COMP3217 Security of Cyber-Physical Systems 2022 Coursework 2: Detection of Manipulated Pricing in Smart Energy CPS Scheduling

Problem

The problem stems from the exploitation of smart energy scheduling schemes by manipulating the energy prices at certain hours to allow a lower price for the attacker. A way to prevent this is through machine learning to predict abnormal pricing.

This report summarizes the modelling of 5 users, each of whom has 10 smart home appliances that uses an energy scheduler to model these tasks over a period of 24 hours to achieve the lowest price. The energy scheduler is computed through linear programming which displays how the 50 tasks are distributed to lower the total cost.

To prevent such attacks a machine learning model is trained using training data to predict and classify normal vs abnormal pricing strategies with the hope of preventing pricing scheduler exploitation.

Computing Labels

The labels were predicted using a support vector machine (SVM) classifier which was imported from 'sklearn'. We use the linear SVC (support vector classification) to create a model from the training data given. SVC takes two input arrays: X holds the data which is used for classification, in this case the pricing for each hour and Y which contains the corresponding classification for data in X.

Support Vector Machines in this case is used for binary classification, the labelling works by separating the two classes of data i.e. abnormal and normal schedules. The SVM finds the best hyperplane that separates all data points between the two classes. The larger the margin between the data points and the hyperplane means a better label accuracy.

When classifying the data the model checks if the data points are on which side of the hyperplane and based on the difference will assign a class to those sets of data points.

In the approach on the main python file the program reads the training data and separates the data and the classifier while maintaining the same order. Then create and train the model. Finally use the model and use the test data as an input to return an array of the corresponding test data. The values are as follows –

[1. 1. 0. 0. 1. 1. 0. 1. 1. 0. 0. 0. 1. 0. 0. 1. 1. 1. 1. 1. 0. 1. 0. 0. 0. 1. 0. 1. 0. 1. 0. 1. 0. 0. 1. 0. 0. 1. 1. 0. 0. 0. 0. 0. 0. 1. 0. 1. 1. 0. 1. 0. 1. 0. 1. 1. 1. 0. 1. 0. 0. 0. 0. 1. 1. 0. 0. 1. 1. 1. 0. 0. 0. 1. 0. 0. 1. 1. 1. 1. 1. 1. 0. 1. 1. 1. 1. 1. 1. 1. 0. 0. 0. 1. 1. 1. 0. 0. 1. 0.]

Linear Programming Based Scheduling Algorithm

The scheduling algorithm is PuLP which is a LP modeler that can generate models as well as solves the LP equation. Using the labels created for the test data, only the data that has an abnormal schedule (those with classification of 1) will be modelled. The modelling will be to minimize cost with a feasible schedule that manages all the task constraints like the deadlines as well as the max energy usage per hour for that specific task. Using these an equation is created that is solved and the energy consumed in kW against each hour is plotted using bar graphs for each day of abnormal scheduling. The bars in the graphs are split by each user's consumption per hour.

Results

Looking at the graphs plotted the exploitation of the scheduling system is very obvious as throughout the hours of 8,9,10,12,15,17,18 mostly have 0 energy utilization which should not occur as retroactively the prices should be lower on these hours, but the scheduler doesn't assign any task to those times. It is very likely the attacker assigns their tasks to these hours.

The labels 51 abnormal scheduling data out of 100. The training accuracy was found by running the model again but using the 1000 training data without the classifier. After getting the result comparing between the result and the classification of the training data to figure out the training accuracy. Every time the classification is the same a counter is increased and then at the end divided by 1000 which is the number of training data. The training accuracy at the end of this process was 95.43954395439543 which signifies the model is very accurate, so the selection of abnormal scheduling is majority correct.

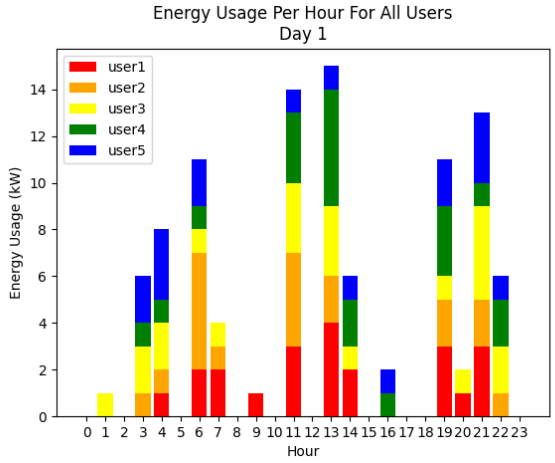
GitHub

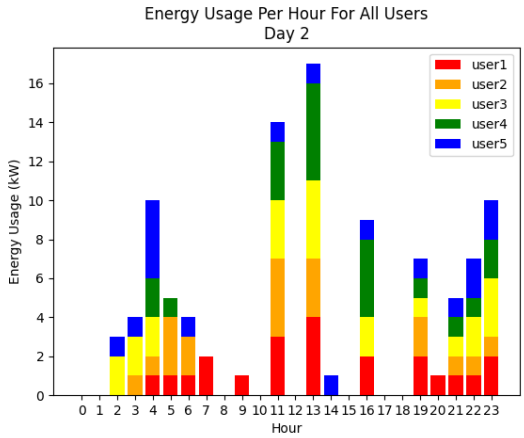
https://github.com/yadc1g19/COMP3217-Lab2.git

