BMS
INSTITUTE OF TECHNOLOGY AND MANAGEMENT
Avalahalli, Doddaballapur Main Road, Bengaluru – 560064

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DETAILS OF THE PUBLICATIONS FOR THE ACADEMIC YEAR 2018-19

List of Publications in reputed Journals/Conferences for 2018-19

Title	Publication
A Comprehensive Review on Automatic Diagnosis of Diabetic Maculopathy in Retinal Fundus Images	Springer
Review of Existing Research Contribution Toward Dimensional Reduction Methods in High-Dimensional Data	Springer
A Survey of MTC Traffic Models inCellular Network	Springer
Effectiveness of Recent Research Approaches in Natural Language Processing on Data Science-An Insight	Springer
Qualitative Study of Security Resiliency Towards Threats in Future Internet Architecture	Springer
Multivariate Solutions for Digital Rights Management UsingHardware and Software Methods-Survey	IEEE
Efficacy of Computer Vision Technique to Identify and Extrapolate the Tuberculosis Bacilli	IEEE
Network Traffic Classification Techniques-A Review	IEEE
Prediction of Traffic Density in Internet Offline Mode	IEEE

Details of Publications in International Journals for the academic year 2018-19

Faculty Name	Title	Name Of The Journal	ISSN	Page No
Dr. Anil G N	Secured E-voting System using Etherum Block Chain Technology	International Journal for Scientific Research & Development	pp. 637-640	
	A survey on Energy Efficiency Techniques in	IJIRCCE, Volume 7, Issue 4	ISSN: 2320 9801	

	5G Networks			
Prof. HemaMalini B H	SALES FORECASTING USING RANDOM FOREST AND XG BOOST	Journal of Adv Research in Dynamical & Control Systems, Vol. 11, 02-Special Issue 2019		
Prof. Bharathi R	Prediction and Classification of Cardiac Arrhythmia	IRJET, volume 6,issue 6,june 2019 Volume: 06 Issue: , June 2019	ISSN 2395-0056	
Dr. Anupama H.S	Human Facial Expression Recognition using Machine learning Algorithms	International Journal for Scientific Research & Development	ISSN 2321-0613	01
Dr. Anjan K	Secured E-voting System using Etherum Block Chain Technology	International Journal for Scientific Research & Development	pp. 637-640	
Mr. Muneshwara M.S	Survey of Object Detection using Deep Neural Networks.	International Journal of Advanced Research in Computer and Communication Engineering	ISSN (Online) 2278-1021	02
	Survey on Faster Region Convolution Neural Network for Object Detection	International Journal on Future Revolution in Computer Science & Communication Engineering	ISSN: 2454-4248	03
	Review Paper on Dynamic Mechanisms of Data Leakage Detection and Prevention	International Journal of Computer Sciences and Engineering Vol 7/Issue 2	2347-2693	
	A Survey On Soft Computing Techniques Methods In Agriculture Field	International Journal of Advance Research in Computer Science and Management Studies Volume 7, Issue 4, April 2019	ISSN: 2321-7782	
Prof. Anand R	Comparative Study of Spam Detection in Twitter by Different Approaches of Sentimental Analysis and Machine Learning Algorithm	IJESC, Vol 9, Issue 6, Jun 2019	ISSN: 2250-1371.	

	Automatic Text Summarization	IJESC, Vol 9, Issue 6, Jun 2019	ISSN:2250-1371	
Prof. Jagadish.P	Automatic Text Summarization	IJESC, Vol 9, Issue 6, Jun 2019	ISSN:2250-1371	
	Comparative Study of Spam Detection in Twitter by Different Approaches of Sentimental Analysis and Machine Learning Algorithm	IJESC, Vol 9, Issue 6, Jun 2019	ISSN: 2250-1371.	
Mrs. Ambika G.N	Empowering Agricultural Automation To Optimize Utilization Of Water And Fertilizer By Implementing Internet Of Things (Iot)	EPRA International Journal of Research & Development	ISSN(Online): 2455-7838	04
	Ddos Attack Detection Using Data Mining Cluster Analysis	EPRA International Journal of Research & Development	ISSN(Online): 2455-7838	05
Mrs. Radhika K.R	Framework for novel subspace clustering using search optimization methodology	International Journal of Engineering & Technology	ISSN 2710-2714	06

Publications in International Journals for 2018-19

Human Facial Expression Recognition using Machine learning Algorithms

M. Aishwarya[1] Anupama H. S.[2]
[1,2]Department of Computer Science & Engineering
[1,2]B.M.S Institute of Technology, Bangalore, India

Abstract— The human facial expressions play an important role in recognizing one's intention or mood of that respective person. Facial expressions are the changes that occur on the face based on the internal emotions of the person. This paper focuses on using black and white images for the recognition of the facial expression and also identify the emotions involved in the expression. Here Machine Learning technique is used to train the system to understand one's facial expressions which will in turn help it to judge the state of mind of the person and provide appropriate user experience.
Key words: Facial Expression, Machine Learning, Deep Learning, Emotions, Keras

I. INTRODUCTION

It is well known that a person's nature can be know from their body language, and one of the important parts of this language are facial expressions. Expression adds value to conversations in a way word cannot. In fact, sometimes expressions alone are sufficient to convey information. With technology becoming an essential part of one's life, everyone is spending a growing number of hours with it. There arises a need for technology to be more responsive and adjust or change itself to suite the users changing needs. One step in this direction is enabling the machines to understand one's facial expressions which will in turn help it to judge the state of mind of the person and provide appropriate user experience.

A person can teach machines to learn to recognize the expressions of a human being by showing different pictures of various people and by showing different expressions. Expressions could be angry, sad, and happy and so on. This paper mainly focuses on developing a system which detects the face and recognizes the expressions accordingly. Fig 1 shows the basic structure of recognizing the expressions.

Fig. 1: Basic Structure of Facial Recognition System

II. PROPOSED APPROACH

In this work the FER2013 dataset consisting of 32298 images is used. The dataset consists of 7 different classes of emotions.

Of the total images, 12.9% of them are Angry, 1.5% images are of Disgust, 14.4% images show Fear, 25.3% images are Happy faces, 17.2% of images are of Sad faces, 11.3% of images show Surprise, and 17.4% of images are of Neutral kind.

