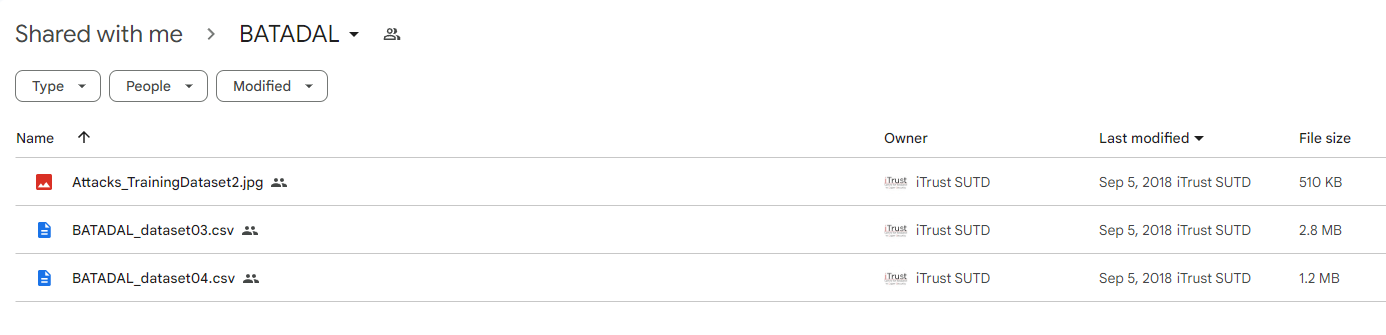


Fig3. BATADAL2017

**Dataset details**

1. BATtle of Attack Detection Algorithms (BATADAL2016)

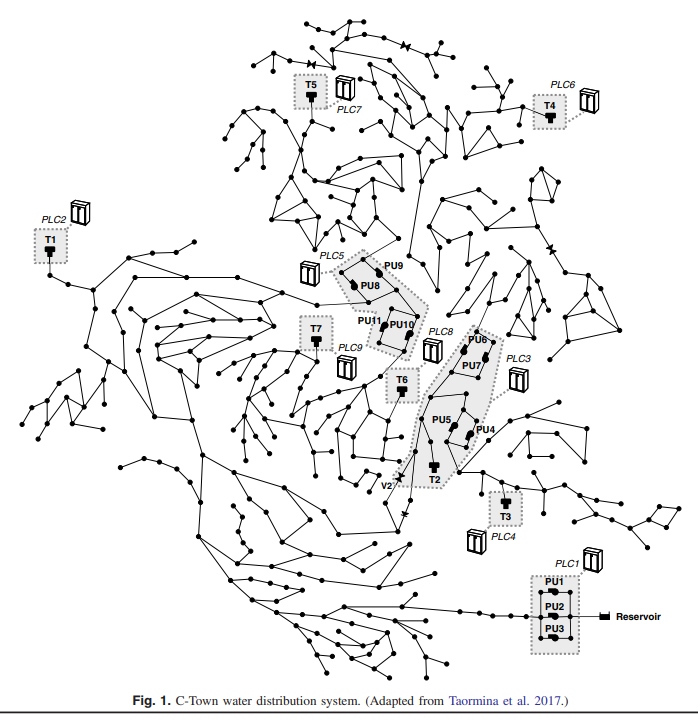


Fig4. Image of water distribution system

Water distribution system consists of

* Pipes to deliver water from pump to destinations
* Pumps to pump water
* Tank to store water, working with PLC in order to know when to turn on the pump
* PLC to control pump, to measure water level in the tank.

Value of components can be transformed to features. There’re 2 files, BATADAL\_dataset03.csv all benign, BATADAL\_dataset04.csv mix benign and attacks. We will use BATADAL\_dataset04.csv in this paper because it contains both benign and malicious.

Features of BATADAL

* 7 Tank water levels, denoted L\_<tank\_id>
* 12 Pressure for actuated valve, denoted P\_<junction id>
* 12 flows for actuated valve, denoted F\_<actuator id>
* 12 statuses for actuated valve, denoted S\_<actuator id>
* Total 43 features

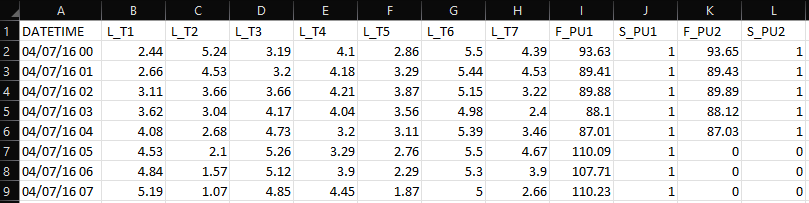
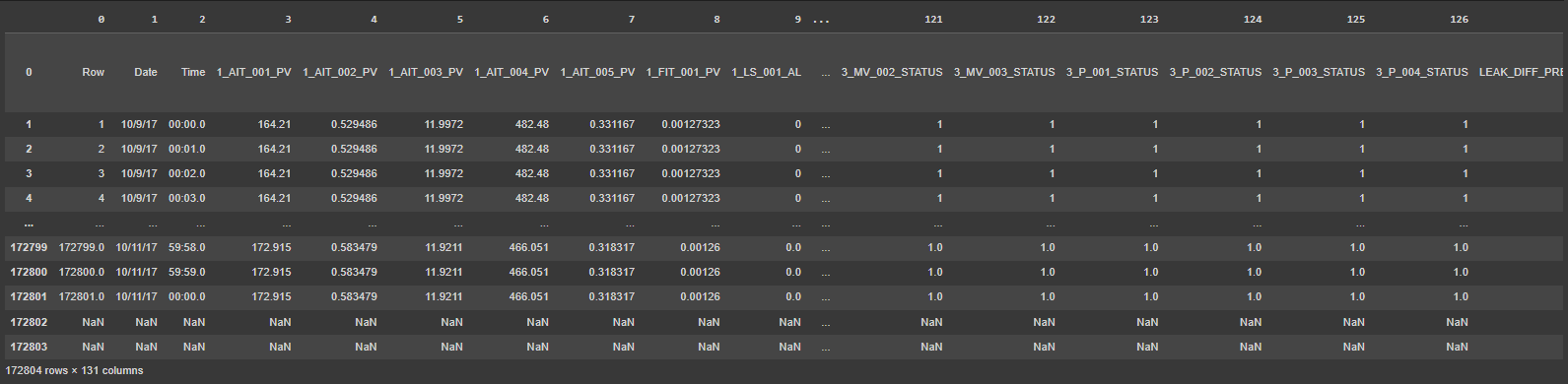


Fig5. Head of dataset BATADAL03.csv



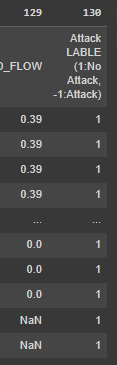


Fig6 WADI2019

1. Water Distribution (WADI2019)

In CISS 2020, dataset get more complex to make it closer to real Water Distribution system.

Dataset contain 130 features and 172,801 row.

Dataset contain 2 classes. Attack = 162824, No Attack =9977

All features are collected from the system that was built within iTrust lab.

The data has no details of each feature. The data has already labeled which are ready to use in Machine learning to find relation between features and classes.