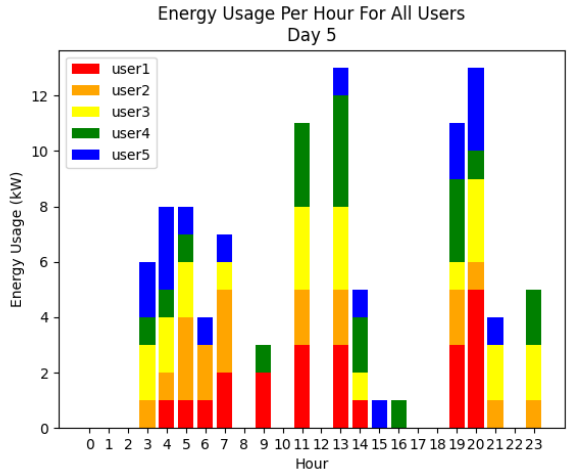
Running

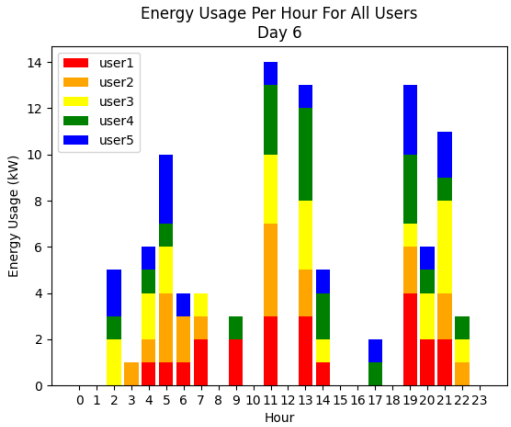
To set up the python requirements type 'make setup'

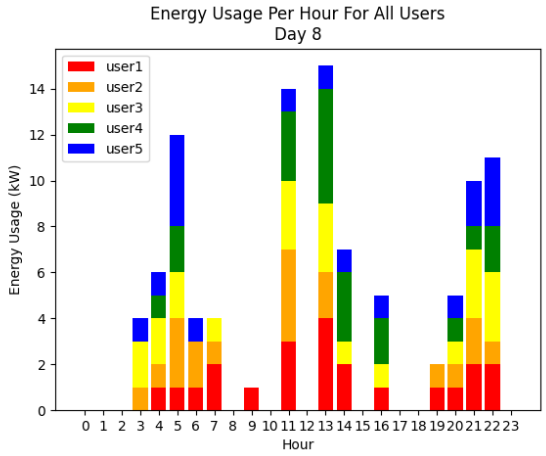
To run the scheduler type 'make'

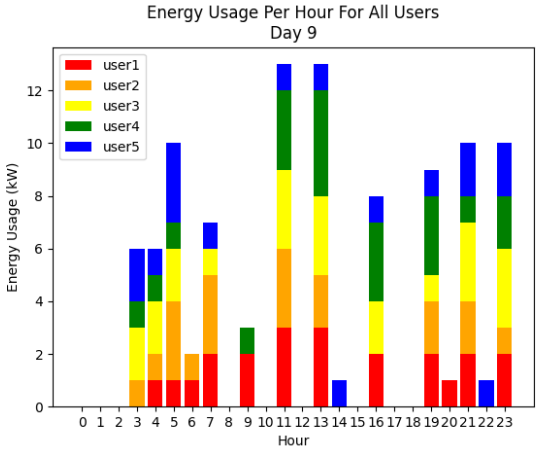

Energy Usage Per Hour For All Users
Day 1
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

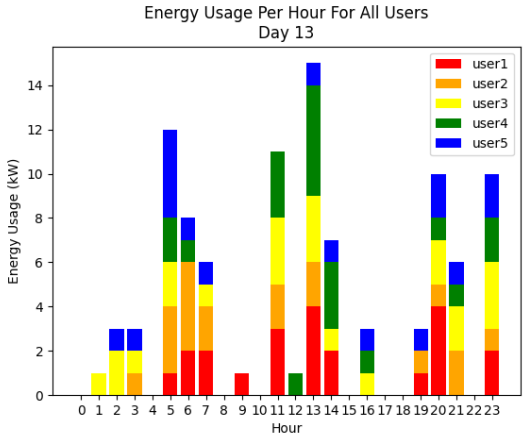

Energy Usage Per Hour For All Users
Day 2
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

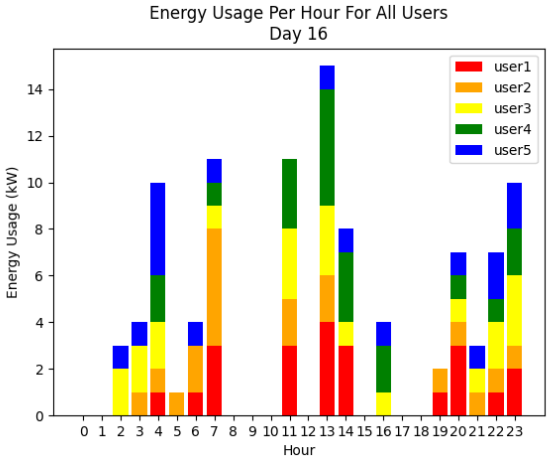

Energy Usage Per Hour For All Users
Day 5
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

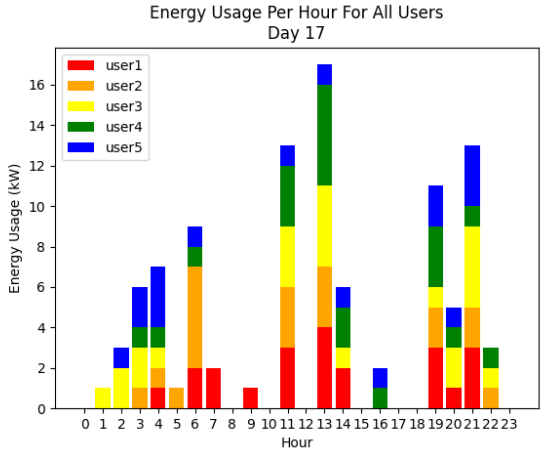

Energy Usage Per Hour For All Users
Day 6
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

