ISSN (Print): 2321 -4058, (Online): 2321 -4392

The International Journal of Advances in Computer Science and Cloud Computing (IJACSCC)

Volume No. 12
Issue No. 1
January - April 2024

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN (Print): 2321 -4058, (Online): 2321 -4392

The International Journal of Advances in Computer Science and Cloud Computing (IJACSCC)

Aim & Scope

The International Journal of Advances in Computer Science and Cloud Computing (IJACSCC) is a peer reviewed Journal in the field of Computer Science and Engineering. IJACSCC is an international forum for scientists, researchers and engineers involved in all aspects of Computer Science and Cloud Computing to publish high quality, referred papers. The Journal offers survey and review articles from experts in the field, promoting insight and understanding of the state of art, and latest trends in the field. The content include original research and innovation ideas, applications from all over the world. All published papers are also available freely with online full-text content.

ISSN (Print): 2321 -4058, (Online): 2321 -4392

Editor-in-Chief

Publication and Distribution Head

Reviewers

ISSN (Print): 2321 -4058, (Online): 2321 -4392

International Journal of Advances in Computer Science and Cloud Computing

(Volume No. 12, Issue No. 1, January - April 2024)

Contents

ISSN (Print): 2321 -4058, (Online): 2321 -4392

Drought Prediction using Machine Learning Algorithm

[1]Aishwarya M Iyengar, [2]Deepika K, [3]Kanthi Utkarsha Bharat, [4]Mitaigar Divya, [5]Vaidehi M

[1,2,3,4]Student, Department of Information scienceand Engineering, DayanandaSagar College of Engineering, Bangalore, India

[5]Faculty, Department of Information scienceand Engineering, DayanandaSagar College of Engineering, Bangalore, India

E-mail: [1]amiyengar97@gmail.com, [2]deepikahathwar@gmail.com, [3]utkarshakanthi97@gmail.com, [4]divyamitaigar@gmail.com, [5]dm.vaidehi@gmail.com

ABSTRACT

Drought prediction is of critical importance to early warning for drought managements. This work provides a synthesis of drought prediction based on statistical, dynamical, and hybrid methods. Statistical drought prediction is achieved by modeling the relationship between drought indices of interest and a suite of potential predictors, including large-scale climate indices, local climate variables, and land initial conditions. Dynamical meteorological drought prediction relies on seasonal climate forecast from general circulation models (GCMs), which can be employed to drive hydrological models for agricultural and hydrological drought prediction with the predictability determined by both climates forcing and initial conditions.

SVM model has been applied for classification of real time data obtained from Meteorological department. Here we considered parameters like maximum rainfall, minimum rainfall and precipitation. The prediction is base on the dataset collected for a period of ten years.

Challenges still exist in drought prediction at long lead time and under a changing environment resulting from natural and anthropogenic factors.

Keywords- Drought, Support Vector Machine(SVM),Support Vector Classification (SVC),Confusion Matrix, Machine learning

I. INTRODUCTION

One of the major challenges of agricultural systems is how to mitigate the impacts of droughts. Droughts impact agricultural systems economically as well as environmentally. With respect to economic impacts, droughts damage agricultural production, and can cause economic damage to industries connected to agricultural production, in addition to causing unemployment as a result of reduced production.

From an environmental perspective, droughts can deprive crops and soils of essential precipitation as well as increase the salt content in soils and irrigation systems. To mitigate the impacts of drought an effective and timely monitoring system is required.

Effective monitoring of droughts can aid in developing an early warning system. An objective evaluation of the drought condition in a specific area is the first step for planning water resources in order

to prevent and mitigate the impacts of future occurrences of drought. The evaluation and forecasting of drought is made possible by the use of drought indices.

The evaluation and forecasting of drought is made possible by the use of drought indices. Application like drought prediction depends on the measurement of the environmental factors that are based on recorded data. Severity of drought prediction using the traditional methods is complicated by the variant phenomenon of natural parameters. Efficient drought prediction is not possible in traditional methods as they lack the real time information.

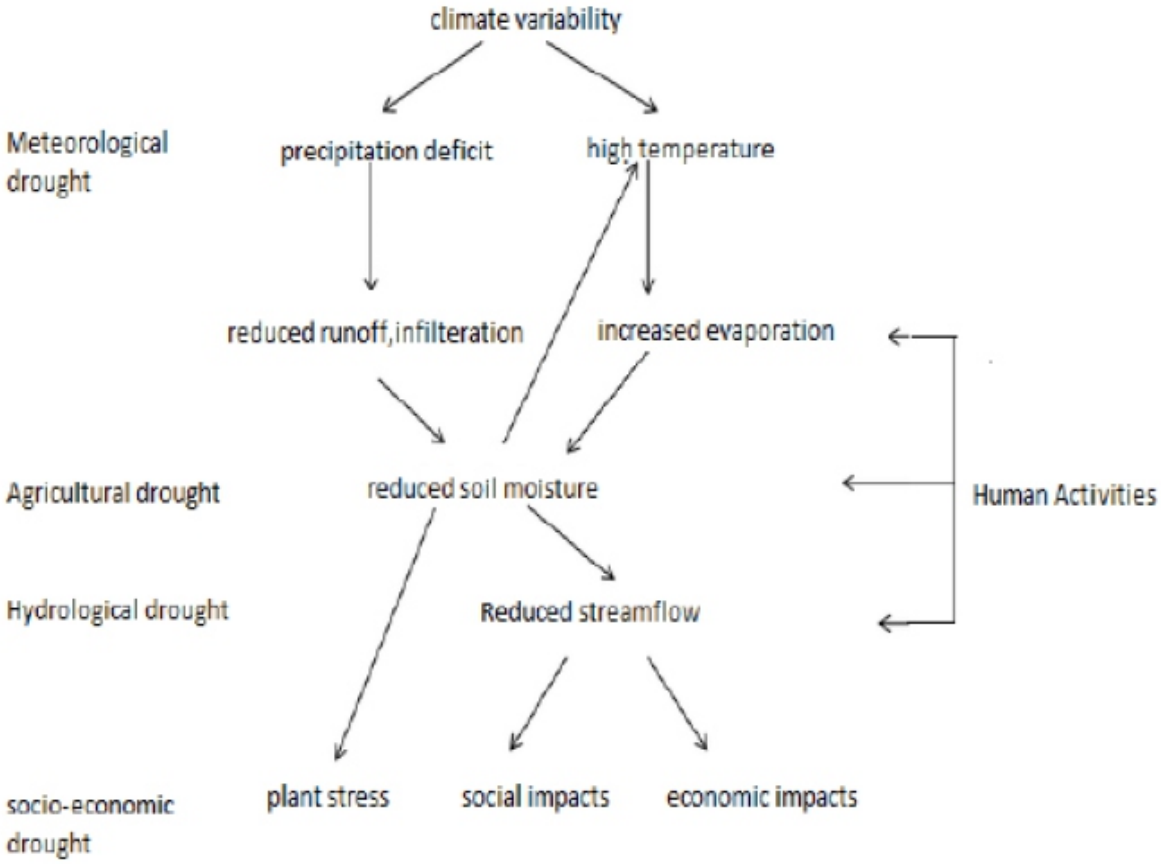


Figure1-Interaction of different variables in hydrological cycle during drought

The support vector machine (SVM) has been applied to drought prediction and it typically yields good performance on overall accuracy. However, the prediction accuracy of the drought category is much lower than that of the non-drought and severe drought categories.

II. DATA SET

One of the toughest issues to resolve in deep learning has nothing to do with neural networks; it's the matter of obtaining the correct information within the right format.

Getting the correct information suggests that gathering or distinguishing the information that correlates with the outcomes you would like to predict; i.e. information that contains an indication regarding events you care regarding. the information must be aligned with the matter you're trying to resolve. Kitten footage don't seem to be terribly helpful once you're building a facial identification system. validating that the information is aligned with the matter you ask for to resolve should be done by a knowledge human.

If you are doing not have the correct information, then your efforts to create AI resolution which should come back to the information assortment stage.

The right finish format for deep learning is mostly a tensor, or a multi-dimensional array. therefore, information pipelines engineered for deep learning can typically convert all information – be it pictures, video, sound, voice, text or statistic – into vectors and tensors to that algebra operations are often applied. That information oft must be normalized, standardized and clean to extend its utility, and people where all steps in machinelearning ETL. Deep learning offers the DataVec ETL tool to perform those information preprocessing tasks.

Deep learning, and machine learning additional typically, wants an honest coaching data set to figure properly. Assembling and constructing the coaching set – a large body of known information – takes time and domain-specific data of wherever and the way to collect relevant info. The coaching set acts because the benchmark against that deeplearning nets are trained. Hence, they learn to reconstruct before they're unleashed on information they haven't seen before. At this stage, knowledgeable humans got to notice the correct data and remodel it into a numerical illustration that the deep-learning algorithmic program will perceive, a tensor. Building a coaching set is, in a sense, pre-pre-training. Machine learning generally works with 2 data sets: training-set and test set. All three ought to at random sample a bigger body of data. The first set of data is that the network a neural network.

The second set is your test set. It functions as a seal of approval, and you don't use it till the top. when you've trained and optimized your knowledge, you check your neural internet against this final sampling. The results it produces ought to validate that your internet accurately recognizes images or acknowledges them at least 'x' percentage of them.

If accurate predictions are not obtained, then the coaching set must be retrained. Here we investigate the hyper parameters accustomed to tune the network. This process enhances the quality of knowledge the pre-processing technique.

III. DATA CLEANING

In drought severity prediction data cleaning is the initial step that has been done by collected the required real time dataset which contains the parameters for predicting drought using some of the machine learning algorithm. Data preprocessing is a very important and quite underestimated step in Machine Learning pipelines. It provides cleaned and relevant datasets which then can be used in further steps like classification or regression. The data which is fed to the SVM classifier to predict if a given image segment belongs to foreground or background. After collection of measurement data such as maximum temperature, minimum temperature, precipitation and rainfall, data cleaning is done to remove irrelevant data, incomplete data, missing data so that it can be fed into the SVM which gives the result if the drought has occurred.

IV. METHODOLOGY

Data collection is done which contains the parameters required for predicting drought like minimum temperature, maximum temperature, precipitation and rainfall. After that the incomplete data, inaccurate data, inconsistent data, missing data, duplicate data are all resolved by using data cleaning. Data cleaning is done for the data which is irrelevant and the data which is more frequent is used.

4.1Support Vector Machine (SVM):

In machine learning, support-vector machines are supervised studying models with associated gaining knowledge of algorithms that analyze facts used for classification and regression analysis. Given a fixed of education examples, every marked as belonging to one or the other of two classes, an SVM education algorithm builds a version that assigns new examples to 1 category or the other, making it a non probabilistic binary linear classifier (although strategies inclusive of Platt scaling exist to apply SVM in a probabilistic category setting).

An SVM model is an illustration of the examples as factors in space, mapped so that the examples of the separate categories are divided through a clear gap which is as wide as possible. New examples are then mapped into that identical area and predicted to belong to a category based totally on which aspect of the space they fall.

Further to acting as linear category, SVMs can efficaciously carry out a non-linear classification using what's known as the kernel trick, implicitly mapping their inputs into excessive-dimensional function spaces.

More formally, a support-vector machine constructs a hyperplane or set of hyperplanes in an excessive- or countless-dimensional space, which can be used for classification, regression, or different tasks like outlier's detection. Intuitively, a good separation is finished by using the hyperplane that has the most important distance to the closest education-facts point of any elegance, because in general the larger the margin, the lower the generalization mistakes of the classifier where as the unique problem may be stated in a finite-dimensional space, it frequently takes place that the units to discriminate aren't linearly separable in that space.

Because of this, it changed into proposed that the unique finite-dimensional area be mapped into a far better-dimensional space, possibly making the separation simpler in that space. To maintain the computational load reasonable, the mappings utilized by SVM schemes are designed to make certain that dot products of pairs of input statistics vectors can be computed easily in phrases of the variables in the authentic space, via defining them in phrases of a kernel function k (x , y) ,selected to in shape the hassle. The hyperplanes in the higher-dimensional space are defined as the set of factors whose dot product with a vector in that space is consistent, wherein such a fixed of vector is an orthogonal (and for that reason minimal) set of vectors that defines a hyperplane.
H1 in the below figure does not separate the class.
H2 does, but only with a small margin.
H3 only separates the small margin.

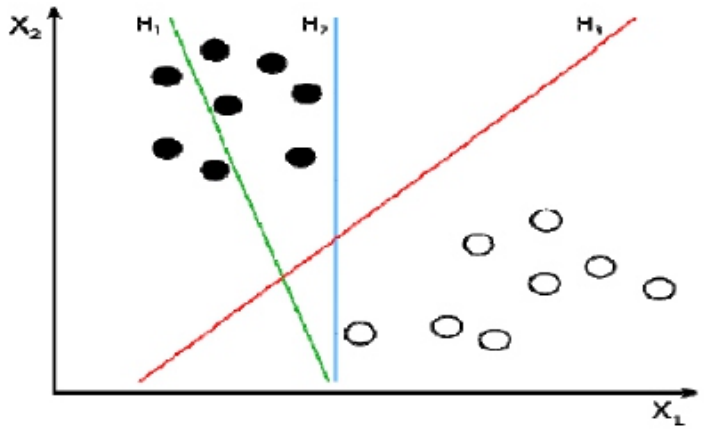


Figure 2- SVM algorithm graph

Linear SVM

Linear SVM is the newest extremely fast machine learning (data mining) algorithm for solving multiclass classification problems from ultra large data sets that implements an original proprietary version of a cutting plane algorithm for designing a linear support vector machine. Linear SVM is a linearly scalable routine meaning that it creates an SVM model in a CPU time which scales linearly with the size of the training data set.

We are given a training dataset of the n points of the form:

$$(\vec{x}_1, y_1), \ldots, (\vec{x}_n, y_n),$$

Where the yiare either 1 or -1,each indicating the class to which the point $y_{\bar{i}}$ belongs. Each is a p dimentional real vector. We want to find the ”maximum-margin hiperplane” that divides the group of points $x^{\bar{}}_I$for which y_i=1 from the goup of points y_i=-1,which is defined so that the distance between the hiperplane and the nearest plane $x^{\bar{}}_I$ from either group is maximized. Any hyperplane can be written as the set of points $x^{\bar{}}$satisfying the below equation.

$$\vec{w} \cdot \vec{x} - b = 0,$$

Where $w^{\bar{}}$is normal vector to hyper plane. This is much like Hesse normal form, except that $w^{\bar{}}$ is not necessarly a unit vector.

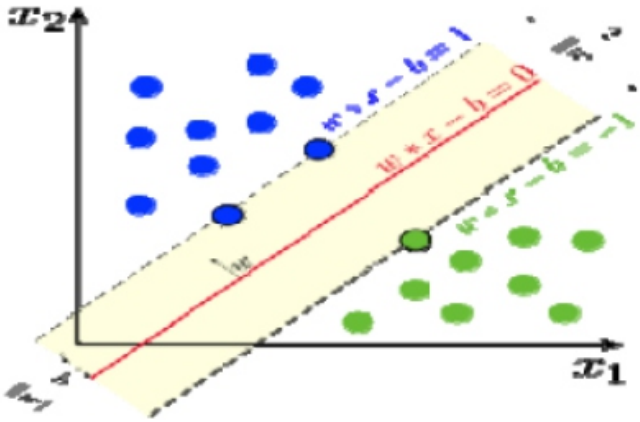


Figure3- Max margin hyperplane and margins for an SVM trained with samples from 2 classes

4.2 Python

Python is an OOPs based software, mostlyhigh-level language. It is a strong language designed for high end applications. Python could be a developer friendly language. It is the most preferred language for AI. It works dead as a glue language furthermore i.e. to attach existing parts along. Due to the benefits of learning, quantifiability and flexibility of Python, it is one amongst the quickest growing languages.

Python's support and ever evolving libraries build it a decent alternative for any project whether or notinternet App, Mobile App, IoT, information Science or AI. Python gives numerous focal points for Machine Learning:

It has various bundles for Machine Learning and different calculations. The prime models are numpy, pandas, keras, tensorflow. These bundles are well-archived, which is useful in beginning with new activities and arrangements. It additionally accelerates the way toward fixing bugs.

Its libraries are essentially ground-breaking. It implies that they involve numerous highlights supportive in complex calculations. The improvement is quick, productive and stable. It is additionally normal that they utilize a scope of calculation speed upgrades. These focal points make these devices develop and dependable.

Another significant preferred standpoint of utilizing Python libraries is an extensive help from the network as the engineers can without much of a stretch discover instructional exercises and tips profitable in an improvement procedure. A steady network makes the begin edge lower - it is simpler to utilize new innovations starting with no outside help.

Python libraries used for the prediction of drought are:

1] Pandas

Pandas is an open-source Python Library giving elite information control and investigation apparatus utilizing its incredible information structures. The name Pandas is gotten from the word Panel Data – an Econometrics from Multidimensional information.

Using Pandas, we will accomplish 5 typical steps within the process and analysis of knowledge, no matter the origin of knowledge — loading, preparing, manipulating, modeling, and analyzing. Python with Pandas is utilized in a wide scope of fields including scholastic and business areas including account, financial matters, Statistics, examination, and so on.

Library options are:

- Data Frame object for knowledge manipulation with integrated classification.
- Tools for reading and writing knowledge between in-memory data structures and completely different file formats.
- Knowledge alignment and integrated handling of missing data.
- Reshaping and pivoting of knowledge sets.
- Label-based slicing, fancy classification, and subset of huge knowledge of datasets.
- Organization column insertion and deletion.
- Cluster by engine permitting split-applycombine operations on knowledge sets.
- Knowledge set merging and change of integrity.
- Hierarchical classification to figure with high dimensional knowledge in a very lower dimensional organization.
- Time series-functionality: Date vary generation and frequency conversion, moving window statistics, moving window linear regressions, date shifting and insulation.

- Provides knowledge filtration.
- This library is very optimized for performance, with vital code methods written in Cython or C.

2] Scikit-learn:

Scikit-learn (previously scikits.learn) could be a free code machine learning library for the Python programing language. It options varied classification, regression and agglomeration algorithms as well as support vector machines, gradient boosting, random forests, k-means and DBSCAN, and is meant to interoperate with the Python numerical and logical and scientific libraries like NumPy and SciPy.

