

ULAB JOURNAL OF SCIENCE AND ENGINEERING

A RESEARCH PUBLICATION OF ULAB

November 2017

Vol. 8, No.1

ISSN 2079-4398 (Print)
ISSN 2414-102X (Online)

CONTENTS

Editorial	1
Analysis of Household and Demographic Characteristics to Identify Key Determinants of Poverty in Bangladesh: A logistic Regression Analysis <i>Sacchidanand Majumder and Soma Dey</i>	3
A Technical Method for Problem Solving in a Holistic Approach <i>Mirza Mohtashim Alam, Md. Kabirul Islam, Md. Samaun Hasan, and Mizanur Rahman</i>	13
Importance of Generic Construction of Block-Cipher Based Compression Function <i>Rashed Mazumder, Mohammad Shahriar Rahman, Muhammad Shahin Uddin, and Mohammad Badrul Alam Miah</i>	23
Numerical Study on Advection Diffusion Equation for Human Lung Model Channel <i>Mahtab U. Ahmmmed and Monika Khatun</i>	29
A Note for Contributors	37
Copyright Form	39



School of Science & Engineering
UNIVERSITY OF LIBERAL ARTS
BANGLADESH

ULAB JOURNAL OF SCIENCE AND ENGINEERING

Vol. 8, No.1, November 2017



House 56, Rd 4/A @ Satmasjid Road Dhanmondi, Dhaka-1209, Bangladesh
Phone: 966-1255, 966-1301, 0171-309-1936. Web: www.ulab.edu.bd

Editorial

Vol. 8, No.1, 2017

WE are pleased to present the eighth volume of the ULAB's Journal of Science and Engineering (JSE). It's been another successful year for us. Since 2010, ULAB's JSE has maintained its position as the most prestigious national publication in the field of science and engineering.

In the first volume, we found many ordinary papers were being submitted, but the quality of submitted paper is gradually improving in the subsequent volumes. Based on peer-review, this year we have accepted 4 papers.

The first paper describes an analysis of socio-economic status of household to identify the key determinants of poverty in Bangladesh using principal component analysis.

The second paper focuses on the development of a model based on the Gestalt Theory of learning to enhance engagement of the students in the classroom related to problem solving intelligence and creativity.

The third paper presents a framework for the necessity of generalization of diverse block-cipher techniques through a unified approach.

Finally, the fourth paper shows a numerical solution of one-dimensional advection-diffusion transportation equation, which is generated from lumped-parameter model of human lung channel. It also presents a simulation to show accuracy.

According to the publication policy all papers submitted to this journal have been subject to a rigorous peer-review. We continuously strive to publish original research that contains elements with technical novelty in a timely manner. The journal's focus is on traditional areas of both theoretical and practical applications of physics, mathematics, statistics, environmental science, electronics, computer science, information and communication engineering. In addition, we shall gladly accept submissions on emerging technologies and other emerging areas related to the above fields.

You are most welcome to read this issue of the ULAB Journal of Science and Engineering. To continue publishing a high-quality journal, JSE's editorial board seeks excellent contributions containing original research or reviews. Our editorial board works tirelessly to provide contributors with a prompt and thorough review process.

We would like to extend our heartfelt thanks to every author, reviewer and reader for your support and dedication to JSE. We strongly believe that together, we shall elevate the journal to even higher levels of quality, impact, and reputation.

Mohammad Shorif Uddin, *Editor-in-Chief*

Sazzad Hossain, *Editor*

S. M. Mahbubur Rahman, *Editor*

A. K. M. Muzahidul Islam, *Editor*

Tama Fouzder, *Editor*

Analysis of Household and Demographic Characteristics to Identify Key Determinants of Poverty in Bangladesh: A logistic Regression Analysis

¹Sacchidanand Majumder and ²Soma Dey

¹Monitoring Specialist, Dhaka Ahsania Mission, Dhaka.

E-mail: mithu.m2011@gmail.com

²Lecturer, Faculty of Business Administration, BGC Trust University Bangladesh, BGC Biddyanagar, Chandanaish, Chittagong.

E-mail: somaais99@gmail.com

Abstract

The objectives of this study are to analyse socio-economic status of household and to identify key determinants of poverty in Bangladesh using the BDHS (2014) data. The principal component analysis was used to create an asset index which gave Social Economic Status (SES) of each household. Finally, based on this data, a logistic regression was estimated with SES as the dependent variable and a set of demographic variables as the explanatory variables. The result shows that the probability of a household being poor depends on the ownership of assets and other household data. Land ownership, electricity connection and other durable goods, a house with cemented floor, walls and roofs, and quality source of drinking water have positive impact on SES. The multivariate analysis shows that increase in the educational level of household head and numbers of literate members in household have an impact on the probability of a household being non-poor. The logistic model of rural and urban poverty suggests that most of the variation is explained by rural poverty. The other demographic factors that affect the probability of a household being poor are household size, age of household's head and dependency ratio.

Keywords: Asset Index, Logistic regression model, Poverty, Principal component analysis.

© University of Liberal Arts Bangladesh

All rights reserved.

Manuscript received on 21 May 2017 and accepted for publication on 30 August 2017.

1 INTRODUCTION

The poverty of a person arises due to insufficiency of different necessities such as literacy, housing, health, provision of public services, etc., that are substantial contributor in the subsistence level of living [1]. Poverty is multi-dimensional in nature and depends on interactions of various socio-economic factors. A measure of the socio-economic status of households is an important element in most economic and demographic analyses. This measure is very useful not only in estimating poverty and inequality within the society but also can be used as a control variable in assessing the effect of other variables associated with wealth [2].

Methods for measuring household's socio-economic status can be categorized into two major groups: money-metric measures- the conventional approach to the measurement of poverty which uses income and/or expenditure data and alternative or proxy measures- multidimensional approaches which employ several socio-economic indicators to measure poverty[3]. Most measurements and analysis of poverty have been done based on income in developed countries and consumption or expenditure in developing countries [4]. However, collecting data on income and expenditure can be time and money consuming [5]. In addition, in low-income countries, measurement of consumption and expenditure is fraught with difficulties such as problem of recall and reluctance to divulge information. Furthermore, prices are likely to differ substantially across times and areas, necessitating complex adjustment of the expenditure figures to reflect these price differences [6]. For this reason, an asset based approach was essential to determine socioeconomic status as an alternative tool for classifying the households in their socio-economic status.

An asset-index approach to measure the poverty is one alternative to income or consumption and expenditure. This approach, although lacking data on income, consumption and expenditure, collects information on ownership of a range of

durable assets, which include: car/track; refrigerator; television; radio; bicycle; telephone and solar power; housing characteristics, which include material of dwelling floor; roof and toilet facilities; and access to basic services, which includes electricity supply and sources of drinking water. This approach was used by Achia, Wangombe and Khadioli, 2010 [7] to determine the explanatory variables for poverty using demographic and health survey data of Kenya.

Various authors developed an asset index using the demographic health survey variables such as durable goods, source of drinking water, toilet facility and housing quality to describe the household welfare instead of using a household's income or expenditure [2], [8], [4], [9], [10], [11].