The data is in csv format with the above 2 columns. Each image is a 48 x 48 sizes and grayscale, so the colour channel is 1. 28709 images are used for training and 3589 images are used for testing. After that values are normalized by dividing it with 255 to get values between 0 and 1.

In this work Keras [7] has been used for the further process of recognition.

With the Keras framework, the neural network used in this work is CNN (Convolution Neural Network). It is one of the main networks which helps in recognizing the images and classification of them and getting better efficiency.

III. IMPLEMENTATION OF CNN IN PROPOSED WORK

This model consists of convolution layer followed by max pool layer. After that it is then add a flatten layer and finally a dense layer to obtain SoftMax output [1, 2]. Of the many activation functions available the Rectified linear Activation unit or ReLU activation is the most widely used activation functions. It is better than the Sigmoid and Tanh activations as these can cause the neural network model to get stuck at a point and take a long time to complete.

It has observed that, proposed approach has run all the models on only one epoch for testing purposes. Accuracy tends to improve on increasing the number of epochs. Table 1 shows the Max Pooling. Max pooling is used as it helps in speeding up the training process without affecting the predictions [5]. It is also a verified and recommended option

```
model = Sequential ()
model.add (Conv2D (64, kernel_size= (3,3), activation =
'relu',
input_shape = input_shape))
model.add (MaxPooling2D (pool_size= (2,2)))
model.add (Conv2D (64, (3, 3), activation = 'relu'))
model.add (MaxPooling2D (pool_size= (2,2)))
model.add (Flatten ())
model.add (Dense (256, activation='relu'))
model.add (Dropout (0.5))
model.add (Dense (num_classes, activation='SoftMax'))
```

Table 1: Snippet of the Code Showing Speeding up the Training Process without Affecting the Predictions

Code: Time: 16 s 162ms/step
Train loss: 1.6362089985419916
Train accuracy: 37.493468947072
Test loss: 1.636460276425931
Test accuracy: 37.80997492420736

It is been observed that by speeding the training process accuracy is obtained is more, which is better than random guessing which gives 14.28%. But when testing on a new image it is observed that the model gives high values to multiple dissimilar emotions. Figure 1 shows the values obtained for dissimilar emotions.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

Survey of Object Detection using Deep Neural Networks

Mrs. Swetha M S[1], Ms. Veena M Shellikeri[2] , Mr. Muneshwara M S[3], Dr. Thungamani M[4]

Assistant Professor, Dept. of ISE, BMSIT & Management, Bangalore, India[1]

Student, Dept. of ISE, BMSIT & Management, Bangalore, India[2]

Assistant Professor, Dept. of CSE, BMSIT & Management, Bangalore, India[3]

Assistant Professor, Dept. of CSE, GKVK, Bangalore, India[4]

Abstract: Object detection using deep neural network especially convolution neural networks. Object detection was previously done using only conventional deep convolution neural network whereas using regional based convolution network [3] increases the accuracy and also decreases the time required to complete the program. The dataset used is PASCAL VOC 2012 which contains 20 labels. The dataset is very popular in image recognition, object detection and other image processing problems. Supervised learning is also possible in implementing the problem using Decision trees or more likely SVM. But neural network work best in image processing because they can handle images well.

Keywords: Object Detection; Neural Network, Artificial Neural Network (ANN), Feed-forward networks, Feedbacks networks

Fig 1: Object Detection using Deep Neural Network

1. INTRODUCTION

Object detection is detecting a specific object from an image of multiple and complex lines and shapes. Object detection is used in face detection, object tracking, image retrieval, automated parking systems [12]. The number of the applications is increasing in number. The main use of object detection is image classification or more precisely image retrieval. For understanding the convolution neural network, deep neural network is important. Papers in deep neural network are studied to understand the concepts of convolution neural network. NIPS paper on Regional based convolution neural network is also referred for further comparison [3]. Object detection is being used in various other fields like defense, architecture etc.

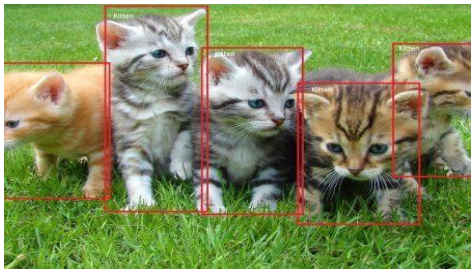

Fig 2: End to End object detection

1.1 Deep Neural Networks: A deep neural network is a neural networks with a certain level of complexity, a neural network with more than two layers. Deep neural networks use sophisticated mathematical modeling to process data in complex ways.A neural network is a technology built to simulate the activity of the human brain specifically pattern recognition and the passage of input through various layers of simulated neural connections. The phrases –deep learning ― is also used to describe these deep neural networks, as deep learning represents a specific form of machine learning

Survey on Faster Region Convolution Neural Network for Object Detection

Mrs. Swetha M S[1]
Assistant Professor, Department of IS&E, BMS Institute of Technology & Management, Yelahanka, Bangalore - 560064, Karnataka,
E-mail: swethams_ise2014@bmsit.in

Ms. Srishti Suman[2]
Department of IS&E, BMS Institute of Technology & Management, Yelahanka, Bangalore -560064, Karnataka,
E-mail: srishtibeg@gmail.com

Mr. Muneshwara M S[3]
Assistant Professor, Department of CSE, BMS Institute of Technology & Management, Yelahanka, Bangalore - 560064,
E-mail:muneshwarams@bmsit.in

Dr. Thungamani M [4]
Associate Professor, Department of CSE,
Assistant Professor, Dept. of CSE, COH UHS
Karnataka,Campus GKVK BANGALORE 560065,
E-mail: thungamani_k@rediffmail.com

Abstract: Convolution Neural Networks uses the concepts of deep learning and becomes the golden standard for image classification. This algorithm was implemented even in complicated sights with multiple overlapping objects, different backgrounds and it also successfully identified and classified objects along with their boundaries, differences and relations to one another. Then comes Region-based Convolutional Neural Networks(R-CNN)which is further more described into two types that is Fast R-CNN and Faster R-CNN. This R-CNN method is to use selective search to extract only 2000 regions from the image and cannot be implemented in real time as it would take 47 sec approximately for each test image. Then comes the fast R-CNNin which changes are made to overcome the drawbacks in R-CNN algorithm in which the 2000 region proposals are not fed to the CNN instead the image is fed directly to the CNN to generate Convolutional feature map. This was then replaced by faster R-CNN which came up with an object detection algorithm that eliminates the selective search algorithm to perform the operation. This algorithm takes 0.2 sec approximately for the test image and we will be using this for real time object detection.So, basically in this paper we are doing research on Faster R-CNN that is being used for object detection method.