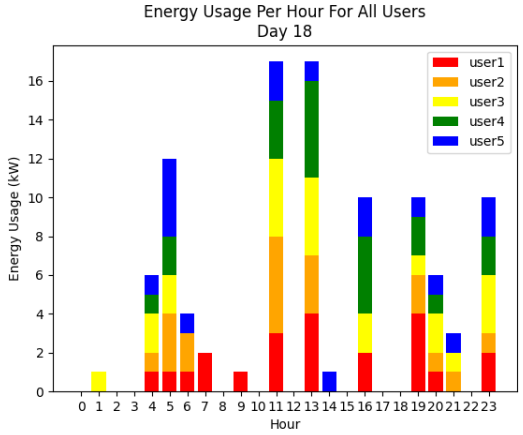

Energy Usage Per Hour For All Users
Day 8
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

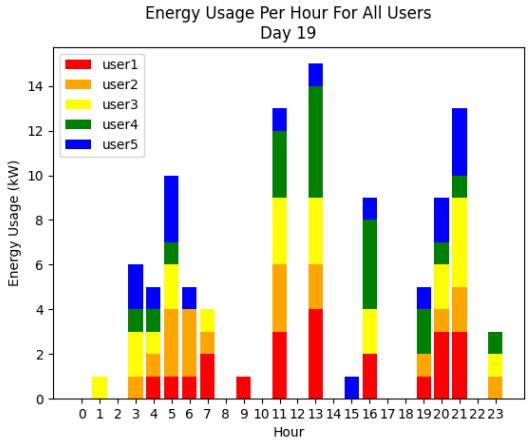

Energy Usage Per Hour For All Users
Day 9
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

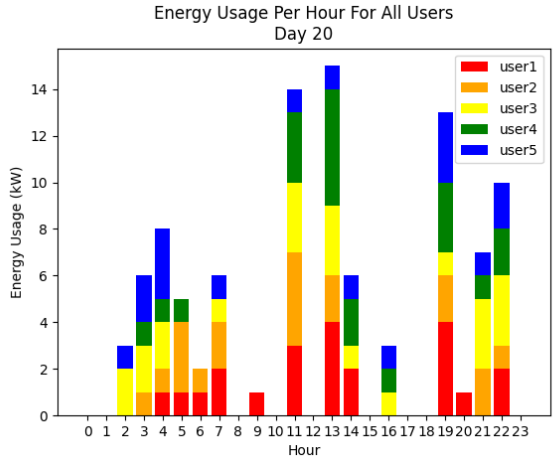

Energy Usage Per Hour For All Users
Day 13
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

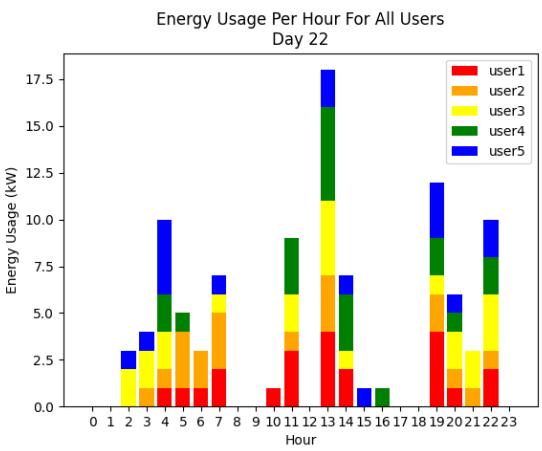

Energy Usage Per Hour For All Users
Day 16
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

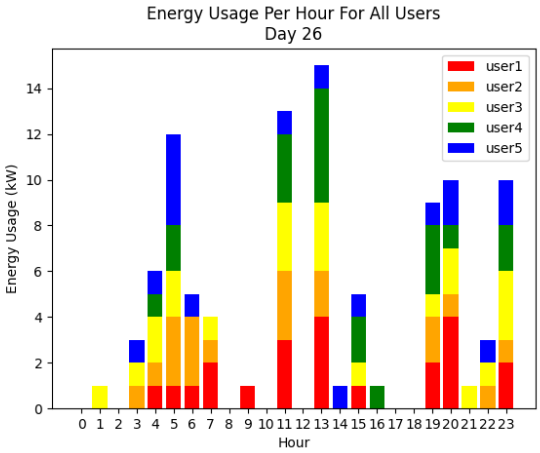

Energy Usage Per Hour For All Users
Day 17
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

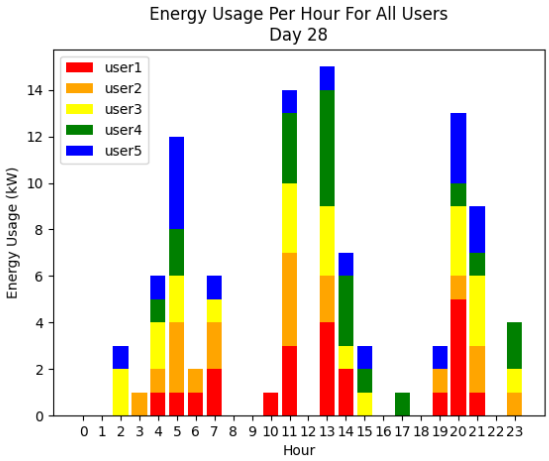

Energy Usage Per Hour For All Users
Day 18
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

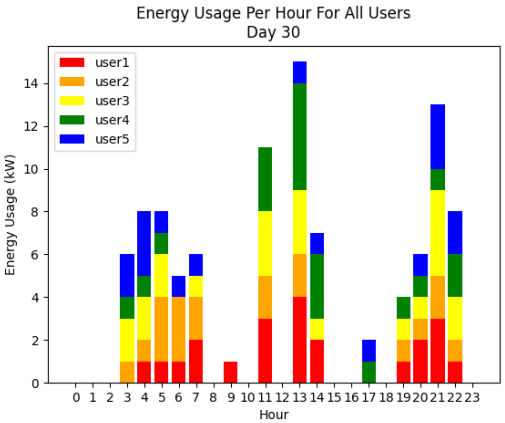

Energy Usage Per Hour For All Users
Day 19
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