Operations and computations done using sklearn:

- Importing the Dataset
- Exploring the data
- Data visualization
- Learning and predicting
- Selecting features/fields
- Preparing the Data
- Training set and Test set

4.3 GUI(Graphical User Interface)

GUI could be a desktop app that helps you to move with the computers. They are accustomed to perform totally different tasks within the desktops, laptops, alternative electronic devices, etc..,.

- GUI apps like Text-Editors are accustomed produce, read, update and delete differing kinds of files.
- GUI apps like Sudoku, Chess, Solitaire, etc.., are games that you'll play.
- GUI apps like Chrome, Firefox, Microsoft Edge, etc.., are accustomed surf the net.

Few GUI aps are more prevalent and compatible with laptops and desktops. These GUIs motivate one to design for various other applications. A graphical user interface program consists of a set of graphical elements that are placed within one or many of windows/applets/panes. Most elements are “contained” at intervals a window. Therefore, the window acts as a instrumentation to carry varied graphical user interface elements. Instrumentation is a section on the screen that contains smaller areas. I.e. the window could be a instrumentation, that contains elements like buttons, menus, scroll bars etc.

GUI in python

Python offers multiple choices for developing interface (Graphical User Interface). Out of all the interface ways, tkinter is most typically used technique. It's a customary Python interface to the Tkinter interface toolkit shipped with Python. Python with tkinteroutputs the quickest and simplest way to make the interface applications.

Tkinter

Tkinter provides with a spread of common GUI components that we will use to create our interface – like buttons, menus and varied types of entry fields and show areas. We tend to decision these components widgets. We tend to visit construct a tree of appliances for our GUI , every widget can have a parent widget, all the high to the basis window of our application. for instance, a button or a text field must be within some quite containing window. The appliance categories offer us with lots of default practicality.

They need ways for configuring the GUI's look – for instance, arrangement the weather in step with some quite layout – and for handling varied types of user driven events. Once we've created the backbone of our GUI, we are going to have to customize it by desegregation it with our internal application category. Tkinter is associate degree integral Python module accustomed produce straightforward interface apps. It's the foremost unremarkably used module for interface apps within the Python.Tkinter is the commonplace GUI library for Python. Python once combined with Tkinter provides a quick and simple thanks to produce GUI applications. Tkinter provides a strong object-oriented interface to the Tk GUI toolkit.Creating a GUI application victimization, Tkinter is a straightforward task.

Steps to use Tkinter

1. Import the Tkinter module.
2. Create the GUI application main window.
3. Add one or a lot of of the preceding widgets to the GUI application.
4. Enter the most event loop to require action against every event triggered by the user.

4.4 Confusion matrix

In the field of machine learning and specifically the problem of statistical classification, a confusion matrix, also known as an error matrix, is a specific table layout that allows visualization of the performance of an algorithm, typically a supervised learning one(in unsupervised learning it is usually called a matching matrix).Each row of the matrix represents the instances in a predicted class while each column represents the instances in an actual class (or vice versa). The name stems from the fact that it makes it easy to see if the system is confusing two classes (i.e. commonly mislabeling one as another).

It is a special kind of contingency table, with two dimensions ("actual" and "predicted") and identical sets of "classes" in both dimensions (each combination of dimension and class is a variable in the contingency table).

		Predicted	
		Positive	Negative
Actual	Positive	True Positive (TP)	False Negative (FN)
	Negative	False Positive (FP)	True Negative (TN)

Figure 4 - Table of confusion matrix

Below are the formulas of different functions that can be derived from the confusion matrix above.

$$precision = \frac{TP}{TP + FP}$$

$$recall = \frac{TP}{TP + FN}$$

$$F1 = \frac{2 \times precision \times recall}{precision + recall}$$

$$accuracy = \frac{TP + TN}{TP + FN + TN + FP}$$

$$specificity = \frac{TN}{TN + FP}$$

Figure 5- formulas of confusion matrix

V. DATA FLOW DIAGRAM

A data flow sheet is that the graphical illustration of the flow of knowledge through associate system. DFD is extremely helpful in understanding a system and might be expeditiously used throughout analysis. A DFD shows the flow of knowledge through a system. It views a system as an operation that will transform the inputs into desired outputs. Any advanced systems won't perform this transformation during a single step and an information can some times bear a series of transformations before it turns into the output.

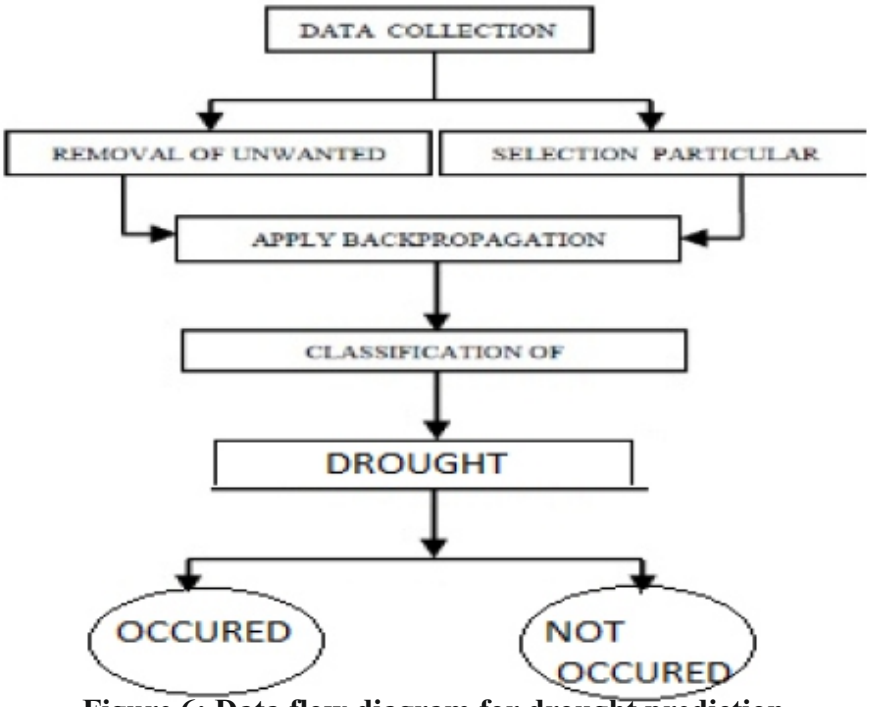


Figure 6: Data flow diagram for drought prediction

With a data flow graph, clients can picture how the framework will work that the framework will achieve and how the framework will be executed, old framework information stream charts can be drawn up and contrasted and another frameworks information stream outline to attract correlations with actualize an increasingly effective framework.

Data flow graphs can be utilized to furnish the end client with a physical thought of where they input, at last as an impact upon the structure of the entire framework.

In the perspective of Drought prediction, Data Flow Diagram (DFD) is a special chart type which lets graphically portray the flow of data through various application components. Data Flow Diagrams can be effectively utilized for perception of information preparing or organized plan, for creating an outline of the drought prediction framework, so as to investigating the high-level state configuration in terms of information flows and recording the key information flows

VI. ARCHITECTURE OF SVM ALGORITHM

The architecture of the SVM algorithm looks exactly the same as below diagram, where the real time dataset which is collected is divided into two sets, one being the training set and the other testing test. Here we train the dataset considered as training set and test if it has predicted properly by giving the testing dataset.

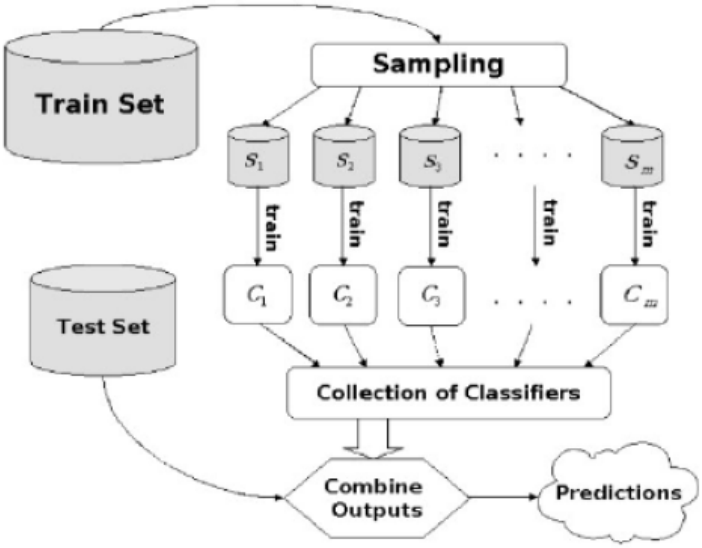


Figure 7: flowgraph of SVM

VII. EXPERIMENTAL RESULTS

This paper looked into the drought prediction problem using support vector machine algorithm. Data is collected for large period and stored in a file. In our application data collected for several years is used for drought prediction. We proposed a support vector machine algorithm for long term drought prediction.

The drought occurs mainly due to lack of precipitation and due to high temperature. Support vector machine model was found to provide better prediction results, recording lower prediction errors and therefore can be more reliable and efficient for long term drought prediction.

CONCLUSION

Drought has a great impact on agriculture, economy not only in India but across the whole world. In this paper we have proposed a method for drought prediction after analysis of dataset. This system describes the drought prediction scheme using the support vector machine algorithm. Frontier technologies and approaches are used to solve the practical problem of adverse natural phenomenon in large area. Developing applications using this can correlate and predict natural calamities ranging from earthquakes to hurricanes that are normally occurring in the normal fashion but may have cross

correlation to observable physical parametric variations around the globe. This will be of great advantage.

REFERENCES

[1] AdeyinkaK.A Kanbi, ,MuthoniMasinde, "Towards the

[2] Development of a Rule-basedDrought Early Warning Expert Systems using Indigenous Knowledge",2018

[3] Norbert A Agana, AbdollahHomaifar,"A Deep Learning BasedApproach for long-termDrought prediction", 2017.

[4] Feeza Khan and SairaMemom Imran Ali Jokhia , Sana Hoor, Jokhio "Wireless SensorNetwork based Flood /Drought Forecasting System",2015 GetachewBerhan,ShawndraHill,TsegayeTadesse,andSolo mon Atnafu,"Drought PredictionSystem for Improved Climate Change Mitigation",2014

[5] XiaotianGu,NingLi,"Study of Droughts and Floods Predicting System Based on Spatial-Temporal Data Mining",2012

[6] Satish G Dappin, Vaidehi M,Nithya G Nair, T R Gopal Krishnan Nair, "Severity prediction of drought in a large Geographical area using distributed Wireless sensor networks",2009

[7] Xiao-Yi Lu, Zhen Fu, In-Sook Lee, Myonga-Soon Park, "A mechanism to improve performance of zone based broadcasting protocol in recovery phase," international journal of multimedia and ubiquitous engineering volume 3, no 2,April 2008.

[8] Bang Wang, Wei Wang, VikramShrinivasan, Kee Chiang Chua, "information coverage for wireless sensor networks," IEEE communication letters, Vol 9, Nov 2005.

[9] Theodore S Rappaport, "wireless communications principles and practice" second edition 2006,

[10] Jingcaiwang, Ziqiang Xia, LidanGuo,Dongye Liang, "Recognizing and forecasting the hydrologic drought in the upper Weihe basin",2011

[11] Wang W, C Men and W. Lu, "Online prediction model based on support vector machine Neurocomputing", 2008

[12] Chang CC and C J Lin,"A Library for support vector machines", 2009

[13] Barros A P, G J Boden,"Toward long lead operational forecast of drought: An experimental study in the Murray Darling River Basin",2008

[14] Cancelliere A, G Di Mauro, B Bonaccorso, G Rossi, "Drought forecasting using the standardized precipitation index", 2007

[15] Kamban P, AElshorbagui, "Cluster based hydrologic prediction using genetic algorithm- Trained Neural Networks",2007

ISSN (Print): 2321 -4058, (Online): 2321 -4392

Energy Efficient Small UAVS By Applying Simple Clustering Along with Reactive Routing Protocols

[1] Hafiz Waleed Ahmad, [2] Lukui Shi, [3] Nelofar Aslam
[1,2,3]Hebei University of Technology, Tianjin 300401, China.
E-mail: [1]201652102001@stu.hebut.edu.cn, [2]shilukui@scse.hebut.edu.cn

ABSTRACT

The main feature of Flying Ad-hoc Network (FANET) is the node mobility, self-organizing and network delay sensitive application between the unmanned aerial vehicles (UAVs) which have led to extend the communication range and expand the connectivity of UAVs at infrastructure-less area. FANET is a vibrant research nowadays, due to which it has paved a way to produce effective small UAVs, as it is specially designed to let the UAVs communicate with each other. Protocol selected in mobile ad-hoc networks should have best results in terms of Quality of Service (QoS) parameters such as high throughput, better packet delivery ratio and minimize energy consumption for data transmission from source to destination. In this work, multi cluster-based approach is implemented for different number of nodes that minimizes the energy consumption for small UAVs and increases the throughput. Reactive protocols such as AODV and DSR have been implemented and simulated using NS-2 simulator and further E-clustering algorithm has been applied to evaluate node energies. The simulation results verify that performance of FANET is significantly increased by using the proposed clustering algorithm in case of throughput and residual energy.

Keywords- Ad-Hoc Routing, Clustering, UAV, FANET, Reactive Protocols

I. INTRODUCTION

An Unmanned Ariel Vehicle (UAV) is structure-less vehicle that can be monitored either by pilots or autonomously controlled by on-board computers. Large numbers of UAVs communicate with each other via wireless links dynamically to form a temporary multi-hop radio network called UAV ad-hoc network.

Due to their flexibility, adaptability, and easy arrangement, FANETs are becoming a promising solution for various civilian and military applications, such as border security [1], wind pressure estimation [2], disaster investigation [3], forest fire disclosure [4], agricultural scheme [5], relaying networks [6,7], search and rescue movement [8], civil surveillance [9], and traffic control [10]. FANETs are essentially an ad-hoc network created by multiple small UAVS, which allows portable and flexible communication solutions in infrastructure-less areas.

Routing is most delicate event in every network scenario as it is used to find the shortest path in order to do the efficient data transfer from source to destination node.

A. Clustering Algorithm

The reason behind the vast use of clustering in networks is the cost efficiency in terms of energy consumption. The algorithm distributes the member nodes into groups named as clusters. A particular member is selected as Cluster Head (CH) among the group of member nodes. The nodes can take part in the race of being CH on the basis of their distance from the base station and high residual energy. CH is in charge to establish an efficient route, exchange information and data circulation between cluster

members. The sending node first transfers the data packets to the CH which then sends data to the base station. At first, the algorithm forms the clusters, then CH is selected and actual data is transmitted.

B. Routing Protocols

Energy efficient ideas proposed in the literature mostly modified reactive routing protocols (RRP) such as DSR and AODV to build energy efficient path since the routing overhead is very high in proactive routing protocols (PRP). The routing table of these protocols is only updated if there is some data to send.

The key purpose to apply on-demand routing protocols such as DSR and AODV is the reactive nature. These protocols create a radio transmission path only when being required by the sending node. The node tries to search the path towards destination only when it has information to send. It spreads the route request message and waits for the reply from the sink node. It looks for the path to destination in its own route cache. The intermediate nodes that receive such route request message rebroadcast it, and the process continues. These transitional nodes rebroadcast the first received route request message and discard the following similar messages in order to reduce the routing overhead. The procedure continues in radio transmission range till the destination is reached and the route to sink is found.

In this paper, a novel idea is introduced of employing both clustering algorithm and RRPs for energy aware FANET scenario. In this scheme, Initially, UAVs are distributed in different groups by using E-clustering algorithm and one CH is elected among each UAVs group on the bases of energy evaluation and distance to the base station as well as to the member nodes of the group. After successful distribution and selection of CH, the packets are sent by using DSR and AODV routing protocols. This approach considerably evaluates the energy and optimizes the network performance.

Remaining part of the paper is arranged as follows. In section 2, the summery of previous work is written. In section 3, our proposed E-Clustering algorithm and protocol scheme for FANETs are described. In section 4, Network simulator 2(NS2) [11] simulation setup and performance metrics are presented. Section 5 describes simulation results and evaluation parameters. Finally, we conclude the remarks in section 6.

III. RELATED WORK

Even though FANET is the sub-part of the Ad-hoc network architecture, still the network design of the FANETs does not allow someone to use MANETs and VANETs approach directly. New approaches need to be proposed or modification of existing techniques is necessary. In the case of FANETs, the research is still in its initiation. Bilal et al. [12] used the clustering technique, in which one UAV is selected as a CH and each CH has a fixed number of UAVs. Nelofar et al. [13] presented the energy-aware weighted grid clustering algorithm that maximizes the lifetime and minimizes the overall energy consumption of the renewable wireless sensor networks. They give a new idea of energy harvesting along with reducing its consumption. In [14], topology based protocols such as AODV and DSR have been used in order to get the better throughput and delay of FANET. In [15], they proposed a TCP-ICCW (Initial Constant Congestion Window) routing protocol that detects the congestion immediately after it begins to block the data traffic.

These protocols design route on-demand when requested by the transmitting node. DSR routing divided into two parts, route recovery and route maintenance. In route recovery it starts checking the path in the route caches on the request of sender node.

If the path exists from source to destination, the sender sends the packet to the destination. In step 2, the route is maintained to minimize the packet loss in process of data transfer. In order to reduce the link breakage between the nodes, an acknowledgment is sent back to the sender when data is transferred from one node to another. The error message is sent backward to the source through the same route if the acknowledgment is not picked at any level that declares the breakage of link between the nodes. The proposed model considerably maintains the energy and improves the network performance.

IV. PROPOSED MODEL

The mobile nodes are randomly scattered in the 500×500 square meter area. Nodes start moving from the initial position towards the final position with the speed of 15 m/s. The clustering algorithm starts working and forms ad-hoc architecture of multiple groups containing miscellaneous UAVs as shown in the figure 1. The network area is distributed into three different groups. At this level the phase is divided into three parts:

A. Cluster Head selection

Initially, each UAV in the network advertises to become the CH. The selection of CH is completed on the basis of residual energy and proximity to the destination and the member nodes.

B. Cluster Establishment

After successfully selection of CH, each member UAV sends a cluster join request message to its chosen CH and establishes a cluster. Cluster join request message contains nodes ID to recognize each node separately and CH ID of each cluster to identify it. To minimize the energy consumption and increase the efficiency of the network, CH generates the scheduling time for the member nodes for data communication by putting the nodes into sleep mode when there is no packet to send. All the member nodes are informed to send the data according to its given time duration and goes to sleep mood as per the assigned time period. The member nodes only need to keep the information of their respective CH node and need not to create a new routing table.

