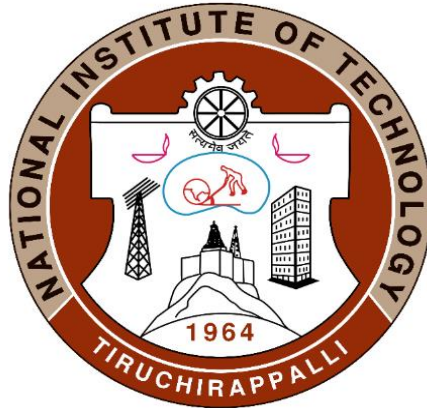# National Institute of Technology, Tiruchirappalli, Tamil Nādu

Master of Computer Applications

Batch: 2020 - 23

Section - A

Information Security

Report on

Anomaly Detection in Smart Meter

Submitted to: Submitted by:

Dr. (Mrs) B.Janet   **Nitansshu Jain**

                                                 205120063

Problem Definition

Energy consumption in buildings and industry is often wasted due to user behaviour, human error, and poorly performing equipment. In this context, identifying abnormal consumption power behaviour can be an important part of reducing peak energy consumption and changing undesirable user behaviour. With the widespread rollouts of smart meters, normal operating consumption can be learned over time and used to identify or flag abnormal consumption. Such information can help indicate to users when their equipment is not operating as normal and can help to change user behaviour or to even indicate what the problem appliances may be to implement lasting changes.

- Modern smart grids rely on advanced metering infrastructure (AMI) networks for monitoring and billing purposes. However, such an approach suffers from electricity theft.

- Electricity theft results in high financial losses for several countries such as the United States and India. Other developing countries lose almost 50% of their electricity revenue due to theft.

- Here we present an approach to identify the suspect customers, using the customer power usage pattern.

Problem Description

Electricity theft or tampering with the electricity meter has been around ages.

Meter tampering means doing any act which causes the meter to run slower or shut down at all and is basically theft of electricity from the company that supplies power. There are multiple ways to tamper with an electricity meter and some of them include turning the watthour meter upside down, replacing the meter with items such as copper wires or knives, or drilling a hole in the meter and inserting something to stop the disc at night and removing the object in the morning so that no one would suspect electricity theft. Extreme measures of electricity theft include breaking the meter itself or replacing your meter with someone else's.

Tampering is usually associated with a utility customer that wants to reduce their electric bill. Residential and commercial customers have tried many methods over the years, often creating conditions that are dangerous for themselves, their neighbours and utility.

In the past, older electromechanical meters were very limited in their ability to monitor for tampering. Often, to find a tampering instance, the utility relied on meter readers to notice an issue during the monthly onsite reading. Occasionally the tampering would be obvious, but often the energy thieves would be creative in their attempts to get around the system and steal power.

Thieves often try removing a meter from the socket or even taking a meter from another location and replacing their original meter to reduce their electric bill.

Electricity meter tampering by consumers

Consumers have the resources and knowledge to carry out successful tampering with an electricity meter and in a country like India where there is an absence of street cameras and a large population, it is easy to get away with the act.

Electricity meter tampering by the suppliers

One may think that it is only consumers who attempt electricity theft and meter tampering, but this is not true. Often suppliers of electricity will tamper with the meter themselves and blame the consumer in an attempt to make some extra money.

Latest Digital Metres

A 'smart meter' is different from traditional electrotechnical meters as they have systems to measure consumption, a clock to stamp time information, communication systems and fault reporting and diagnostic capabilities.

Detection of Meter Removal

Thieves often try removing a meter from the socket or even taking a meter from another location and replacing their original meter to reduce their electric bill. In either case some AMI systems have been designed to alert the utility of these conditions. In fact, these systems detect and report the number of times a meter has even been turned off/on with date and time stamps and can even locate the meter if it has been moved from its registered address.

Detection of Unusual Readings

Smart meters are now able to measure and report real-time information that was previously unavailable to the utility. These include detecting and reporting meter anomalies such as reverse current flow and flagging meters that aren't registering energy consumption.

With such advancements, still the smart electric metres can be tampered by smart lineman or technician. They are very smart, experienced and have very deep knowledge of metres. They know the ways how to tamper the electric metres.