Keywords: *Convolution Neural Networks (CNN), Region-based Convolutional Neural Networks(R-CNN),Fast R-CNN,fasterR-CNN*

*****

I. INTRODUCTION

In recent years, with the rapid development of machine learning and deep learning, a number of research areas with respect to these concepts has increased immensely. Along with this there is a continuous improvement of convolution neural networks(CNN). It efficiently improves applications such as face recognition, object detection, object tracking, object relationship etc. Convolution Neural Network is efficiently improving applications such as face recognition, object detection, object tracking, object relationship etc. Object detection is one of the most important applications in the field of deep learning and image processing, and has been the focus of research.

Convolution neural network has made great progress in object detection. Object detection has therefore developed from the single object recognition to the multi-object recognition to real-time object recognition. Since the R-CNN was proposed in 2014, which is based on deep convolutional neural networks, it has developed greatly. Subsequently, lots of improved methods based on the R-CNN, such as Spp-net, fast R-CNN, faster RCNN and R-FCN , emerged in the object detection area. These methods achieved high accuracies, but their network structures are relatively complex. The goal of R-CNN is to take in an image, and correctly identify where the main objects (via a bounding box) in the image. The inputs are images and the outputs will be bounding boxes and the labels for each objects in the images. R-CNNproposes a bunch of boxes in the image and see if any of them actually correspond to an object.R-CNN creates these bounding boxes, or region proposals, using a process called Selective Search . At a high level, Selective Search looks at the image through windows of different sizes, and for each size tries to group together adjacent pixels by texture, color, or intensity to identify objects.R-CNN warps the region to a standard square size and passes it through to a modified version of AlexNet.On the final layer of the CNN, R-CNN adds a Support Vector Machine (SVM) that simply classifies whether this is an object and if it is an object then what is that object. The steps included in R-CNN are:

1. Generate a set of proposals for bounding boxes.
2. Run the images in the bounding boxes through a pre-trained AlexNet and finally an SVM to see what object the image in the box is.

SJIF Impact Factor: 5.705 Volume: 3 | Issue: 8 | August | 2018 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)

EMPOWERING AGRICULTURAL AUTOMATION TO OPTIMIZE UTILIZATION OF WATER AND FERTILIZER BY IMPLEMENTING INTERNET OF THINGS (IoT)

AMBIKA.G.N ,
Assistant Professor, Dept of CSE, B.M.S Institute of Technology and Management
Yelahanka, Bangalore-64

ABSTRACT

India is a place that is known for various climate conditions and adaptable soils. Consistently Indian agriculturists are confronting the issue of sudden rain in their zones with no right climate estimate which prompts harm of the effectively developed yields. The second real issue relating to Indian ranchers is the absence of adequate information about their dirt. The dirt guaging of how the dirt structure is changing step by step because of various climate condition and other outer elements, and which harvest will be ideally suited to be developed in such soil are a portion of the issues normal to the ranchers. This paper makes an endeavor as an evaluation in proposing the arrangement and in the meantime builds up a model of a gadget utilizing IoT for the utilization of the ranchers on Indian rural land. The arrangement proposed will have a unified information server to examine the information and answer to the agriculturist the prudent strides to be taken ahead of time for the wellbeing of the yields. The arrangement proposed will have eco-accommodating vitality administration through the sunlight based plant and wind vitality which make the IoT gadget more versatile and in the meantime makes implementable in any country ranges of India.

KEYWORD: - *Internet of Thing; Wireless Sensor Network; Agricultural Automation*

I INTRODUCTION

The Internet of Things (IoT) is a novel worldview in Information and Communication Technology (ICT) today. IoT is viewed as an overall system of various heterogeneous physical articles: gadgets, vehicles, structures, sensors, actuators, cell phones, Radio Frequency Identifiers (RFID) and different things inserted with hardware, programming, sensors, and system availability that empower these items to gather and trade information for setting up a savvy situation. This ultra present day innovation will make day by day life less demanding by giving savvy mechanical condition. In spite of the fact that the term Internet of Things is broadly utilized today yet it is elusive from the current writing what IoT implies and what are the ramifications of IoT on social, financial and innovation. Regardless of the fluffiness around the term IoT, clearly in not so distant future we will be joined by at whatever time, anything, anyplace substance and administrations that will yield another a method for living.

Subsequently it can be effectively anticipated that will diminish human exertion and furthermore it will guarantee the intelligence of the application zone by enhancing asset use of any condition. The reference model can be spoken to by four layers has distinctive fields of utilization zones , like shrewd home condition, savvy social insurance framework, brilliant horticultural framework and so on. However no such confirmation found towards wide utilization of in agribusiness in underdeveloped nations. Subsequently we need a structure for the same. This report shows a structure for shrewd farming framework. The savvy horticultural framework

SJIF Impact Factor: 5.705 Volume: 3 | Issue: 8 | August | 2018 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)

DDoS ATTACK DETECTION USING DATA MINING CLUSTER ANALYSIS

Ms. Ambika G N
Assistant Professor, Dept of CSE, BMS Institute of Technology and Management, Bangalore-560064

ABSTRACT
DoS/DDoS attacks are detected by invoking a statistical approaches that compares source IP addresses normal and current packet statistic to discriminate whether there is a DoS/DDoS attack. It first collects all resource IP's packet statistics so as to create their normal packet distributions. To detect the DoS/DDoS attack, feature data points are extracted from IP packet statistics dataset and are given as input to the clustering algorithms (K-Means algorithm, Fuzzy-c means algorithm and K-Medoids algorithm) which determines the presence of attacked packets. Analysis is made on the performance of each algorithm.
DDoS attacks are detected with the help of clustering algorithms each giving different false alarm rate, accuracy and execution time depending upon the different input data size.
KEYWORDS: *Denial of Service (DoS), Distributed Denial of Service (DDoS), K-means, Fuzzy c-means and K-medoids Algorithms.*

INTRODUCTION

Network Security is one of the most important issues that can be considered by commercial organizations to protect its information from malicious attacks. The problems of detecting malicious traffics have been widely studied and still as a intrested research topic in the recent decades. Many researches have been designed and implemented an Intrusion Detection System (IDS) to analyze, detect and prevent the malicious activities such as Distributed/Denial of Service Attack (DDoS/DoS).