C. Data Routing

Member UAVs start sending the data packets one by one to the respective CH by using the reactive protocols of AODV and DSR. The UAV that currently sends the data to the CH would be on active state. All CHs of each cluster first receive the data from the member UAVs and then send it to the base station.

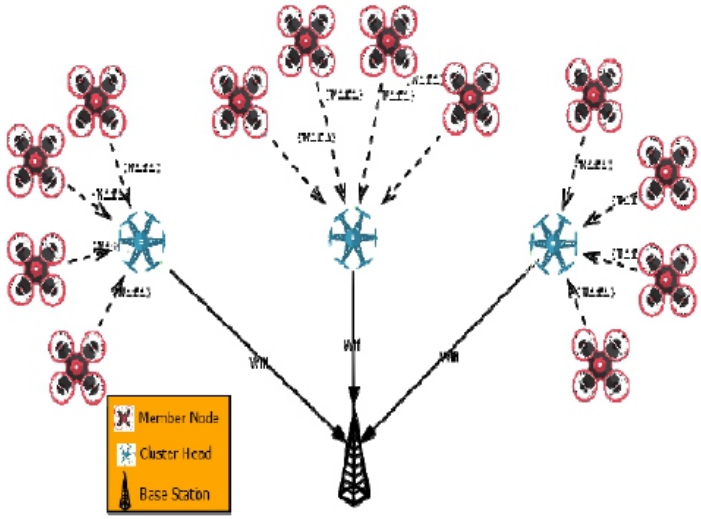


Fig 1: FANET Clustering architecture

D. UAVs Station Model

In order to continually oversee and amend the locations and positions of nearby UAVs in the MAC table, GPS and IMU are installed apparently in our proposed model. UAVs also contain omni-directional antenna. All the UAVs are equipped with IEEE 802.15.11 MAC protocol in the model.

E. Radio Propagation Model

The free space propagation model has been employed and used the Friis transmission equation 1 to drive the antenna parameters.

Where P_r is received power, P_t is transmitted power, G_t is transmitter's gain, G_r is receiver's gain, λ is the wavelength and R is the transmission range. For instance, setting the parameters in NS2 discrete event modular as shown will results in a transmission range of 1000m, P_r =-95dBm, P_t = 0.005W, Frequency= 2.4 GHz and $G_t = G_r$ = 0dBm.

F. Mobility Model

We assumed a Reference Point Group Mobility (RGPM) model in our proposed model because it imitates the random movements of multiple UAVs in a cluster with a reference point to achieve a target. The CH UAV is worked as reference point in our proposed model which provides necessary information about speed, direction and altitude of member UAVs in the cluster. The location of every member UAV is amended according to the CH UAV.

G. Routing Protocols

The routing protocols used in our study are DSR and AODV. These protocols are reactive by nature and they have best used in the environment where energy evaluation is the priority. In DSR the route is created when required and UAVs utilize the given path in efficient way to reduce the concussion and evaluate the energy between the nodes. Route discovery procedure in AODV is on-demand that is more efficient for mobile ad-hoc network's dynamic nature.

The interface queue type in DSR protocol is CMUpriqueue, because it does not obey the drop tail priqueue model as specified in AODV. CMU pri-queue transmits the routing protocol packet in priority manner. On the other hand drop tail pri-queue interface in AODV starts dropping the packets when the queue is full.

H. Clustering Algorithm

Proposed clustering algorithm is the E-Clustering algorithm that not only maintains the efficient route for the UAVs to send the data packets but also saves the energy.

$$CH = Maximum\left(RE\right) + Minimum\left(\frac{DM}{DS}\right) \quad (2)$$

CH selection of the network is done by implementing the above formula (2). Here RE is the residual energy of the node and described more clearly below (3), DM is the distance of member node and DS is the distance of sink node. At the beginning of the simulation, CH selection takes place by calculating the ratio of distance of each DM and DS. The node with high energy and minimum distance between all the member nodes and the base station is elected as CH node.

V. SIMULATION PROCESS AND EVALUATION PARAMETERS

A. Simulation Process

We used NS2 discrete modular for simulation work and created structure to display the performance of our proposed methodology. We have constructed and implemented our E-Clustering algorithm along with RRP. The network scenario consist of 9, 12 and 15 nodes respectively, where 3 nodes are treated as the CH (i.e., master nodes) and remaining nodes are called as member nodes(i.e., slave nodes). Slave nodes in every cluster form ad-hoc architecture of 2, 3 and 4 nodes accordingly. In first round each master node is connected to 2 slave nodes in the network whereas in second round master nodes are connected to 3 slave nodes of each group. The master nodes in third round are connected to 4 slave nodes of each cluster. All the UAVs consist of IEEE 802.11 MAC protocol. By considering the low cost budget, each UAV has 100 Joule of energy at the beginning. Results are generated by using the both AODV and DSR protocols in each round. Further details are mentioned in Table 1.

B. Evaluation Parameters

Throughput:

The rate of successful data packets transmission from sending flying node to the sink flying node through a radio communication channel in a given unit of time is called throughput. It can be calculated mathematically as in following method (4):

$$Throughput = \frac{No.ofPackets \times SizeofPacket \times 8}{GivenTime} \quad (3)$$

$$Throughput = \sum_{N=1}^{n} \frac{NP \times SP \times 8}{T} \quad (4)$$

Where N is the number of nodes, n represents the total nodes. NP is number of transferred packets successfully. SP is the size of packet and T is referred as given time.

C. Residual Energy:

Residual energy is the remaining energy of the node after successful routing transmission of the network. It is calculated by subtracting the consumed energy from the initial energy. Mathematically it is written as: Residual Energy= Initial Energy - Consumed Energy

$$RE = IE - CE \quad (5)$$

$$\sum_{N=1}^{n} RE = \sum_{N=1}^{n} (IE - CE) \quad (6)$$

$$\sum_{N=1}^{n} RE = \sum_{N=1}^{n} IE - \sum_{N=1}^{n} CE \quad (7)$$

RE represents the Residual energy whereas IE and CE are the Initial energy and the consumed energy respectively. N represents the node and n is the total number of nodes.

Parameter	Value
Energy Model	For nodes energy
Initial Energy	100(Joule)
Receiving Power	0.5W
Transmission Power	0.9W
Sleep Power	0.05W
Area Dimensions	500m×500m
Number of nodes	9,12,15
Routing Protocols	AODV,DSR
MAC Protocol	802.11
Speed of nodes	15m/s
Data rate	1Mbps
Mobility Model	RGPM
RadioPropagation Model	Free spacepropagation
Interface queue type	Drop tail pri-queue, CMU pri-queue

VI. PERFORMANCE EVALUATION AND RESULT ANALYSIS

Fig. 2 and 3 reveals the performance of FANET in terms of average throughput and residual energy. In Fig 2, x-axis indicates the total number of nodes taken in each set whereas y-axis represents the average throughput in bits/sec. Fig 3a, 3b and 3c shows the number of nodes used in x-axis and instant residual energy of the nodes in y-axis. The simulation results illustrate that the proposed E-clustering algorithm and reactive protocols are able to show the QoS requirements and supply sufficient progress of the network significantly in terms of throughput and residual energy. The proper communication without link breakage increases the life time of UAVs and reduces the energy consumption. Hence the residual energy increases gradually. The more the residual energy is, the more period of time nodes can survive in the network. We operated simulation of three different scenarios by changing the number of UAVs. We observed that DSR protocol performs better in case of throughput because it transmits the packets in priority manner. A lot of variation occurs in energy aware graphs between the DSR and AODV protocols and results are almost same when less number of UAVs are being used. Although DSR protocol shows slightly improve results of instant residual energy. In Fig. 3c. It is clear that DSR protocol perform better than AODV concerning in remaining energy of the nodes.

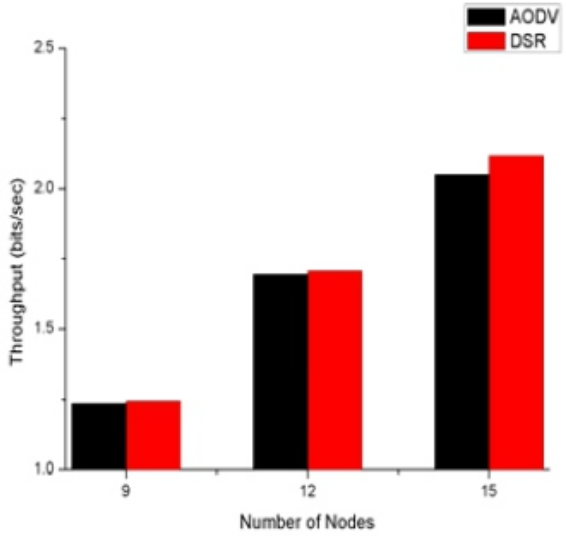


Fig. 2. Average throughput with 9, 12 and 15 nodes.

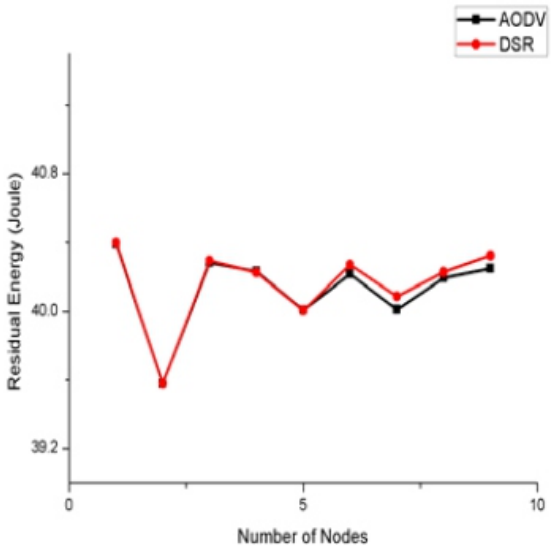


Fig. 3a. Residual energy with number of nodes 9.

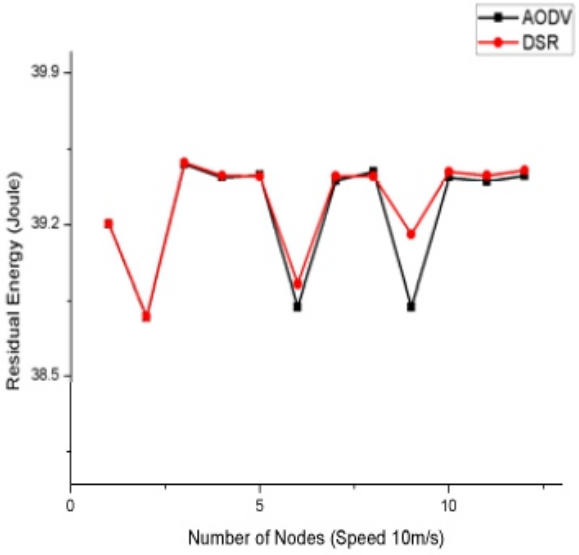


Fig. 3b. Residual energy with number of nodes 12.

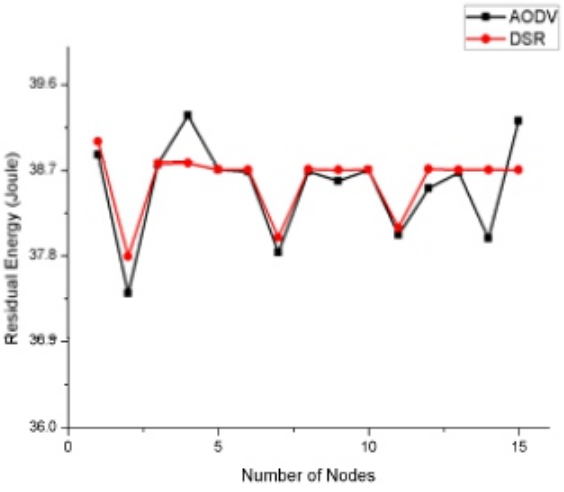


Fig. 3c. Residual energy with number of nodes 15.

VII. CONCLUSION

Replacing or recharging batteries is not possible instantly in ad-hoc network. Energy consumption increment directly affects the lifetime of the UAVs and reduces the network performance. In this paper we proposed an energy aware E-clustering algorithm along with DSR and AODV protocols that not only reduces the energy consumption but also improves the throughput of the network. The proposed E-clustering algorithm can select the CH node whose energy is higher in the group. The CH is more capable to handle with the requests from member nodes of the cluster efficiently and provides the reliable communication among the UAVs. The performance of the E-clustering algorithm is better in case of throughput and residual energy.

Energy is the limited recourse of communication in ad-hoc network. In future we can extend our work in the sense that the energy of the UAVs can be controlled and save more time of utilization of UAVs by using the machine learning algorithm. The network performance can be improved by training the network to select the best and closest routing path.

REFERENCES

[1] Z. Sun, P. Wang, M. Vuran, M. Al-Rodhaan, A. Al-Dhelaan and I. Akyildiz, "BorderSense: Border patrol through advanced wireless sensor networks", Ad Hoc Networks, vol. 9, no. 3, pp. 468-477, 2011.

[2] A. Cho, J. Kim, S. Lee and C. Kee, "Wind Estimation and Airspeed Calibration using a UAV with a Single-Antenna GPS Receiver and Pitot Tube", IEEE Transactions on Aerospace and Electronic Systems, vol. 47, no. 1, pp. 109-117, 2011.

[3] M. Erdelj, E. Natalizio, K. Chowdhury and I. Akyildiz, "Help from the Sky: Leveraging UAVs for Disaster Management", IEEE Pervasive Computing, vol. 16, no. 1, pp. 24-32, 2017.

[4] C. Barrado, R. Messeguer, J. Lopez, E. Pastor, E. Santamaria and P. Royo, "Wildfire monitoring using a mixed air-ground mobile network", IEEE Pervasive Computing, vol. 9, no. 4, pp. 24-32, 2010.

[5] H. Xiang and L. Tian, "Development of a low-cost agricultural remote sensing system based on an autonomous unmanned aerial vehicle (UAV)", Biosystems Engineering, vol. 108, no. 2, pp. 174-190, 2011.

[6] F. Jiang and A. Swindlehurst, "Optimization of UAV Heading for the Ground-to-Air Uplink", IEEE Journal on Selected Areas in Communications, vol. 30, no. 5, pp. 993-1005, 2012.

[7] D. Freitas, T. Heimfarth, I.F Netto, C.E. Lino, C.E. Pereira, A.M. Wagner, and T. Larsson, "UAV relay network to support WSN connectivity. In Proceedings of the International Congress on Ultra", Modern Telecommunications and Control Systems, Moscow, Russia, pp. 309–314, 18–20 October 2010.

[8] George, S. P. B. and J. Sousa, "Search Strategies for Multiple UAV Search and Destroy Missions", Journal of Intelligent & Robotic Systems, vol. 61, no. 1-4, pp. 355-367, 2010.

[9] I. Maza, F. Caballero, J. Capitán, J. Martínez-de-Dios and A. Ollero, "Experimental Results in Multi-UAV Coordination for Disaster Management and Civil Security Applications", Journal of Intelligent & Robotic Systems, vol. 61, no. 1-4, pp. 563-585, 2010.

[10] E. Semsch, M. Jakob, D. Pavlicek, and M. Pechoucek, "Autonomous UAV Surveillance in Complex Urban Environments", In Proceedings of the IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology, Milan, Italy, pp. 82–85, 15–18 September 2009.

[11] "The Network Simulator - ns-2", Isi.edu, 2019. http://www.isi.edu/nsnam/ns. [Accessed: 30- Nov- 2018].

[12] W. Zafar and B. Khan, "A reliable, delay bounded and less complex communication protocol for multicluster FANETs", Digital Communications and Networks, vol. 3, no. 1, pp. 30-38, 2017.

[13] N. Aslam, K. Xia, M. Haider and M. Hadi, "Energy-Aware Adaptive Weighted Grid Clustering Algorithm for Renewable Wireless Sensor Networks", Future Internet, vol. 9, no. 4, p. 54, 2017.

[14] M. Khan, I. Khan, A. Safi and I. Quershi, "Dynamic Routing in Flying Ad-Hoc Networks Using Topology-Based Routing Protocols", Drones, vol. 2, no. 3, p. 27, 2018.

[15] N. Aslam, K. Xia, A. Ali and S. Ullah, "Adaptive TCP-ICCW Congestion Control Mechanism for QoS in Renewable Wireless Sensor Networks", IEEE Sensors Letters, vol. 1, no. 6, pp. 1-4, 2017.

ISSN (Print): 2321 -4058, (Online): 2321 -4392

Efficient Deep Learning Hyperparameter Tuning on the Cloud (Intelligent Distributed Hyper-Parameter Tuning with Bayesian Optimization using Cloud Infrastructure)

[1] Mercy Prasanna Ranjit, [2] Gopinath Ganapathy
[1]Advanced Analytics and AI, Microsoft India Corporation Private Limited Bangalore, India
[2]Department of Computer Science, Bharathidasan University, Trichy, India
E-mail: [1]mercy.prasanna.peter@gmail.com, [2]gganapathy@gmail.com

ABSTRACT

The paper discusses how we can leverage cloud infrastructure for efficient training and hyperparameter tuning of deep neural networks on the cloud. With the introduction of Horovod framework distributed training of deep learning models has been made trivial on the cloud thereby reducing the time taken to run a single iteration, but the hyperparameter tuning exercise on high dimensional hyperparameter spaces remains a challenge. The paper experiments Bayesian Sequential Gaussian Process Optimization of hyperparameters on the cloud at different levels of concurrency for the warmup runs. Two different distributed hyper-parameter tuning approaches were experimented on the cloud – Training on multiple nodes with higher warm-up concurrency Vs Distributed Training on multiple nodes with Horovod and reduced number of warm-up runs. The results indicate that greater number of warm-up runs results in better exploration of the search space. The hyper parameter choices of every run were optimized using Bayesian optimization technique to take advantage of the learnings from previous runs. The hyper parameter tuning and distributed training with Horovod was performed using Azure Machine Learning Service for Video Activity Recognition problem using LRCN network with transfer learning from Resnet50 backbone.

Keywords - Distributed Training, Horovod, Hyperparameter Tuning, Deep Learning, Bayesian Optimization, Automated Machine Learning, Neural Architecture Search

I. INTRODUCTION

Deep Learning training and hyper parameter tuning requires exploring a vast space of neural network architectures and hyper parameter values for arriving at the ones which works the best for your problem.