Proposed Solution

In this theme, we propose to implement:

Machine Learning Algorithm for Efficient Power Theft Detection using Smart Meter Data

The AMI networks rely on smart meters located in the customer's premises to regularly report their energy consumption. This approach has the potential to hinder traditional physical electricity theft attacks including line hooking or meter tampering.

My solution contains EDA and algorithms developed for the Anomaly Detection in Smart Meter Data challenge.

I have taken the data set from Kaggle which contains a time series of reading from a single smart meter.

We present:

1. Clustering Approach for detecting anomalous days based on mean and std of the readings during the day.

2. Monte Carlo Approach for detecting single anomalous readings.

Technology Stack used:

- Python
- Libraries:
  - ➢ Pandas – To extract the required data
  - ➢ NumPy – Basic Numerical Operations
  - ➢ Matplotlib – To visualize the data plot
  - ➢ Sklearn – For using clustering algorithm
- Jupyter Notebook

Code and Results are found [here](#) .

<u>Advantages</u>

- ➢ This model can easily detect the misbehaviour of the electric meter.
- ➢ We can trace the exact location of the house as we all the data already available with us like house at which faulty meter is present, location, etc.
- ➢ It identifies abnormal consumption power behaviour which can be an important part of reducing peak energy consumption and changing undesirable user behaviour.
- ➢ This way lots of due bills will be recovered and profitable to the country as everyone should pay their fair share.

<u>Disadvantages</u>

- ➢ It's a hectic task to be done by employees to reach at each home, check the number of appliances present, mark the units possible from each appliance, mark heavy appliances, their effect on metre reading. After collecting all the required data which is optimally needed to build a model, we can perform machine learning on the collected data to predict the result. Hence all it requires is a lot of time and manpower to collect all the data.
- ➢ Such algorithms should begin to operate after as little as 3 months after collecting huge amount of data and feeding into the model to get good results.

<u>Novelty of Solution and Future Scope</u>

The clustering algorithm will cluster these customers into clusters. The customer's profile that belongs to the largest cluster are chosen for further investigation into the power usage patterns. These customers are identified as trustworthy customers.

The selected genuine customer's profile data are the input to the smart meter data analytics system.

The current approach is working on dataset with 2 features (Periodic Readings and Power Consumption). But accuracy can be increased further with a larger dataset and more layers.

For a larger dataset with a greater number of features, a time-series based model can be trained for fine tuning of hyperparameters to recognize highly complex, time variant power usage patterns and determine fraudulent customers.

After analysis of Power usage, patterns of different localities with more features, the system can be used by the authorities at higher levels of hierarchy.
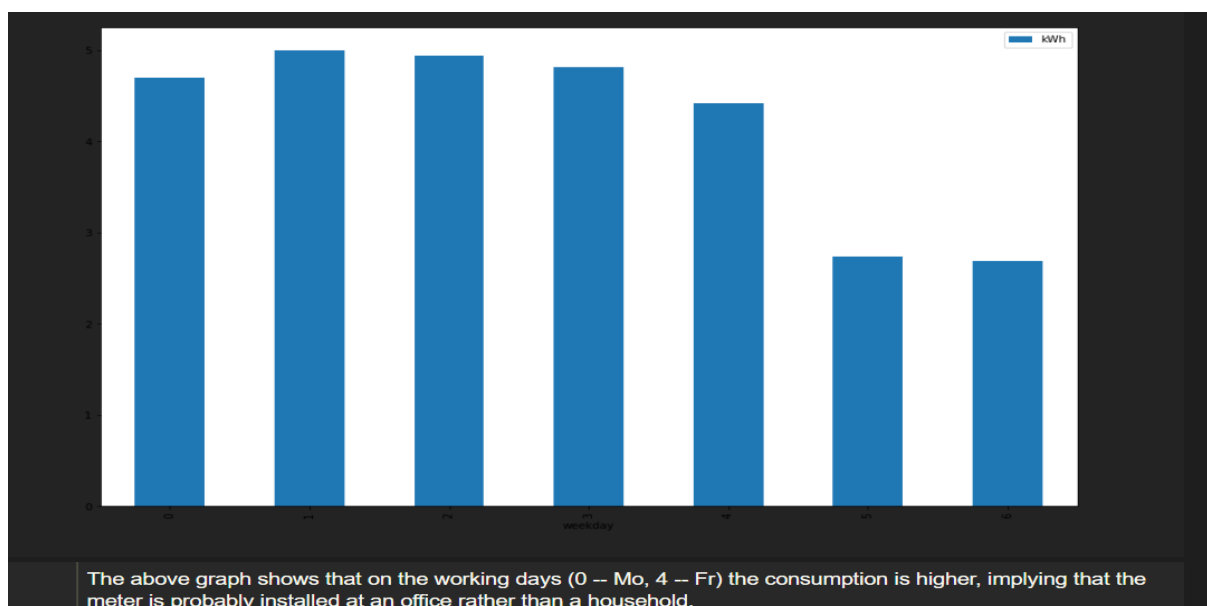
With the knowledge of power usage patterns, specific power demand for future can be predicted, which can help reduce transmission losses and installation of power storage infrastructure at specific locations.