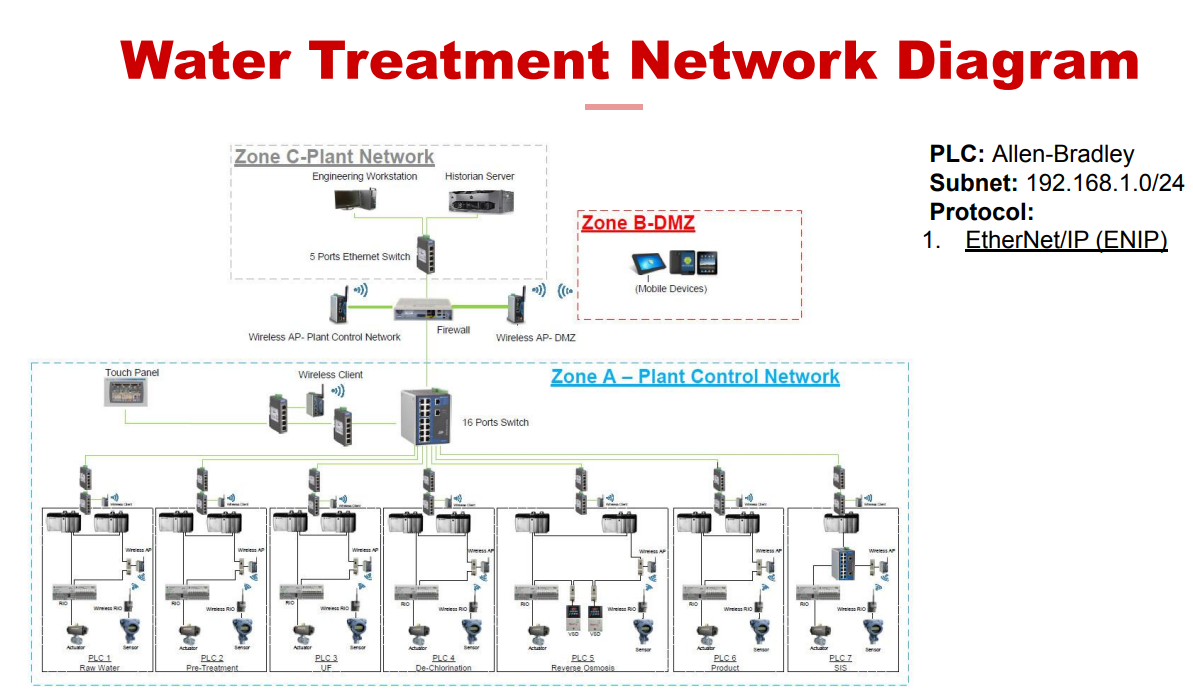


Fig7. WaDi2020 Network Diagram

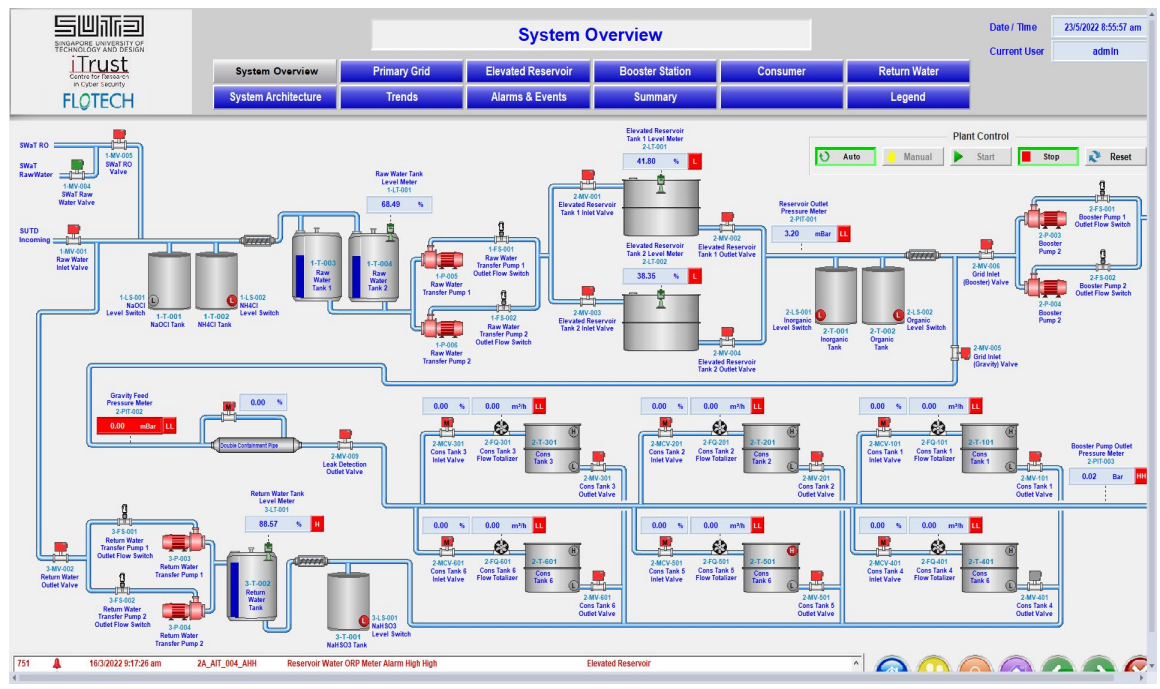


Fig8. WaDi2020 Water distribution diagram

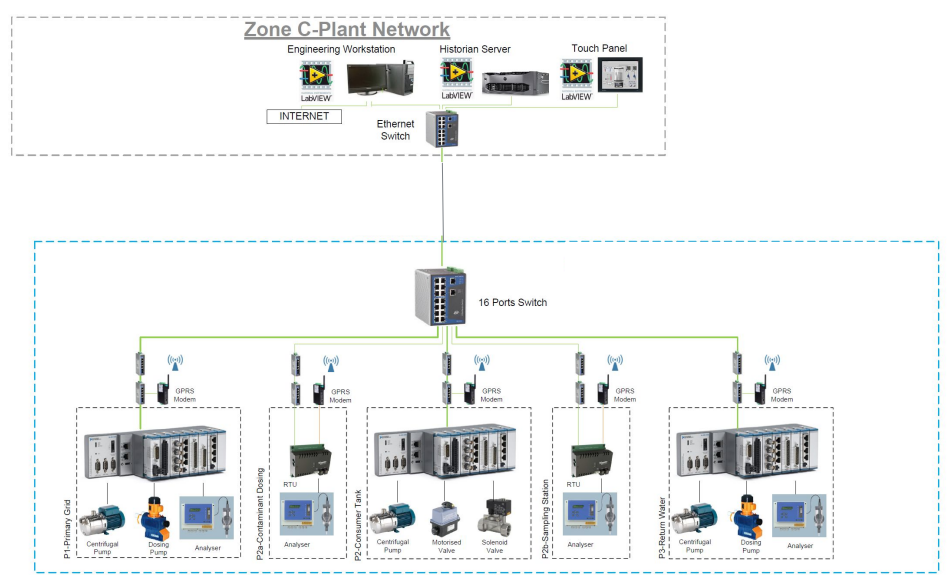


Fig9. Wadi2020 Control diagram

Example of Attack on WADI2019

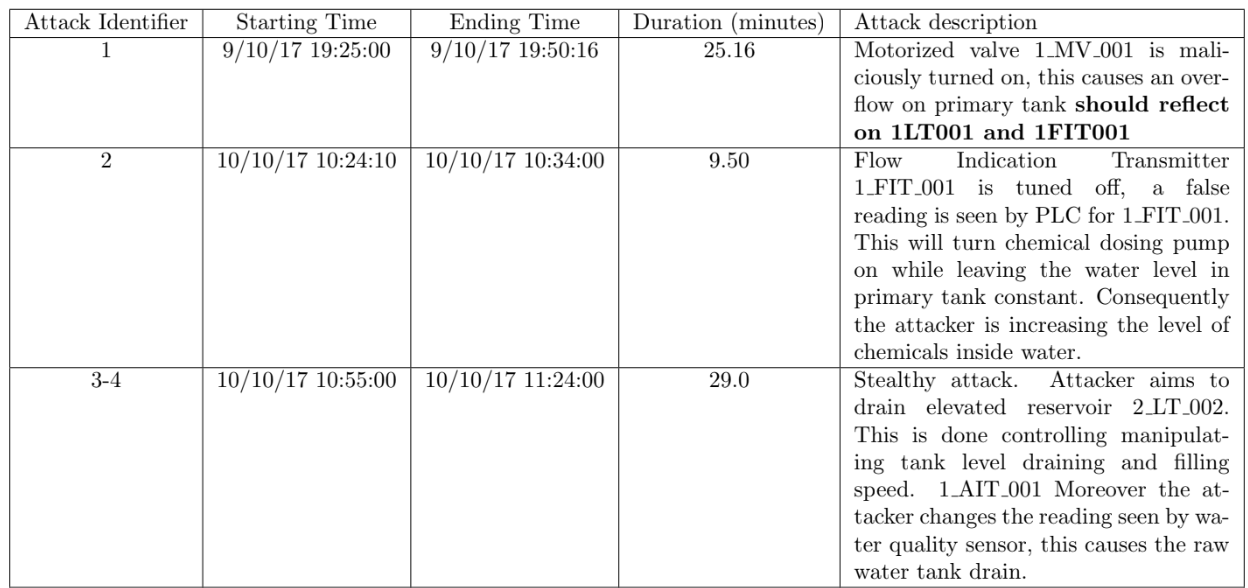


Fig10. Example attack on WADI2019

This project mainly focused on WADI2019. Most methods will be done with WADI2019

BATADAL2017 will be use only to give more understanding on feature, e.g., what kind of feature has high correlation to classes.

**Method**

**Data Preparation:**

Visualize data, contains 172084 rows and 131 columns

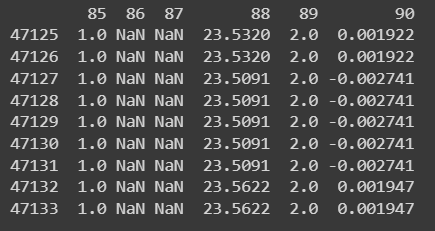
****

Inspect first 3 columns is Row, Date, Time. These’re not correlated to classes, remove them.