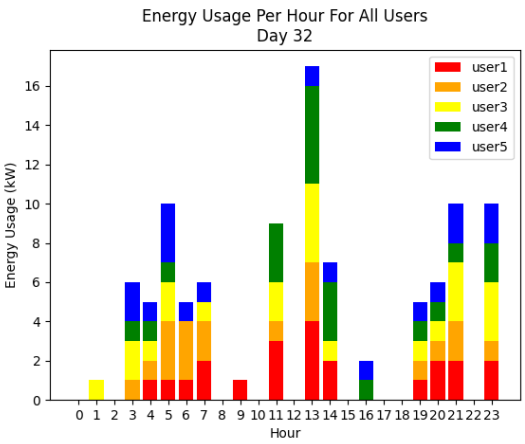

Energy Usage Per Hour For All Users
Day 20
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

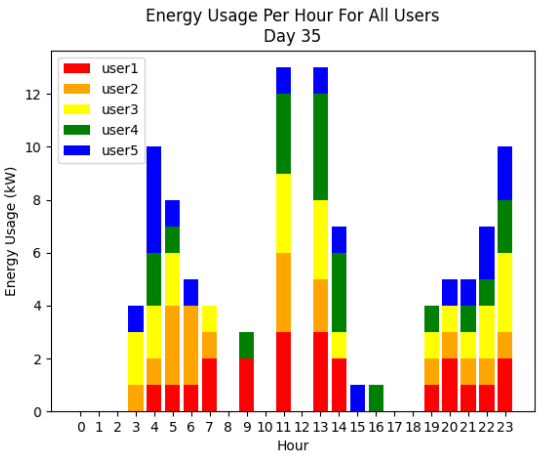

Energy Usage Per Hour For All Users
Day 22
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

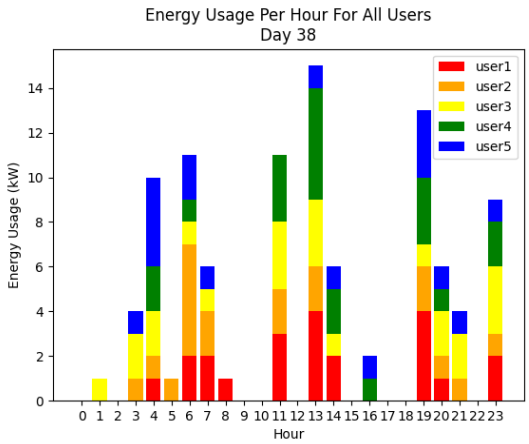

Energy Usage Per Hour For All Users
Day 26
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

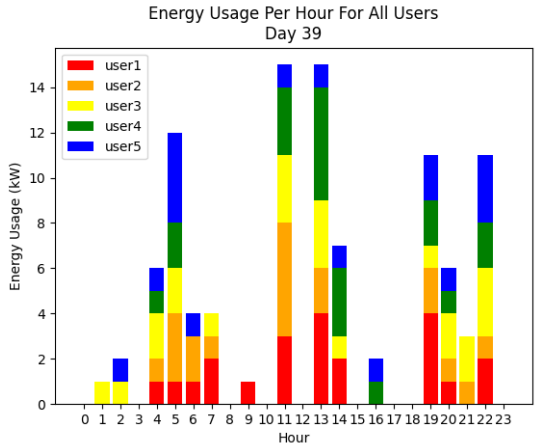

Energy Usage Per Hour For All Users
Day 28
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

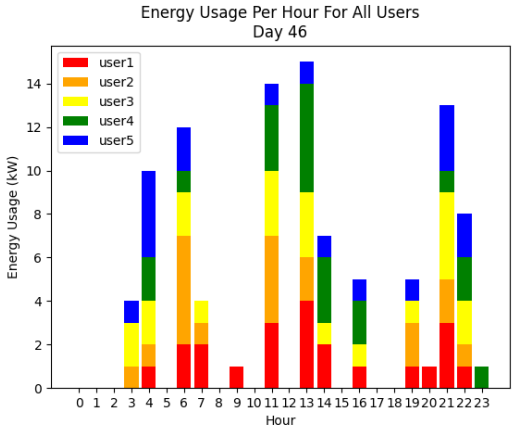

Energy Usage Per Hour For All Users
Day 30
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

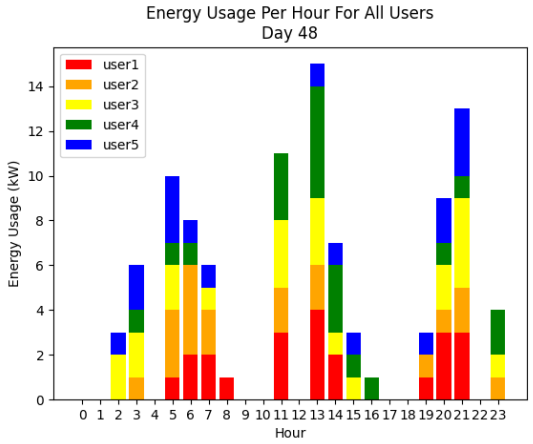

Energy Usage Per Hour For All Users
Day 32
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

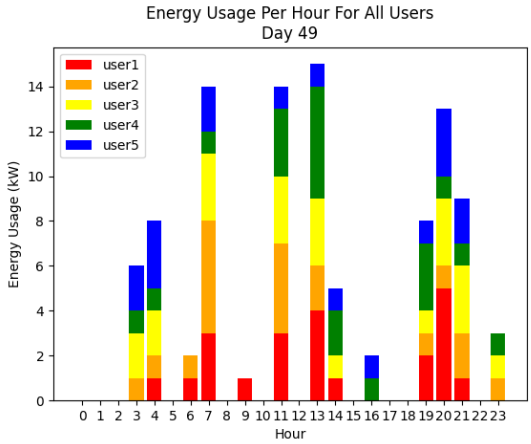

Energy Usage Per Hour For All Users
Day 35
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