It will avoid high financial losses to the countries, and help in the growth of the counties.

Screenshot of Results
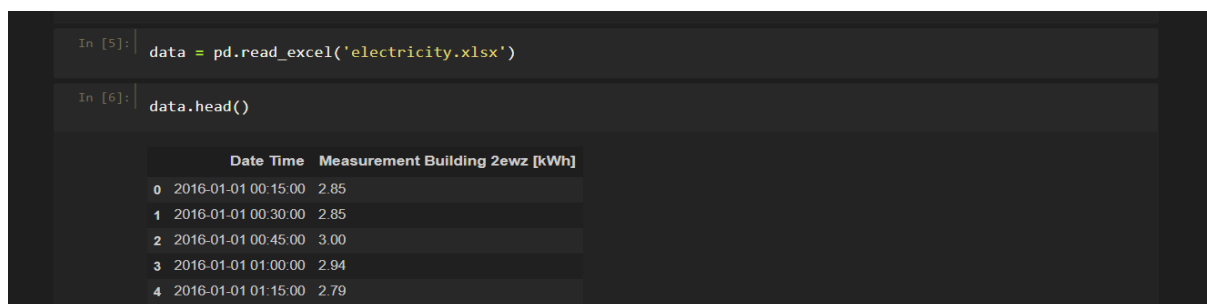
Figure 1 Dataset to work upon
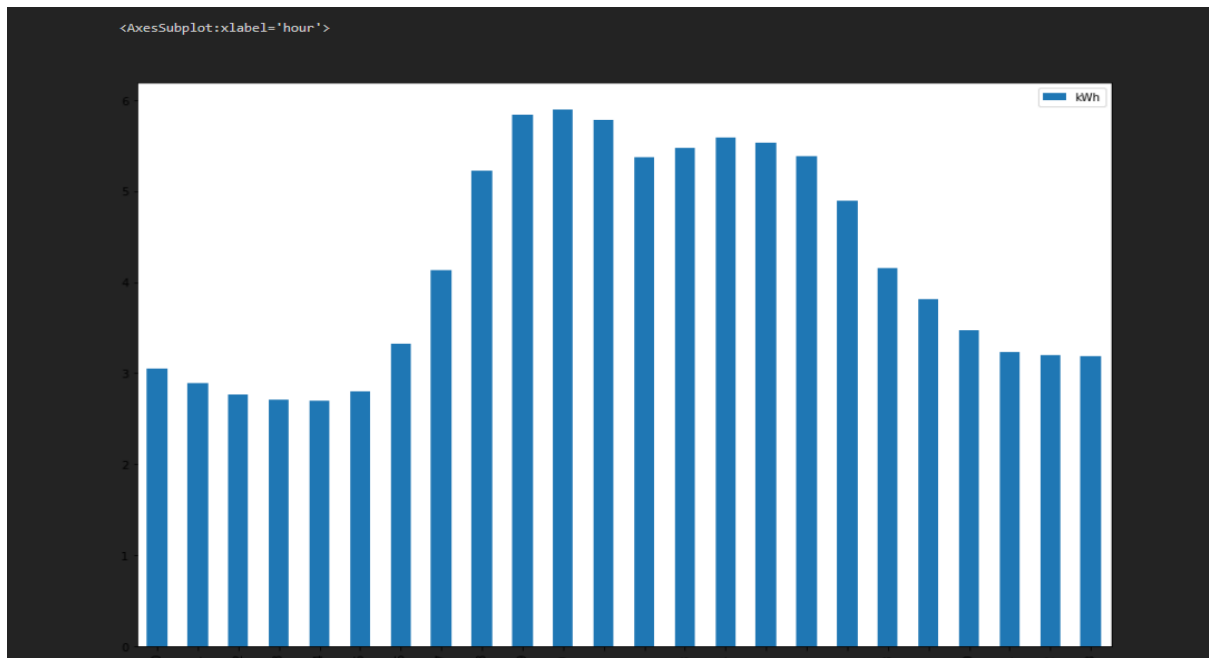