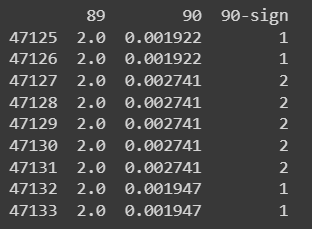
Check negative value and create list, check if value in this list columns contain positive value. We will get list of columns contain both positive and negative values, omit column ‘130’ as class



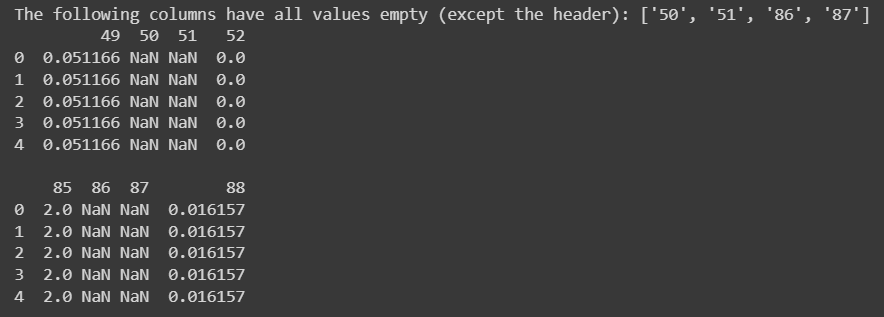
Inspect columns contain both positive and negative values.



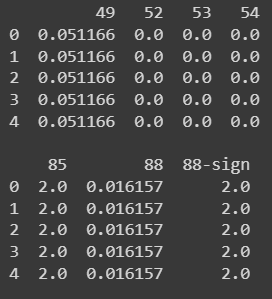
Create new column based on value on columns which contains both positive and negative, if value is positive, assign 1 to new column, unless assign 2 to new column. Make the value on column ‘88’, ‘90’, ‘115’ to all positive by multiply all negative with (-1). Inspect results at column ‘90’ and ’90-sign’



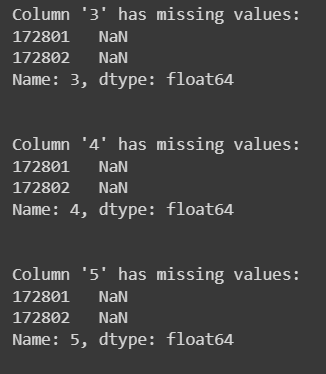
Find empty columns. Inspect them.

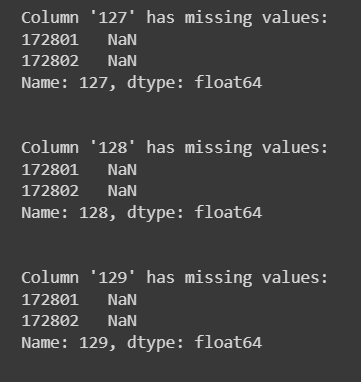


Drop empty columns. Inspect the result.



Find single empty value. Inspect row 172801 and 172802 are empty in many columns but not all columns.

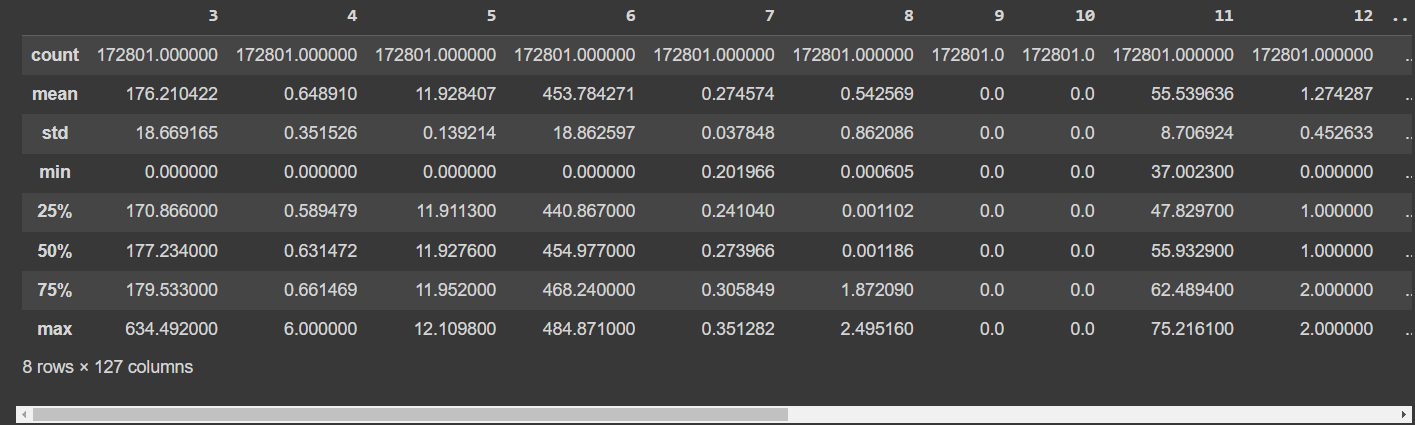




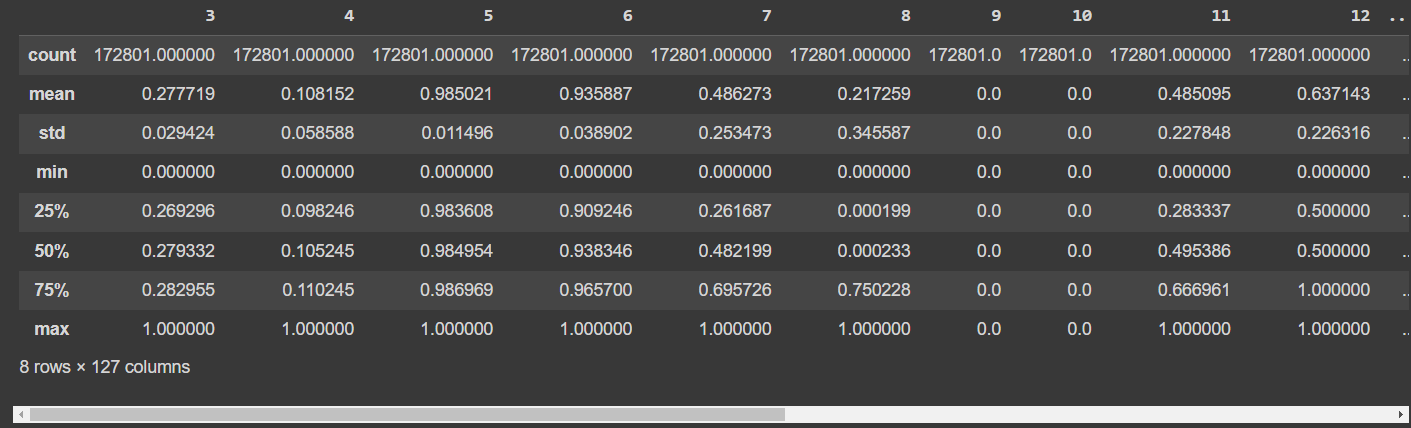
Remove row 172801 and 172802. Check and found no missing value left.



Inspect Data description before normalize.



Normalize data using MinMaxScaler, except last column for class. Inspect data after normalized. Data range inclusive between [0, 1]



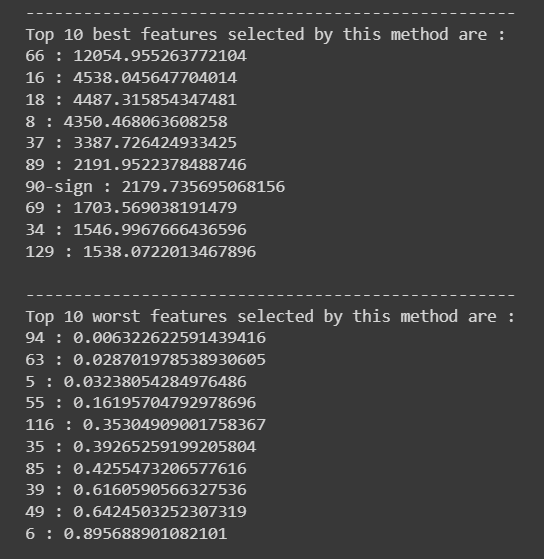
**Preprocess:**

Train\_test\_split data, given test data = 30%. Specify stratify feature = y=[‘130’]

List all current features.