This has become imperative with the introduction of automated machine learning where multiple machine learning pipeline configurations and neural architectures are evaluated in parallel to arrive at an optimal model. This is usually a time consuming and computationally expensive exercise especially compounded when you are working with image data and neural networks where there are variety of network architectures and parameters to explore like the number of layers and nodes, number of filters, filter size, stride size, optimizer, learning rate, decay factor etc.

With the introduction of Horovod framework, it was made easier to adapt the code for distributed training and hence faster training of deep neural networks. Cloud together with container services provides the ability to spin compute dynamically in the cloud, scale as required and deploy deep learning jobs with dependencies packaged as container images, track run metrics and outputs and dispose compute once the job is completed. These capabilities have opened up avenues for quicker experimentation in the cloud. The distributed runs when coupled with Bayesian optimization or

Reinforcement learning enables making intelligent choices based on past runs for faster convergence towards hyper-parameter values and network choices that works the best. This paper makes use of Bayesian Optimization to explore the hyperparameter space at different levels of warm-up concurrency.

Approach 1 described in Fig. 1 consists of distributing the hyper-parameter tuning across multiple nodes with each node running one hyperparameter combination. The training of the network is not distributed in this approach. More runs will be performed in this approach simultaneously with each run taking longer to complete. With four nodes in the machine learning compute cluster, each node runs with different hyperparameter choices simultaneously. This method will have four warmup runs and only the fifth run can run Bayesian optimization for the first time. The execution time of every run varies and hence usually no runs complete at the same time and all runs benefit from the Bayesian optimization except the warmup runs.

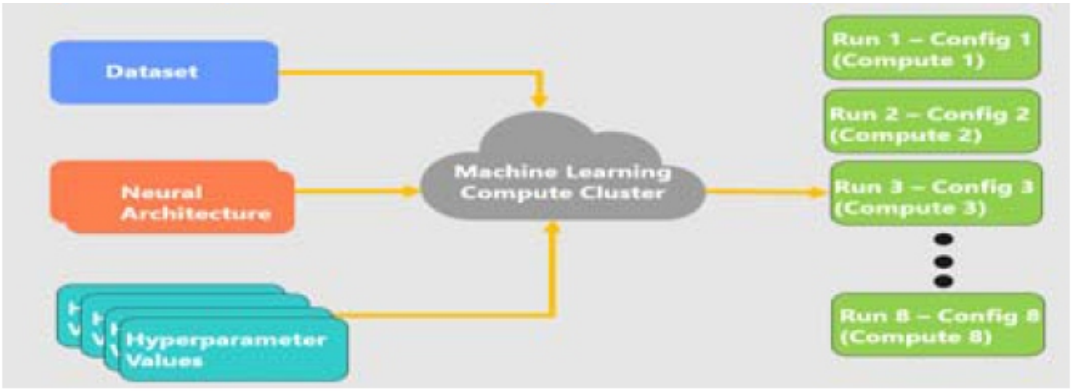


Fig 1: Distributed hyper-parameter tuning with Bayesian Optimization.

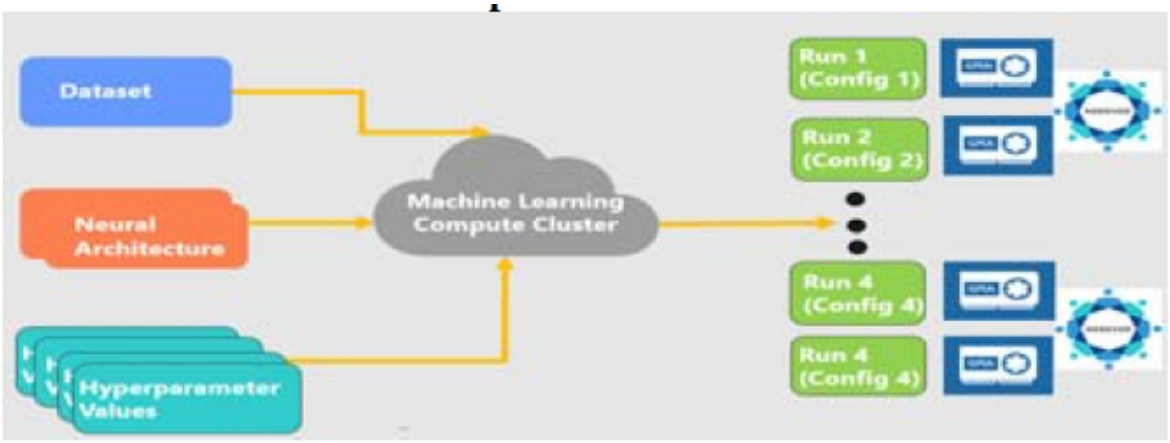


Fig 2: Distributed training with horovod and hyper-parametter tuning with Bayesian Optimization.

The second approach in Fig. 2 is distributing the training with horovod framework where each run is distributed across nodes. The number of runs running concurrently is reduced as the training is distributed. With the machine learning compute cluster of 4 nodes and horovod distribution of training across 2 nodes, each submission will only have 2 runs each running one hyperparameter combination. This method will have only two warmup runs and only the third run can run Bayesian optimization for the first time. Since horovod is used for training each run in a distributed way, training time for each run is reduced.

The experiments sought to measure how different number of warm-up runs can impact the search space exploration and convergence of hyperparameters when using Bayesian optimization. We did not alter the number of nodes when the experiments were in progress and Bayesian optimization was used to suggest only one hyperparameter combination at a time when a run is completed and the node is available to pick up a new combination.

II. RELATED WORK

[1] Discusses Bayesian optimization as a method of finding the maximum of expensive cost functions. The paper discusses the optimization process employing Bayesian technique of setting a prior over the objective function and combining it with evidence to get a posterior function that permits a utility-based selection of the next observation to make on the objective function. The paper also discusses the exploration (sampling from areas of high uncertainty) and exploitation (sampling areas likely to offer improvement over the current best observation) trade-off as one of the challenges where too much exploration, and many iterations can go by without improvement and too much exploitation leads to local maximization which is not desired.

[2] Discusses the intelligent choice of samples for Bayesian optimization of objective function by using a Gaussian process upper confidence bound rule (GPUCB) This objective function based on this rule prefers both points x where f is uncertain (large $\sigma t-1(\cdot)$) and such where we expect to achieve high rewards (large $\mu t-1(\cdot)$), it implicitly negotiates the exploration–exploitation tradeoff.

[3] Discusses the representation of hyper parameter optimization objective function as multidimensional Gaussian distributions. The paper also discusses an acquisition function that encodes the measure of usefulness of trying a hyperparameter combination. The probability of improvement acquisition function is that we pick the next point based on the maximum probability of improvement (MPI) as Expected Improvement (EI) function with respect to the current maximum. The paper discusses an approach to parallelize the Exploration–Exploitation Tradeoff by using GPBUCB, a principled algorithm for choosing batches, based on the GP-UCB algorithm for sequential GP optimization. the cumulative regret of the parallel algorithm only increases by a constant factor independent of the batch size providing a rigorous theoretical support for exploiting parallelism in Bayesian global optimization.

[4] Discusses Google Vizier, a Google-internal service for performing black-box optimization in the cloud that has become the de facto parameter tuning engine at Google. Google Vizier is used to optimize many of their machine learning models and other systems, and also provides core capabilities to Google's Cloud Machine Learning HyperTune subsystem. It discusses the features such as transfer learning and automated early stopping that the service provides in addition to the underlying infrastructure and Gaussian Process Bandit Optimization algorithm.

[5] Discusses the use of Bayesian optimization based acquisition function that indicates which machine learning pipeline to try next in the context of automated machine learning where the system automatically tries out different machine learning pipelines that maximizes or minimizes the objective function. The paper describes the use of Non-linear matrix factorization with Gaussian processes for modeling the performance of different machine learning pipelines on different datasets. The paper discusses an approach that optimizes the entire pipeline of preprocessing, algorithm selection and hyper parameter tuning and not just hyperparameter tuning in isolation.

[6] Discusses the distributed deep learning framework Horovod, an open source library that improves on both obstructions to scaling: it employs efficient inter-GPU communication via ring reduction and requires only a few lines of modification to user code, enabling faster, easier distributed training in TensorFlow. Horovod is also available via the Keras abstraction which we used in our experiment.

III. EXPERIMENTAL SETTINGS

The Input dataset for the experiment was sampled from the Kinetics 400 dataset from Google DeepMind which was part of the ActivityNet Large- Scale Activity Recognition Challenge. The experiment was performed for three sport activities – Archery, Bungee Jumping and Bowling with 997, 907 and 930 records, respectively. The experiment extracted 360p images at 1 fps (frames per sec). The shape of the input dataset for the LRCN network was (None, 10, 299, 299, 3) where None referred to the no. of input images, 10 refers to the time units corresponding to the ten second video clips and (299,299,3) refers to the height, width and no of channels in the input image frames.

The LRCN network used Resnet50 for feature extraction and stacked LSTM for action sequence classification. The experiment was carried out in Azure cloud on a 4 node NC6 cluster each powered by NVIDIA Tesla K80 GPU. A separate experiment was performed to identify the best optimizer as SGD with Nesterov acceleration. Figure 3 shows the activity classification approach.

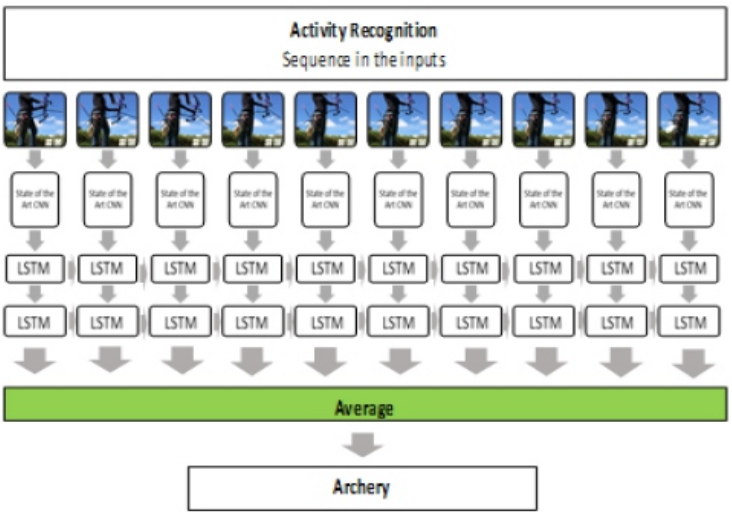


Fig 3: LRCN using two-layer LSTM stack and Resnet50 backbone.

The experiments used the configuration mentioned in table I for the hyper-parameter tuning convergence for different approaches.

Problem	Activity Recognition in Videos
Training Iterations	15
Backbone CNN	Resnet50
Network Type	LRCN
Optimizer	SGD
Nesterov Acceleration	True
LR Decay	No
Hyper-tuning parameters	Learning Rate, Momentum and Batch Size.

Table 1: Experiment Configuration

The hyperparameter tuning was done for three different hyperparameters - learning rate, batch size and momentum values for SGD. Total of thirty-one runs were submitted for both the experiments. The first experiment ran four runs in parallel. The execution times of these runs varied which meant none of these runs had the same completion time. The runs chose hyperparameter values from the sampling space using Bayesian optimization of hyperparameters that optimized the selection of hyperparameters that maximized the validation accuracy using the history of previous runs. The first four runs can be considered as warm-up runs as it did not have any history to use. As the completion times of runs were sequential, the no of history runs available for Bayesian optimization also increased linearly.

The second experiment used horovod distributed training framework for distributed training across nodes. Each run was distributed across two nodes. Hence two runs were performed in parallel with each run distributed across two nodes. At any time only two runs were performed in parallel. Thirty-one runs were performed in total. The first two runs did not have any history and hence can be considered as the warm-up runs. The training time of each run was lower as it distributed the training across two nodes, but the no of concurrent runs was less. The training time of each run was different and hence no runs completed at the same time which implied that the number of runs used for the Bayesian optimization also increased linearly. The difference from Approach 1 is that the number of warm-up runs was just 50% of what Approach 1 had.

The experiments aimed to see how Bayesian tuning with different no of warm-up runs performed towards the search for the best hyper parameters. The no of nodes for training in both the experiments were same. Different levels of concurrency for the warm-up runs was achieved using horovod. Table II below shows the experiment settings for distributed hyper parameter tuning for neural networks in the cloud.

	Experiment 1	Experiment 2
Horovod enabled	No	Yes.
No of runs	31	31
No of Parallel Runs	4	2
No of Warm-up runs Bayesian Optimization Runs	4	2
No of history runs for Bayesian optimization at run n.	N	N

Table II: Distibuted Hyper Parameter Tuning Experiment Settings

IV. RESULTS

A. Distribution of Validation Accuracy

The hyperparameter values that was chosen based on Bayesian optimization and their corresponding validation accuracies were measured across all the runs in both the experiments.

Fig 4: Validation Accuracy Distribution with Distributed Hyperparameter Tuning Approaches

Fig.4 shows the validation accuracy distributions obtained with both the approaches. Approach 1 which had more warm-up runs for Bayesian optimization yielded runs with higher validation accuracy. Table III shows the inter quantile range values of validation accuracies observed using both the approaches.

Validation Accuracy	Experiment 1	Experiment 2
Max	85.25	82.79
Median	80.33	77.87
First Quartile	77.87	73.96
Third Quartile	81.97	80.13

Table III: Validation Accuracy Distribution

B. Distribution of Hyper-parameter values.

The hyper-parameter values for both the experiments were sampled between 0.001 and 0.05 for learning rate, 0.6 and 0.9 for SGD momentum and 16,14 and 32 for batch-size.

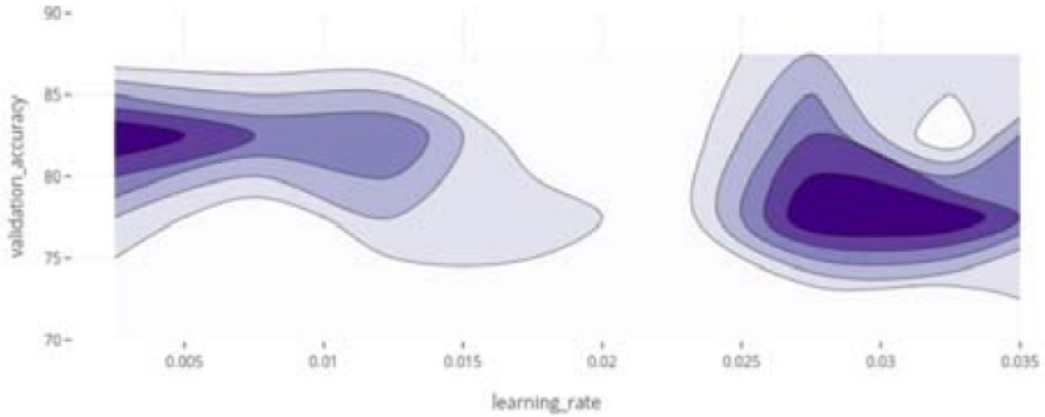


Fig 5: Frequency 2D contour histogram of Learning Rate Vs Validation Accuracy for Bayesian Hyperparameter Tuning

Fig.5 shows higher validation accuracy values were corresponding to learning rates sampled between 0.02 and 0.03 and 0.001 for Experiment 1 which was distributed hyperparameter tuning with Bayesian optimization and four concurrent runs. This is also the high frequency sampling region which is indicated from the darker color shades.

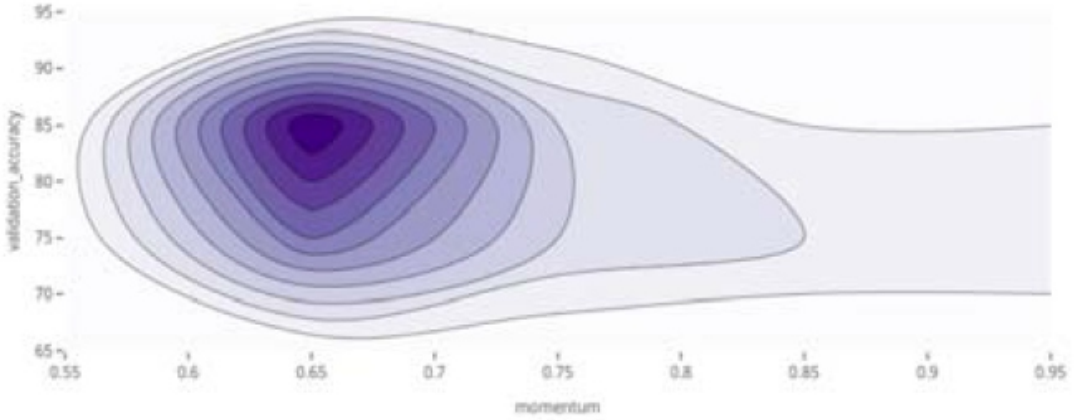


Fig 6: Frequency 2D contour histogram of Momentum Vs Validation Accuracy for Bayesian Hyperparameter Tuning

Fig.6 shows higher validation accuracy values were corresponding to SGD momentum values frequently sampled around 0.6 for Experiment 1. There were also momentum values greater than 0.7 which led to higher accuracy but the frequency of them being less.

Momentum	Validation Accuracy	Learning Rate
0.610612	85.25	0.028512
0.6	85.25	0.035443
0.6	85.25	0.03439
0.607167	83.61	0.035
0.6	82.79	0.001
0.715265	81.97	0.005194
0.6	81.97	0.029682
0.767591	81.15	0.009031
0.613719	81.15	0.027869
0.778186	80.33	0.043299
0.977457	80.33	0.0119
0.618248	80.33	0.002759

Table IV: High Frequency Sampling Regions Experiment I

Table IV shows samples of well performing momentum and Learning Rate samples for Experiment 1.

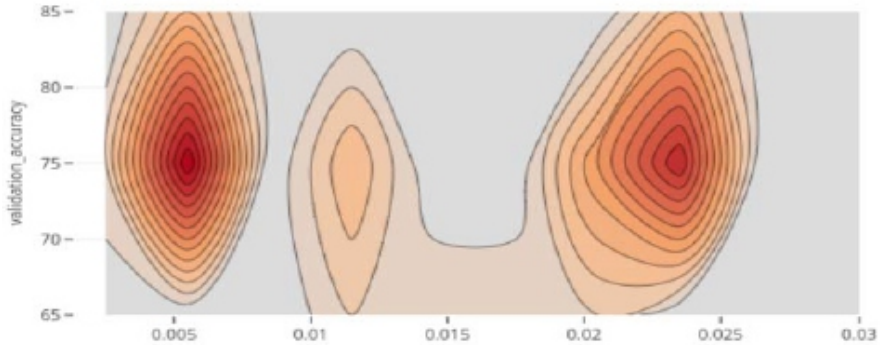


Fig 7: Frequency 2D contour histogram of Learning Rate Vs Validation Accuracy for Bayesian Hyperparameter Tuning with Horovod

Fig.7 shows higher validation accuracy values were corresponding to learning rates sampled around 0.005 and 0.02 for Experiment II which was distributed hyperparameter tuning with Bayesian optimization and two concurrent runs using horovod. This is also the high frequency sampling region which is indicated from the darker color shades.

