Technology Review for managing or exploiting IoT Data

Contents

[Introduction 3](#_Toc520884811)

[About Internet of Things (IoT) Data 3](#_Toc520884812)

[About Anamoly Detection 3](#_Toc520884813)

[Benefits of Using Anamoly Detection with IoT Data 3](#_Toc520884814)

[Limitations to Using Anamoly Detectionwith IoT Data 3](#_Toc520884815)

[Using Anamoly Detection with IoT Data 3](#_Toc520884816)

# Introduction

In this age of global digitalization the use of IoT (The Internet of Things) devices is getting a huge use in managing the huge amount of data or information. This data helps in providing the organisations to store and access more information and a greater knowledge enabling to access more information than what was possible before. It helps them to make better decisions and introduces them to new opportunities. Fast and easy accessibility of data is in demand in this age of fast growing internet oriented digitalized time. With big data, the data can be stored in much higher volumes than before also in a much greater variety than before and various locations throughout the entire organisation(Lee and Lee, 2015).

There are many advantages of using this approach such as reduced transmission cost, depending less on transmission, lower latency and improved privacy and potential security. There are some limitations too in using the edge analytics, as it needs a bigger management system. Managing the huge amount of information stored in the process can cause difficulties in operating the process. Transmitting and communicating this huge amount of data can be quite challenging. Thus with the use of the edge analytics, the transmission load can be quite decreased if the analytical workload on the device or in the gateways before the transmission can be reduced as much as possible.

IoT will increase the cost of the products and services during the stage of development while increasing the efficiency and productivity gains and thus finally reducing the overall cost.

# About the IoT (Internet of Things) Data

IoT (Internet of Things) represents a collection of different configurations of connected sensors such as light, motion or water detectors, RFID tags, tracking devices etc.(Höller *et al.,* 2014). Which helps in collecting the different type of data such as the data relating the weather, soil conditions etc. It refers to the devices (except phones and personal computers) which can connect to the internet all on its own. As some specialized cars, TVs, fridges, even some specific medical devices are able to connect to the internet all by itself; it can thus be identified as IoT devices. With the advancing technologies, there will be many more devices in the future which will be able to connect to the internet.



Fig 1: Internet of Things (IoT)

Source: (Höller *et al.,* 2014).

The purpose of using these devices is to transmit data and with the increased use of these devices with time; there will be a massive increase in transmitted data, which will be used for analysing and collecting feedback.

Tesla and Samsung are examples of organisations that utilize this technology at their workplaces. This data is sent back to the base from various devices inside the home in order to develop the products and for improving the software in use. In order to help with autonomy specializes cars on the road can use this data. The higher the amount of the gathered data, the more reliable it is.

The use of IoT could be quite beneficial in several sectors of society such as in the healthcare, agriculture, construction and in building maintenance, building smart cities, weather forecasting, environment (examining air and water quality, flora and fauna tracking), inventory tracking needs, in other tracking systems in transport, in event management etc.

# About anomaly detection in big data

Anomaly detection is finding out the mismatched data or any type of inconsistent data, which has a pattern in the systems. It can be used for various purpose such as for detection of any kind of intrusion in network security, fraud detection banking, for healthcare research and so on. There is a wide range of various type of methods of using this process such as the nearest neighbour method (“KNN”), different clustering techniques and various statistical algorithms of anomaly detection (Rettig *et al.,* 2015).

There are two main methods used in analysing the data one is the statistical approach, and the other is the approach based on Machine Learning. Approaching the data analysis with the help of Machine learning is more effective than the statistical approach.



Fig 2: Anomaly detection using machine learning

Source: (Rettig *et al.,* 2015)

There are three main ways of anomaly detection – supervised, semi-supervised and unsupervised. In the supervised method, the data is split into three parts with one of the section run through a model for identifying anomalies, second part tests the model, and the last part is used to validate the model. In the semi-supervised method, the model is developed for the normal data and then is used as an error detection technique. In the unsupervised method, a data set is taken, and it is assumed that most of the data is normal(Goldstein and Uchida, 2016). Then it tries to find the data that does not seem to fit the remaining part of the set.

# Detecting anomaly with IoT Data

It has been notified that huge amount of data is generated in the processes of the business world. With the increase of use of devices and the complex generated from those devices, anomaly detection can be useful for these huge amounts of complex data generated through the use of IoT(Buczak and Guven, 2016).

For example, the sensors in a Tesla motor car can be used to detect the abnormality in the data in case of bad weather conditions, detecting a heavy that the car can stay in its lane to avoid it, controlling the wipers and so on. The car could even use all the incoming data in order to enable it to be programmed in order to get support on the power output. In this way, the other systems of the car can keep the drivers to be safe. This also ensures that the car does not get any shortage of input power. As the consumers’ demand for smart devices to cope with these type of problems, the use of anomaly detection could be quite profitable for the business. Moreover, reliable product performance will help to increase the sales of the company.

# Limitations to Using anomaly detection with IoT Data

There are some limitations as well as using anomaly detection with IoT data, and they are variety, veracity, volume and velocity(Dua and Du, 2016). Variety is the problem related to the variety of data that anomaly detection deals with. Advanced techniques have to be developed for detecting multiple data types simultaneously. Veracity is related with the accuracy of the detection. With the huge data handled in the process, maintaining the accuracy can be sometimes troublesome. Volume is the problem occurring in managing the huge data. Velocity is related to the problems arising from the high rate of the incoming data. Monitoring errors coping with the high speed can cause difficulties in the operation.

All of these big four needs to be taken care of while working on the data from IoT. Thus, more advanced techniques need to be developed in the future for handling these factors.

# Using anomaly detection with IoT Data

Nowadays users are becoming more aware of privacy. The data generated from the IoTis assumed to be safe in the device. However, in reality, there seems to be a different scenario. Recently there was an incident with Samsung TVs being used to spy on the users with cameras and microphones. TheTV is able to record any information or spoken word and transmit the information to another party. Although Samsung ensures that it follows standard encryption for securing the information about their products, the capturing of the information continues, where detection of anomaly can be useful to prevet unauthorized access of the information from the third party. Although anomaly detection can be used in these matters, still it needs to be ensured that the type of data being shared for the right purpose or not.



Fig 3: Using anomaly detection with IoT Data

Source: (Odebol*t al.,* 2018)

Manufacturers need to ensure that the devices they are offering are safe for use to their customers. They need to ensure that the devices will not be hacked and the data will not be intruded or sold to a third party or used for any other purposes than they are intended originally. The amount of data in the anomaly detection in an IoT device may be small in amount. However, more the devices are used in household or at the workplaces; the more data will be used by an individual.

Anomaly detection not only copse up with monitoring the data for smooth operation, but it should also ensure the security of that data as well(Odebol et al*.,* 2018). As there is a huge amount of data to be monitored in the process, the safety should be provided with the growth of the advanced techniques in IoT. The businesses using these advanced techniques should understand this as Samsungdid. This couldhelp them in the development of their productswhile ensuring the safety of data used and the comfort of the userswhile using it. In recent times, the security of data has become a big problem. Thus if the companies are able to assure their customers that the information that they are sharing in the process is safe then better marketing of their products will be possible. For example, Tesla can make their cars safer with the use of more advances technologies introduced in itso that the people could rely on the thought that the car they are using is safe.