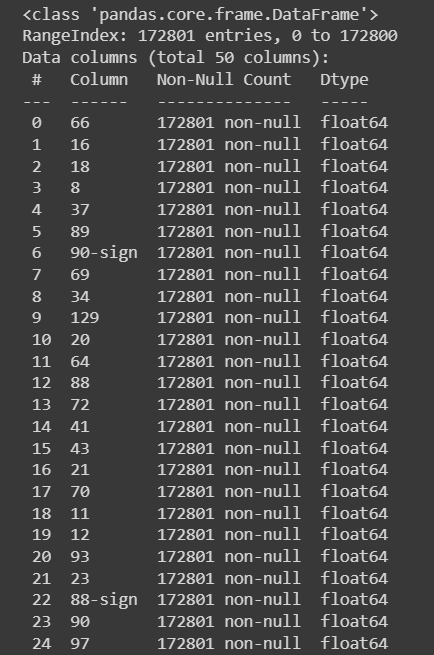
Rank each feature by scores. Inspect top 10 best and worst features.



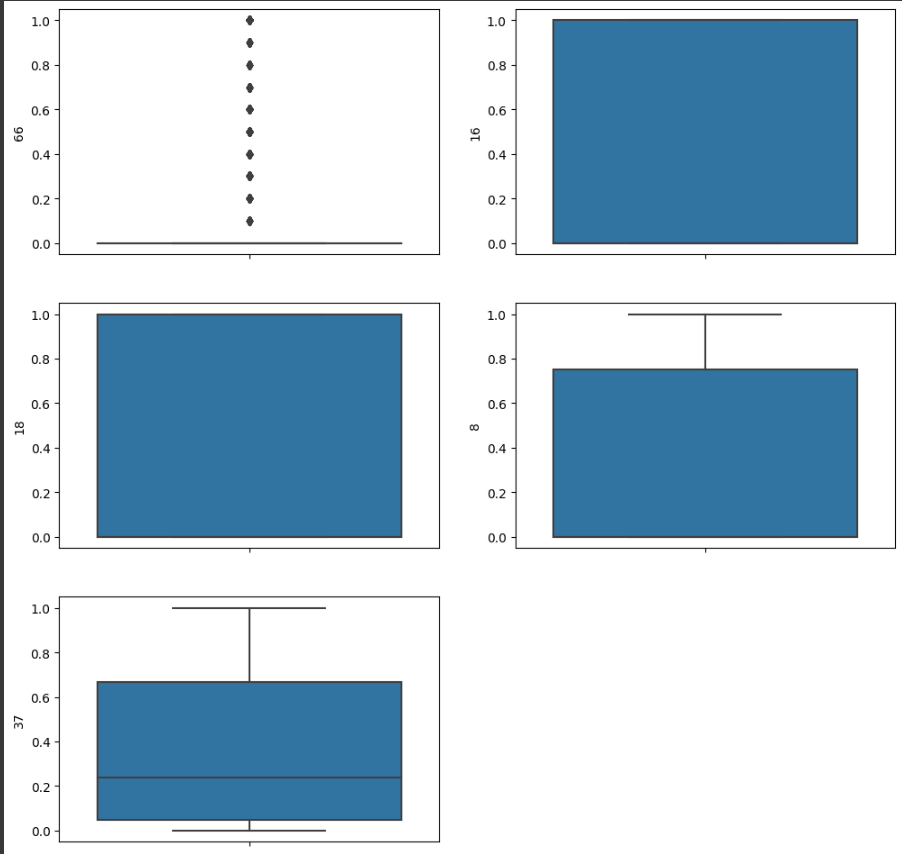
Select only features that score higher than 100. Inspect features count = 49



Inspect type of features, float64.

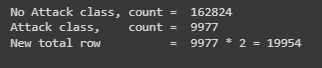


Boxplot on top 5 features, ‘66’, ‘16’, ‘18’, ‘8’, ‘37’. These features are highly correlated.



Inspect number of attack class = 9977, number of no attack class = 162824.

Downsampling number of No Attack class from 162824 to 9977.



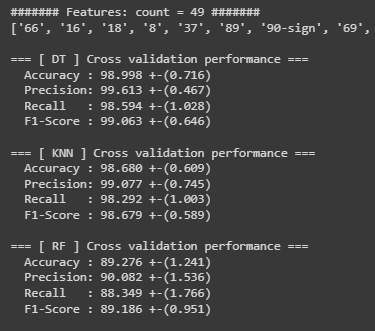
Inspect description after down sampling to make balance class.



**Learning Techniques:**

Train models with train dataset. Using 3 machine learning models, Decision tree, K-Nearest Neighbor, Random Forest Classifier. Save model to model\_<model name>.csv

Evaluate using test dataset. Using K-fold cross validation, K=10. Specify 4 criterias for each model to evaluates, Accuracy, Precision, Recall and F1-Score. Inspect result.



With full features selection(only score higher than 100). All 3 models yield very good result. DT yields highest Accuracy, Precision, Recall and F1-Score. DT F1-Score = 99.063 +-(0.646)

In this project, we need to detect attack class. We need to focus on recall which will be discussed later.

**Post-process:**

Try 5 Ensemble modes. Inspect results compare to single ML model.

Ensemble1: Majority Votes

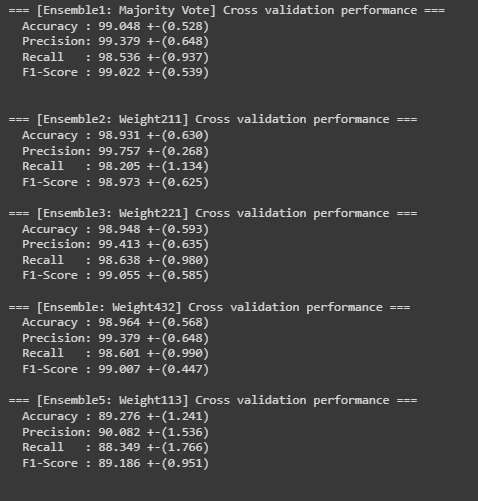
Ensemble2: Voting with adjusted weight, DT=2, KNN=1, RF=1

Ensemble3: Voting with adjusted weight, DT=2, KNN=2, RF=1

Ensemble4: Voting with adjusted weight, DT=4, KNN=3, RF=2

Ensemble5: Voting with adjusted weight, DT=2, KNN=1, RF=3

Inspect Accuracy, Precision, Recall and F1-Score



Single Decision Tree model get higher score in every criteria compare to 5 Ensemble models. Ensemble4 with given weight DT=4, KNN=3, RF=2 get highest score among 5 ensemble models and the score is very close to Decision Tree model.

**Experimental Results**

**Dataset size**

**Dataset contains 130 columns(features)**

**Dataset contains 172801 row**

**Attack = 162,802 rows, No Attack = 9977 rows**

**Data type is float64**

**Experiment detail(train\_test\_split, how to meature, measurement name selected)**

**Split train:test to 70:30.**

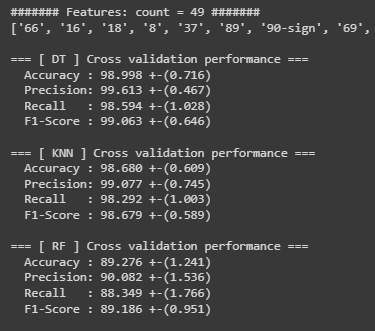
**Measure 3 models(DT, KNN, RF) using Accuracy. Precision, Recall.**

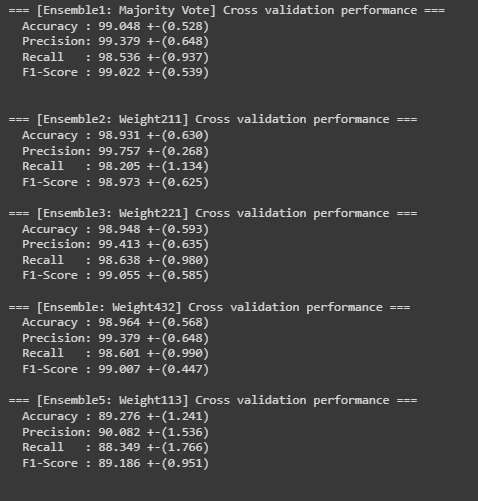
**We will focus on recall because this project aims to detect attack class.**