The use of assets by development economists has been increasingly advocated in the past decade in order to complement income and consumption based measures of welfare and wealth in developing countries [2], [12]. Since the early 1990s, researchers working on household surveys in developing countries have used asset or wealth indices constructed using principal component analysis as a proxy for household income or consumption expenditure (*inter alia*, [2], [9], [13], [14]). Among the multidimensional approaches to the measurement of poverty, the asset index method applied to demographic and health survey data has gained increasing popularity since the last couple of years. Data of household's assets such as durable and semi-durable goods are employed to depict household welfare in this method. It was developed and tested in a large number of countries to measure inequalities in household income, use of health services, and health outcomes [15]. It is considered as an indicator of the level of wealth that has consistency with expenditure and income measures [16]. In addition, an asset index requires data that are easily and quickly collectable and less intensive which feasibly result in smaller measurement error.

The use of demographic and health survey data to the measure of poverty is not unique. The World Bank in its series of socio-economic differences in health nutrition and population has also constructed PCA based asset indices using DHS data. Filmer and Pritchett, 2001 [2] used Demographic and Healthy Survey data to show that the relationship between wealth and enrollment in school can be estimated without income or expenditure data, by using household asset variables. PCA provided acceptable and reliable weights for an index of asset to serve as a measure for wealth. In the four countries examined -India, Indonesia, Nepal and Pakistan- this approach produced reasonable results.

Sahn and Stifel, 2000 [9] employed demographic and health survey data in an analysis of poverty in nine African countries; they used principal component analysis to construct asset index. Sahn and Stifel, 2003 [4] performed the robustness tests on asset indices which demonstrated that the asset index reliably predicts poverty and serves as a proxy for long term wealth with less error than data on expenditures.

Filmer and Pritchett 1998 & 1999 and Filmer 2000 [8], [17], [18] discovered how educational attainment profile differed by wealth and gender in more than 35 countries using the DHS data. The analysis of poverty is mostly based on multivariate regression methods that attempt to identify the determinants of poverty at the household level, using reduced form models of various structural relationships that affect poverty [19].

Booyesen 2002 [20] measured differences in socio-economic status of South African households based on 19 variables from demographic and health survey data. The asset index used represented a comparable indicator of poverty in South Africa. Geda et al. 2001 [21] employed binomial and ordered logit analysis and identified some variables such as size of household, places of residence (urban or rural), level of schooling and engagement in agricultural activity, both in rural and urban areas as the key determinants of poverty.

Oyugi et al 2000 [22] used Probit Model for determining of poverty to analyse the Welfare Monitoring survey (1994) data. The predictors (household characteristics) used in the study included holding area, livestock unit, the proportion of household members able to read and write, household size, sector of economic activity (agriculture, manufacturing/industrial sector or wholesale/retail trade), source of water for household use, and off-farm employment. The result showed that almost all the variables used were important determinants of poverty.

Rodriguez and Smith 1994 [23] used a logistic regression model to estimate the effect of different economic and demographic variables on the probability of a household being in poverty in Costa Rica. The source of the data was from National Household-Income (1986). Their results showed that poverty was higher for the household whose heads had a lower level of education.

Mwabu et al. 2000 [24] identified the following variables as key determinants of poverty: unobserved region-specific factors, mean age, size of household, place of residence (rural or urban), level of schooling, livestock holding and sanitary conditions and they employed levels regression approach in this purpose.

Achia et al. 2010 [7] used logistic regression to identify the key determinants of poverty in Kenya based on DHS data; but in their study they did not consider gender of household head or possible interaction effects. Hence, this study focuses on a joint application of PCA and regression model in the study of the determinants of poverty. The joint effect of two or more variables (i.e., interaction effects) is also thoroughly discussed.

The objective of this study is to develop an asset index, derived from Bangladesh DHS 2014 data. An asset index has been developed using principal component analysis (PCA) following Achia, Wangombe and Khadioli 2010 [7] from asset ownership variables in Bangladesh DHS 2014 data. Finally, a logistic regression analysis has been done to identify the key determinants of poverty in Bangladesh.

2 METHODOLOGY

2.1 Source of Data

The data used to analyze the poverty is taken from Demographic and Health Surveys (DHS) 2014 for Bangladesh. The survey covered both rural and urban populations. The survey collected information relating to demographic and detailed information on asset ownership, access to public services and housing characteristics. A household was defined as a person or a group of people related or unrelated to each other who live together in the same dwelling unit and share a common source of food.

The survey is based on a two-stage stratified sample of households. In the first stage, 600 Enumeration Areas (EAs) were selected with probability proportional to the EA size, with 207 clusters in urban areas and 393 in rural areas. A complete household listing operation was then carried out in all the selected EAs to provide a sampling frame for the second-stage selection of households. In the second stage of sampling, a systematic sample of 30 households on average was selected per EA to provide statistically reliable estimates of key demographic and health variables for the country as a whole, for urban and rural areas separately, and for each of the seven divisions. With this design, the survey selected 18,000 residential households to conduct the survey. Finally, 17,300 households were surveyed and the data was collected, summarized and presented in the household and demographic survey report.

2.2 Computation of an Asset Index using Principal Components Analysis

We applied the statistical procedure of principal component analysis (PCA) to create an asset index based on data from the Bangladesh Demographic Household Survey (2014). The BDHS 2014 included information regarding the ownership of durable goods, housing characteristic, access to services along with basic demographic information concerning household size and composition. The asset index used in the DHS 2014 is a measure that has been used in many DHS and other country-level surveys to measure inequalities: in household characteristics, in the use of health and other services, and in health outcomes [25]. It serves as an indicator of household-level wealth that is consistent with expenditure and income measures [26]. In this Study, an asset index has been developed using PCA following Achia, Wangombe and Khadioli 2010 [7]. The main objective of the PCA approach is to construct an aggregated one-dimensional index over the range of different dichotomous variables capturing housing characteristics, household durable and semi durable-assets that indicate the living standard of households in Bangladesh.

Using PCA, the household variables were recoded into dichotomous variables, distinguishing between a household that owns the particular asset with the household that does not own that particular asset, or for which a particular statement about access to services is true with one that does not own the asset or for which the statement is not true. Hence, all variables take on a value of zero or one. The only variable that is included in the PCA as a continuous variable is the number of household members sharing a room for sleeping purpose.

Principal component analysis (PCA) is a data analysis technique that can be traced back to Pearson, 1901 [27]. It can be used to compress data sets of high dimensional vectors into lower dimensional ones. This is useful, for instance, in visualization and feature extraction. PCA has been extensively covered in the literature [28-32]. PCA is one of the core methods of factor analysis, where we endeavour to uncover underlying relationships between observed and unobserved latent variables [33].

PCA is a multivariate statistical technique used to describe the variation of a set of multivariate data in terms of a set of uncorrelated linear combinations of variables. In PCA, each successive linear combination is derived so as to explain as much as possible of the total variation in the data, while being uncorrelated with other linear combinations [2], [5]. The first principal component explains the highest variability in the original data set and is used to estimate household well-being. An asset index is given by this component which provides discrimination between households, with the assets which vary most across households being given larger weight [34].