IDS"s can be classified into two types :

- Misuse Intrusion Detection (MIS) and
- Anomaly-Intrusion Detection (AID).

Misuse detection constructs from known attack behavior based on the pattern matching, which can Be used later as signature-based for attack possibilities. However, Anomaly-Intrusion Detection creates from the long term of normal usage behavior profile of network traffic. In general, IDS"s can be approached by data mining techniques to detect unusual access or attacks to secure internal networks.

Denial of Service attack consists of dangerous threats that are able to disturb a CIA (Confidentiality, Integrity and Availability) services on the network. It consists of a series of attacks able to degrade the network quality service in highly predictable manner. A very common example of this type of attack is Distributed Denial of Service (DDoS) attack. In this instance, multiple computers are being used to send attacks to a victim in the same time during the attack. Zombies are common names given for the computers under the control of the attacker through Handlers. Handlers are the software packages that attacker uses for communication with the zombies. Zombies may or may not be known that they are attacking a victim of network. In general, the attacker acquires the control with zombies by communicating with

International Journal of Engineering & Technology, 7 (4) (2018) 2710-2714

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.15229
Research paper

Framework for novel subspace clustering using search optimization methodology

Radhika K. R [1] *, Pushpa C. N [1], Thriveni J [1], Venugopal K. R [1]

[1] *Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India*
**Corresponding author E-mail:radhika@bmsit.in*

Abstract

Improving the yield as well as the perform of subspace clustering is one of the less-investigated topics in high-dimensional data. After reviewing existing approaches, it seriously felt that there is a need for classification of data points retrieved from a different number of subspace. The proposed study has presented a novel framework that targets to improve the accuracy of subspace clustering by a ddressing the problem associated with the exist of occlusion noise and dimensional complexity. An analytical approach as been proposed to design this framework with more emphasis on outlier minimization followed by obtaining optimal clusters. The technique also introduces a simple search optimization method, which is less iterative and is more productive for identifying the élite outcomes in each iterative step. The study outcome shows superior accuracy with a low rate of error when compared with the conventional approach.

Keywords: Accuracy;Elite outcomes; *High-dimensional Data; Optimal Cluster, Subspace clustering;*

1. Introduction

The emergence of high-dimensional data may observe in most of the trending domains that pose issues over techniques of data mining for throughput and effectiveness. As the reason of sparsity continuously increases in this data type, accommodating clusters is a demanding task [1]. The approaches of cluster ensembling are acquiring the massive amount of attention due to its usefulness in applications such as bioinformatics, data mining techniques and pattern identification.

In comparison with the conventional approaches towards clustering, the cluster ensembling method enables the integrate of many clustering solutions attained via various sources of data and joined into a unified solution to ultimately give a stabilized robust outcome [2]. The application point of view of high-dimensional data is not constrained to one single field, such as face images is a set of high-dimensional data as the pixel number is typically large and the image set for a given face lies about in a linear subspace of 9-dimensions [3]. Other application areas include the image segmentation and representation, disease detection, computer vision, unsupervised learning and motion segmentation [4].

Another example of high-dimensional data occurrence is in the scenario wherein the technology of DNA microarray produces enormous amounts of data involving probes of micrometer scale dimension. In the process of analyzing text files, the dimension number can be equated to the vector of word-frequency [5]. High-dimensional spaces have peculiar characteristics essential for clustering. Clustering is a tool to analyze the data aiming to bind data into multiple homogenous groups [6]. The primary task in data mining and data analysis of high-dimensional data is data clustering. It targets to uncover the structure, which is latently inherent in the data set and is applicable for domains such as image processing, bioinformatics, pattern recognition [7].

Most often, high-dimensional data reside in the low-dimensional structure rather than being uniformly distributed over the ambient space provision. The issue of data separation depending on subspaces, which are underlying and encounter multiple applications in the field of computer vision, image processing, temporal video segmentation and motion segmentation. As data is distributed arbitrarily in a subspace and there are no surrounding centroids, the methods of standard clustering take the benefit of spatial data proximity on individual clusters, which are not permissible in subspace clustering [8].

Subspace clustering is widely applicable for pattern identification and computer vision related applications.It is an extremely challenging role to know that how subspace structures of low-dimensional data exist in the high-dimensional data in the presence of complex noise.The statistical structures of complex noise are highly complicated and are not included in the group of Laplace or Gaussian noise. It is a technique used to perform the segmentation operation on the high-dimensional data that are taken up from many subspaces union.

Subspace clustering initiates the task of finding a subspace belonging to the low-dimensional class in which the data from the individual groups can simultaneously accommodate its subspace structure. The classifications of subspace clustering methods are algebraic methodologies, iterative methods, spectral clustering derived methods and statistical technique of clustering [9]. An extension to the conventional method of clustering is the subspace clustering technique. Apart from this, another reason due to which the struggle for the high-dimensional data continues is the dimensionality curse. In a dataset as the number of dimensions tends to increase, measuring distances, in this case, would be pointless. Hence, an algorithm that can satisfy the need of high-dimensional datasets with the increasing number of sets is required. This manuscript presents one such solution. Section 2 discusses the existing literature where different techniques are discussed for detection schemes used in power transmission lines followed by the discussion of research problems and proposed solution Section 2. Section 3 presents algorithm implementation followed by the discus-

Publications in International Conferences for 2018-19

A Comprehensive Review on Automatic Diagnosis of Diabetic Maculopathy in Retinal Fundus Images

I. S. Rajesh[1(✉)], M. A. Bharathi[1], and Bharati M. Reshmi[2]

[1] Department of CSE, BMSIT & M, Bengaluru, Karnataka, India
is.rajesh081@gmail.com
[2] Department of Information Science and Engineering, BEC, Bagalkot, Karnataka, India

Abstract. Diabetic Maculopathy (DM) is one of the major problems of diabetes mellitus and it is one of the key reasons for the vision problem. It arises due to the leakage of blood from injured retinal veins. The development of DM is moderate and soundless and it is found in 10% of the world diabetic population. If diabetic maculopathy is not noticed in the underlying stage the effect this on macula is irreversible and can prompt vision loss. Therefore, screening of diabetic eye helps in finding diabetic maculopathy at the beginning stage which prevents the vision loss. In this review paper, the anatomy of the human eye and a brief overview of diabetes, diabetic retinopathy and diabetic maculopathy is presented. The literature review of various methods/techniques used for detection of DM in retinal fundus images and the performance metrics used to measure these methods are discussed in details. Issues involved in DM detection are also mentioned in this paper.