**Result**

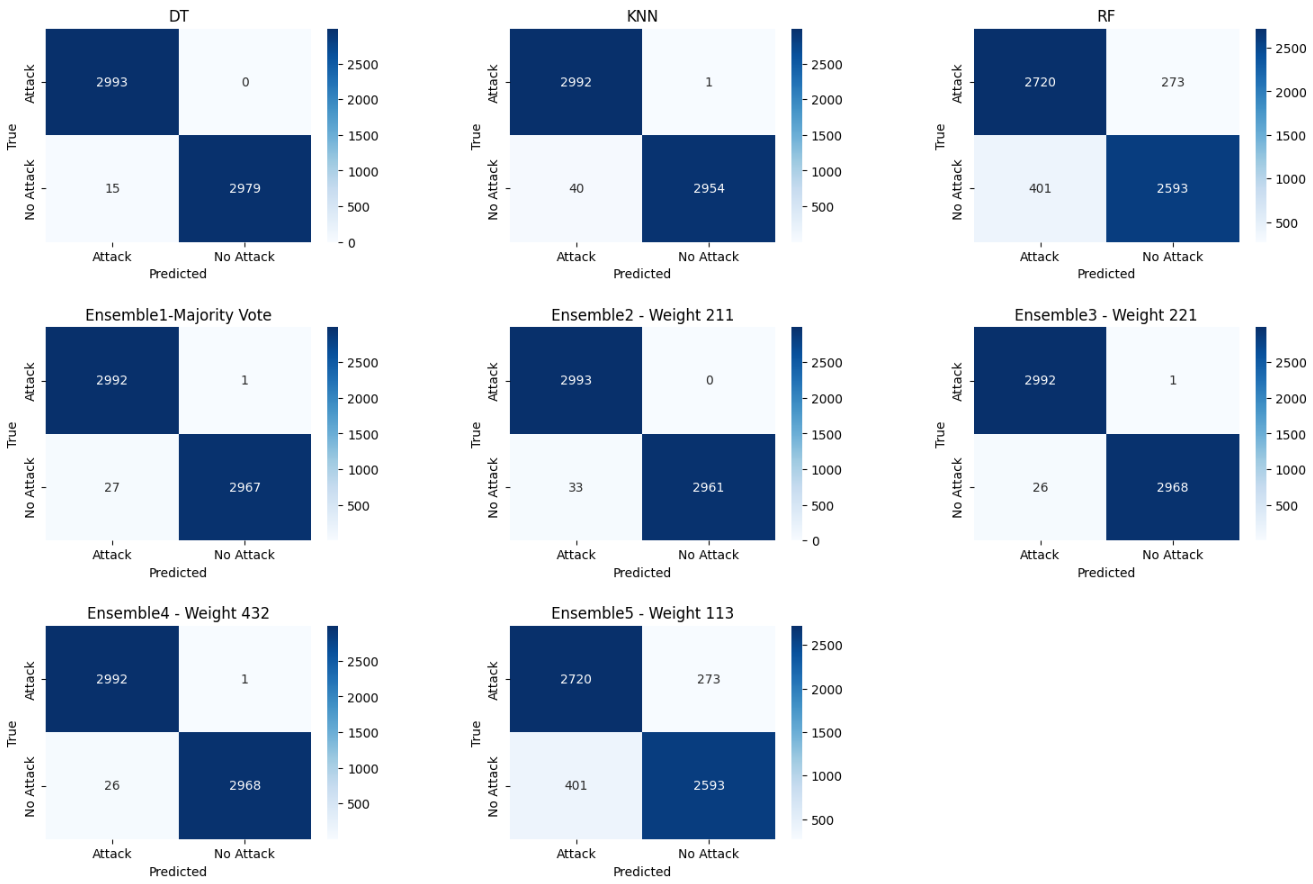
Decision tree yields highest on every categories(Accuracy, Precision, Recall, F1-score) over K-Nearest Neighbor and Random Forest

Decision tree also yields higher scores on every categories when compare to 5 ensemble modes with combination of DT, KNN and RF.



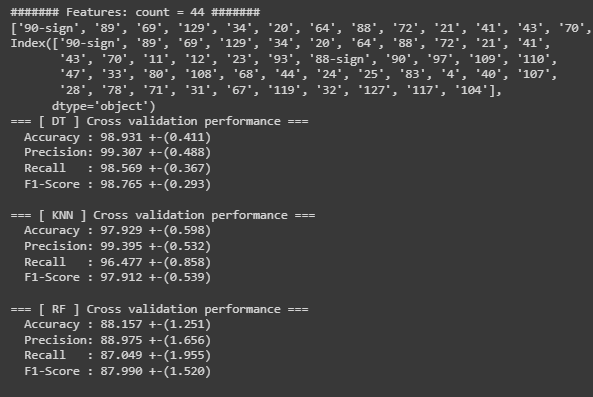


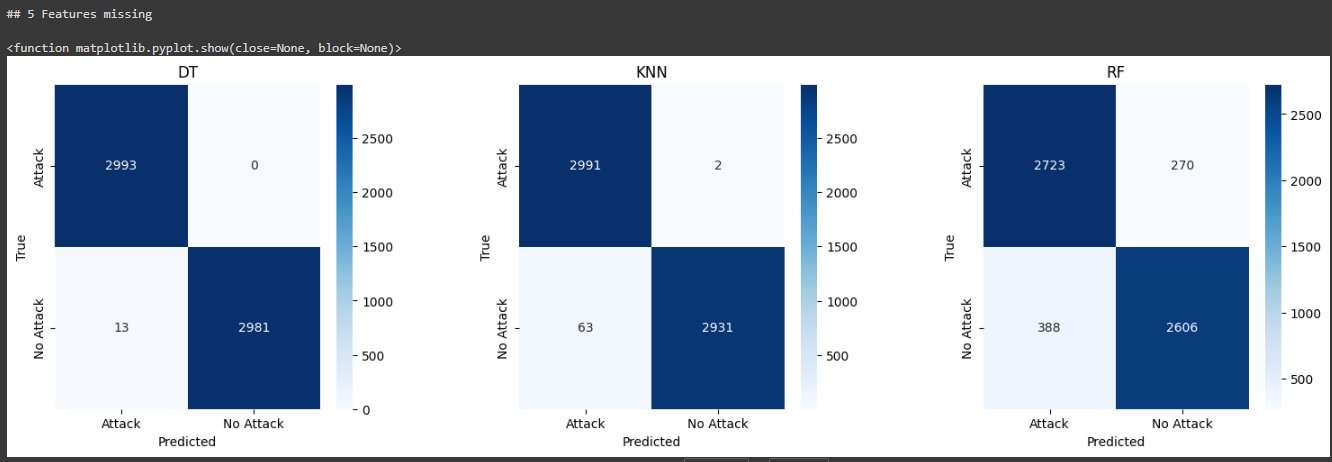
Inspect confusion matrix to compare DT, KNN, RF and 5 Ensemble models. With full features with feature score higher than 100. Random forest show higher false negative than DT and KNN.



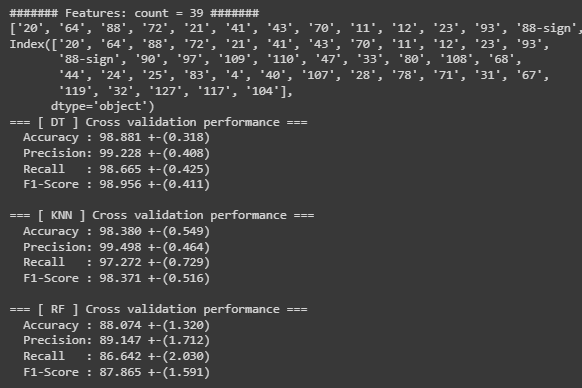
In war era, some features might not be available but an army need to know if there’s any attack happen within the Water Distribution System. We cut out some features and inspect results.