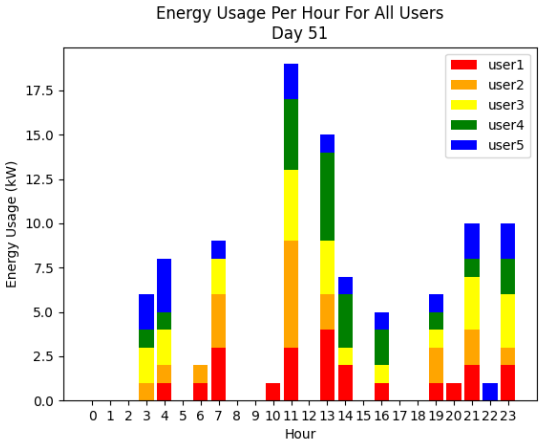

Energy Usage Per Hour For All Users
Day 38
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

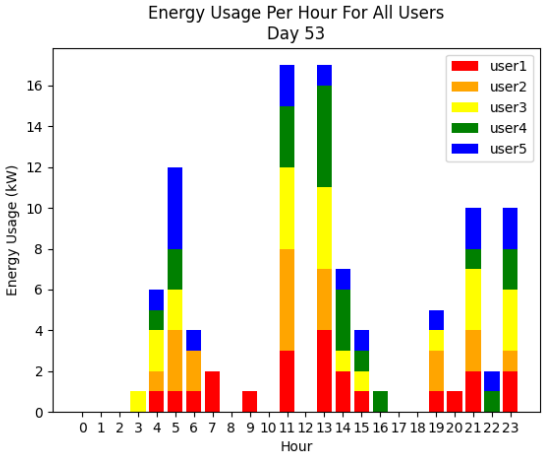

Energy Usage Per Hour For All Users
Day 39
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

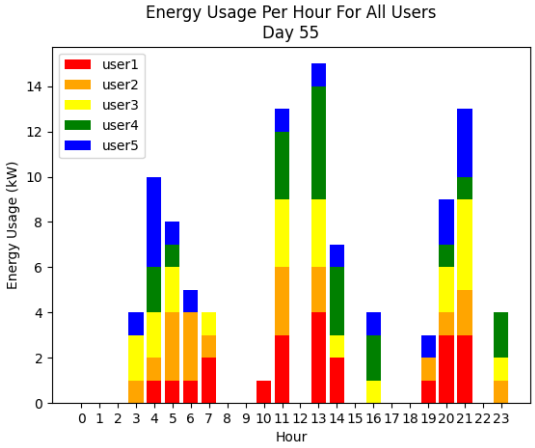

Energy Usage Per Hour For All Users
Day 46
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

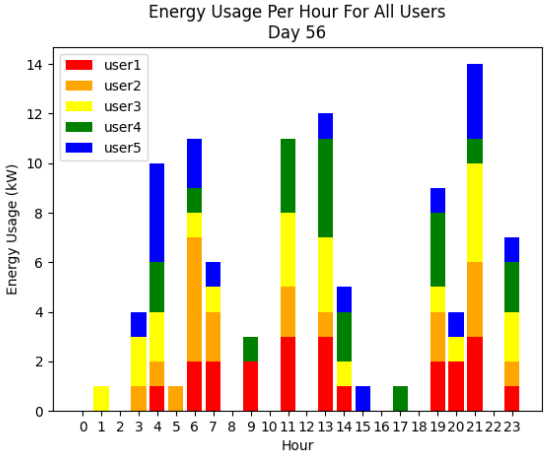

Energy Usage Per Hour For All Users
Day 48
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

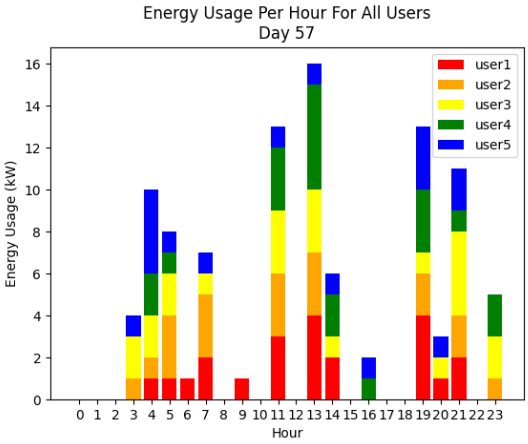

Energy Usage Per Hour For All Users
Day 49
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

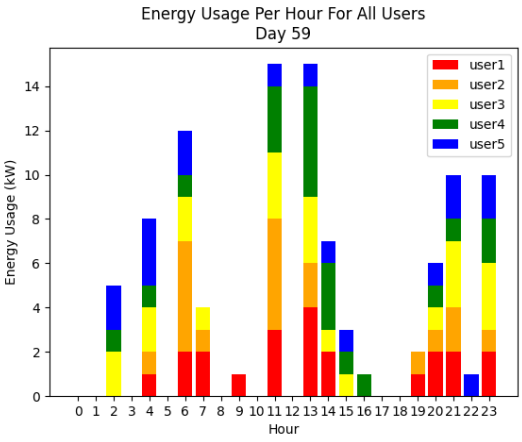

Energy Usage Per Hour For All Users
Day 51
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

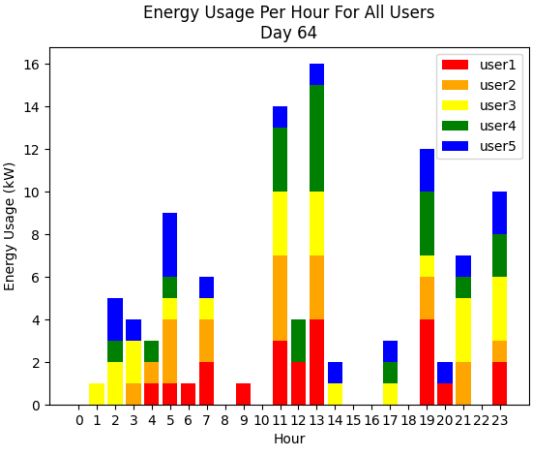

Energy Usage Per Hour For All Users
Day 53
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