Keywords: Retinopathy (DR) · Diabetic maculopathy (DM) · Optic disc (OD) Hard exudates (HEs) · Blood vessels (BVs)

1 Introduction

The human eye is a fundamental body part associated with vision [1]. Figure 1 demonstrates the retinal anatomical structure. The lens of the human eye helps in focusing light beams onto the retina and iris decides how much light is let into the eye. Optic nerve associates the eye to the cerebrum and conveys the electrical signals framed by the retina to the visual cortex of the mind.

The retina is a sensitive layer situated at the posterior of the eye. Uncountable photoreceptors present in the retina catch the light beams and change them into electrical signals. These electrical signals drive to the brain along the optic nerve where they changed into pictures. Figure 2 exhibits the structure of the retina and its primary parts. The optic nerve is the brightest region of the retina where Blood Vessels (BVs) begin. BVs are responsible for supply of nutrition and oxygen to the retina and it must be normal for the proper working of the retina and macula. The central portion of the macula is called fovea [2].

S. M. Thampi et al. (Eds.): SIRS 2018, CCIS 968, pp. 410–420, 2019.
https://doi.org/10.1007/978-981-13-5758-9_35

Review of Existing Research Contribution Toward Dimensional Reduction Methods in High-Dimensional Data

International Conference on Computer Networks and Communication Technologies
pp 409-419 | Cite as

- P. R. Ambika (1) Email author (ambikatanaji@gmail.com)
- A. Bharathi Malakreddy (2)

1. Department of CSE, City Engineering College, , Bengaluru, India
2. Department of CSE, B M S Institute of Technology and Management, , Bengaluru, India

Conference paper
First Online: 18 September 2018

Part of the Lecture Notes on Data Engineering and Communications Technologies book series (LNDECT, volume 15)

Abstract

Dimensionality Reduction is one of the preferred techniques for addressing the problem of the curse of dimensionality associated with high-dimensional data. At present, various significant research works have been already carried out toward emphasizing the dimensional reduction methods with respect to projection-based, statistical-based, and dictionary-based. However, it is still an open question to explore the best technique of dimensional reduction. Hence, we present a compact summary of our investigation towards finding the contribution of existing research methods of dimensional reduction. The paper outlines most frequently adopted techniques of dimensional reduction. At the same time, this survey also emphasizes on exploring the problems addressed by the present researchers with an aid of their own techniques associated with both advantages, limitations, and addressing the issues of the curse of dimensionality. The survey also introduces the latest research progress and significant research gap associated with the existing literature.

Keywords

High-dimensional data Dimensional reduction

Springer Link

A Survey of MTC Traffic Models in Cellular Network

International Conference on Computer Networks and Communication Technologies
pp 681-693 | Cite as

- T. N. Sunita (1) Email author (sunita.neelagiri@gmail.com)
- A. Bharathi Malakreddy (1)

1. Department of Computer Science, B.M.S. Institute of Technology, , Bengaluru, India

Conference paper
First Online: 18 September 2018

Part of the Lecture Notes on Data Engineering and Communications Technologies book series (LNDECT, volume 15)

Abstract

Machine-Type Communicating (MTC) Devices (MTCD) are usually wireless devices, for example, sensors, actuators and smart metres which can talk with each other through exchanging data and take decisions with little or no human intervention. Cellular networks are considered to be one of the best technologies for accommodating MTC. The characteristics generated by MTC traffic are completely different from Human-to-Human (H2H) communications. There will be no control on the increasing number of MTCDs and because of which volume of MTC traffic keeps on increasing. In this paper, we make a comprehensive survey on MTC traffic issues over cellular network and solutions to improve the MTC over cellular network. This paper provides a brief overview of 3GPP standards supporting MTC. We also survey MTC traffic issues in heterogeneous networks consisting of cellular networks, capillary networks. Finally, we review recent standard activities and discuss the open issues and research challenges.

Keywords

M2M Machine-to-machine Machine-type communication Traffic issues Traffic models

References

1. Niyato, D., Wang, P., Kim, D.I.: Performance modeling and analysis of heterogeneous machine type communications. IEEE Trans. Wireless Commun.

Multivariate Solutions for Digital Rights Management Using Hardware and Software Methods-Survey

S A Nihitha[1] Navya M[2] Anjan K Koundinya [3] Shobha G[4] Hrishikesh Dewan[5]
1,2,4 *Department of Computer Science, R V College of Engineering, Bengaluru, India*
[3]*Dept. of Computer Science & Engineering, BMSIT&M, Bengaluru, India*
[5] *Co-Founder, CTO at Ziroh Labs, Bengaluru, India*
E-mail: {[1]nihitha.sa, [2]navinikki, [3]annjank2}@gmail.com,
[4]shobhag@rvce.edu.in, [5]hrishikesh@ziroh.com

***Abstract*— Digital Rights Management is a system which is established to protect the secure content from eavesdroppers. The secure content has to be transmitted from the service provider to the client by protecting it from the unauthorized users. To implement remote control protection of the secure content, the protection must be persistent and should stay with the content. This paper gives a brief overview about the existing solutions of DRM. The existing multivariate solutions present in hardware and software is discussed. A comparative study between the hardware and software solutions mentioned highlights the pros and cons of both the solutions.**

Keywords—Digital Rights Management,Digital Content,security,software methods,hardware methods

I. INTRODUCTION

Digital Rights Management (DRM) technology has emerged to protect and manage the commerce, intellectual property ownership and confidentiality rights of digital content creators and owners, as content travels through the value chain from creator to distributor then to the consumer and from consumer to other consumers [1]. DRM offers a secure framework for digital content distribution and provides a marketplace to implement previously unimaginable models. DRM is a popular term for field like content management, which came into being in the mid-1990s, when content providers, technology firms and policy makers began to confront the effect of ubiquitous computer networks on the distribution of copyrighted material in digital form [2]. So far, there is no unique or standard definition for DRM. In fact, depending on
the outlook of the individual defining the term, it can have a number of connotations. Slowinski [3] defines DRM as a set
of actions, procedures, policies, product properties and tools that an entity uses to manage its rights in digital information according to requirements. DRM is an attempt to provide remote control of the digital content provided by the owner.
Content protected by DRM includes documents processing such as Microsoft word, PDF, AutoCAD files, E-books etc., video formats such as CSS employed in DVDs, internet music like Apple's FairPlay, Napster, television content, streaming video content.