Given p variables $X_1, \dots, X_p$ measured in n households, the p principal components $Y_1, \dots, Y_p$ are uncorrelated linear combinations of the original variable, $X_1, \dots, X_p$ given as:

$$\begin{aligned} Y_1 &= a_{11}X_1 + a_{12}X_2 + \dots + a_{1p}X_p \\ Y_2 &= a_{21}X_1 + a_{22}X_2 + \dots + a_{2p}X_p \\ &\vdots \\ Y_p &= a_{p1}X_1 + a_{p2}X_2 + \dots + a_{pp}X_p \end{aligned}$$

This system of equations can be expressed as $y = Ax$, where $y = (Y_1, \dots, Y_p)$, $x = (X_1, \dots, X_p)$ and A is the matrix of coefficients.

The coefficient of the first principal component, $a_{11}, \dots, a_{1p}$ are chosen in such a way that the variance of Y_1 is maximized subject to the constraint that $a_{11}^2 + \dots + a_{1p}^2 = 1$. The variance of this component is equal to λ_1 , the largest eigenvalue of A . The second principal component is completely uncorrelated with the first component and has variance equal to λ_2 , the largest eigenvalue of A . This component explains additional but less variation in the original variable than the first component subject to the same constraint. Further, principal components (up to the maximum of p) are defined in a similar

way. Each principal component is uncorrelated with all the others and the squares of its coefficients sum to one. The principal component analysis involves finding the eigenvalues and eigenvectors of the correlation matrix.

2.3 Logistic Regression Model

To verify whether there is any association between dependent and independent variables, contingency table is constructed here. Chi-square test of independence is applied to examine the effect of household characteristics on socio-economic status. To identify the factors, most strongly associated with it, the enter method of logistic regression model is performed.

In DHS 2014, the socio-economic status is computed in the five categories like as poorest, poorer, middle, richer and richest. In this study, for the purpose of regression analysis, the socio-economic status is recoded into two categories (poor and non-poor). Here, poorest and poorer categories are considered as poor, and middle, richer and richest categories are considered as non-poor.

The analysis uses logistic regression, which estimates model with a binary response and a set of explanatory variables. In logistic regression model, a dichotomous variable socio-economic status of household was introduced to determine whether the household is poor or not.

Here,

$$\text{Socio-economic Status} = \begin{cases} 0, & \text{if the household is non-poor} \\ 1, & \text{if the household is poor} \end{cases}$$

The logistic regression model is given by

$$\text{logit}(P_i) = \log\left(\frac{P_i}{1-P_i}\right) = \sum_i \beta_i X_i$$

Where

$$P_i = P\left(Y_i = \frac{1}{X_i}\right) = \frac{\exp(\sum \beta_i X_i)}{1 + \exp(\sum \beta_i X_i)} = \text{Probability that the } i^{\text{th}} \text{ household is poor}$$

Y_i = poverty status of i^{th} family;

$Y_i = 1$ if the family is poor, and zero if the family is non-poor,

X_i = i^{th} predictor variable; and β_i = i^{th} parameter associated with X_i .

3 RESULTS AND DISCUSSION

3.1 The Asset Index

Table 1 shows all variables used in the construction of the asset index and the result of PCA. Using information on the range of assets and housing characteristics, 94 dichotomous variables and one continuous variable are selected for principal component analysis. The results of PCA indicate that the first principal component yields eigenvalue 8.313 and it explains 8.751% of the variation in the original variables and each subsequent component explains a decreasing proportion of variance. The scree plot in figure 1 shows the proportion of variance explained by each principal component and indicates that the first four components would sufficiently explain the original variables.

The results indicate that majority of households (92%) are more likely to have own homestead, whereas minority of households (45%) are more likely to have own land usable for agriculture. Most of the households (63%) are likely to have own livestock. Most of the households are likely to have mobile phone and electric fan (89%, & 60% respectively) than other durable goods. A total of minority households (44%) have TV. Further, majority of households (63%) have reportedly access to electricity which are 41%, 48% and 61% in 2004, 2007 and 2011 respectively in accordance with BDHS [35], [36], [37]. A few numbers of households (1%) have car/truck/microbus. In accordance with the results, majority households (53%) use wood for cooking fuel, whereas minority households (22.3%) use agricultural crop as a source of cooking fuel. The remaining sources of cooking fuel are accessible in negligible number of households. Tube-well is found as the most common source of drinking water of households in Bangladesh (87.8%). The rest of the sources of drinking water are accessible in negligible number of households. In consistence with the results, the majority households (59.5%) use pit latrine (with or without slab). Only 16.1% and 12.5% households use ventilated improved latrine and flush latrine to septic tank respectively. The situation of no latrine facility is improved from 6.1% in 2007 [36] and 4% in 2011 [37] to 3.2% in 2014. Almost 84% of households live in dwelling with tin roofs. About 67.1% households live in dwelling with earth/sand floor in the main room. Further, 40.1% and 28% households use tin and cement respectively in constructing walls of the main room.

The output from a PCA is a table of factor scores or weights for each variable (see Table 1). Generally, Scoring factor (factor score) of each asset is pointed out the impact of that asset whether positive or negative on socio-economic status of each household. For instance, livestock has a negative factor score indicating a negative impact on socio-economic status whereas; ownership of land for agriculture has a positive factor score indicating a positive impact on the index. Electricity connection and other durable goods (radio, TV, DVD/ VCD, computer, refrigerator, motorcycle/scooter, car/truck/microbus, telephone, mobile phone, IPS/generator, AC, auto bike/tempo/CNG, water pumps, almirah/ wardrobe, electric fan) have positive factor scores. Among these assets, ownership of a refrigerator and TV are the variables that get the highest scores (.716 and .643 respectively) indicating significant impact on socio-economic status. Further, ownership of homestead gets the lowest scores .001 pointing out relatively low impact on the index. Separated kitchen room and number of rooms used for sleeping have positive score indicating significant impact on socio-economic status. As expected, poor source of drinking water, sanitation facilities and low quality construction material (e.g. mud walls, hemp/hay/bamboo roofs) get the negative

factor scores in the index. Having a house with cemented floor, cemented walls, and cemented roofs scores the highest weights in each of these construction materials (.722, .769 and .701 respectively). Piped into dwelling as source of drinking water achieve the highest score (.467) mentioning relatively higher positive impact on socio-economic status than other sources of drinking water. Different types of cooking fuel, natural gas gains the highest score .599, followed by LPG (.286) indicating relatively higher positive impact on socio-economic status than using other fuels.