Figure 2 Average Consumption per day of the week
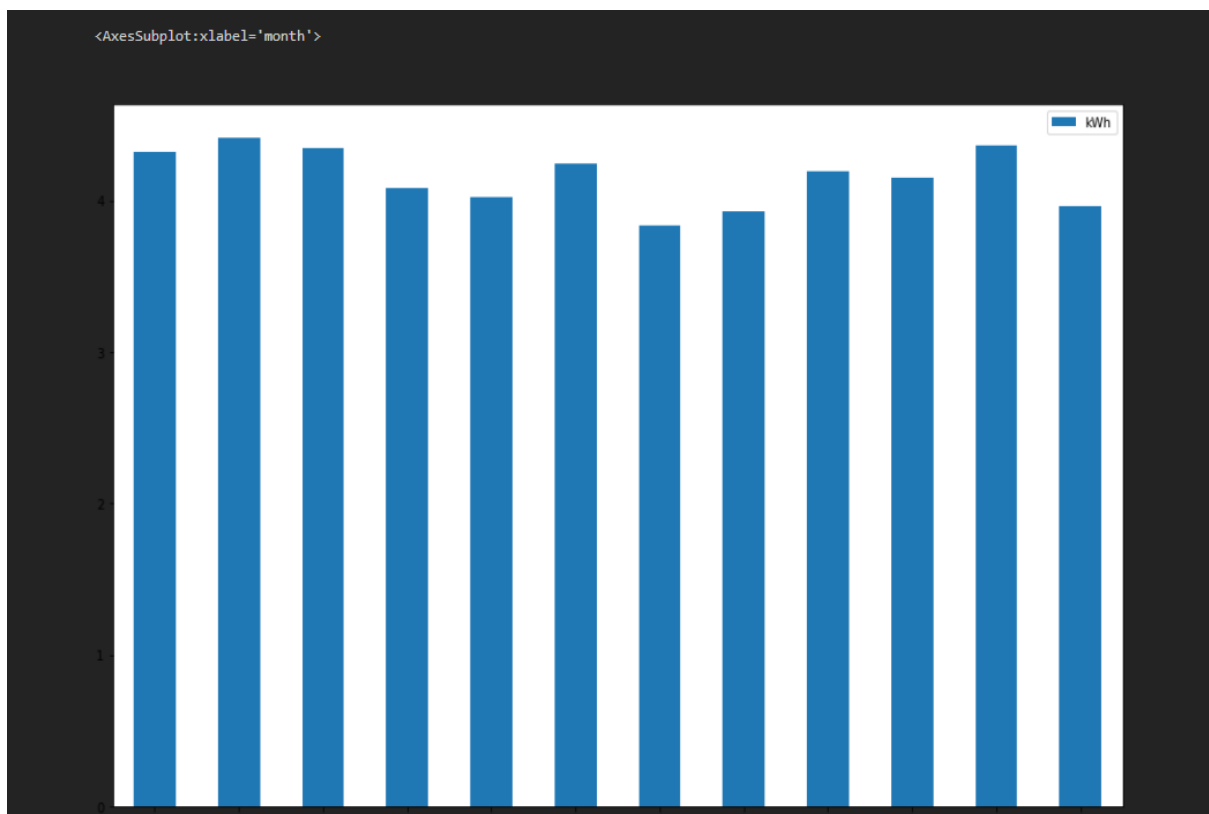