The digital content has to be monitored regularly and restrictions must be provided on the use of the digital content after it has been delivered. persistent production is required so that the users do not share and copy the content. Basically, DRM is the chain of hardware and software services and technologies governing the authorized use of digital content and managing any con sequences of that use throughout the entire lifecycle of the content [4]. DRMmay also be referred as "content management systems" (CMS) or "content/copy protection for removable media" (CPRM). Digital millennium copyright act(DMCA) is a law designed to increase copyrights holders' rights and interfere with users' ability to access content. DRM implements fair use principles that allows individuals to interact with content to promote learning, equity, culturalproductions, and innovations between the consumers and the content owners.

DRM system requires persistent content protection which implies that protection has to stay with the content. For example, when a digital content in the form an MP3 or a movie is shared to a user with the help of cryptographic techniques, there's no guarantee that the content is secure because the user can save, copy and share the content in a free form. Those is a breach in the security of the DRM system existing. Therefore, the digital content has to be protected from unauthorized interception and modification and to process protected content and enforce rights/policies for that content it uses tamper resistant mechanisms. This can be implemented by various techniques in hardware or in software or both for example, a trusted model or a cryptographic mechanism etc.

II. LITERATURE SURVEY

- An architecture called eTRON has been proposed as a necessary security measure for cyber-physical

ISBN: 978-1-5386-6078-2

Generalized Adaptive Security for Computer Systems

H S Srihari[1], Anjan K Koundinya[2], G N Srinivasan[3]

***Abstract*— Developing technologies like the Internet of Things (IoT) and the advent of Big Data Analytics have posed newer threats to security and consequently increased the security threat significantly and necessitated a more sophisticated approach to deal with the multitude of devices and systems which connect and communicate online. Thus, the earlier goal of building a robust security solution for a system or application is no longer a valid solution. Instead, the systems these days demand are adaptive solutions which will automatically detect and configure itself for the changing situations. The solution to this challenge needs the applications of soft computing technologies like learning systems and Artificial Intelligence to learn, predict, prevent and defend any unforeseen security threats. This is the goal of the adaptive security mechanism and this paper proposes a model to dynamically change for the security solution for the scenario and the application demand.**

***Index Term*—adaptive security; threat analytics; Machine learning security; aspect-oriented programming**

I. Introduction

The advent of interconnected systems with a multitude of devices and more importantly the connection between these IoT devices and big data has resulted in the need for a security system of incident response which must be modified to adopt the continuous evaluation method which is far more reliable than the traditional approach.

To compete with adaptive products, conventional security software requires extensive self-aware behaviour monitoring for normal system and software actions or, conversely, defining and logging them as out of the ordinary. Adaptive security provides finer-grained controls to adapt to changes in the network and computing environment, as well as dashboards for better monitoring. The software autonomously blocks behaviors but must have the ability to allow for human intervention. Security staff are notified and alerted of new behaviors, which they can selectively allow, to enable continued functioning in the changing environment.

Since many applications are too complex to be solved ad hoc, mechanisms need to be developed to deal with security as a separate aspect. However, the implementation of security mechanisms often interacts or even interferes with the core functionality of the application. This results in tangled, unmanageable code with a higher risk of security bugs. It is imperative that organizations shift their security mindset from incident response" to „continuous response", where systems are assumed to be compromised and require continuous monitoring and remediation.

H S Srihari is with Dept of Computer Science and Engineering, RV College of Engineering, Bengaluru, India (Email: hssrihari98@gmail.com)
Anjan K Koundinya is with Dept of Computer Science and Engineering, BMS Institute of Technology and Management, Bengaluru, India (Email: anjank@rvce.edu.in)
G N Srinivasan is with Dept. of Information Science and Engineering, RV College of Engineering, Bengaluru, India

II. Design and Architecture

The design approach to solve an enterprise security issue can be largely done in 2 ways:

A. Use of complex adaptive system
B. Aspect Oriented Programming

A. Complex Adaptive System

The new approach to information security architecture has to try to mimic a complex adaptive system that can adjust to constantly emerging and changing security threats. This is the essence of Adaptive Security Architecture, to serve as the enterprise security immune system.

This can be achieved by developing an Adaptive Security Architecture (ASA), which aims to contain active threats and to neutralise potential attack vectors. Gartner defines an ASA along four security capabilities:

- **Preventive capability**: This is the set of policies, products and processes that prevent a successful attack. Preventive capabilities protect information from unauthorized modification, destruction, or disclosure, whether accidental or intentional.
- **Detective capabilities**: These are the controls designed to identify attacks that have evaded the preventive measures and reduce the threat amplification. Detective capabilities provide visibility into malicious activity, breaches and attacks. These controls include logging of events.
- **Retrospective capabilities**: These provide a way to shrink the attack surface, slow the rate of the attack and reduce remediation time. Response/Retrospective capabilities provide the process, procedures and technology necessary to take appropriate action in response to a variety of cybersecurity events. These include forensic investigations, network changes, remediation changes and automated response capabilities.
- **Predictive capabilities:** These capabilities enable the organisation to predict attacks, analyse security trends and move from a reactive to a proactive security posture. Predictive capabilities provide security intelligence from the monitoring of internal and external events to identify attackers, their objectives and methods prior to the materialization of attacks.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Efficacy of Computer Vision Technique to Identify and Extrapolate the Tuberculosis Bacilli

Vishakha Yadav, Thippeswamy G
Department of CSE, BMSIT
Bengaluru, India

***Abstract*— Globally, Sputum smear microscopy using the Ziehl-Neelsen (ZN) stain is in place for diagnosing active Mycobacterium Tuberculosis bacilli. The competent interpretation may suffer due to the rigorous nature of the test, which ideally restrains the diagnosis process. In conventional microscopic examination, sensitivity is the crucial determining variable. The sensitivity parameter values fluctuate between 20% and 80%. Automated detection of TB bacilli could hasten diagnosis, enhance quantitative classification and reduce errors.**

The digital microscopy assisted screening and detection of TB is a great boon in the current technology driven era. Adequate number of the digital images can be acquired in any given time framework. The broader section of images will be vital and significant in computer-assisted detection of TB. Proficient diagnosis will be independent of resource constrained environment.