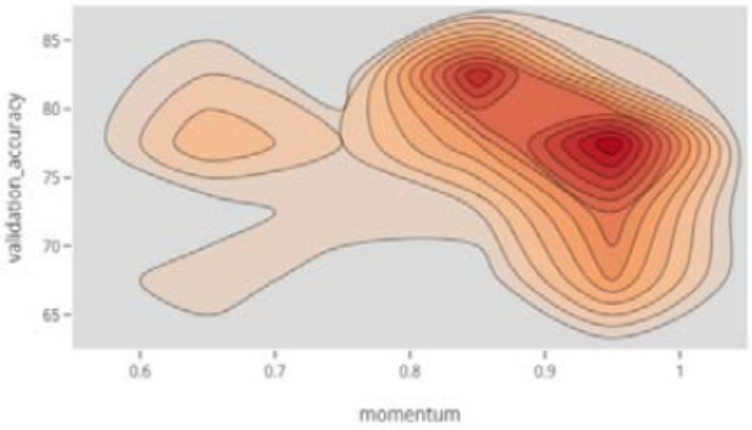


Fig 8: Frequency 2D contour histogram of Momentum Vs Validation Accuracy for Bayesian Hyperparameter Tuning with Horovod

Fig.8 shows higher validation accuracy values were corresponding to SGD momentum values frequently sampled around 0.8 and 0.9 for Experiment 2. There were also momentum values less than 0.7 which led to higher accuracy but the frequency of them being less.

Momentum	Validation Accuracy	Learning Rate
0.883153	82.79	0.0005
0.877294	82.79	0.0005
0.863048	82.79	0.0005
0.619106	81.97	0.023239939
0.800283	81.15	0.022215887
0.897316	81.15	0.0005
0.909958	80.33	0.005180786
0.89335	80.33	0.004044698

Table V: High Frequency Sampling Regions Experiment II

Table V shows samples of well performing momentum and Learning Rate samples for Experiment 2.

C. Covergence of Hyper-parameter values.

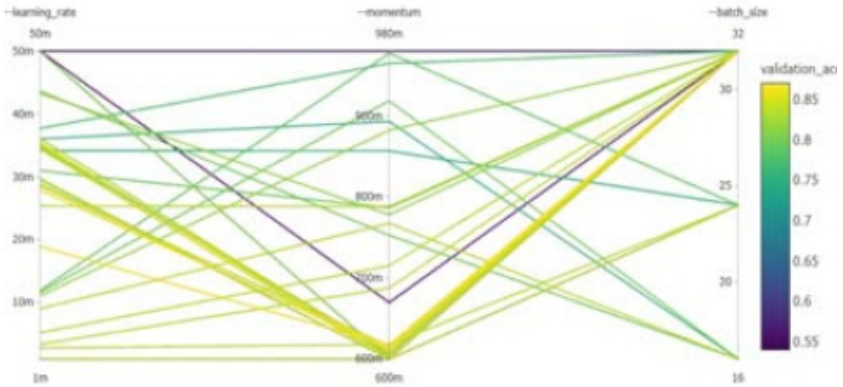


Fig 9: Parallel Coordinates Chart for Experiment I

Fig.9 is a parallel co-ordinates chart that color codes the best performing hyperparameter values for batch size, SGD momentum and learning rate for Experiment 1 which was distributed hyperparameter tuning with Bayesian optimization and four concurrent runs. The batch size converged to size 32, momentum converged to values around 0.6 and learning rate to values between 0.2 and 0.3.

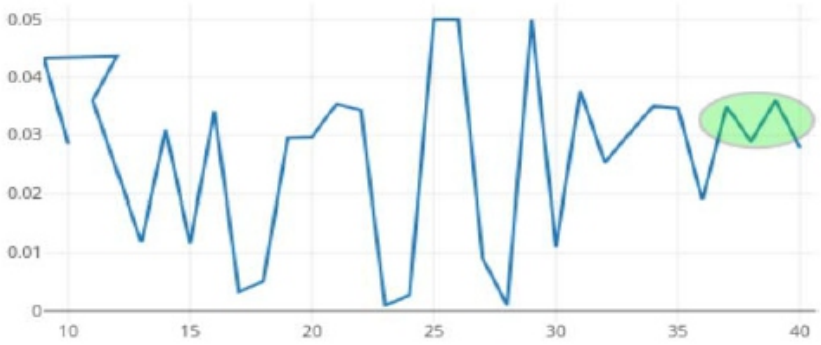


Fig 10: Convergence of Learning Rate for Bayesian Tuning

Fig. 10 shows as the runs progressed the learning rates started to converge to values between 0.02 and 0.03. The sampled regions around lower learning rates like 0.001 were not explored further by Bayesian tuning and hence not taken to convergence.

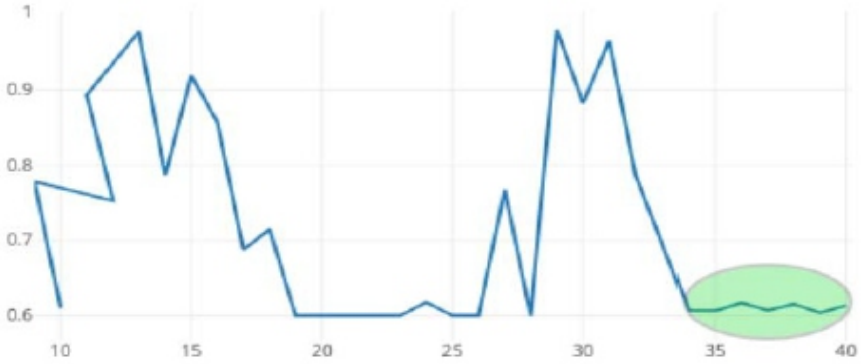


Fig 11: Convergence of Momentum for Bayesian Tuning

Fig. 11 shows as the runs progressed the momentum started to converge to values around 0.6. The sampled regions around higher momentum greater than 0.8 were not explored further as the Bayesian optimization tuning considered it not better and hence not taken to convergence.

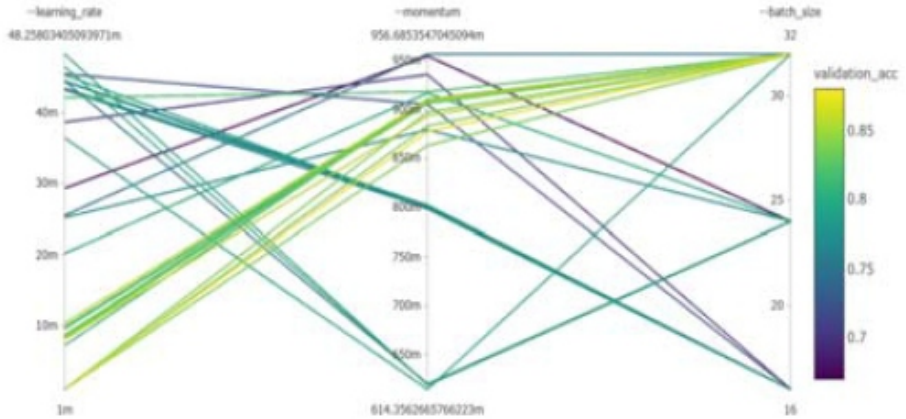


Fig 12: Parallel Coordinates Chart for Experiment II

Fig.12 is a parallel co-ordinates chart that color codes the best performing hyperparameter values for batch size, SGD momentum and learning rate for Experiment 2 which was distributed hyperparameter tuning with Bayesian optimization and Horovod with two concurrent runs. The batch size converged to size 32, momentum converged to values between 0.8 and 0.9 and learning rate to lower values like 0.0005.

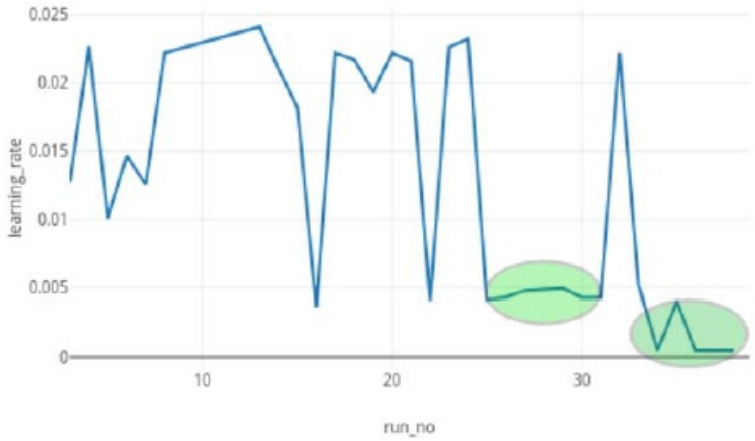


Fig 13: Convergence of Learning Rate for Bayesian Tuning with Horovod

Fig. 13 shows as the runs progressed the learning rates started to converge to lower values around 0.0005 The sampled regions around higher learning rates like 0.02 were not explored further by Bayesian tuning and hence not taken to convergence.

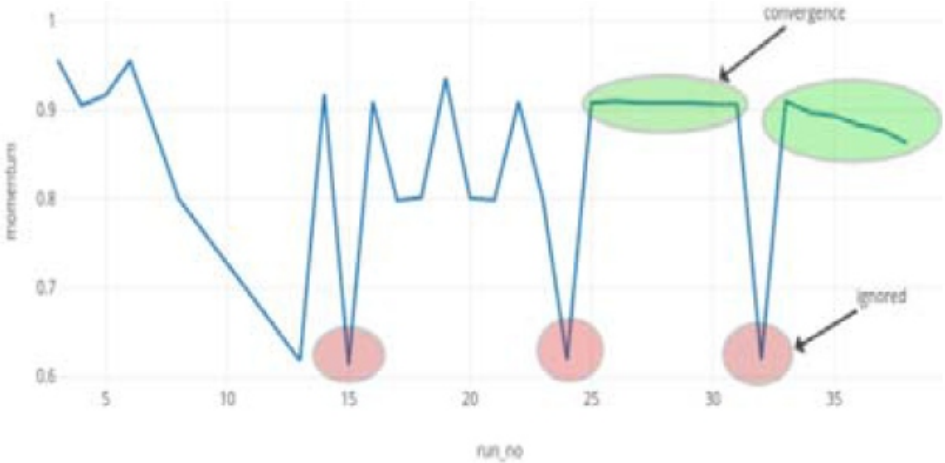


Fig 14: Convergence of Momentum for Bayesian Tuning with Horovod

Fig. 14 shows as the runs progressed the momentum started to converge to values between 0.8 and 0.9 The sampled regions around lower momentum values like 0.8 were not explored further as the Bayesian optimization tuning considered it not better and hence not taken to convergence.

From the results of both the experiments we saw different convergence regions, Experiment 1 with four concurrent runs and Bayesian Optimization converged to higher learning rates and lower momentum values whereas Experiment 2 with two concurrent runs and distributed training with Horovod and Bayesian optimization converged to higher momentum and lower learning rates. Both the convergence regions performed reasonably well as we saw from the convergence table values in Table IV and Table V. D. Unexplored Hyperparameter Regions Some regions of hyperparameters were left unexplored with Bayesian optimization tuning with both the approaches. This attributed to the limited number of runs,

vast combinations to explore across the three hyperparameters – learning rate, momentum and batch size and also the exploitation – exploration tradeoff setting for the Bayesian Optimization tuning.

Fig 15: Unxplored regions of Learning Rate and Momentum for Baysian Tuning–Experiment I

Fig. 15 shows the unexplored regions Experiment 1 which was distributed hyperparameter tuning with Bayesian optimization and four concurrent runs. The explored regions seem to be fairly distributed with still scope for lot of improvement.

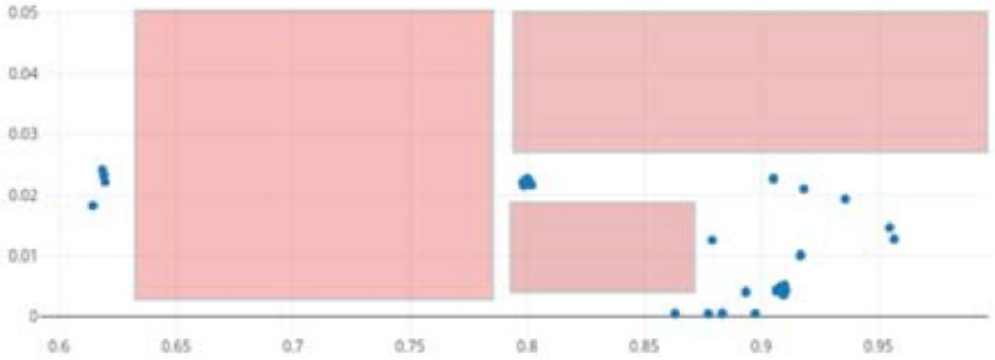


Fig 16: Unxplored regions of Learning Rate and Momentum for Baysian Tuning with Horovod– Experiment II

Fig. 16 shows the unexplored regions Experiment 2 which was distributed hyperparameter tuning with Bayesian optimization, horovod for distributed training and two concurrent runs. The explored regions do not seem to be fairly distributed with still scope for lot of improvement.

Though both the approaches have scope for improvement, experiment 1 which was initiated with more warm-up runs due to higher concurrency seemed to have reasonable coverage in the hyperparameter space across the three hyperparameters.

Experiment 2 where we used only two concurrent runs for Bayesian tuning though it yielded convergence of hyperparameters with reasonable accuracy did not have good coverage across the hyperparameter space for learning rate and momentum. This can be more acute when we are exploring higher dimension spaces of hyperparameters.

V. CONCLUSION

The experiments indicated that Bayesian Optimization can be very helpful to explore higher dimensional hyperparameter spaces especially when initiated with more warm-up runs to guide the exploration-exploitation process.

With availability of horovod for distributed training, each iteration can be completed faster with more compute thereby accelerating time towards convergence. The number of machine learning computes were not altered during this exercise, future work can explore varying computes in the cloud with more compute deployed during the warm-up phase and decreasing compute as the optimization marches towards convergence. This can significantly improve costs taking advantage of the convergence of the Bayesian optimization process.

REFERENCES

[1] Eric Brochu, Vlad M. Cora, Nando de Freitas (2010) A Tutorial on Bayesian Optimization of Expensive Cost Functions, with Application to Active User Modeling and Hierarchical Reinforcement Learning. arXiv: 1012.2599v1

[2] Niranjan Srinivas., Andreas Krause, Sham M. Kakade, Matthias Seeger (2010) Gaussian Process Optimization in the Bandit Setting: No Regret and Experimental Design. arXiv:0912.3995v4

[3] Thomas Desautels, Andreas Krause, Joel Burdick (2012) Parallelizing Exploration–Exploitation Tradeoffs with Gaussian Process Bandit Optimization. In Proceedings of the 29th International Conference on Machine Learning, Edinburgh, Scotland, UK

[4] Daniel Golovin, Benjamin Solnik, Subhodeep Moitra, Greg Kochanski, John Karro, D. Sculley (2017) Google Vizier: A Service for Black-Box Optimization. In Proceedings of the 23rd Knowledge Discovery and Data Mining Conference, Halifax, NS, Canada

[5] Nicolo Fusi., Rishit Sheth , Melih Huseyn Elibol (2018) Probabilistic Matrix Factorization for Automated Machine Learning. arXiv:1705.05355v2

[6] Sergeev, A., Del Balso, M. (2018) Horovod: fast and easy distributed deep learning in TensorFlow. arXiv:1802.05799v3.

ISSN (Print): 2321 -4058, (Online): 2321 -4392

Client- Side Web Development Learning Environment with Utilization of Real Time Collaboration Tools (WEBLECT) using WEBRTC for Blended Learning

[1] John R. Del Rosario, [2] Benilda Eleonor V. Comendador
[1,2]Polytechnic University of the Philippines
E-mail: [1]john.delrosario@live.com.ph, [2]bennycomendador@yahoo.com

ABSTRACT

The learning process is aided by employing collaboration-based information possibly improving its retention through the already proven effectiveness of blended learning models. Going with the interaction and experience based blended learning, actual application of a problem-solving scenario makes a person try to accomplish the task based on how it was achieved in the past before trying anything else. With enough experience of tackling a problem a learner should be able to tap previous knowledge to accomplish an endeavor. Allowing a more meaningful approach to learning enables learners to retain as much information as possible. In this study a survey was conducted to gain understanding on web development learner's ideas on learning better through collaboration. The proponent used different studies as a reference for enhancing learners' experiences in web development learning which was eventually developed in to a learning management system with real-time collaboration tools. Web RTC was used in providing the real-time functionalities within the system that allowed learners to communicate in real-time thereby enhancing their experience and allowing them to share and collaborate ideas.

Keywords - Blended Learning, Experiential Learning, Web Development, Web, WebRTC

I. INTRODUCTION

Interactive teaching is becoming a feasible way of allowing learners to understand more about subject matters in a way that enables them to better grasp concepts through visualization. In general, the way in which individual concepts and theories are initially learned seems to play an important role in the degree to which this information is used later on. [1] Even in a classroom setting particularly computer classes where activities are subject to so much disorganization, reaching out to every student is a challenge. Enabling real time communication heightens interactions and increases the possibility of learners actually retaining information in events that need learners to acquire the knowledge in the form of condition-action pairs mediated by appropriate goaloriented hierarchies. [1]. Allowing learners to interact through activities that challenge them should allow better retention of information as they are given more point-of-reference moments wherein they required a particular piece of information. Therefore any tool allowing such interaction heightens the experience of education and retention.

Blended learning is a formal education program in which a student learns at least in part through online delivery of content and instruction with some element of student control over time, place, path, and/or pace and at least in part at a supervised brick-and-mortar location away from home. By combining traditional classroom model and application of technological tools in learning, students are exposed to an improved learning experience. [2] By using the aforementioned technology on a learning tool gives possibilities of learners cooperating in activity scenarios where in previous practices are confined. Having these learners subjected to exchange of information technically exposes them to greater amount

of experience thus possibility having them learn more. Not only through these exchanges but also will they learn through the exposure to different environments that would require them to collaborate to others in order to gain the information, thus allowing them to mark a piece of event in their memory that this particular event required them to acquire a piece of information relevant to their objective which makes this kind of learning admirable for blended learning.