TABLE 1
RESULTS FROM PRINCIPAL COMPONENTS ANALYSIS

Variables	Mean	Std. Dev.	Component Score	N		Mean	Std. Dev.	Component Score	N
Materials of floor					Type of latrine				
Earth/ sand	.6707	.470	-.821	17300	Flush to piped sewer system	.0249	.156	.324	17300
Wood planks	.0020	.045	-.008	17300	Flush to septic tank	.1250	.331	.541	17300
Palm/bamboo	.0009	.029	-.014	17300	Flush to pit latrine	.0148	.121	.065	17300
Parquet or polished wood	.0002	.013	.002	17300	Flush to somewhere else	.0150	.121	.156	17300
Ceramic tiles	.0201	.140	.378	17300	Flush, don't know where	.0054	.073	.109	17300
Cement	.3039	.460	.722	17300	Ventilated improved pit latrine	.1614	.368	.190	17300
Carpet	.0012	.034	.036	17300	Pit latrine with slab	.3709	.483	-.293	17300
Others	.0010	.031	.003	17300	Pit latrine without slab	.2236	.417	-.347	17300
Materials of walls					No facility/ bush/ field	.0316	.175	-.151	17300
Palm/ trunks	.0206	.142	-.120	17300	Composting toilet	.0001	.011	.004	17300
Dirt	.1106	.314	-.211	17300	Bucket toilet	.0004	.020	-.015	17300
Bamboo with Mud	.0799	.271	-.161	17300	Hanging toilet	.0268	.161	-.131	17300
Stone with Mud	.0002	.015	-.002	17300	Others	.0002	.015	-.011	17300
Plywood	.0001	.011	.003	17300	Source of cooking fuel				
Cardboard	.0001	.008	-.006	17300	Electricity	.0049	.070	.085	17300
Tin	.4007	.490	-.402	17300	LPG	.0217	.146	.286	17300
Cement	.2793	.449	.769	17300	Natural gas	.1253	.331	.599	17300
Stone with lime or Cement	.0082	.090	.109	17300	Biogas	.0016	.040	.052	17300
Bricks	.0765	.266	-.060	17300	Kerosene	.0015	.039	.051	17300
Wood planks/ shingles	.0151	.122	-.070	17300	Coal, lignite	.0023	.048	-.030	17300
Others	.0085	.092	-.066	17300	Charcoal	.0032	.057	.002	17300
Materials of roofs					Wood	.5293	.499	-.139	17300
No roofs	.0003	.019	.008	17300	Straw/ shrubs/ grass	.0100	.100	-.007	17300
Thatch or palm leaf	.0140	.117	-.083	17300	Agricultural crop	.2227	.416	-.337	17300
Palm/ Bamboo	.0007	.026	-.008	17300	Animal dung	.0743	.262	-.148	17300
Wood planks	.0001	.011	.008	17300	No food cooked in house	.0010	.031	.000	17300
Cardboard	.0001	.011	-.008	17300	Others	.0022	.047	-.001	17300
Tin	.8395	.367	-.604	17300	Double goods				
Wood	.0022	.047	-.007	17300	Has electricity	.6335	.482	.589	17300
Ceramic tiles	.0017	.042	.101	17300	Has Solar Electricity	.1086	.311	-.193	17300
Cement	.1256	.331	.701	17300	Has radio	.0350	.184	.075	17300
Roofing shingles	.0131	.114	-.038	17300	Has television	.4421	.497	.643	17300
Others	.0025	.050	-.015	17300	Has DVD/VCD Player	.0686	.253	.361	17300
Source of drinking water					Has computer/laptop	.0554	.229	.485	17300
Piped into dwelling	.0383	.192	.467	17300	Has refrigerator	.2032	.402	.716	17300
Piped to yard or plot	.0247	.155	.182	17300	Has bicycle	.2662	.442	-.044	17300
Public tap or stand pipe	.0254	.157	.172	17300	Has motorcycle/scooter	.0729	.260	.294	17300
Tube-well or Borehole	.8776	.328	-.413	17300	Has car/truck/microbus	.0084	.091	.150	17300
Protected well	.0019	.044	-.003	17300	Has telephone (land-line)	.0166	.128	.293	17300
Unprotected well	.0034	.058	-.043	17300	Has mobile telephone	.8891	.314	.256	17300
Protected spring	.0001	.011	.004	17300	Has IPS/Generator	.0275	.164	.396	17300
Unprotected spring	.0009	.029	-.022	17300	Air Conditioner	.0047	.068	.222	17300
River/ dam/lake/pond/ canal	.0168	.128	-.075	17300	Has auto bike/tempo/CNG	.0166	.128	.017	17300
Rain water	.0055	.074	-.034	17300	Has rickshaw/van	.0587	.235	-.095	17300
Tanker truck	.0003	.019	.030	17300	Has water pumps	.0725	.259	.376	17300
Cart with small Tanker	.0012	.034	.061	17300	Has Almirah/ Wardrobe	.4439	.497	.552	17300
Bottled water	.0026	.051	.050	17300	Has electric fan	.6000	.490	.611	17300
Others	.0013	.036	.010	17300	Has own homestead	.9182	.274	.001	17300
					Has own land usable for agriculture	.4471	.497	.146	17300
					Has own livestock	.6336	.482	-.459	17300
					Has separate room used as kitchen	.1369	.344	.398	17300
					Number of rooms used for sleeping	2.1871	1.176	.260	17300

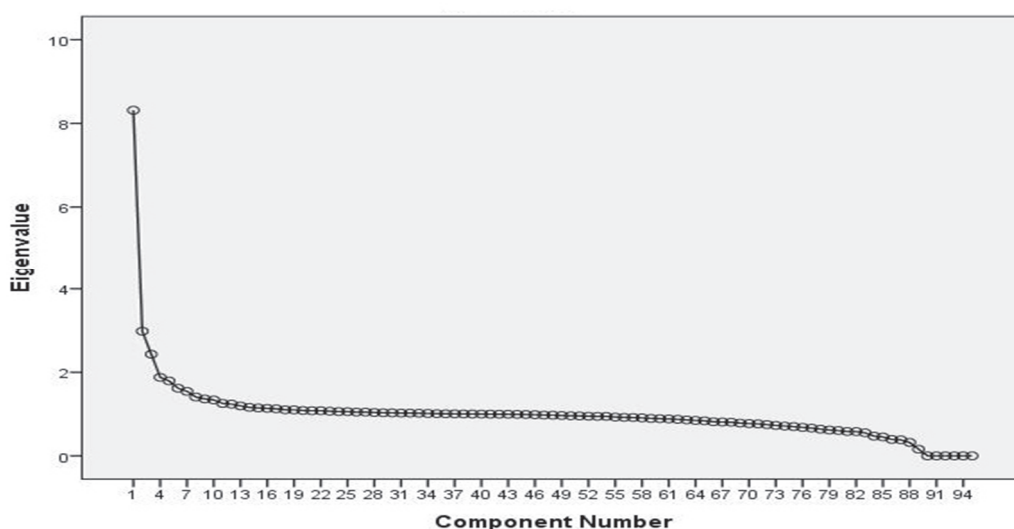


Figure 1: Scree Plot

3.2 Cross Tabulations

This section illustrates socio-economic status cross- tabulates by characteristics of household. Initially, a set of predictors such as Household size, Age of household's head, Educational attainment level of household's head, Number of literate members (7 years and above) in household, Dependency ratio, Sex ratio, Land ownership of household, Division of residence and Place of residence are selected to check whether these variables have association with socio-economic status. On the basis of findings of chi-square test are executed.

TABLE 2
VALUES OF PEARSON'S χ^2 -STATISTIC ON CROSS-CLASSIFYING SELECTED PREDICTORS WITH SOCIO-ECONOMIC STATUS

Variables	χ^2 -value	df	P-value
Household size	39.706	3	.000
Age of household's head	16.386	3	.001
Educational attainment of household's head	2837.500	3	.000
No. of literate members (7 years and above) in HH	1099.500	3	.000
Dependency ratio	230.648	3	.000
Sex ratio	7.511	3	.057
Land ownership of household	1064.706	3	.000
Division of household	744.551	6	.000
Place of household	2133.769	1	.000

The result indicates that there exists a highly significant association between socio-economic status and the following predictor variables: Household size, Age of household's head, Educational attainment level of household's head, Number of literate members (7 years and above) in household, Dependency ratio, Land ownership of household, Division of household and Place of household (See Table 2).