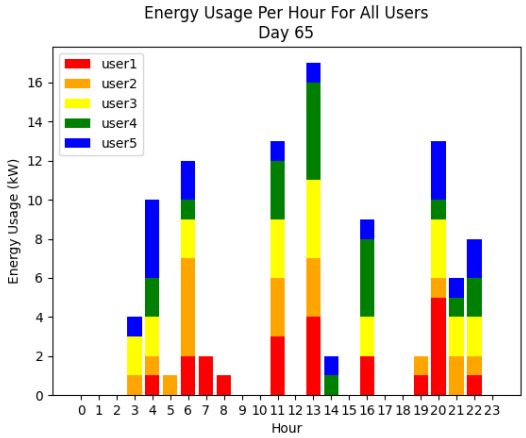

Energy Usage Per Hour For All Users
Day 55
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

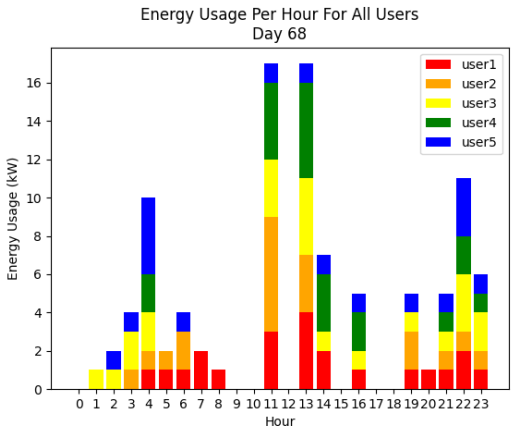

Energy Usage Per Hour For All Users
Day 56
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

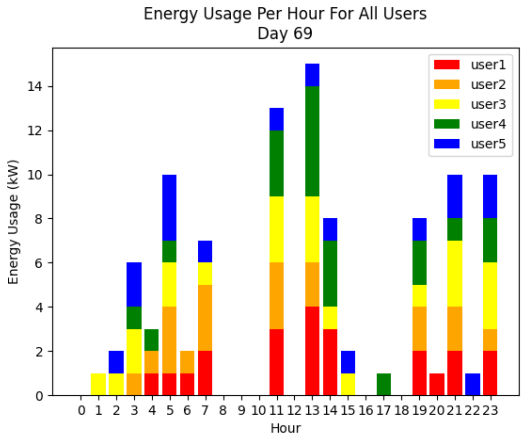

Energy Usage Per Hour For All Users
Day 57
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

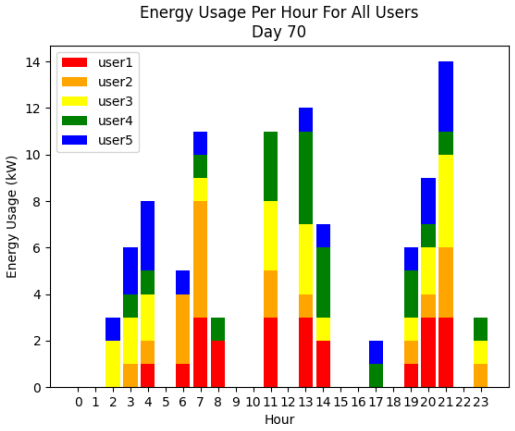

Energy Usage Per Hour For All Users
Day 59
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

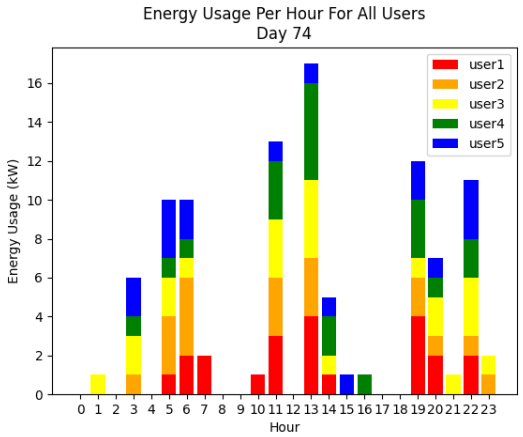

Energy Usage Per Hour For All Users
Day 64
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

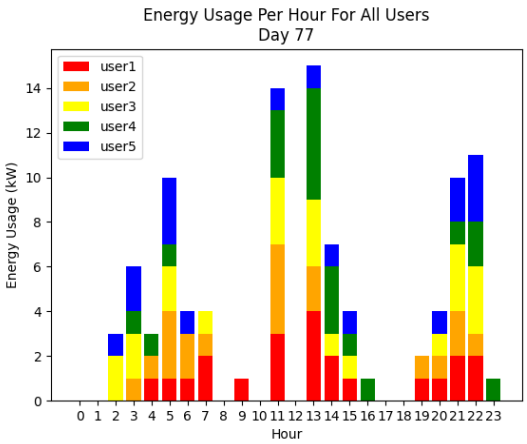

Energy Usage Per Hour For All Users
Day 65
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

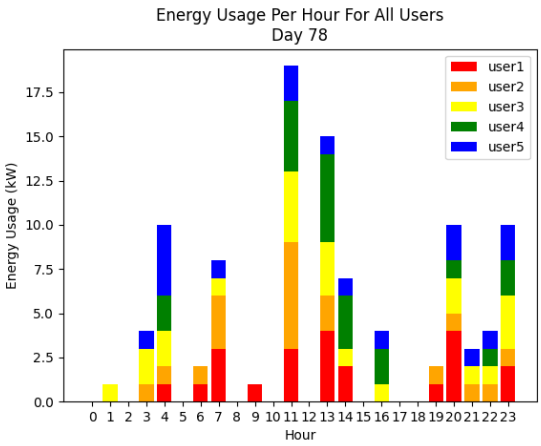

Energy Usage Per Hour For All Users
Day 68
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