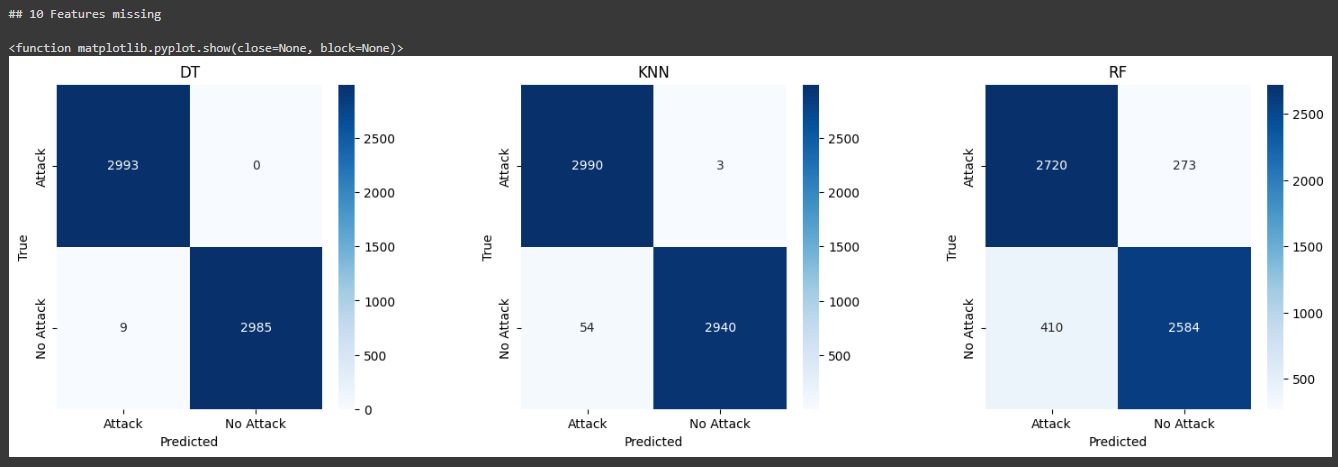
Take out top 5 features, 44 features left



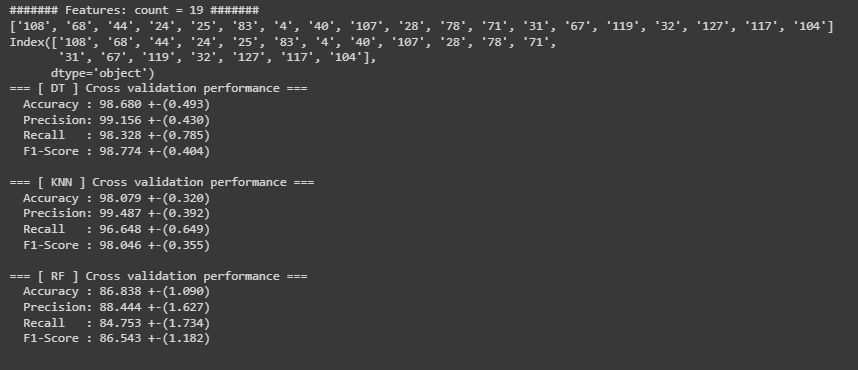


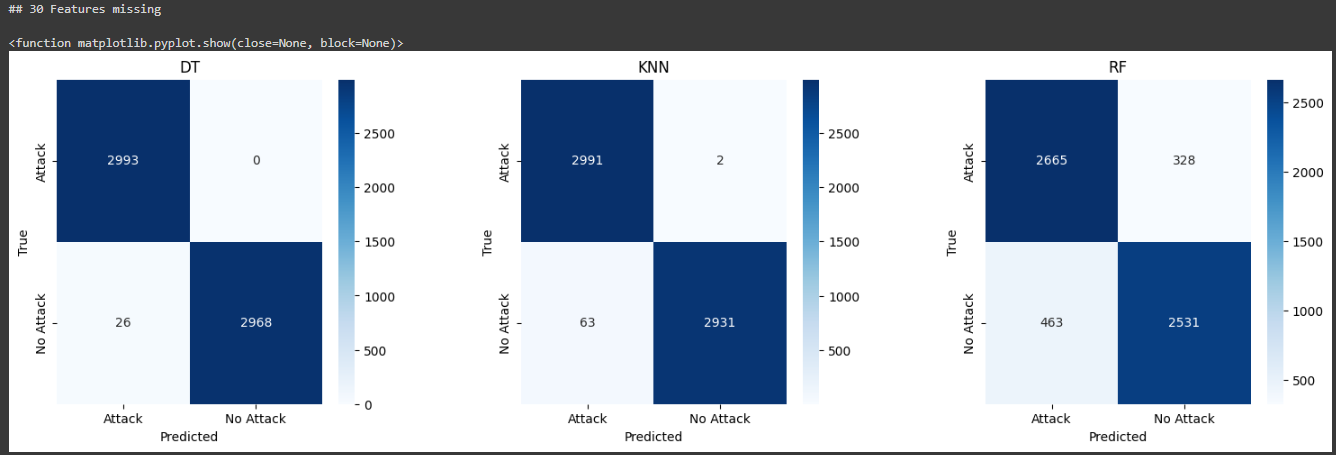
Take out top 10 features, 39 features left



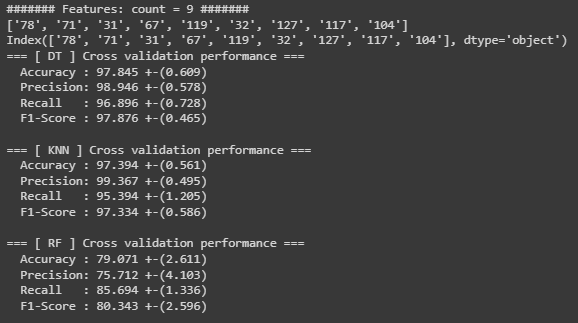


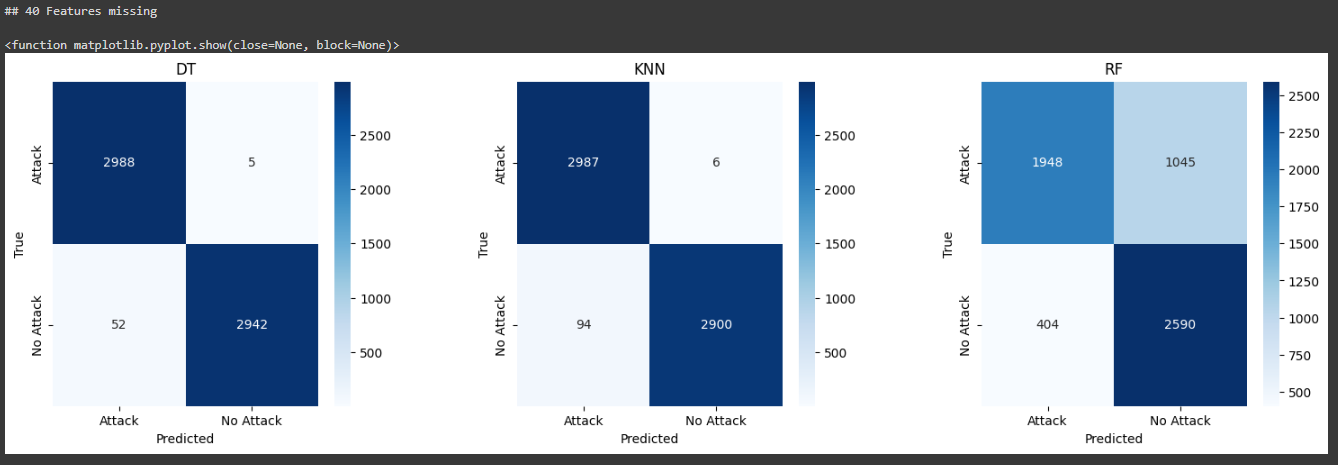
Take out top 30 features, 19 features left



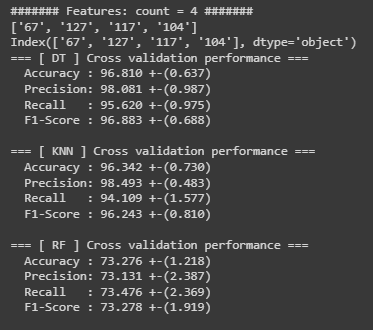


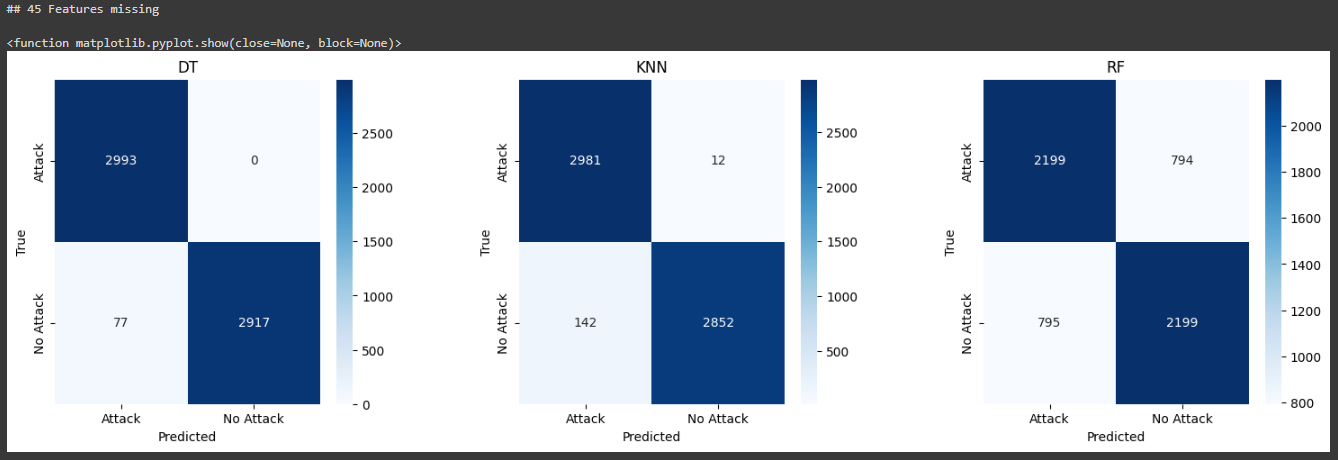
Take out top 40 features, 9 features left