The distribution of households by place of residence and SES results show that most of the households (52%) in rural are poor and the remaining 48% households are non-poor; while, a total of 15.8% households are poor in urban and the rest of 84.2% households are non-poor. According to the division, the highest (55.3%) poverty cases have in Rangpur and the lowest (26.7%) poverty cases have in Dhaka. According to the distribution of households by education attainment level of household's head and SES results show that the groups with the highest (61.5%) poverty ceases have no education while those with the higher education have lower cases of poverty. The results also display that with the increasing number of literate member in household; the numbers of cases being poor are decreased.

The distribution of households by dependency ratio and SES result shows that the households with high dependency ratio are poorer than the households with a low dependency ratio. The sex ratio is not significant in describing poverty of household. According to the distribution of household by land ownership and SES results show that the poverty is the highest (48.9%) with no land ownership of household and gradually become lower with increasing land ownership.

The distribution of household by household size and SES result shows that 45.3% households are poor with 1-2 members, 38.4% and 40.7% households are poor among those who have 3-4 members and 5-6 members respectively, and 36.9% household are poor, of those household who are constrained 7 and more members. Further, the distribution of household by age of household's head and SES results illustrate that the highest (41.5%) are poor of those whose head belongs to age less than 35.

3.3 Logistic Regression Analysis

The final model that is fitted to the data is given by

$$\text{logit}(p) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + \beta_7 X_7 + \beta_8 X_8$$

Where, X_1 =Household size, X_2 =Age of household's head, X_3 = Educational attainment of household's head, X_4 =No. of literate members (7 years and above) in HH, X_5 =Dependency ratio, X_6 = Land ownership of household, X_7 = Division of residence, X_8 = Place of residence.

For the study purpose, entire method of binary logistic regression analysis is used. Using the DHS 2014 data, the logistic has been estimated to determine the factors affecting SES in Bangladesh. Table 3 presents the results of the fitted logistic regression model. The result shows that all variables have highly significant ($p < .005$) impact on socio-economic status (SES).

The result of logistic analysis (Table 3) shows that the poverty of household is increased gradually with increasing household size (odds ratio: 1.058, 1.316, and 1.348). The result also indicates that increasing age of household's head, the probability of household being poor is decreased (Table 3).

TABLE 3
EFFECTS FOR THE BEST FITTING LOGISTIC REGRESSION MODEL

Variables	B	S.E. (B)	P-value	Odds Ratio	95% C.I. for EXP(B)	
					Lower	Upper
Household Size						
1-2 members (RC)			.000	1.000		
3-4 members	.056	.087	.518	1.058	.892	1.255
5-6 members	.275	.100	.006	1.316	1.082	1.602
7 and more members	.252	.111	.023	1.348	1.045	1.634
Age of Household Head						
Less than aged 35(RC)			.025	1.000		
Aged 35-44	-.106	.056	.060	.900	.806	1.005
Aged 45-59	-.099	.057	.083	.894	.808	1.014
Aged 60 and above	-.189	.062	.003	.828	.733	.936
Educational Attainment Level of Household Head						
No education (RC)			.000	1.000		
Primary	-.419	.052	.000	.658	.595	.728
Secondary	-1.314	.058	.000	.269	.240	.301
Higher	-2.306	.104	.000	.100	.081	.122
Number of Literate member in Household						
No member (RC)			.000	1.000		
1 member	-.440	.115	.000	.644	.514	.807
2 members	-.917	.117	.000	.400	.318	.502
3 members and more	-1.268	.125	.000	.281	.220	.360
Dependency Ratio						
No Dependency(RC)			.000	1.000		
Ratio less than 50%	.031	.079	.692	1.032	.883	1.206
Ratio 50-75%	.195	.075	.010	1.215	1.049	1.408
Ratio above 75%	.540	.070	.000	1.717	1.497	1.968
Land Ownership of Household						
No land (RC)			.000	1.000		
Less than 1 acre	-.725	.046	.000	.485	.443	.530
1-2 acres	-1.216	.076	.000	.296	.255	.344
Above 2 acres	-1.749	.087	.000	.174	.147	.206
Division of Household						
Barisal (RC)			.000	1.000		
Chittagong	-1.347	.075	.000	.260	.225	.301
Dhaka	-1.293	.074	.000	.274	.238	.317
Khulna	-.748	.074	.000	.473	.409	.547
Rajshahi	-.580	.074	.000	.560	.484	.647
Rangpur	.111	.074	.134	1.118	.966	1.293
Sylhet	-.795	.078	.000	.451	.388	.526
Place of Household						
Urban (RC)				1.000		
Rural	1.812	.047	0.000	6.125	5.586	6.715

RC= Reference Category

The result of regression analysis (Table 3) reveals that educational attainment level of household's head has highly significant ($p=.000$) effects on the socio-economic status (SES) of household. It is displayed in the table 3 that with increasing educational attainment level of household's head, the probability of household being poor is decreased gradually. The odds ratio shows that the households head with primary, secondary and higher education are .658, .269 and .100 times less poor as compared to the households head who has no education. The result also illustrates that with increasing number of literate members (7 years and above) in household, the probability of household being poor is decreased gradually (odds ratio: .644,

.400 and .281). Again, due to increasing dependency ratio, the probability of household being poor is increased gradually. The result indicates that with the increase in land ownership of household the probability of household being poor is decreased gradually (odds ratio: .485, .296 and .174). The result indicates that there exists comparatively higher level of poverty in Rangpur division. The odds ratio of those divisions mentions that the households in Rangpur are 1.118 times more likely to be poor by comparison with the households in Barisal. The result of logistic analysis explains that place of household has strong significant ($p=.000$) effects on SES. The odds ratio indicates that the rural households are 6.125 times more likely to be poor as compared to the households live in urban.

4 CONCLUSION

Poverty measures on the basis of asset ownership are increasingly being used in research but there are some limitations on their use. According to Filmer and Pritchett 2001 [2], the asset-based measures are more reflective of the long-run household wealth, failing to capture short-run wealth to the household. Therefore, if we are interested to see an effect that is associated with current resources to the household, then an index based on asset may not be the best measure. Also, Falkingham and Namazie 2002 [38] pointed out that the ownership does not capture the quality of the asset (Owning a poor-quality asset will not help to live a better standard of living). But, asset-based measures do not account for this fact. Also, some variables may have a different relationship with the asset index across sub-groups; for example, ownership of agricultural land may be more reflective of wealth in rural areas than urban areas.

The multivariate analysis shows that an increase in educational level of household head has an impact on the probability of a household being non-poor. Achieving higher education can lead a household from being poor to non-poor. The logistic results indicate that increasing number of literate members can lead a household from being poor to non-poor. It is observed that with the increased land ownership of household, the probability of household being poor is decreased.