Numerous Computer vision techniques have been fascinating the researchers' over many decades. The advent of computational infrastructure has made it possible to address the various processing complexities of computer vision algorithms. ICT based environment will be conducive in the treatment and review of TB diagnosis.

AI can definitely assist physicians to make better clinical decisions or even replace human judgement in certain functional areas of healthcare.

I. INTRODUCTION

In the developing countries, tuberculosis (TB) is the primary and foremost cause of death in the infectious disease category. Developed countries have almost eradicated it.

Nonetheless, TB remains as the ninth leading cause of death worldwide [1] (second only to HIV/AIDS) [12]. Screening and diagnostic is dependent on the assortment of healthcare epidemiological settings. Cost-effective screening seeks Genesis of new diagnostic tools, which is conducive in providing worthwhile solution. Nevertheless, in several developing countries the viability and cost-effectiveness of such tests looms uncertainty [3]. Normalization in various clinical diagnoses is the need of the hour. Traditional and molecular microbiologic methods lack sensitivity [4].

Given the nature of the disease, the microbiological identification of tuberculosis is quite perplexing. The paucibacillary pattern of the bacilli may not always help in concluding the bacilli of TB. With the diagnostic advancements, it is still challenging to conclude about the presence of Tuberculosis as the suspect may have very few bacilli [4].

In developing countries, the constrained sources of diagnostic settings lead to inadequate investigation often. Therefore, an appropriate program could expose several undiagnosed cases. By improving upon the screening program approaches, standards and practices, we can gain confidence of thorough investigations and figure out the risk factors associated with the identified, suspected patients.

In countryside set up availability of requisite resource health personnel and definite diagnostic routines, staples the vital investigative decision making process [3]. In the year 2017, India, accounted for about a quarter of the world's TB cases. The demographics of plausible TB cases were populated through varied channels [2]. Revised National TB Control Programme (RNTCP) is an on-going Centrally Sponsored Scheme, being implemented under the umbrella of National Health Mission. An Information and Communication Technology approach is conducive in manoeuvring such national programmes. The crux of the RNTCP programme is Active Case Finding (ACF) drive. It concentrates on diversely vulnerable populations. The quintessential objective is to primarily discover the passive cases and scrutinize the chronic factors associated with probable passive to active TB cases [2].

As per the National Strategic Plan 2017-2015, the government of India is aiming at the eradication of TB by 2025. Various measures are being manifested to reinforce the disease investigation for better assessment of the liability. Significant Investigation must comprise of:

1. Initial case discovery
2. Consolidation of examination and documenting the concerning remarks
3. Collating and Reporting the reduction in the active cases
4. Enforce preventive measures in place
5. Methodical categorization of the risk severity Drug defence mechanism is the basis for the categorization of patients.

The TB control guidelines - 2016 of India, categorizes patients in to either of the drug-sensitive TB, Mono, Poly, Multi and Extensively Drug Resistant TB. The Revised

978-1-5386-7705-6/18/$31.00 ©2018

NETWORK TRAFFIC CLASSIFICATION TECHNIQUES-A REVIEW

Yoga Durgadevi Goli
Department of Computer Science and Engineering
BMSIT&M
BANGALORE, INDIA
durgadevigy@bmsit.in

Dr. Ambika R
Department of Electronics and Communications Engineering
BMSIT&M
BANGALORE, INDIA
ambikar@bmsit.in

***Abstract*— With the growth in the amount of devices associated with the internet; the data that is getting circulated over the internet is also increasing. It is an undeniable fact that this data has significant presence for individuals as well as for organizations. A network needs to handle this massive amount of data traffic which contains malicious data as well. Therefore, it is very essential to distinguish between normal and abnormal traffic by analyzing the network traffic. A number of network traffic classification techniques are available. The researchers are trying to find the traffic classification techniques that do not depend on port numbers or that do not read the packet payload contents. In this study, an analysis of various traffic classification techniques and the application of several Machine learning techniques for traffic classification is carried out. This survey paper also presents a brief review of various machine learning techniques for traffic classification.**

Keywords— Network security, Network Traffic, Traffic classification, Machine Learning.

I. INTRODUCTION

With the increased use of Internet, the quantity of devices that are linked to the Internet is increasing day by day. As the quantity of devices is growing, more data is getting circulated on the internet which contains malicious data as well. A network should handle this massive amount of data traffic and needs to identify malicious data in the data traffic. In order to perform this, there is a need of monitoring the network flow and detect any network intrusion. It is required because of numerous security threats that the people encounter are increasing day by day. Identifying numerous network attacks, especially unanticipated attacks, is also an inevitable practical problem. An attack detection system developed for this purpose can be used. An Intrusion Detection System (IDS) is one such system which is used to generate an alert by trying to discriminate between malicious or normal traffic by observing network traffic over the internet linked devices. It can also identify an attack, which may be an enduring attack or an intrusion that has previously happened.

The IDSs are generally classified into two categories: Signature-based detection and anomaly-based detection. Signature based detection uses a latest database of known attack's signatures to detect incoming attacks. Anomaly-based detection uses a classifier which categorizes the given data into normal and abnormal data. [1].

Based upon where they monitor for intrusive behavior, IDSs are classified into two types: Network based and Host based. A network based IDS (NIDS) detects intrusions by observing traffic over the devices that are connected to the network. A host based IDS (HIDS) recognizes intrusions by monitoring activities related to a specific host.

This survey paper focuses on various methods for network traffic classification, with special emphasis on machine learning methods and their descriptions.

The remaining part of the paper is organized as follows: Section II describes the elementary information about various techniques for network traffic classification. Section III presents the basic concepts of Machine Learning. Section IV focusses on machine learning techniques for Network Traffic Classification. Finally, the conclusion is provided in section-V.