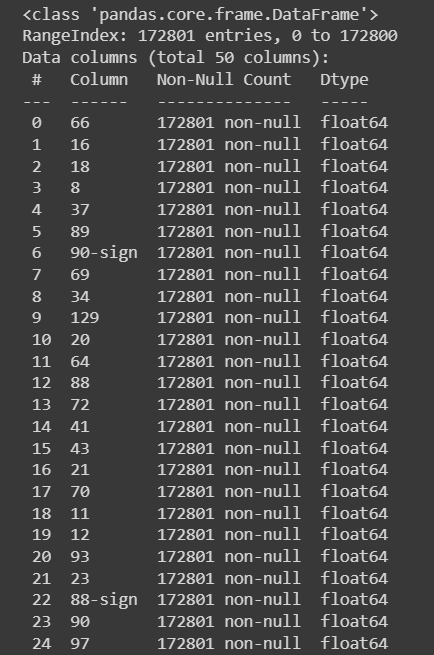
Take out top 45 features, 4 features left



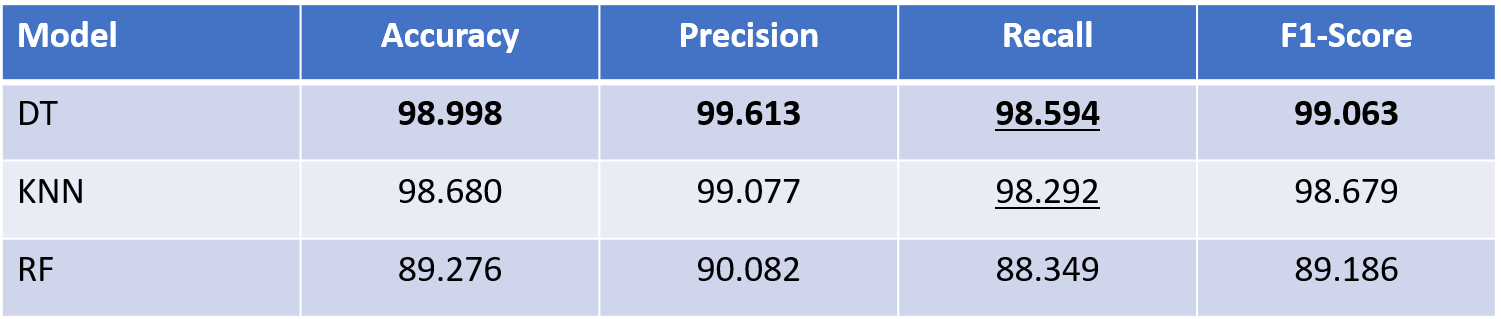


**Analyze and discuss results**

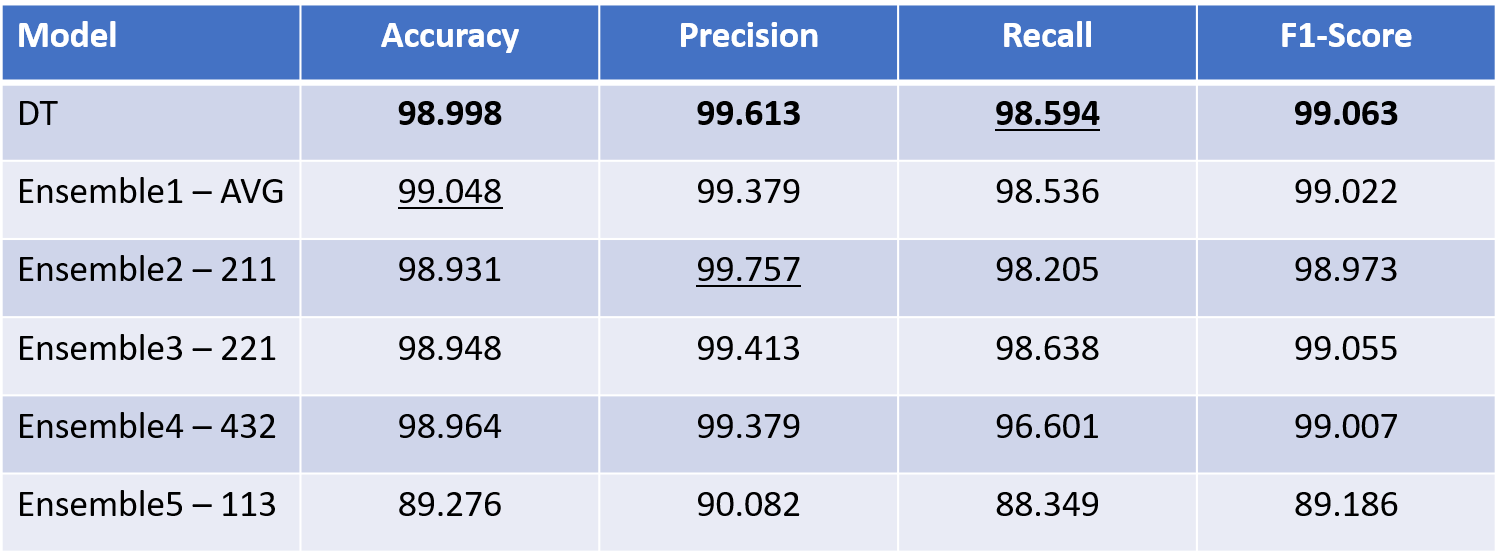
During features selection, when create another column beside column which contain both positive and negative value. We found that 90-sign(6th) get higher features score than 90(23rd). And 88(12th) get higher feature score than 88-sign(22nd). This mean for feature 90, sign(positive/negative) is more significant than it’s value. But for feature 88, sign(positive/negative) is less significant than it’s value.



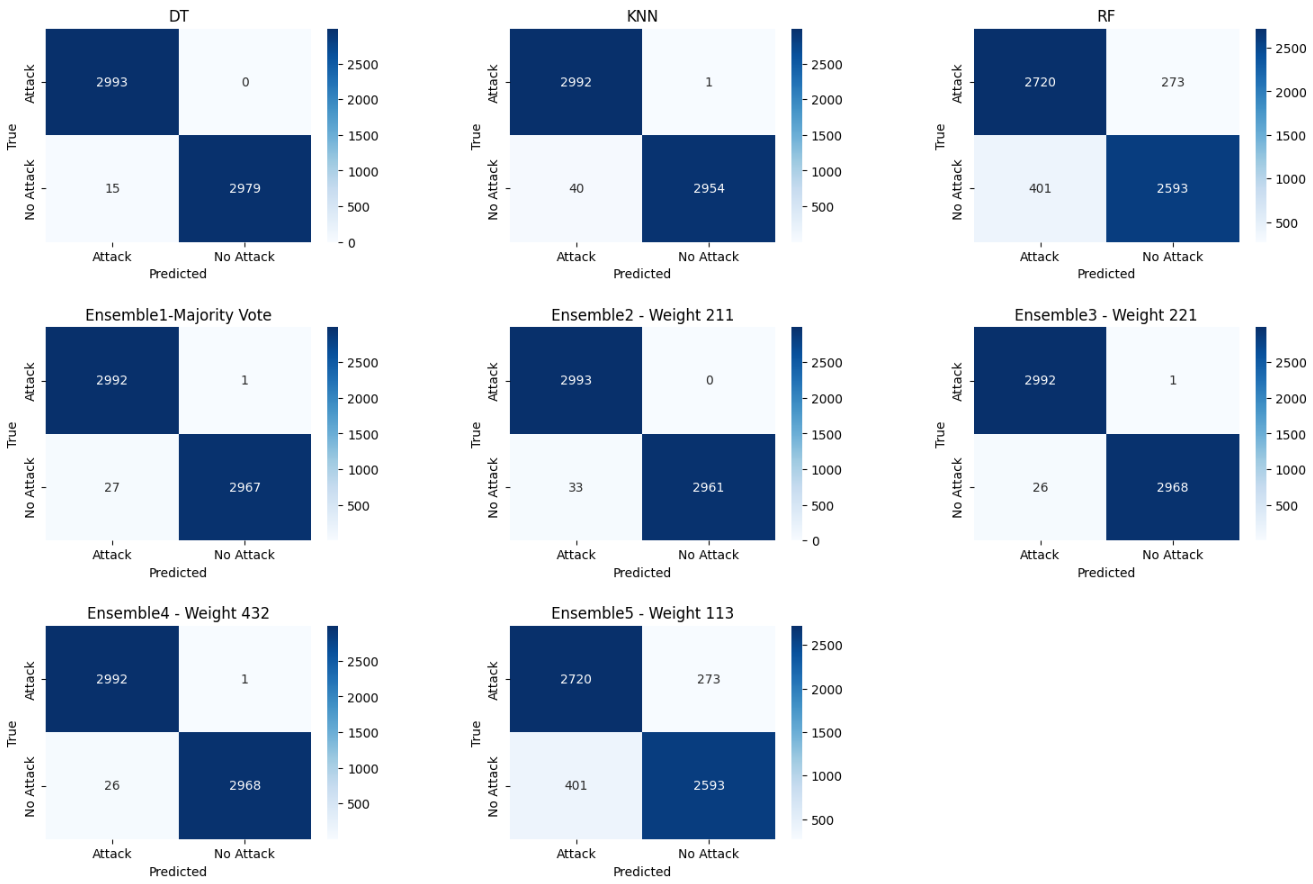
The result show that Decision Tree give the highest accuracy, precision, recall and F1-score and suitable for detect attack in Water Distribution system. KNN also give very high result on all criteria. RF is not good sine there’re lots higher in False Positive and False negative.