The rural/urban variable is statistically significant and this variable can be the reason for a household being poor. The logistic regression of rural and urban poverty suggests that most of the variation is explained by rural poverty. The other demographic factors that affect the probability of a household being poor are the household size, age of household's head, and dependency ratio. The rural/urban variability can be argued that the assets includes in the asset index are by their nature urban rather than rural and therefore are biased against rural areas. Also, formal housing, water and sanitation facilities are urban services, which support the conclusion of having significant results in rural areas. As the country develops, the rural population will get access to these services, which will help the household to be non-poor. This study shows the key determinants of poverty on the basis of demographic and household data. This paper focuses on the point that education is a significant tool to fight poverty. Bangladesh needs to consider education seriously since the experience in developing countries has proved its potential in poverty reduction. Policy and decisions makers should review the policies for achieving and ensuring education for all. This will involve investing more in education. The rural standard of living is far less than the urban standard of living in Bangladesh. Government should come up with policies that can ensure reduction of the plight of the poor people in rural Bangladesh.

ACKNOWLEDGMENT

The authors express their gratitude and thanks to Prof. Dr. Soma Chowdhury Biswas, Department of Statistics, University of Chittagong for her valuable criticisms during the preparation of this paper.

REFERENCES

- [1] Bourguignon, F. and Ckavrarty, S. R. Multidimensional poverty orderings. Indian Statistical Institute, Calcutta. Working Paper No. 2002-22. 2002.
- [2] Filmer, D., and Pritchett, L. Estimating wealth effects without expenditure data or tears: An application of educational enrollment in states of India. *Demography*, 38(1), 115-132. 2001.
- [3] Booysen, F. le R., Van der Berg, S., Burger, R., Von Maltitz, M., and Du Rand, G. Using an Asset Index to Assess Trends in Poverty in Seven Sub-Saharan African Countries. *World Development*, 36(6), 1113-1130. 2008
- [4] Sahn, D.E., and Stifel, D.C. Urban-rural inequality in living standards in Africa. *Journal of African Economics*, 12, 564-597. 2003
- [5] Vyas, S., and Kumaranayake, L. Constructing socio-economic status indices: how to use principal components analysis. *Health Policy and Planning*, 21(6), 459-468, 2006.
- [6] Deaton, A. and Zaidi, S. "Guidelines for constructing consumption aggregates for welfare Analysis". Working Paper 192, Washington D.C., WorldBank. 1999.
- [7] Achia, T.N.O, Wangombe, A. and Khadioli, N. (2010). A Logistic Regression Model to Identify Key Determinants of Poverty Using Demographic and Health Survey Data. *European Journal of Social Sciences*, 13(1), 38-45, 2010.
- [8] Filmer, D. and Prichett, L. "The effect of household wealth on education attainment: Evidence from 35 countries", *Population and development review* 25, (1), 85-120, 1998.
- [9] Sahn, D. and Stifel, D. Poverty Comparisons over time and across countries in Africa. *World Development*, 28: 2123-2155, 2000.
- [10] McKenzie, D. Measuring inequality with asset indicator, *Journal of population economics* 18, (1), 229-260, 2005.
- [11] Montgomery, M., Gragnolati, M., Burke, K., and Paredes, E. Measuring living standards with proxy variables. *Demography*, 37, 155-74, 2000.
- [12] Carter, M., and May, J. One Kind of Freedom: Poverty Dynamics in Post- Apartheid South Africa. *World Development*, 29(12), 1987-2006, 2001.

- [13] Gwatkin DR, Rustein S, Johnson K et al. Socio-economic differences in Brazil. Washington, DC: HNP/Poverty Thematic Group of the World Bank. 2003. Accessed 5 January 2004 online at: [<http://www.worldbank.org/poverty/health/data/index.htm#lcr>].
- [14] Kolenikov, S. and Angeles, G. The use of discrete data in principal component analysis: Theory, simulations and applications to socioeconomic indices. Working Paper, MEASURE/Evaluation Project, No, WP-04-85, 2009. Chapel Hill, NC: Carolina Population Center, University of North Carolina.
- [15] Rutstein, S., K. Johnson, and D. Gwatkin. Poverty, health inequality, and its health and demographic effects. Paper presented at the 2000 Annual Meeting of the Population Association of America, Los Angeles, California.
- [16] Rutstein, S. Wealth versus expenditure: Comparison between the DHS wealth index and household expenditures in four departments of Guatemala. Calverton, Maryland: ORC Macro, 1999.
- [17] Filmer, D., and Pritchett, L. The Effect of Household Wealth on Educational Attainment: Evidence from 35 Countries. *Population and Development Review*, 25(1), 85-120, 1999.
- [18] Filmer, D. The Structure of Social Disparities in Education: Gender and Wealth. *Annals of World Bank Policy Research*, Working paper 2268, 2000.
- [19] Glewwe, P. Investigating the determinants of household welfare in Côte d'Ivoire. *Journal of Development Economics*, 35(2), 307-337, 1991.
- [20] Booyesen, F. le R. Using demographic and health surveys to measure poverty: An application to South Africa. *Journal for Studies in Economics and Econometrics*, 26(3), 53-70, 2002.
- [21] Geda, A., De Jong, N., Mwabu, G. & Kimenyi, M. Determinants of poverty in Kenya: A household level analysis. Institute of Social Studies (ISS), The Hague, Working paper, 2001.
- [22] Oyugi, Lineth Nyaboke. The Determinants of Poverty in Kenya. MA Thesis, Department of Economics, University of Nairobi, 2000.
- [23] Rodriguez, A.G., and S.M. Smith. A comparison of determinants of urban, rural and farm poverty in Costa Rica. *World Development*, 22 (3), 381-397, 1994.
- [24] Mwabu, Germano, Wafula Masai, Rachel Gesami, Jane Kirimi, Godfrey Ndeng'e, Tabitha Kiriti, Francis Munene, Margaret Chemngich, and Jane Mariara. Poverty in Kenya: Profile and Determinants, Nairobi: University of Nairobi and Ministry of Finance and Planning, 2000.
- [25] Rutstein, S., K. Johnson, and D. Gwatkin. Poverty, Health Inequality, and Its Health and Demographic Effects. Paper presented at the 2000 Annual Meeting of the Population Association of America, Los Angeles, California. 2000.
- [26] Rutstein S. Wealth versus Expenditure: Comparison between the DHS Wealth Index and Household Expenditures in Four Departments of Guatemala. Calverton, MD: ORC Macro. 1999.
- [27] Pearson, K. On lines and planes of closest fit to systems of points in space. *Philosophical Magazine* 2(6) 559-572, 1901.
- [28] Bishop, C. Pattern Recognition and Machine Learning. Springer-Verlag, 2006.
- [29] Diamantaras, K., Kung, S. Principal Component Neural Networks - Theory and Application. Wiley, 1996.
- [30] Haykin, S. Modern Filters. Macmillan, 1989.
- [31] Cichocki, A., Amari, S. Adaptive Blind Signal and Image Processing – Learning Algorithms and Applications. Wiley, 2002.
- [32] Jolliffe, I. T. Principal Component Analysis. Springer-Verlag, 2nd edition, 2002.
- [33] Morciano, M., Hancock, R. And Pudney, S. Disability costs and equivalence scales in the older population. ISER Working Paper Series, 2012(09), 2012.
- [34] Chuma, J. and Molyneux, C. Estimating inequalities in ownership of insecticide treated nets: does the choice of socio-economic status measure matter? *Health Policy and Planning*, 24, 83-93, 2009.
- [35] BDHS. Bangladesh Demographic and Health Survey 2004: National Institute of Population Research and Training (NIPORT), Mitra and Associates, and ORC Macro. Dhaka, Bangladesh and Calverton, Maryland, USA, 2004.
- [36] BDHS. Bangladesh Demographic and Health Survey 2007: National Institute of Population Research and Training (NIPORT), Mitra and Associates, and Macro International. Dhaka, Bangladesh and Calverton, Maryland, USA, 2007.
- [37] BDHS. Bangladesh Demographic and Health Survey 2007: National Institute of Population Research and Training (NIPORT), Mitra and Associates, and Macro International. Dhaka, Bangladesh and Calverton, Maryland, USA, 2011..
- [38] Falkingham J, Namazie C. Measuring health and poverty: a review of approaches to identifying the poor. London: Department for International Development Health Systems Resource Centre (DFID HSRC), 2002. Accessed 5 April 2006. at: [<http://www.eldis.org/static/DOC11501.htm>].