Since the mid-1980s, organizations around the world have depended on video conferencing to help them conduct business in a cost-effective, efficient, and more productive manner. Real world deployments have traditionally focused on the conference room as the implementation, the business meeting as the application, and reduced travel expenses as the benefit.[3]

It is no question that implementing real time communications can benefit any entity in a number of ways depending on the use case, though it can be challenging to do the implementation of such technology. Despite criticisms to the web being dead [4] HTML and JavaScript are also emerging as a popular development platform for stand-alone applications, especially for smart phones and tablets. [5][6]JavaScript eventually became a key component in enabling continued evolution of the world wide web and through the introduction of Ajax made it a more interactive and dynamic environment. [7]Following this trend came WebRTC which utilizes the web as a media for real time communications.

WebRTC is being shipped as an API within the Web browser through JavaScript. All the platforms supported by the said technology is based upon the native APIs that are implemented based on the WebRTC specifications. [8] Having a common codebase for the technology would mean that development of applications using it would mean less overhead as there will be little to no differences in the usages of the APIs hence the more likely for it to be plausible for implementations of innovations especially in the field of education wherein the need for accessibility is an important factor. Being open source also has its merits because compared to all other implementations having the technological solution that costs nothing and is free for all to modify and use benefits all parties – both user and the technology. [9]

II. PROPOSED SYSTEM

2.1 Related Studies

Previous blended learning environment implementations lacked on the collaboration aspect as stated by most of the studies. The main reason for not being able to provide for the needs in this aspect was the lack of technology to fully support what the community wants which is to be able to replicate the brick and mortar type of learning as much as possible within a blended learning setup. Furthermore, the technology before also did not come simple, cheap or effective enough to be able to integrate it with the concepts of learning already known. These studies provided the proponent a venue for improving the conditions of learning in this aspect as well to demonstrate the available technology toolset as of the time of writing of the study. Due to these reasons, the desire to create a learning environment with collaboration tools deriving from an open-source publicly available technology was met and thus the author developed WEBLECT.

2.2 Introduction to blended learning

Today's education are based on a variety of learning models that are always adjusted to align with the strategic objects. Both the effectiveness of the learning model and the susceptibility of the students to get

more information are taken into consideration in choosing what model to apply and what are to adjust in it in order to make the most out of the learning application. Some researchers coined traditional schooling as a factory model wherein the students are expected to be an output of the ideals of the school which is basically the opposite of what our education should be which is to deal with the deficiencies of the students in order to progress them to what they ought to be.

It has been described as a defunct methodology because what the school should be bringing to students are the levels of content that the students are capable of, not the other way around. In doing so the learning process encourages the students to pursue their own interest because they are not burdened by keeping up with the demands of the learning process and instead enable them to be at their own pace and measure their own learning. [10][11]

With the generation of computerization and information age almost all its applications that are found feasible are made and eventually made its way into the realm of learning. Taking blended learning's meaning literally wherein it being defined as a composition of different approaches, models and styles of learning computerized media, it has been made to cater to the learners' needs. [12] Through the course of time it has been made that this learning model coincide with the traditional brick-and-mortar way of teaching and learning as the subject matters that require the usage of certain kinds of technology eventually required the mixture of both. With this need came the transition and dilemma whether the combination of both elements is actually good enough to sustain the previous ways of learning and be good enough to take its effectiveness one step further.[13]

2.3 Blended learning problems in the communication domain

Blended learning has always been a challenge to implement effectively. For most of the part the communications aspect of blended learning has always been the most critical in that the focus of the communications must be learner-centric.

Previous efforts to smoothen communications was not that effective for the learners felt that the tools in use, that is online content, discussion boards and emails, were lacking interaction and too out of focus. [14] As technology became more capable interactions between students and student-teachers became more of the focus as well as these were still elements of normal classroom settings that are proved to contribute to other student's learning. [15] This concept then paved the way to interactions-astransaction paradigm [16] wherein the factors outlined in some researchers through interactivity correlates to the overall learning experience of students and should be taken into consideration when designing a course outline for blended learning. And with that employment of communication aides for learning became a norm that technology caught up with it and enabled more opportunities to enhance the learning experience for both teachers and students alike. With technology courses being a challenge to teach as it forces a classroom to combine traditional face to face learning, technology application either becomes a leverage or a distraction as stated current blended learning environments have difficulties in bridging the gap between learners and materials interaction. [17][18][19]

2.4 Evolution of enabling technology that can support blended learning

Through the utilization of capable blended learning methodologies and technology, educators are able to identify the extent of the students' competences and are the one to adapt what they will serve to the learners in order to maximize their learning capability without the cost of the students' welfare and confidence.[20] Technology surmounts geographical limitations of traditional communication and at

this point in time is being pushed even further by enabling it at real time. The application in education made it possible to support remote learning without physical interaction but through blended learning interestingly this technique is also being applied and is demanding even more collaborative functionalities in order to simulate local classroom environments. [12][20] But technology almost always does not come free and is a product of extensive research and development. With regard to blended and ubiquitous learning the first concepts of using computer technologies in teachingcame with the idea that any electronic instrument could aid in teaching then with computers came elearning.

[21] By then most of the implementations of communication agents was mostly through asynchronous methodologies wherein users will only tap the agent on the time that is mostly convenient for them. [22] Some examples of asynchronous implementations are through message boards, blogs, and messaging systems [20][23] and improved reference materials called wikis which are now in extensive use and the one at most recent which is social media. [24]

On the other hand is synchronous learning which is the most similar of all ubiquitous learning implementations to traditional classroom learning methodology wherein the interactions are done in real time. [25] The feeling of having communications in real time heightens the feeling of having a real conversation and interaction [26] which has been seen to be directly correlated with learning satisfaction and retention. [27]

2.5 Differences of technology that can be utilized in blended learning

Given the differences between the technologies now and back in the past it can be seen that it has improved much that the openness of technology makes the capability knock almost at our doorsteps. Both synchrony and asynchrony in communications is not a problem anymore as the technology tackling it evolves every single day.

Computer networking being implemented in both wired and wireless formats through Ethernet paved the way to it become the medium for other technologies for communication. [28] With the medium in place implementations then came starting with the hypertext transfer protocol or commonly known as HTTP which aimed and eventually became the standard information exchange for the World Wide Web. [29] The exchange of information became more demanding as the usage of the World Wide Web grew from basic content exchange demand to requests of applications being in place in the web ranging from simple to complex which required a more interactive version of served content.

[7]XMLHttpRequest or now commonly known as AJAX answered the need for the level of dynamicness as it allowed the once static content served from initial HTTP requests to be appended or manipulated using retrieved additional content from server.[30] Though it alleviated the need for a dynamic functionality it was not a perfect solution because this was still implemented through HTTP wherein a content was only served whenever it was requested by a client which is not really a 2 way communication that fulfilled the purpose of the new dynamic-ness which became the demand.

The need for a real time communication through the World Wide Web was fulfilled by the emergence of the protocol called Web Sockets. The need for the protocol came from the limitations of XMLHttpRequest. With Web Sockets the communication between machines became bidirectional removing the need for client-server to wait for a resource request and now only requires a negotiation to initiate the direct communications.

This eliminated the workaround used to make this possible in the previous technologies and making implementation more seamless. [31] Demands seems to move along with the advancement of technology as requirements for more complex and challenging web applications are envisioned. Moving further from client-server model the industry demanded a model wherein machines could communicate directly with each other eliminating the need for a server to mediate with communications.

Doing so could eliminate the costs of maintaining an additional server and would really scale well as only the peers themselves would talk in between the communications. Superseding the Web Sockets in this particular area is the WebRTC which enables bidirectional peer to peer communication that allows sharing of media and data more efficiently than its predecessors. With the data stream going through less machines the chances of data being lost decreases therefore increases reliability and the communications' latency decreases therefore improving overall performance. [32] What sets WebRTC apart from other technologies is that it is an open source project which means that there will be no costs in gaining hold of its usage as opposed to other technologies. WebRTC is also build as a specification and what this means is that the functionality which is now build in directly into browsers and some mobile devices will soon reach other kinds of devices as well. The other notable implementation also provide real time communications but with caveats is the notable Real-Time Messaging Protocol or also known as RTMP which is a proprietary protocol that enables performant transmission media for data and multimedia but can only be used on Adobe Flash [33], which is also notable mentioning that is being avoided in favor of HTML5 which is also open source and is built-in within browsers. [34]

2.6 System Architecture

The system is developed through a multi-tier architecture design that consists of the application, database and communications server. Figure 3 describes the overall system architecture of WEBLECT. The application server is responsible for serving the application to the connecting clients over HTTPS. WebRTC only allows connection through a secure protocol for security reasons so HTTPS is the only viable option. It is responsible for authenticating the users and facilitating data transfer. The application server is served through Microsoft's IIS Server. The communications server is responsible for the signaling processes of WEBRTC which is required to establish the peer-to-peer connection sessions, which allows the clients to communicate directly to each other. The server implements the Socket.IO software through the NodeJS platform.

Once sessions are established, the clients can exchange data directly, that is without server facilitation and network traffic intervention, to each other and in real time. (WebRTC 1.0: Real-time Communication Between Browsers, 2016) The database server contains the application repository which hosts the data for the tool which includes user, course, activities and assessment records. The database server is implemented through Microsoft's SQL server. The tool in which the study is focused on should aid in the learning of web development through the features that is integrated in it. The activities dashboard provides the pending and upcoming activities for students as well as the pending assessments for instructors for a course. The course and activities management features allow the instructors to create and manage the content of the respective items while allowing the students to view and download the inputted contents in it. The user and roles management allow administrators to manage the accounts within the system and assign roles for each. The assessment management allows administrator accounts to assess activities submitted by students. The Web IDE provides the area for students to code web elements including HTML, JavaScript and CSS and allows them to show the output in the same page. This page is part of the students' activity workflow. The Web IDE also provides the

collaboration tools that transmit and receive data in real-time where the modules are described in Error! Reference source not found..

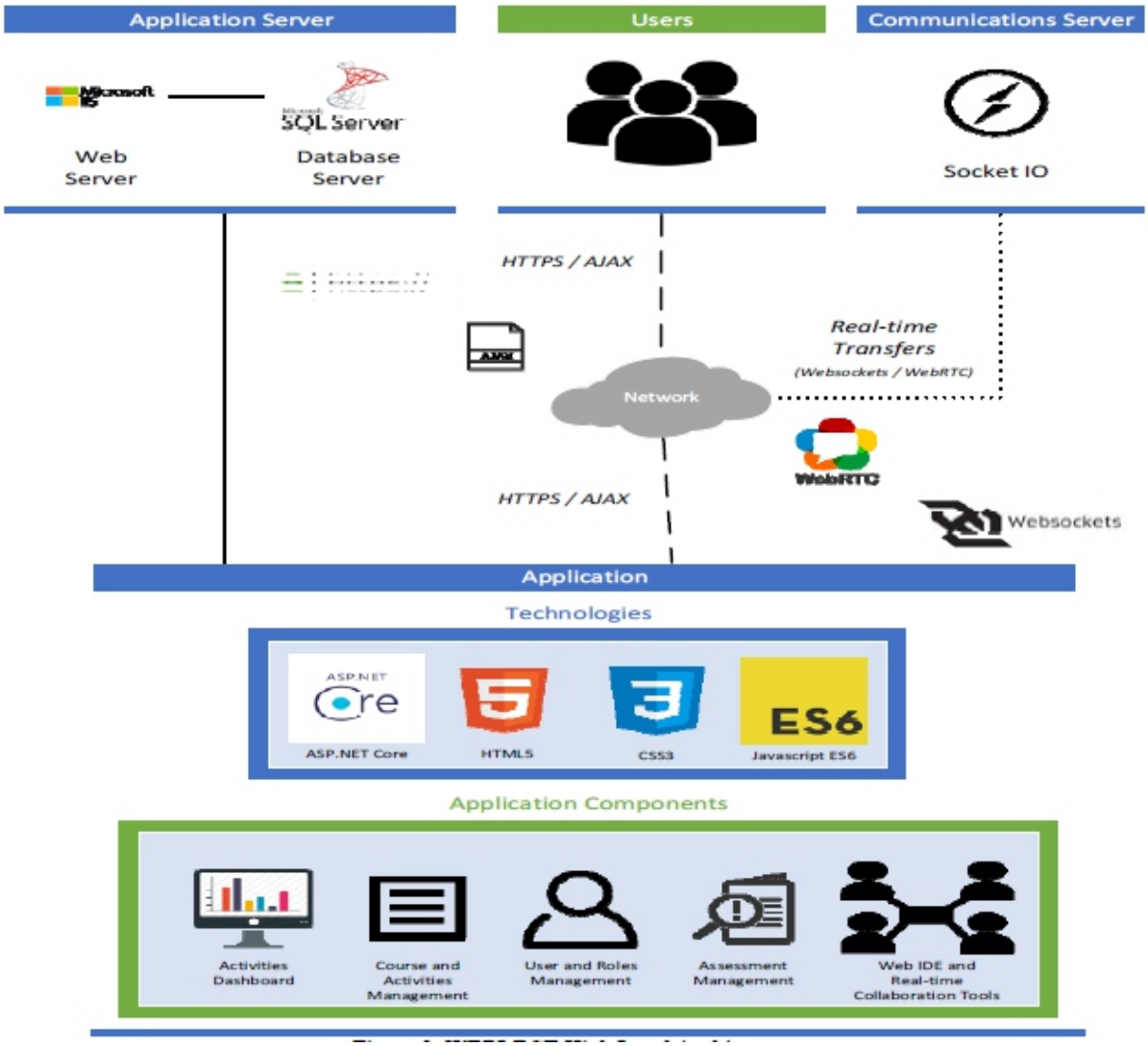


Figure 1. WEBLECT High Level Architecture

The application components can be used by the user logging in first within the system. The system administrator would need to setup the users that will have normal and administrative access to the system.

The admin should then set the courses which provide the high-level element for the student interaction. Next that will be set up is the lessons and the activities within it. When everything has been set up can the collaboration of the users take place in the activity modules where the users are connected to each other through the collaboration modules. After the activity has been submitted can the corresponding administrators view and rate their students' activity sessions. When all the activities of the student for the particular lesson are assessed then can it be assessed; the same with the overall course assessment. The assessed elements can then be viewed by the students when it is presented in their dashboard or when they access the corresponding page.

The application components are used in a manner flow as described in Figure 2.

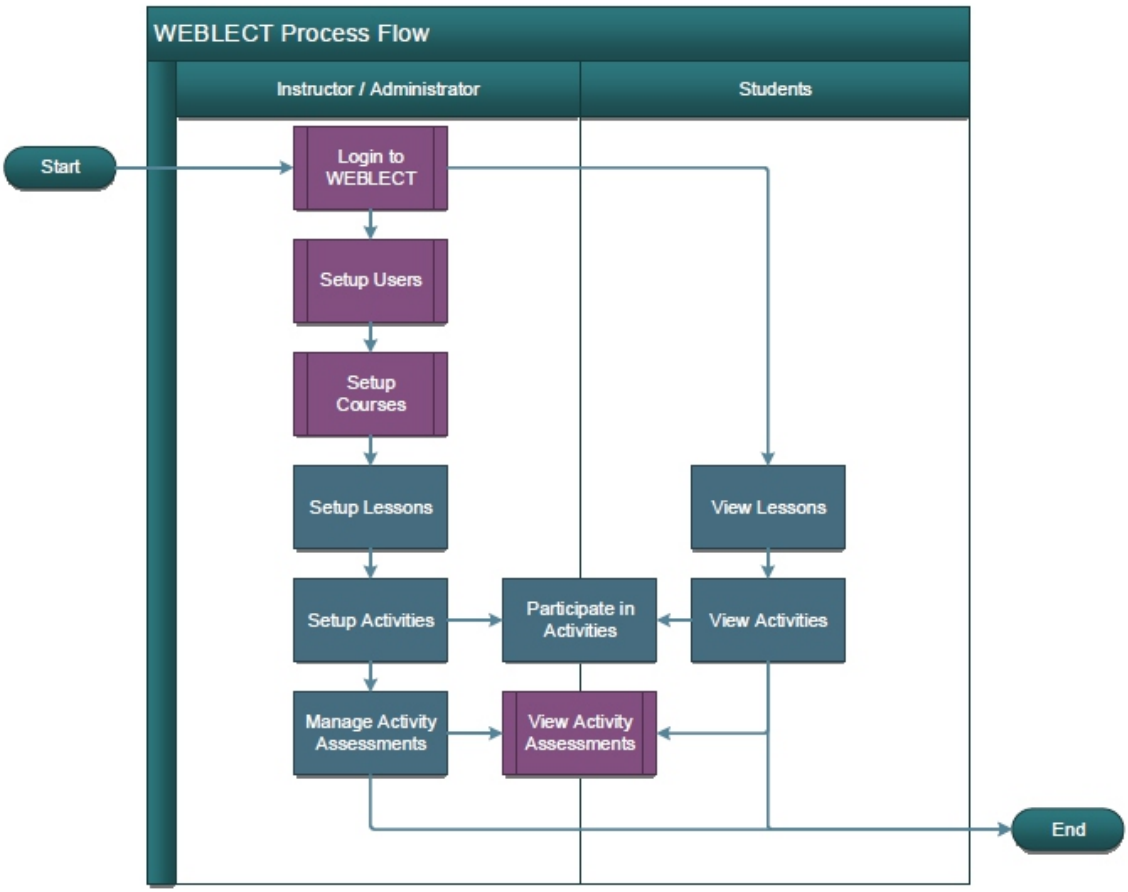


Figure 2. WEBLECT Process Flow Diagram

The real-time communication modules are included through the application inside the application server through the real-time functionalities of Socket.IO and WebRTC. These technologies were chosen because of many reasons mainly with these technologies being free and open-source, secure, and easy to develop and deploy. There is not many, if any, licensing issues and interoperability is great with other existing technologies.

WebRTC also reduces load in operating costs as connections are made by the clients itself and does not rely on servers once connected so concurrency and reliability is high.

As with many existing learning management systems being expandable they suffer from performance issues as extending the base system requires more resources for its servers to perform well; In contrast with the tool developed the modules integrated with it does not piggy back on the actual used servers.