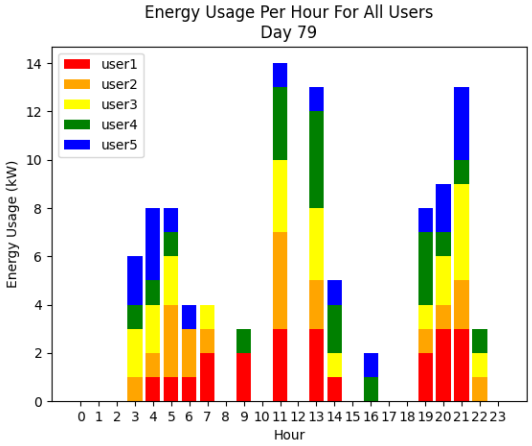

Energy Usage Per Hour For All Users
Day 69
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

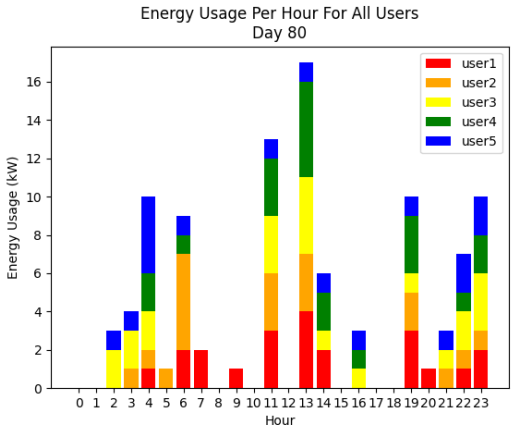

Energy Usage Per Hour For All Users
Day 70
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

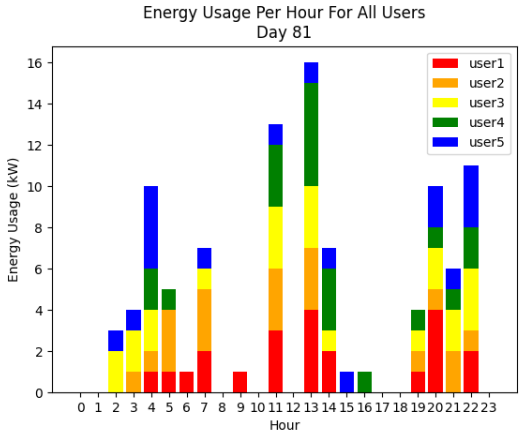

Energy Usage Per Hour For All Users
Day 74
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

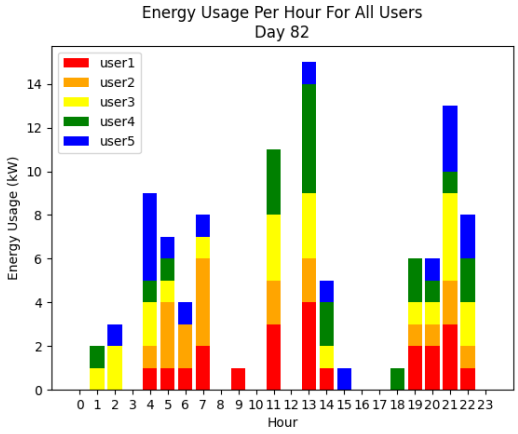

Energy Usage Per Hour For All Users
Day 77
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

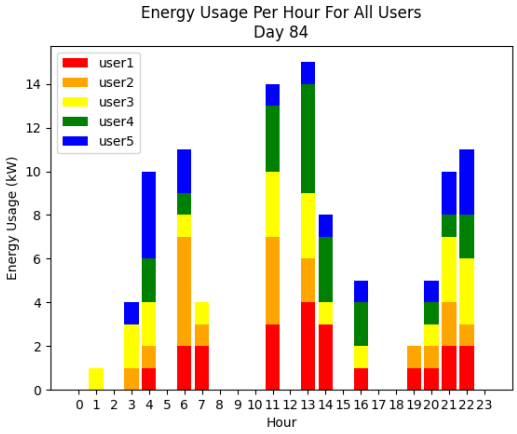

Energy Usage Per Hour For All Users
Day 78
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

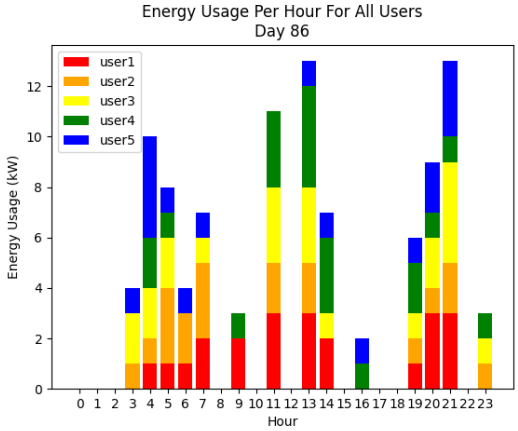

Energy Usage Per Hour For All Users
Day 79
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

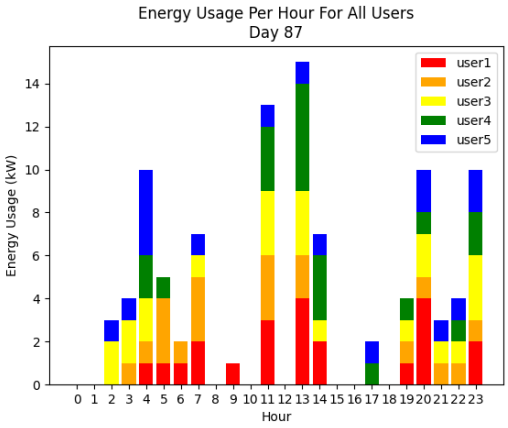

Energy Usage Per Hour For All Users
Day 80
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

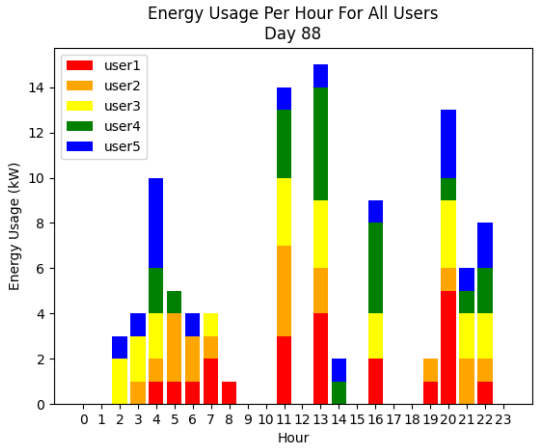

Energy Usage Per Hour For All Users
Day 81
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