Sacchidanand Majumder received his M.Phil. degree in Statistics from University of Chittagong, Bangladesh. He also received his B.Sc.(Hons) and M.Sc. in Statistics from University of Chittagong, Bangladesh. Currently, he has been working as a Monitoring Specialist, UNIQUE II Project in Dhaka Ahsania Mission (DAM), Bangladesh. His current research interests are Poverty Alleviation, Education, Health, Water and Sanitation, and Multivariate Analysis etc.

Soma Dey received her BBA (Hons) and MBA in Accounting and Information System from University of Chittagong, Bangladesh. Now, she has been working as a Lecturer, Faculty of Business Administration, BGC Trust University Bangladesh, BGC Biddyanagar, Chandanaish, Chittagong. Her current research interests are Corporate Governance, Corporate Social Responsibility, Employee Benefits and Poverty Alleviation etc.

A Technical Method for Problem Solving in a Holistic Approach

Mirza Mohtashim Alam¹, Md. Kabirul Islam², Md. Samaun Hasan³ and Mizanur Rahman⁴

Daffodil International University, Sukrabad, Dhaka, Bangladesh

mirza.mct@diu.edu.bd¹, kislam@daffodilvarsity.edu.bd², hasan.mct@diu.edu.bd³, mizan.mct@diu.edu.bd⁴

Abstract

In modern days, engaging brain is a challenging task. In a classroom setting, problem solving requires engagement of brain and utilization of intellectual abilities of the students. Throughout the world, different institutions and academy is trying to increase effective brain engagement in both organizational and academic purpose in order to accelerate productivity. This productivity is considered as learning outcomes in an academic setting. However, success is considered as a dependent variable of engaging human mind set in that particular situation. Additionally, introducing creativity and applicable strategies can be considered as the increasing factor of brain engagement in classroom environments. In this paper, we have presented a model based on the essence of the Gestalt Theory of learning for problem solving in a technology supported learning environment called Education Aid System (EAS). Our intention was to enhance engagement of the students in the classroom related to problem solving and creativity in a holistic approach. In addition, this technical model gives emphasis on joint intelligence of the students for solving problems. This model might ensure intellectual abilities, identify and overcome their difficulties for all the segments of a particular problem of the students and encourage them for working collaboratively on a given problem. The teacher's role in the EAS is to develop insight amongst the students for solving problems.

Keywords— Gestalt Theory, Student Mind, Employability, Creativity, intellectual ability, Brain Engagement

© University of Liberal Arts Bangladesh

All rights reserved.

Manuscript received on 30 June 2017 and accepted for publication on 2 August 2017

1 INTRODUCTION

Problem solving requires intellectual abilities of the students. In a face to face classroom situation especially in higher education, we give students several tasks/problems for finding solutions. Generally, emphasis is given on problem solving individually. However, students have lack of opportunity to involve in solving problems or teacher's task in an interactive manner with the fellow students. Classroom is a floor for learning fundamental and advance strategies, and acquiring skill set for applications in the practical field. Furthermore, it can provide an individual with necessary dimension for increasing thinking capability which is necessary for their future advancements. Gestalt theory of learning talks about problem solving in a holistic approach. Different educationalist, and scientist have tried to connect the Gestalt theory with education as the theory depicts several principles, such as, Law of proximity, Law of Similarity, Law of Closure, Law of Good Continuation, Law of Pragnanz and Law of Figure [1]. Furthermore, Gestalt theory can be directly applied as a substance of education for its tremendous mind mapping capability for problem solving. In learning, Gestalt theory suggests that, fill up knowledge gap by solving related problem with prior knowledge which helps to gain new insights. Moreover, relationship among the elements which creates the problem should be discovered [2]. According to the Gestalt theory of learning, one should perceive things as a whole rather than its parts for better insights.

Different theories of learning support use of computer technology. The main reason is: this technology helps students for knowledge construction in a collaborative manner. Computer mediated learning was found to be an important avenue for acquisition of knowledge and skills and improvement of interest of the students in learning [3] Group interactions through computer aided learning contribute to achieve higher academic grades and increase confidence level of the students [4], [5]. Within the scope of this study, we have proposed problem solving through a computerized system where students can get together in the system for a common interest of their learning.

In this paper, we figure out and present a model called Education Aid System (EAS) which is based on the essence of the Gestalt principles of learning for problem solving. The system offers students to reflect on the given problem individually and then collectively for development of insight for finding solutions to the problems in a face to face classroom environment.

2 RELATED STUDIES

Researchers throughout the world are experimenting different approaches for engaging student's brain in the class room activi-

ties in order to pull out the most creativity and intelligence. Researchers like Agustianto *et. al.*, Permanasari *et. al.*, Kusumawardani *et. al.*, Hidayah *et. al.* used an adaptive learning (AL) process focusing on recommendation and inquiry based learning using Naïve Bayes Classifier (NBC) [3]. In their research, they have tried to develop a learning path (LP) based on the recommendation of adaptive learning process. Another research conducted by Wei-Lun Lin *et. al.* and Yunn-Wen Lien *et. al.* [4], suggested a Dual-Process Theory for creative problem solving. Their research includes the processes which relates to creativity involved by both open ended and close ended creative problem solving [4] and these are both important depending on the individuals. They have also related the divergent thinking capability. A similar study conducted by Mumford, Hestler, Robeldo, Peterson, Day, Hougen and Barren *et. al.*, intended to build peoples mental model that finds the qualitative solutions for the critical and complex problems in the light of creative thought [5]. They have shown that creative problem solving is capable of reside in multiple domains in terms of the attributes of an individual's mental model [5]. Developing a mental model is very crucial factor for both intelligence and creativity in a working environment. That is why these two terms are often called the key terms for sustained employability. Regardless these two aspects, there are some other key factors like problem solving capability, ability to mind map, capability of relating things with prior knowledge do also have direct or indirect effects on learning activities. According to Regina O. Smith *et. al.*, problem based learning, concept maps and the relating factors of learning element open the pathway to deep learning [6].

Researchers are also focusing on information systems which are capable of aiding both teachers and students. Takahiro Sato *et. al.*, in his research [7] have shown a Computer Management Information System which provides guidance of instructional decision making by the teacher by analyzing several data such as student response data.