Comparing to Ensemble models Decision Tree yields higher score in ever criterias over 5 Ensemble models. Among 5 ensemble models. The model which given more weight to Decision tree get higher scores.



Inspect Confusion matrix on DT, KNN, RF an 5 Ensemble models



After cutting the most significant features, there’s little impact to accuracy and recall on DT and KNN model. But there’s huge impact on RF. This mean RF is not suitable for Water Distribution Attack detection.

There’re multiple stages of experiments. Saving .csv file for each stage can save time not to start over from the beginning.

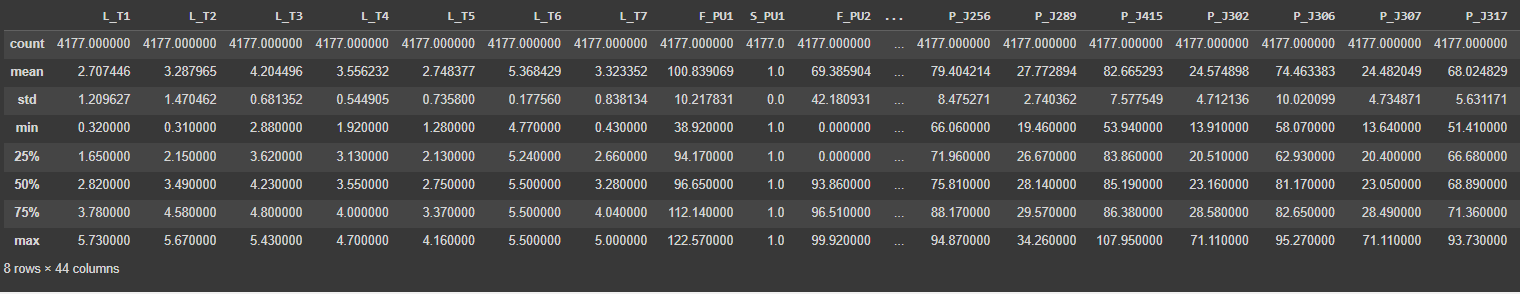
Bonus track: Training with BATADAL Dataset

We need to know more on what kind of feature impact the prediction class the most. So we train the same method in BATADAL2017. Since BATADAL explain every features in details while WADI2019 doesn’t

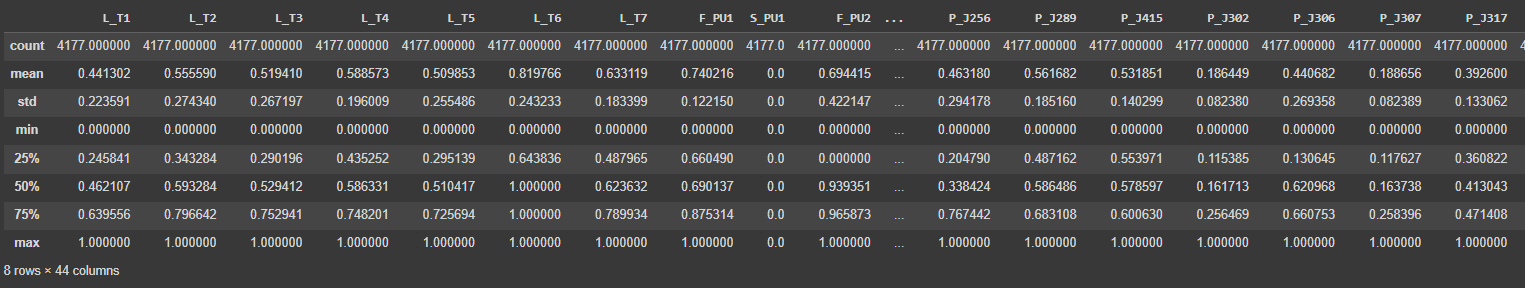
Inspect BATADAL



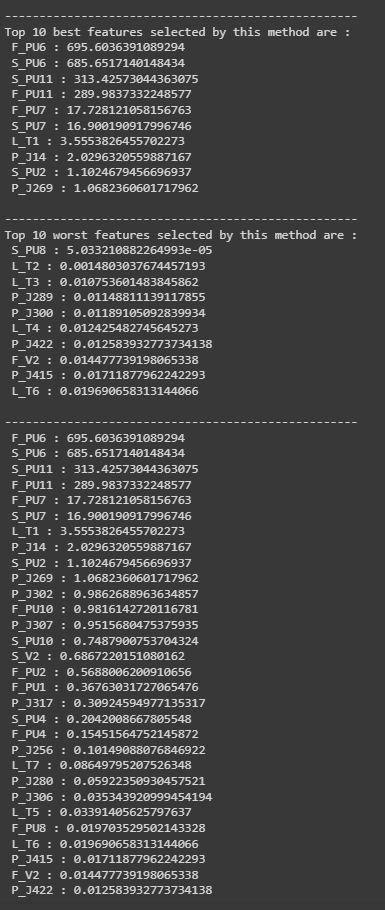
Before Normalize with MinMaxScaler



After Normalized



Inspect Top 10 best feature scores. We can see feature related to Pump Flow and Pump status(F\_PU6, S\_PU6) get highest feature score.

****

**Conclusion**

In conclusion, the feature selection process revealed interesting insights into the significance of sign values and their impact on certain features. Notably, for feature 90, the sign (positive/negative) proved more significant than its numerical value, while for feature 88, the numerical value was more crucial than its sign.

The results of the model evaluation demonstrated that the Decision Tree exhibited the highest accuracy, precision, recall, and F1-score, making it a suitable choice for detecting attacks in Water Distribution systems. KNN also performed exceptionally well across all criteria. However, Random Forest did not fare as well due to a higher occurrence of False Positives and False Negatives.

Comparing individual models to ensemble models, the Decision Tree consistently outperformed the ensembles, particularly when more weight was assigned to the Decision Tree within the ensemble. Moreover, after pruning the most significant features, the impact on accuracy and recall was minimal for Decision Tree and KNN but substantial for Random Forest. This suggests that Random Forest may not be well-suited for Water Distribution Attack detection.

Throughout multiple stages of experiments, it became evident that saving .csv files at each stage could significantly save time by eliminating the need to start over from the beginning.

As a bonus track, training the models with the BATADAL Dataset provided further insights into feature importance. The analysis revealed that features related to Pump Flow and Pump Status, such as F\_PU6 and S\_PU6, received the highest feature scores. This additional experiment with BATADAL helped to better understand which features had the most impact on the prediction class, especially considering the detailed feature explanations provided by the dataset.

**References**

1. Paper: Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks  
   https://par.nsf.gov/servlets/purl/10104860
2. Dataset information:  
   https://itrust.sutd.edu.sg/itrust-labs\_datasets/dataset\_info/
3. BATADAL2016 Dataset:

4 Files already attached

1. WaDi2020 Dataset:

https://drive.google.com/drive/folders/1c28Vfq4NF66Nchu8tQC4vsMQngK5xVTy

1. Secure Water Distribution, explained:

https://youtu.be/8rk4hJvePFo