The real-time communications modules are initiated by user in the application through the browser. This initialization in turn requires the communications server to establish the peer to peer communication of the client computers. When the peer-to-peer communications channel is established all the modules is then connected directly with the other clients through it and does not require the server anymore, courtesy of WebRTC as described in Figure 3.

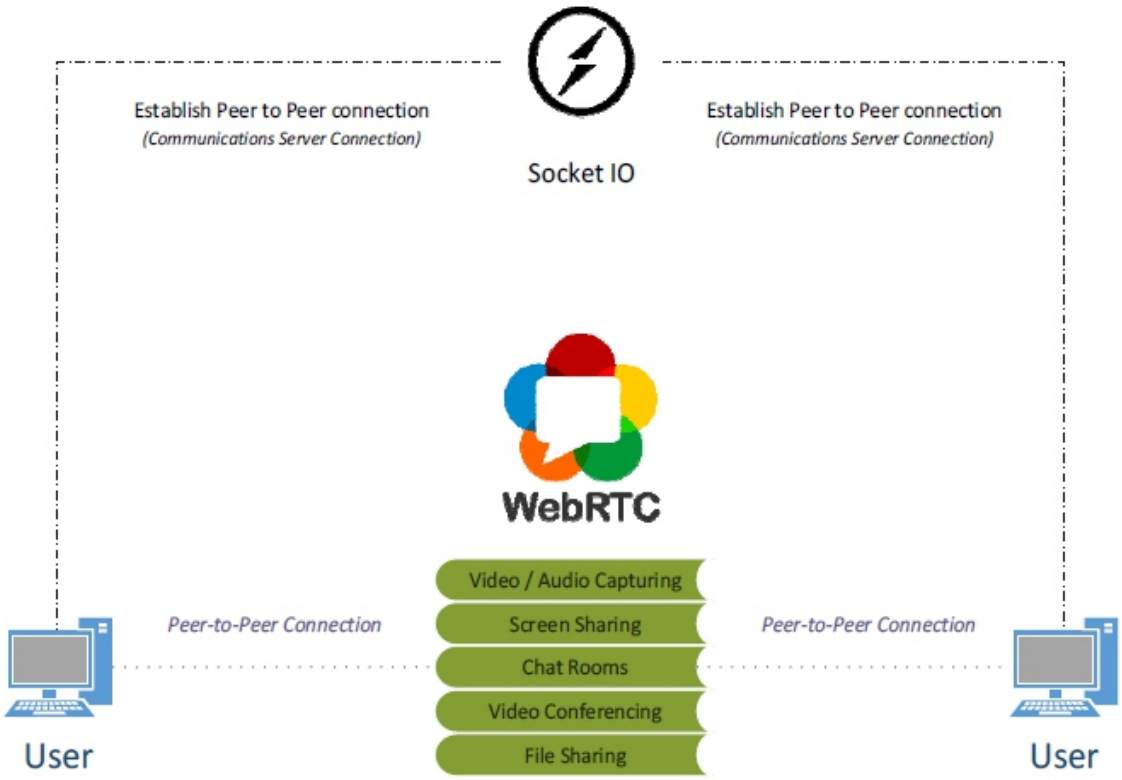


Figure 3.WebRTC Peer to Peer Connection Establishment

The collaboration tools are fired in sequence which starts with the session initiation on the user interaction of the system which is followed by the system prompting the client directly to other users with its guidance using the peer information within its signaling mechanism. Once peer information is exchanged then data is passed through the connected clients peer to peer. The subsequent connection requests of the software as described in the UML sequence diagram in Figure 4.

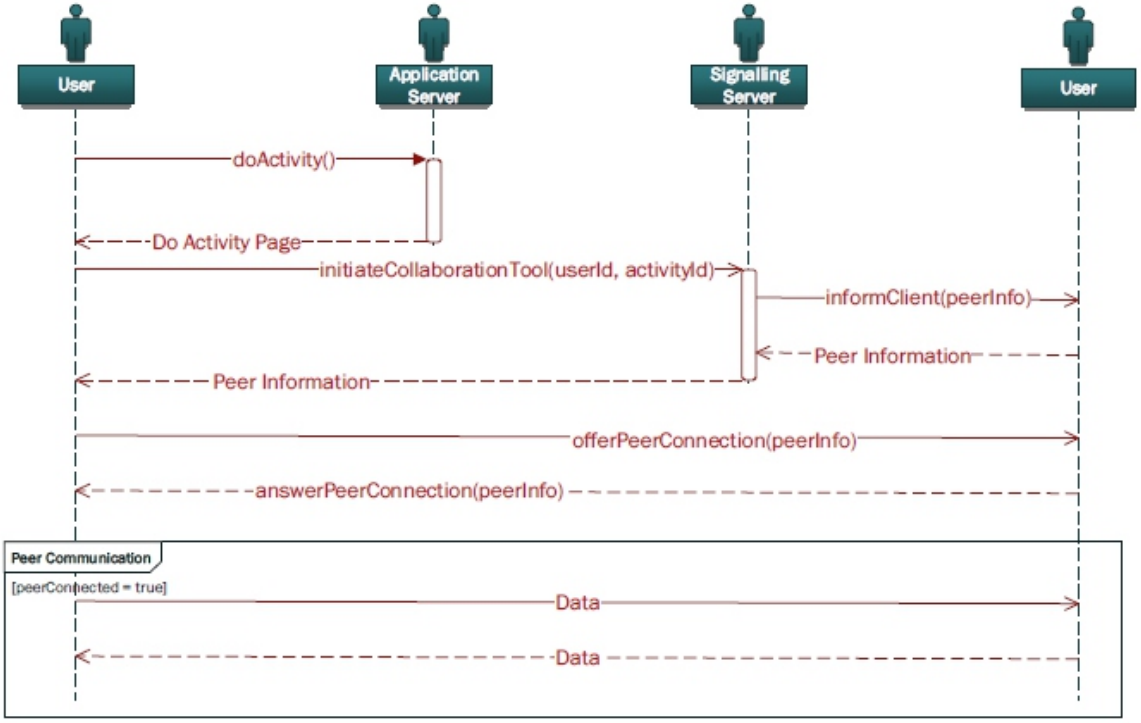


Figure 4. WebRTC High-Level Sequence Diagram

The application was configured to support up to one 200 simultaneous WebRTC connections in a mesh topology per web browser tab to function safely and efficiently. The file attachment limit is configured to 50 megabytes (50 MB) which is transferred in chunks of 16 kilobytes (16 KB) to avoid bad network traffic across simultaneous users. The application is estimated to handle 20,000 concurrent users with normal usage and data. The WebRTC currently supports open-source codecs in its implementation which are VP8 for video and G.711, G.722, iLBC, and iSAC for audio.

Table 1presents the technical features of WEBLECT.

Table 1 - Technical Features of WEBLECT

Features	Specifications
Simultaneous Users Per Browser Tab	200 Users
Concurrent Users	20000 Users
Data Transfer Chunk Size	0.000016 Megabytes (16 Kilobytes)
Maximum File Attachment Size	50 Megabytes
Signaling Server Memory Usage Per User	0.05 Megabytes
WebRTC Supported Video Codecs	VP8
WebRTC Supported Audio Codecs	G.711, G.722, iLBC, and iSAC

The features were measured against a machine hosting all the system tiers namely the application, signaling and database components with a processor of Intel Core i7-4710MQ 2.50 GHz, a random-access memory size of 16 gigabytes (16 GB), and storage space of 500 gigabytes (500 GB) on a Microsoft Windows 10 Pro Operating System. Error!

Reference source not found.
shows the hardware specifications of the machine wherein the demo was run against during the time of the study.

Table 2 - Hardware Specifications

Hardware	Specification
Processor	Intel Core i7-4710MQ 2.50 GHz
Random-Access Memory	16 Gigabytes
Hard Disk Capacity	500 Gigabytes
Operating System	Windows 10 Pro

III. CONCLUSION

Based on the findings of the study there are challenges in learning through a web development course that can be addressed for learners to appreciate diving further in to web development.

The respondents' level of agreement on the importance of collaboration tools in a web development learning environment show that they agree in the inclusion of such tools on the subject's learning environment. The respondents' level of acceptance on the software based on its functionality, reliability, usability and performance implies that they find the software acceptable in such aspects.

And finally there are rooms for improvement and enhancements for the client-side web development learning environment with utilization of real time collaboration tools using WebRTC.

Since the study will be focusing on the implementation of the technology the recommended way forward is to implement other smart systems to integrate with WebRTC. It is also recommended to proceed with further implementation of computer aided learning algorithms within the tool to further its usefulness. Collaboration definitely helps in having more control over the course flow of the lesson and learner inquiry so inclusion of these in a learning environment should step up the students' learning experiences. The software must apply the suggested improvements of the study's respondents which allows them to have a better learning experience.

2. Appendices

REFERENCES

[1] J. D. S. R. D. H. T. S. K. C. K. &. W. S. M. Bransford, "Anchored instruction: Why we need it and how technology can help," Cognition, education, and multimedia: exploring ideas in high technology, 1990.

[2] H. S. a. M. B. Horn, "Classifying K–12 Blended Learning," May 2012. [Online]. Available: http://www.christenseninstitute.org/.I. M. Weinstein, "The New Business Case for Video Conferencing," p. 2, 2013.

[3] R. L. H. T. S. a. J. S. Stephan Herhut, Parallel Programming for the Web, Berkeley, CA: USENIX, 2012.

[4] "Boot to Gecko," [Online]. Available: https://wiki.mozilla.org/B2G.

[5] M. Siegler, "Project Spartan: Facebook's Hush-Hush Plan to Take On Apple On Their Own Turf: iOS.," [Online]. Available: http://techcrunch.com/2011/06/.

[6] Liu, "JavaScript and the Netflix User Interface – Conditional Dependency Resolution," AcmQueue, 2014. Google, "WebRTC," 2014. [Online]. Available: http://www.webrtc.org/home.

[7] S. P. K. Vamshi Ambati, "How can Academic Software Research and Open Source Software Development help each other?," 2004.

[8] M. Y. S. Buket Akkoyunlu, "A Study of Student's Perceptions in a Blended Learning Environment Based on Different Learning Styles," Educational Technology & Society, 2008.

[9] L. M. Miller, "Using learning styles to evaluate computerbased instruction," Computers in Human Behavior, p. 287–306, 2005.

[10] H. Chris Procter, "Reflections on the Use of Blended Learning," Education in a Changing Environment, 2004.

[11] M. B. H. a. H. S. Clayton M. Christensen, Is K–12 Blended Learning Disruptive?, Clayton Christensen Institute for Disruptive Innovation, 2013.

[12] H. Frances Bell, "With regard to respect: a framework for governance of educational virtual communities," International Journal of Web Based Communities, 2004.

[13] R. Donnelly, "Harmonizing Technology With Interaftion In Blended Problem-Based Learning," Computers and Education, pp. pp.350-359, 2010.

[14] E. D. Wagner, "On Designing Interaction Experiences for the Next Generation of Blended Learning," in The Handbook of Blended Learning: Global Perspectives, Local Designs, San Francisco, 2005, pp. 41-55.

[15] M. Keppell, "Authentic Cases and Media Triggers for Supporting Problem-Based Learning in Teacher Education," Authentic Learning Environments in Higher Education, 2016.

[16] C. B. Lorna Uden, "Technology and problem-based learning," British Journal of Educational Technology, 2007.

[17] Ö. Delialioğlu, "Student Engagement in Blended Learning Environments with Lecture-Based and Problem-Based Instructional Approaches," Educational Technology & Society, 2012.
[18] U. Köse, "A blended learning model supported with Web 2.0 technologies," Procedia Social and Behavioral Sciences 2, 2010.
[19] N. G. M. Kundi, "From E-Learning 1.0 to E-Learning 2.0: Threats and Opportunities for Higher Education in Developing Countries," European Journal of Sustainable Development, pp. 145-160, 2014.
[20] G. Salmon, E-moderating - The Key to Teaching and Learning Online, 2007.
[21] M. Ebner, "E-learning 2.0 = e-learning 1.0 + web 2.0?," The 2nd International Conference on availability, reliability and security, pp. 1235 - 1239, 2007. L. Ferret, "Wikis and e-learning," in E-learning concepts and techniques, Bloomsburg, Bloomsburg University, 2006, pp. 73-74.
[22] J. I. S.-J. X. G. Wendy Zhang, "Can E-learning Replace the Traditional Classroom - A case study at a private highschool," ISECON, 2007.
[23] K. P. Rena M. Palloff, Building Online Learning Communities, Jossey-Bass, 2007.
[24] G. Picciano, "Beyond Student Perceptions Issues of Interaction, Presence, and Performance," JALN, 2002.
[25] P. G. J. Ferdy Hanssen, "Real-time communication protocols: an overview," 2003.
[26] R. T. Fielding, J. Gettys, J. C. Mogul, H. F. Nielsen, L. Masinter, P. J. Leach and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999. [Online]. Available: https://tools.ietf.org/html/rfc2616.
[27] "The responseXML attribute of the XMLHttpRequest object explained by the W3C Working Draft," 30 January 2014. [Online]. Available: https://www.w3.org/TR/XMLHttpRequest/#responsexml.
[28] M. Ian Fette, "The WebSocket Protocol," December 2011.[Online]. Available: https://tools.ietf.org/html/rfc6455#section-1.1.
[29] J. Y. K. S. Alan Johnston, "Taking on WebRTC in an Enterprise," IEEE Communications Magazine, vol. 51, no. 4, 2013.
[30] E. M. T. E. H. Parmar, "Real-Time Messaging Protocol (RTMP) specification," 21 December 2012. [Online]. Available: https://www.adobe.com/devnet/rtmp.html.
[31] S. Jobs, "Thoughts on Flash," April 2010. [Online]. Available: http://www.apple.com/hotnews/thoughts-onflash/.
[32] J. R. Lourenço, B. Cabral, P. Carreiro, M. Vieira and J. Bernardino, "Choosing the right NoSQL database for the job: a quality attribute evaluation," Journal of Big Data, 2015.
[33] V. R. B. Craig Larman, "Iterative and Incremental Development: A Brief History," Computer, 2003.
[34] "WebRTC 1.0: Real-time Communication Between Browsers," 13 September 2016. [Online]. Available: https://www.w3.org/TR/webrtc/#examples-and-call-flows.

ISSN (Print): 2321 -4058, (Online): 2321 -4392

Enabling Search Operations on Private Spatial Data in Cloud

[1] A. Merlin Monisha, [2] M. Lilly Florence
[1]M. Tech. Scholar, Adhiyamaan College of Engineering, Hosur-635109
[2]Prof / CSE, Professor Adhiyamaan College of Engineering, Hosur-635109
E-mail: [1]mailtomerlinmonisha@gmail.com, [2]lilly_swamy@yahoo.co.in

ABSTRACT

Cloud offering different kinds of services to users and organizations with different cloud model like public cloud, private cloud and hybrid cloud. Introducing public cloud which provides data storage and query services available for more users along with low cost. Data outsourcing is a common cloud computing model that allows data owners to take advantage of its on-demand storage and computational resources. The main challenge is maintaining data confidentiality regarding intruders. Present methodologies either conciliation the undisclosed of the data or undergo from high communication cost between the server and the user. To overcome this problem, suggest a dual transformation and encryption scheme for spatial data, where encrypted queries are executed entirely by the service provider on the encrypted database, and encrypted results are returned to the user. The user issues spatial related queries to the service provider, using the decrypt key the user can get the response. Finally our proposed method moderates the unique query communication between the authorized user and service provider. Encrypt the data using Advanced Encryption Standard and Indexing and ranking algorithm to process KNN queries.

Keywords - Spatial Databases, Data Encryption, Security, Query Processing, Database Outsourcing.

I. INTRODUCTION

The expansion of spatial information has driven associations to transfer their information onto outsider specialist organizations. Distributed computing enables information proprietors to outsource their databases, disposing of the requirement for exorbitant capacity and computational assets.

The admin was created to detail the working of a hospital record keeping system in respect to patient information from this project. Then patient has to share their location, so that the patient nearby places are displaying. Now patient can give request to the admin. The admin has to receive the request from patient and he has to provide the AES key for each patient. After receiving the AES key from admin the patient can decrypt the records and receiving the original records of patient.

For a little cost, associations with constrained assets can outsource their extensive volumes of information to an outsider specialist co-op and use their powerfully adaptable capacity and computational power. In any case, the reality remains that the information is controlled by an untrusted outsider and this raises basic security issues, for example, secrecy and honesty. Information privacy necessitates that information isn't revealed to untrusted clients and information trustworthiness guarantees that information isn't adjusted before being prepared by the server.

As of late, unique areas, for example, the database and the cryptography network have investigated the issue of questioning scrambled information at the untrusted specialist organization. This outsourcing of information cuts down both venture cost and operational costs for colossal partnerships. In the

meantime, outsourcing involves that clients lose essential control of their information and tasks performed on the information. This thusly infers the information is helpless to security concerns, for example, information privacy.

Recently, mobile devices and navigational systems have become exceedingly common and this has created the need for Location-Based Services (LBSs), which is a motivating application for database outsourcing. This in turn has led to an increase in spatial data which has to be managed and maintained effectively. Spatial data in a LBS includes the location information (i.e., latitude and longitude) besides other descriptive components which require huge storage capacity. Numerous users require LBSs on a daily basis and would like to issue spatial queries in an anonymous manner with a fast response. Also, the data owners do not want to reveal the data to the service provider in order to maintain the confidentiality of the data. With a cloud computing platform, it is possible to enhance query processing without burdening the user and manage the storage efficiently. Therefore, in this work, the aim is to effectively utilize the cloud environment to provide high throughput processing with low latency by performing queries at the service provider.

Thus, one has to consider the following requirements when outsourcing spatial databases in the cloud environment. First, the database content should be kept hidden from the service provider and malicious attackers.

Another important issue to resolve is the development of efficient query processing techniques that can be executed on encrypted data at the service provider, such that user queries are handled entirely at the service provider without requiring multiple rounds of communication with the authenticated users. Several specialized encryption techniques have been proposed for this purpose. A relatively new encryption scheme is the Fully Homomorphic Encryption technique proposed by Gentry et al., which enables direct computation on encrypted data which is stored in the service providers in the cloud.

Different types of queries can be processed without decrypting the data. However, all known homomorphic schemes are too inefficient for use in practice and suffer from high performance overhead.