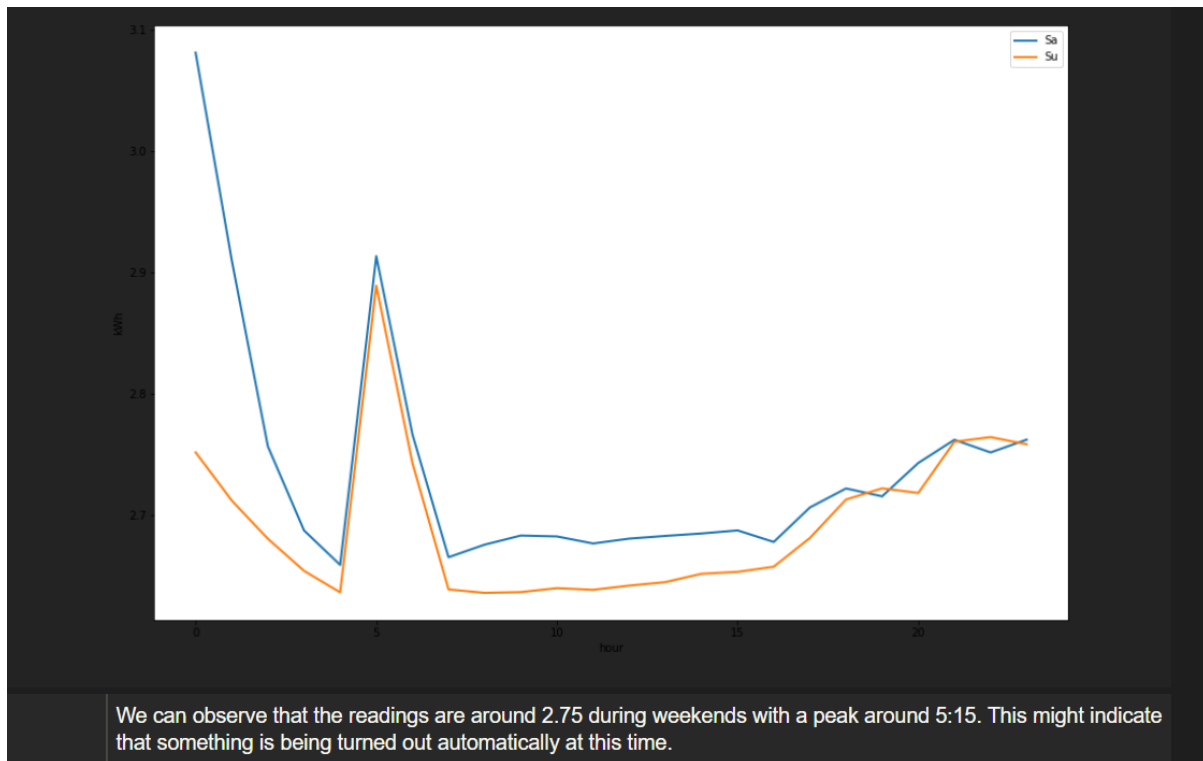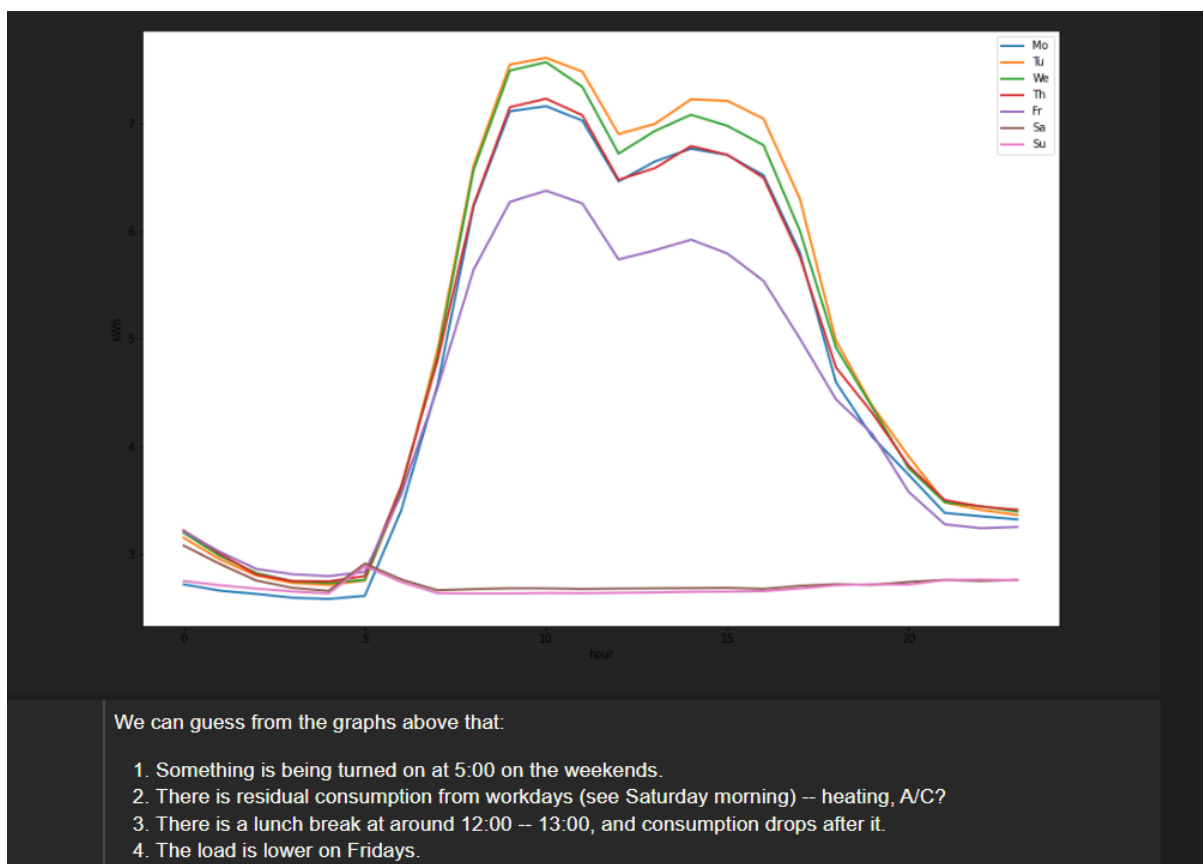