II. RELATED WORK

Recently, many investigators have proposed various approaches to classify network traffic. In this section, we discuss few techniques for network

978-1-5386-7709-4/18/$31.00 ©2018 IEEE

Insights of Effectiveness for Recent Research Approaches in Natural Language Processing on Data Science

Shruthi[1] and Dr.Suma Swamy[2]

[1]Assistant Professor, Department of Computer Science & Engineering
BMSITM, Bengaluru, India
shruthij.research@gmail.com

[2]Professor, Department of Computer Science & Engineering
SMVIT, Bengaluru, India
sumaswamy_cs@sirmvit.edu

Abstract. With the exponentially increasing size and complexity of the data in present time, quality of data has become a major concern with respect to data analytics. The potential capability of Natural Language Processing (NLP) is already known and being harnessed by various researchers to evolve up with some significant analytical process. However, there is lesser number of research works emphasizing on applying NLP over the data with complexity reported in current times in the area of big data. Therefore, the primary contribution of this manuscript is to review the most recent work towards NLP based approaches for data analysis where input data could be either text or non-textual too. The secondary contribution is to gauge the level of effectiveness from the existing research approach with NLP-based practices towards leveraging better data quality in data science.

Keywords: Data Science, Natural Language Processing, Text Mining, Analytics, Big Data, Cloud, Clustering

1 Introduction

The sole purpose of Natural Language Processing (NLP) is to extract significant and highly logical information for any given textual data [1]. Basically, it comes in a category of artificial intelligence that offers potential capability of interactive communication bridge between humans and computers [2]. There are various applications of NLP **for** e.g. summarization, fighting spam, machine translation, extracting information, answering question autonomously, etc. Although, it is a widely known fact that NLP is essentially meant for applying on data but very least importance is given to the complexities associated with the data. At present , there is an exponential rise of data to multi-fold which not only poses a problem in storage but also in performing analytical operation on it [3]-[5]. The presence of cloud environment assists in distributed data storage and retrieval as well as it is characterized by some good analytical tools too [6]-[10]. However, there are many

adfa, p. 1, 2011.

Qualitative Study of Security Resiliency Towards Threats in Future Internet Architecture

M. S. Vidya[1(✉)] and Mala C. Patil[2]

[1] Department of Computer Science and Engineering,
BMSIT and M, Bengaluru, India
rvidyapai@bmsit.in
[2] Department of Computer Science, COHB,
University of Horticultural Sciences, Bagalkot, India
Malapatil2002@yahoo.co.in

Abstract. With the consistent evolution of distributed networks and cloud computing, the communication process of existing Internet architecture are not at par to offer comprehensive security; thereby fails to cater up the dynamic web security demands of online users. This leads to the evolution of Future Internet Architecture (FIA) that claims of enhanced security system. However, a closer look into both existing web security and security of existing FIA projects shows that there are enough security loopholes in both that demands a novel security solution. Therefore, this paper contributes to investigate the effectiveness of existing web security approaches as well as security approaches of FIA in order to explore the open research issues. The finding of the study shows that there is a significant research gap that demands extreme improvement of existing web security in order to fit for secure communication in FIA.

Keywords: Web security Internet Future internet architecture
Attacks · Vulnerability Denial of service Distributed security
IoT .

1 Introduction

The existing version of Internet architecture has been serving since 40 years for all communication needs and has also contributed many successful implementation of communication protocols [1]. However, with the rising demands of distributed network system, they are no more potential especially with respect to security factor. There are various reasons behind this viz. (i) they use IP network that is host centric and cannot cater up any form of distributed communication system, which is the need of present age, (ii) the policy of IP address is encountering exhaustion with the exponential rise of users, (iii) no inclusion of security attributes (except IPv6 that offers distinct and unique IP addresses to promote security), (iv) highly non-flexible posing difficult to incorporate new operation [2]. Therefore, web security has become one of the essential concerns among the network communities [3–5] and this leads to the formation of Future Internet Architecture (FIA) [6]. One of the essential part of FIA is its security

R. Silhavy et al. (Eds.): CoMeSySo 2018, AISC 859, pp. 274–284, 2019.
https://doi.org/10.1007/978-3-030-00211-4_24

Prediction of Traffic Density in Internet Offline Mode

Bhal Chandra Ram Tripathi
Department of Computer Science and Engineering
Global Academy of Technology
Bengaluru, India
Email: bhalchandra.chandra7@gmail.com

Prof. Krishna Prasad R.
Department of Computer Science and Engineering
Global Academy of Technology
Bengaluru, India
Email: rkp_rgp@yahoo.co.in

Dr. Satish Kumar T.
Department of Computer Science and Engineering
BMS Institute of Technology
Bengaluru, India
Email: satish.savvy@gmail.com

Abstract- Today google maps is the defacto app used for the direction and traffic analysis. The proposed work illustrates the solution to a problem of finding traffic between any two points. The technique adopted in this work is predictive form of Machine Learning and the analysis and the prediction of the traffic is done. The use of machine learning method enables traffic analysis in offline mode much easier and expand the span of maps working. The traffic data is collected from users, through API "here" and several other API's to collect the data. These data are used to predict the traffic when needed. The application will behave as a normal direction provider on Internet Connectivity but as soon as the user goes offline, the real use of application prevails.

Keywords: Artificial Intelligence, Machine learning, Prediction

Introduction

It is quite evident that most people today use the map services extensively provided by the google for location tracking or to find the utility centers in online mode. Real time map providing organizations are performing less prediction for producing the result. The API such as google collect the traffic data from the user itself for analyzing and correspondingly respond to users by conglomerating and transforming into result as needed by other users. If there are less no. of data receiving over an area to the API from user, then it is termed as less traffic zone and if more density of data is received over an area from user then it is termed as more traffic zone. The real time API are fully dependent on the users from retrieval to transformation of data to result. The amount of prediction used by the real time API is very less and done only if a negligible amount of data from requested area is received such that not fit to produce an approximate result. The real time API are the best to produce the traffic and the path between any two points in online mode but fail to sustain the result in offline mode. The real time API if run in offline mode will produce a minimum accuracy traffic path, which is unreliable. The proposed algorithm is an attempt to overcome the rough edges of the real time API during offline mode traffic and path determination. The proposed algorithm works on stored data rather than on real time data by performing the extensive prediction and data analysis. The data is collected through the developed API, "here" API, supporting devices for the analysis and stored as raw in the memory. The data is fetched from the memory based on the request and goes through multi stage algorithm to produce the transformed result. The solution solves the problem of finding traffic between two points in offline and performing activities similar to online in offline.

978-1-5386-6894-8/18/$31.00 ©2018 IEEE