One of the practical schemes, which is partially homomorphic, is the order-preserving encryption (OPE) technique introduced by Agrawal et al. OPE hides the original data values while allowing simple comparisons to be correctly evaluated on the encrypted data i.e., the order relation of plaintexts in ciphertexts is preserved. The cloud servers have no knowledge concerning the stored data, the processing function, the result, and any intermediate result values. Therefore, the outsourced comparison is performed in a fully secure manner. This permits range queries on the encrypted data directly at the untrusted service provider without having to decrypt confidential data.

Most existing approaches protect the outsourced data using spatial transformation schemes or conventional cryptographic techniques. However, to the best of our knowledge, with most schemes there is a trade-off between data confidentiality and efficient query processing. To overcome these limitations, we propose a two-layer encoding approach, in which the spatial data points are transformed and then an encryption technique is applied to the transformed spatial space. Encryption allows data to be securely outsourced to the untrusted service provider, while the transformation adds another layer of security to the approach by hiding the original location of the points.

In this paper, the cloud architecture model used comprises of 3 main entities, namely the Data Owner (DO), Service Provider (SP) and Authenticated User (AU). The DO guarantees security by transforming and encrypting the spatial database before outsourcing to the SP. To transform the 2D spatial data points, the DO employs the Hilbert space-filling curve. The DO forms a list of packets defined by the Hilbert ordering. Next, this list is encrypted using the OPE technique, which allows spatial range queries to be performed at the SP without engaging the user and reducing any additional communication overhead.

Additionally, the DO provides the Hilbert transformation key as well as the encryption key to the AUs. The keys are used by the AU to issue encoded range queries to the SP. The query is processed on the encrypted database at the SP and the results are returned to the AU. Lastly, the AU decrypts the query response using the encryption key to obtain the actual result.

The main issue with OPE is that it cannot provide ideal security desired by cloud consumers since the order of plaintext is revealed by the ciphertext. Moreover, with the basic OPE scheme construction, client-side decryption time is much higher than traditional encryption techniques. Thus, in this work, we build on the dual encoding approach proposed in to make it more secure by allowing search on encrypted data at the service provider without using OPE. The simple solution would be to store the encrypted spatial database using a strong and secure encryption method (such as Advanced Encryption Standard (AES)) at the server-side as in [10]. No information can be deduced from this stored encrypted data and hence no query processing can take place at the server. The only way is to send the whole encrypted database to the user, where the user can decrypt and extract the required result.

In spatial database outsourcing applications, the attackers have to be prevented from gaining illegal access to the data. To analyze the security provided by the proposed schemes, it is assumed that the users are trusted by the data owners and, the transformation and encryption key is only provided to the authenticated users. However, the cloud service provider cannot be trusted with confidential data, as the SP is an untrusted third-party that provides services to multiple DOs and they could release sensitive information to competitors. Furthermore, there are malicious attackers lurking around, waiting to eavesdrop and compromise the data confidentiality and query privacy required by the data owner using the cloud server. Outsourced data and user queries can be kept confidential by using cryptography to encrypt the data and prevent attackers and eavesdroppers from prying private information. Thus, in our approach, confidentiality is guaranteed by the dual encoding technique. We show that using both keys for spatial data provides security against known attacks defined in the literature.

A scenario of such an exchange in a LBS application is where a data owner outsources its data to a service provider like Google. In the process, the data owner does not want to expose the sensitive information to the server. The authenticated users send queries to the service provider for information but do not want to reveal their location to the server, which is capable of handling tens of millions of user query requests.

In our approach, we try and achieve a balance between efficient query processing and obscuring data at the server. We achieve efficiency by performing query search at the service provider on the Hilbert Packet List and thus, reduce the time taken to communicate the query response between the user and server i.e., a single round of communication.

Efficient query processing is a key requirement of LBSs for the user and therefore database outsourcing techniques have to achieve a low communication cost. This requires schemes that encode the spatial data

and queries, and then processes spatial queries over the transformed data at the service provider. Most of the existing techniques do not utilize the overcome this shortcoming by performing efficient range queries on the encrypted data at the SP. We conduct an extensive experimental analysis to show the effectiveness of our technique and comparison is done with two existing approaches on different criteria. Furthermore, since LBSs have to handle a huge amount of spatial data, we have demonstrated the capability of our approach in the Experimental Evaluation with two large static spatial datasets (from OpenStreetMap).

II. RELATED WORK

Cloud computing provides benefits to both the data owner and the user. Data owners can store huge amounts of data on the cloud for a low cost. Users can enjoy on-demand provision of services, hence saving time. However, the cloud environment poses data security and privacy challenges. With the excessive use of mobile devices and navigational systems with GPS, location-based services have become widely popular in this domain. Database outsourcing has become common in recent times due to the large amount of spatial data available.

Hacigumus et al. were the first to propose the notion of outsourcing databases to a third-party service provider. Symmetric Cryptography Schemes Yiu et al present a cryptographic based transformation scheme for two-dimensional data to enhance the security of spatial data. The DO uses the R -tree structure to index the database and encrypts each node using the AES encryption. Query processing requires multiple rounds based on the depth of the R -tree between the user and server, thus increasing the communication cost. The SP sends the encrypted root node to the AU and the AU decrypts the node using the key. The AU then requests the child node overlapping with the query region till a leaf node with the data points is reached. However, CRT indexes are built for static data and cannot handle dynamic updates.

Similarly, Kim et al. developed a cryptographic scheme based on the Hilbert-curve transformation (HCT) to balance between data security and query efficiency. They use the Hilbert curve to locally cluster the data by transforming two-dimensional data to a single dimension and thus hiding the coordinates of the original points. Then a straightforward approach is followed and the conventional AES encryption is applied to the transformed data. The encrypted file is securely stored at the SP. For query processing, the entire encrypted file has to be sent to the AU, decrypted and then searched for the records relevant to the query. Since this requires multiple communication rounds, this proves to be highly timeconsuming and data-intensive for usual range queries that require only a portion of the database as the result.

Preserving Location Data Privacy

In addition to the cryptographic techniques mentioned above, Yiu et al. also present three different spatial transformation methods that are based on partitioning and redistributing the locations in the space. Namely: 1) Hierarchical Space Division (HSD), 2) Error- Based Transformation (ERB) and 3) a hybrid of HSD and ERB. However, these techniques preserve the coordinates of the original points and assuming that an attacker can gain background knowledge of the original points and coordinates of these points in the transformed space, information about close by data points can be exposed. Another spatial transformation scheme is proposed by Hossain et al.. Their scheme offers data security by applying a shear transformation as well as the rotation transformation but is not secure against the proximity attack.

Data transformation methods provide a stronger notion of privacy despite being slightly more computationally intensive due to the encoding and decoding operations. In another solution, the data owner encodes the database prior to transmitting it to the service provider. An authorized user that possesses the secret keys, issues an encoded query to the SP. Both the database and the queries are not accessible by the SP and thus, privacy is assured. The main idea is to provide the SP with searching capabilities over the encoded data. Khoshgozaran et al. transform the points using the Hilbert mapping using parameters such as curve order, scale, orientation, etc. as the secret key. Their technique allows approximate search directly on the transformed points.

Privacy and Integrity Guarantee

On the other hand, Ku et al. proposed a technique for outsourcing databases while assuring both data privacy and query integrity. To preserve data privacy, the data points are encrypted with a symmetric key and indexed by the Hilbert value. Whereas, to ensure query integrity, a probabilistically replication method is applied to a portion of the data which is encrypted with a different space key. Then the two encrypted datasets are combined and stored at SP allowing the client to examine the reliability of the query results. Based on the current research in the field, the Hilbertcurve does not take the distribution of spatial points into consideration when transforming the original space. In fact, it divides the space using the same granularity and generated Hilbert values to construct the Hilbert index. Tian et al. resolve this issue by proposing an index modification method for the standard Hilbert curve, which compresses the null value segments to improve the security of the Hilbert curve. Moreover, they also formulate the privacy disclosure risk metric to help analyze the security risks posed by space filling curves.

Whereas in our approach, we assign Hilbert index values to each spatial point and then divide the points into packets based on the packet size. We store the spatial Points in a packet list along with the starting and ending Hilbert index of each packet.

III. PROPOSED SYSTEM

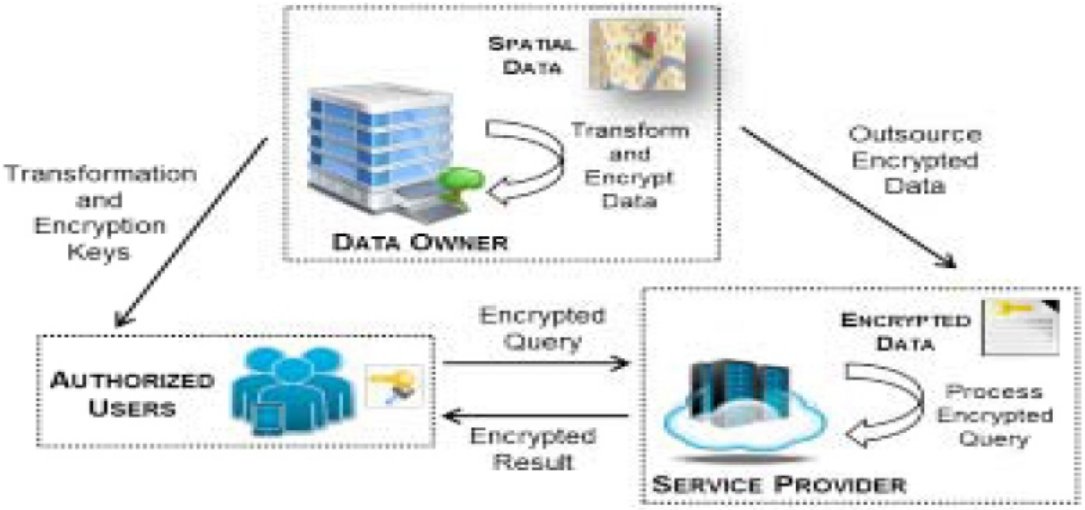
Cloud computing services empower organisations and individuals to outsource the management of their data to a service provider, in order to save on hardware investments and reduce maintenance costs. Only authorized users are allowed to access the data. Nobody else, including the service provider, should be able to view the data. for a instance, a real-estate company that owns a large database of properties wants to allow its playing customers to query for houses according to location. On the other hand, the untrusted service provider should not be able to learn the property locations and, e.g. , selling the information to a competitor.

To tackle the problem, we propose to transform the location datasets before uploading them to the service provider. The application develops a spatial transformation that re-distibutes the locations in space, and a cryptographic-based transformation. The data owner selects the transformation key and shares it with authorized users. Without the keys, it is infeasible to reconstruct the original data points from the transformed points. The proposed transformations present distinct trade-offs between query efficiency and data confidentiality. In addition, we describe attack models for studying the security properties of the transformations. Empirical studies demonstrate that the proposed methods are efficient and applicable in practice.

METHODOLOGY

Java:

Java is general - purpose computer - programming language that is concurrent, class - based, object-oriented, that specifically designed to have as few implementation dependencies as possible.



Algorithm Implement

To overcome these shortcomings of the preliminary approach, we propose to use the secure AES scheme. None of the well-known cryptanalysis attacks have been proven to break AES yet. Since AES only allows equality comparisons on encrypted data. we enumerate the Hilbert cells between fPs, Peg and store them in each packet. Lastly, this data is encrypted using AES and sent to the SP. The AU issues an encrypted spatial range query to the server and all query processing is done at the SP, as it should be done in a true database outsourcing application. The index search at the SP does induce a high query overhead, almost linear with respect to size (D), but with the computing power of the SP, this is not a real concern. Moreover , the order of plaintext in the encrypted packets is obscured, and this makes the new approach attractive and secure. Lastly, the AU decrypts the query results using the AES key with almost no overhead. In this work, we show three different variations of the highlight their advantages over one another.

The end user can give the feedback to the each and every hospital.

RSA :

RSA involves a public key can be known to everyone; it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.

SPACE TRANSFORMATION AND ENCRYPTED:

To preserve the privacy of spatial data, we propose to hide the original spatial data points in two-ways. First, we transform the space by converting the 2 D points to 1D using the Hilbert Space Key. Next, we encode the resulting Hilbert indices and data points using an encryption scheme. Both the transformation key and the encryption key are transmitted by the DO to the trusted AUs over a secure communication channel using SSL without the need for any costly tamper-resistant devices.

PROJECT IMPLEMENTATIONS

Modules:

Anti-Tamper Hardware

With a specific end goal to handle the security flaws posed by outsourcing databases, several prior works resolved the issue by adding a middleware or tamperproof device at the SP to ensure security. This device assists in query processing by encrypting and decrypting the transmitted messages. Assuming a trusted device exists at the server, Damiani et al. propose a fast searchable encryption technique for the non-order preserving AES encryption. The database owners start by building a B-tree over 1D values and encrypt each record at the node level to protect the data from the untrusted SP. However, with numerous users, it is not practical to have an individual device for every AU at the SP. To overcome this, other techniques have to be explored.

PRESERVING LOCATION DATA PRIVACY:

The cryptographic techniques mean, the present three different spatial transformation methods that are based on partitioning and redistributing the locations in the space. Namely: 1) Hierarchical Space Division (HSD), 2) Error-Based Transformation (ERB) and 3) a hybrid of HSD and ERB. However, these techniques preserve the coordinates of the original points and assuming that an attacker can gain background knowledge of the original points and coordinates of these points in the transformed space, information about close by data points can be exposed. Another spatial transformation scheme.

Their scheme offers data security by applying a shear transformation as well as the rotation transformation, but is not secure against the proximity attack.

PRIVACY AND INTEGRITY GUARANTEE

A technique for outsourcing databases while assuring both data privacy and query integrity. To preserve data privacy, the data points are encrypted with a symmetric key and indexed by the Hilbert value. Whereas, to ensure query integrity, a probabilistically replication method is applied to a portion of the data which is encrypted with a different space key. Then the two encrypted datasets are combined and stored at SP allowing the client to examine the reliability of the query results.

PARTITIONED INDEXING METHODS:

The trade-off between security and efficiency in outsourced data, propose a scheme based on the Rˆ -tree. The Rˆ -tree follows a hierarchical encrypted index mechanism where an asymmetric scalarproduct preserving encryption is used. Moreover, the method uses the leaf Minimum Bounding Rectangle (MBR) to hide ordering and hence, protects the data from being disclosed. However, the authors do not provide any substantial definition of security guaranteed by the scheme.

IV. RESULT ANALYSIS

DISTRIBUTION OF ENCRYPTED VALUES:

We tested whether it is possible to statistically distinguish between the output of OPES and the target distribution by applying the Kolmogorov- Smirnov test used for this purpose.

We conservatively try to disprove the null hypothesis at a significance level of 5%, meaning thereby that the distribution of encrypted values generated by OPES differs from the chosen target distribution.10 In addition to the Census data, we used four sizes for the three synthetic datasets: 10K, 100K, 1M, and 10M values.

For each of these input datasets, we experimented with three target distributions: Gaussian, Zipf, and Uniform. We could not disprove the null hypothesis in any of our experiments. In other words, the distribution of encrypted values produced by OPES was consistent with the target distribution in every case.

INCREMENTAL UPDATABILITY:

For an encryption scheme to be useful in a database system, it should be able to handle updates gracefully. We have seen that with OPES a new value can easily be inserted without requiring changes in the encryption of other values.

Recall that we compute the bucket boundaries and the mapping functions when the database is encrypted for the first time, and then do not update them (unless the database administrator decides to re-encrypt the database afresh). We studied next whether the encrypted values remain consistent with the target distribution after updates.

For this experiment, we completely replaced all the data values with new values, drawn from the same plaintext distribution. But we did not update Kp or Kc. We did this experiment with all the four types of datasets, and for each of them we considered Gaussian, Zipf, and Uniform distributions.

KEY SIZE:

The size of the encryption key K depends on the number of buckets needed for partitioning a distribution, the total size being roughly three times the number of buckets. We found that we did not need more than 200 buckets for any of our datasets (including those with 10 million values); for Uniform, the number of buckets needed was less than 10. Thus, the encryption key can be just a few KB in size.

V. CONCLUSION

Database outsourcing is a popular model of cloud computing. In this work, we are trying to achieve a balance between data confidentiality at the server and efficient query processing. We propose to transform the spatial database by applying the encryption to the transformed data. We define several attack models and show that our scheme provides strong security against them. This allows a balance between the security of data and fast response time as the queries are processed on encrypted data at the cloud server.

Moreover, we compare with existing approaches on large datasets and show that this approach reduces the average query communication cost between the authorized user and service. Patient records are stored in cloud storage and those records are encrypted using AES algorithm which will give security of patient records (reports). Patients lost their records in somewhere and they need those records to contact the doctor, in such a case patient can able to give request to the administrator. So the admin person can share the reports in encrypted format also he is providing the AES algorithm. So patient can decrypt the records using the AES key.

REFERENCES

[1] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials,, vol. 15, no. 2, pp. 843–859, 2013.

[2] C. Gentry et al., "Fully homomorphic encryption using ideal lattices." In STOC, vol. 9, 2009, pp. 169–178.

[3] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure multidimensional range queries over outsourced data," The VLDB Journal The International Journal on Very Large Data Bases, vol. 21, no. 3, pp. 333– 358, 2012.

[4] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563–574.

[5] J. K. Lawder and P. J. H. King, "Querying multi-dimensional data indexed using the hilbert space-filling curve," ACM Sigmod Record, vol. 30, no. 1, pp. 19–24, 2001.

[6] Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in Advances in Spatial and Temporal Databases. Springer, 2007, pp. 239– 257.

[7] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "A query integrity assurance scheme for accessing outsourced spatial databases," Geoinformatica, vol. 17, no. 1, pp. 97–124, 2013.

[8] F. Tian, X. Gui, P. Yang, X. Zhang, and J. Yang, "Security analysis for hilbert curve based spatial data privacypreserving method," in 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing. IEEE, 2013, pp. 929– 934.

[9] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," The VLDB Journal, vol. 19, no. 3, pp. 363–384, 2010.

[10] H.-I. Kim, S.-T. Hong, and J.-W. Chang, "Hilbert curve based cryptographic transformation scheme for protecting data privacy on outsourced private spatial data," in 2014 International Conference on Big Data andSmart Computing (BIGCOMP). IEEE, 2014, pp. 77–82.

[11] P. Wang and C. V. Ravishankar, "Secure and efficient range queries on outsourced databases using r-trees," in 2013 IEEE 29th International Conference on Data Engineering (ICDE). IEEE, 2013, pp. 314–325.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005