Figure 3 Average Consumption per hour
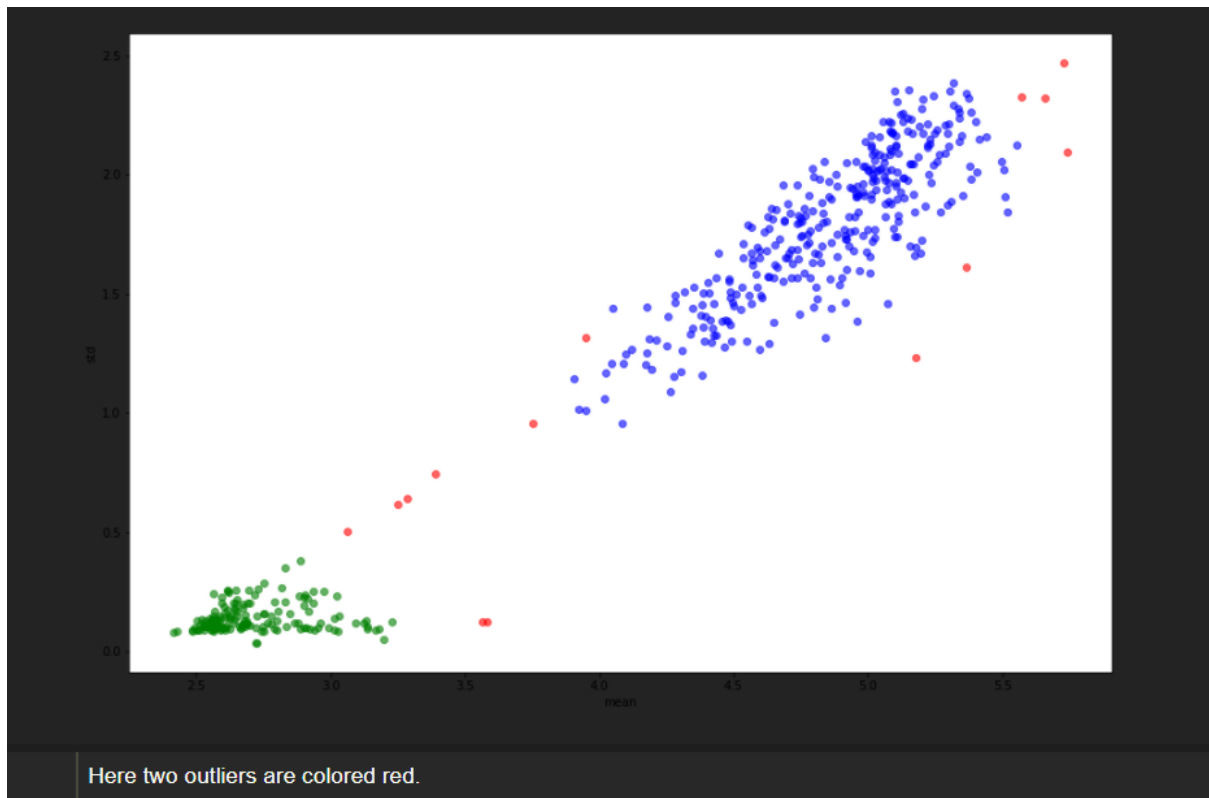