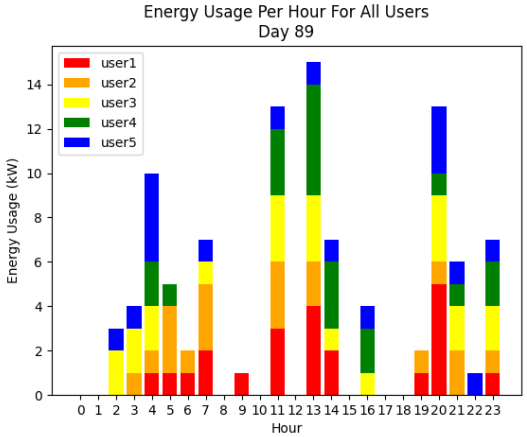

Energy Usage Per Hour For All Users
Day 82
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

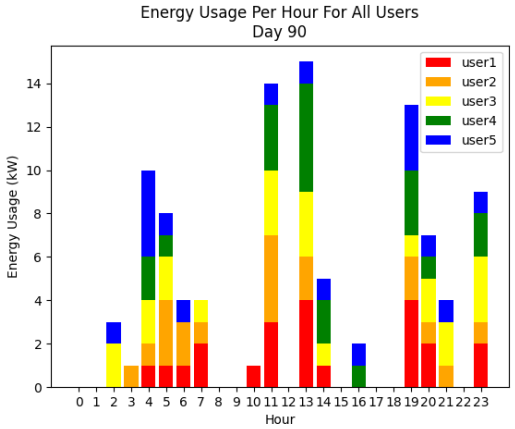

Energy Usage Per Hour For All Users
Day 84
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

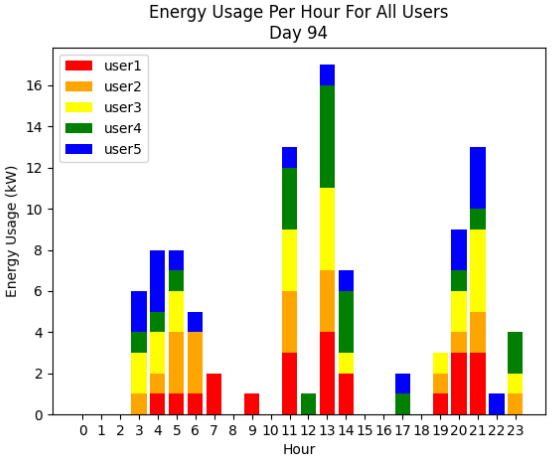

Energy Usage Per Hour For All Users
Day 86
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

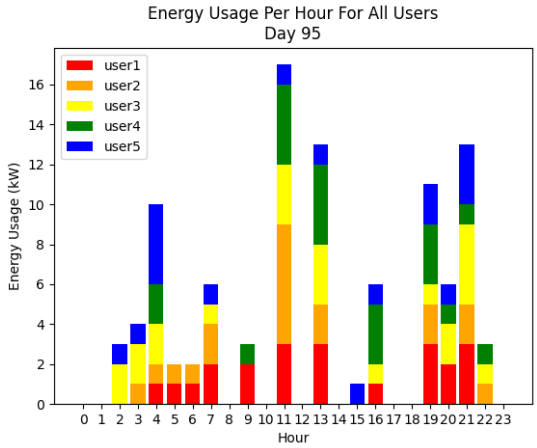

Energy Usage Per Hour For All Users
Day 87
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

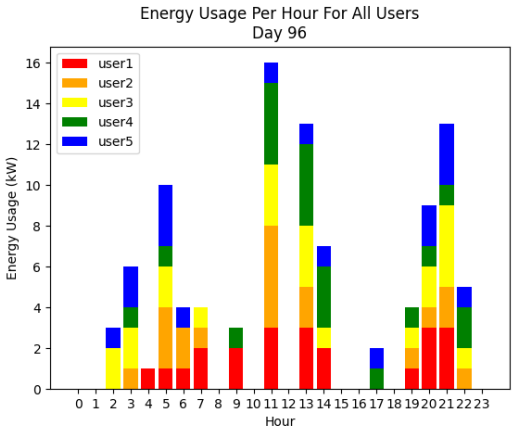

Energy Usage Per Hour For All Users
Day 88
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour

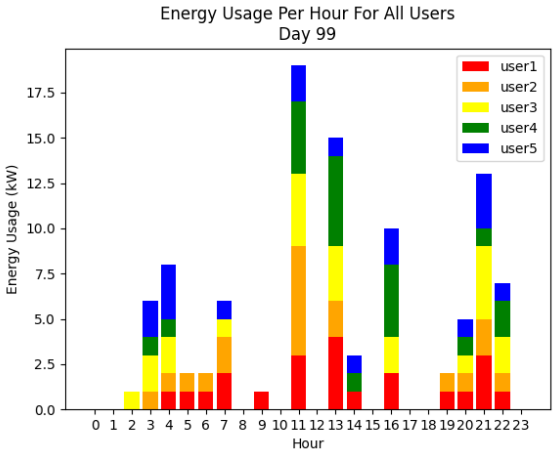

Energy Usage Per Hour For All Users
Day 89
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour


Energy Usage Per Hour For All Users
Day 90
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour


Energy Usage Per Hour For All Users
Day 94
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour


Energy Usage Per Hour For All Users
Day 95
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour


Energy Usage Per Hour For All Users
Day 96
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour


Energy Usage Per Hour For All Users
Day 99
user1
user2
user3
user4
user5
Energy Usage (kW)
Hour