Figure 4 Average Consumption per month

We can observe that the readings are around 2.75 during weekends with a peak around 5:15. This might indicate that something is being turned out automatically at this time.

Figure 5 Workday vs Weekend

We can guess from the graphs above that:

1. Something is being turned on at 5:00 on the weekends.
2. There is residual consumption from workdays (see Saturday morning) -- heating, A/C?
3. There is a lunch break at around 12:00 -- 13:00, and consumption drops after it.
4. The load is lower on Fridays.

Figure 6 Analysis

DBSCAN Clustering

Here two outliers are colored red.

Figure 7 Outliers => Anomalous Days

Mean Shift Clustering

Here two outliers are colored red. Black dots are the cluster centers.
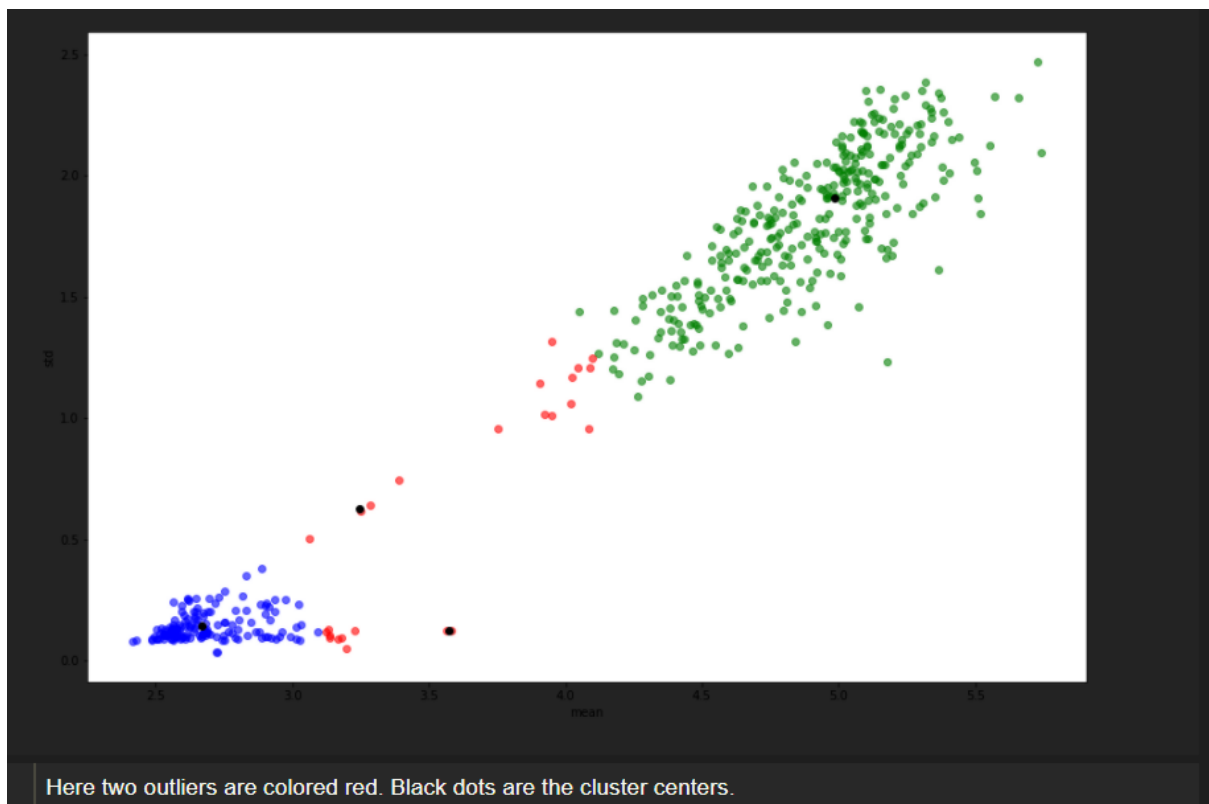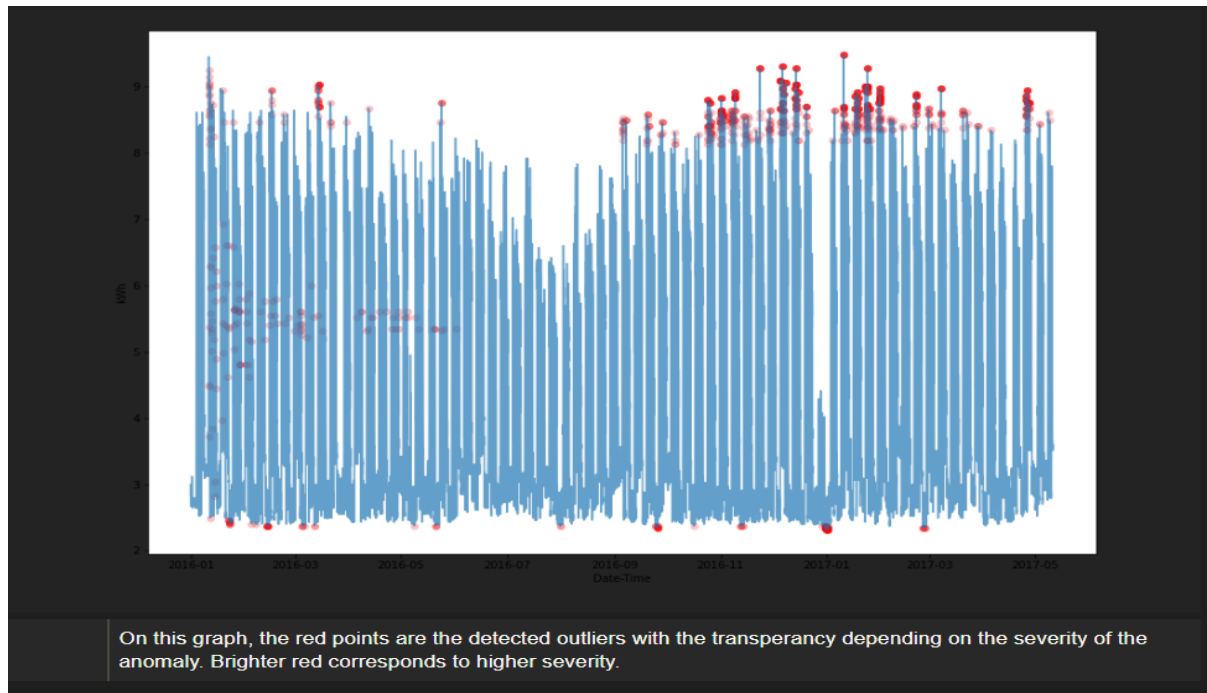
Conclusion of DBSCAN vs Mean Shift Clustering

One advantage of the Mean-Shift algorithm over the DBSCAN algorithm is that it produces centers of the clusters (they are used for clustering), and hence can be more easily adapted for online algorithms. DBSCAN would require recomputing the clustering with a new batch of data.

On this graph, the red points are the detected outliers with the transperancy depending on the severity of the anomaly. Brighter red corresponds to higher severity.

Figure 8 Monte Carlo Classification of Single Measurement

Comparison with existing solution:

AMI meters (smart meters) are used now-a-days, still they are tempered by linemen or technician. With the help of this proposed solution as an addon to the existing AMI meters, it will become nearly impossible to temper the electricity meter. Also, it will be easy to trace the exact location of the house where the anomaly is detected in meter.

_____