The model we intended to develop is to engage students in segmented problem solving activities based on the class lecture. Later, difficulties of each segment shall be placed on to some sort of information system so that, the student can match their difficulties or gaps of each segment with their peer group. After getting new insights again they will be able to save their new insights gained by solving the problem and peer interactions. However, the instructor or facilitator in the class room can access all the difficulties which shall be stored as text form and learn (e.g., feedback, machine learning, alert etc) from the information system for deploying more creative and intellectual problems. In the essence of the Gestalt theory we shall describe our model in the Model Representation section.

3 TECHNICAL MODEL

Our model based on the essence of the Gestalt theory, has several components. The model has several components, such as, set up problem and environment, Individual Problem Solving Phase, Solution Phase, Interaction Phase, Gaining New Insights (Figure 1). Firstly, an information system which we named Education Aid System (EAS) is responsible for storing store all the problem data in respective accounts. Every problem might have one or many difficulties faced by the students. However, these difficulties can be saved in the EAS database by the students through logging in their own account. Furthermore, new insights can be gained through both solving problem and student interaction. Again, gained insights can be stored inside the EAS which can be used later for self development and other purposes such as creating problems with more points of interest by teachers.

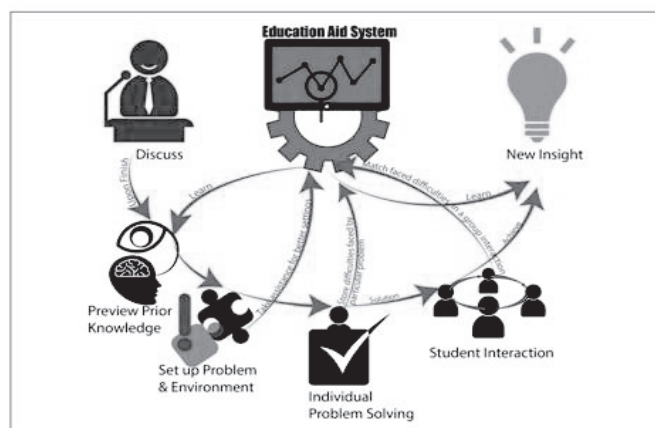


Figure 1: Technical Model of EAS

Secondly, a successful class can be conducted by discussing topic and relating with a reality. Successively, teacher shall setup problem and all the environment variables. Students will try to solve the given problems individually. While solving particular problem students are required to store their difficulties in the EAS for further assistance. Solution of the

particular given problem can be both provided by either teacher or the students depending on the problem structure. After getting the solution, peer group interaction shall be required. In this phase, students are able to match the difficulties with others through their EAS accounts while group interaction. By doing this activity students shall be able to identify the pattern of their weakness or knowledge gaps for a particular problem set. After learning through the EAS and the student interaction process, students are able to build new insights which will be based on prior knowledge.

3.1 Discussion of the topic

Teacher shall discuss topic before providing problem segments. The discussion topic can be in a singular or multiple forms depending on the class.

3.2 Setup problem and environment

Teacher can setup problem based on discussed the topic. Additionally, help from EAS can be achieved while setting up problem in several segments. For the purpose of setting problem one should always bear in mind that, engaging student brain is a function of intellectual ability, creativity and motivation. Also, brain engagement activity requires suitable environment setup and a feedback system for increasing of all factors mentioned above.

Let us consider Brain Engagement Activity as $B_{activity}$, Intellectual Ability as I_a , Creativity as C_r , Motivation as M_o , and environment as env . Then such equation can be considered as,

$$B_{activity} = EngageBrain(I_a, C_r, M_o)_{env} + Feedback. \quad (1)$$

Feedback can be achieved by matching own difficulties with others in the interaction session with the help of EAS system. We might take all the parameters of Engage Brain function under consideration. Intellectual ability needs analyzing ability because one must need to analyze the situation to solve a particular problem. Afterwards, their solving capability shall come in handy. Critical thinking is a must for approaching a problem through many different ways. Adding that, people need their lack of attention to be minimized.

We can consider the equation of Intellectual Ability,

$$I_a = Analyzing\ ability + solving\ capacity + Critical\ Thinking - attention\ distortion \quad (2)$$

Attention distortion is given in a sense of lack of mindfulness. The lesser it hinders the rest of the parameters the more the intellectual ability is. Same concept goes for the equation of creativity.

$$Creativity, \quad C_r = thinking\ capability + feeling + mindmap - attention\ distortion \quad (3)$$

Motivation is a crucial factor for brain activity. People need freedom and sense of success for the feelings of overcoming the challenge in the near future. Plus another thing is needed very often and that is their willingness for engagement. So, we can construct an equation of motivation in such way that it reflects all the parameters.

$$Motivation, \quad M_o = Freedom + Sense\ of\ success + Willingness\ for\ engagement\ to\ activity \quad (4)$$

Additionally, instructor can always seek help from the EAS system where all the knowledge base resides for building more superior qualitative problem with more possible segments.

3.3 Individual Problem Solving Phase

In this phase students tries to solve a particular problem given by the instructor. The problem requires multiple segmented areas and preferably more than one intellectual solution. Additionally, while solving the particular problem students can save their difficulties in the EAS database for future interaction phase by logging in to their terminal.

The total brain activity can be derived as $Total(B_{activity})$ in a group, where, X is an individual student, P_s is an individual problem segment and Y_i is an individual among the rest of the students Y . Therefore, each of the individual X 's total solved segments will be added with the rest of the student Y 's in order to obtain $Total(B_{activity})_{Group}$. In this case, the overlapping segments are deducted.

$$Total(B_{activity})_{Group} = [X. \bigcup P_s + \bigcup Y_i. \bigcup P_s] - [\bigcup Y_i. \bigcup P_s \mid X. \bigcup P_s] \quad (5)$$

Here, we are focusing on one particular students problem namely X and all of his fellow students belongs to group Y. Since the common knowledge must be subtracted according to set union theory, we have taken union and subtracted to equalize the equation. When one student shall sit for problem after signing in his respective terminal he/she will be treated individually since we are taking an individual X and entire problem set P_s into consideration. In every terminal particular student will be treated as X and all the others as Y.

3.4 Solution Phase

Depending on the equation either the instructor or the students shall try to provide an optimal solution to the previously provided problem segments. Solution is needed either way because a particular student X needs to fill the knowledge gaps or fragments. A review might be required before providing the optimal solution. Let us consider the Total Brain Activity equation which has been mentioned before. Let us consider the common problem segments as R. Then the equation can be deduced as,

$$Total(B_activity)_{Group} = [X. \cup P_s + \cup Y_i. \cup P_{s_i}] - [R] \quad (6)$$

After re-arranging we get,

$$X. \cup P_s = Total(B_activity)_{Group} + [R] - \cup Y_i. \cup P_{s_i} \quad (7)$$

In the solution phase, since we are targeting for the individual X's problem P as dependent variable, everything except the X and the X's entire problem solution set we have made as independent variable by rearranging the equation. In the solution phase our system will act for the individual X's problem. We are showing in the equation that group activity is needed for our system since solution of X's individual problem P depends on Total Brain activity in a group. That is how it is related to our system. It signifies that individual's problem depends on Group interaction. If group interaction and knowledge sharing have already been happened there is no necessity of repeating each problem P_s by each of the other individuals Y for a particular person. Otherwise same thing shall be repeated twice. That is why we are removing the overlapping variables.

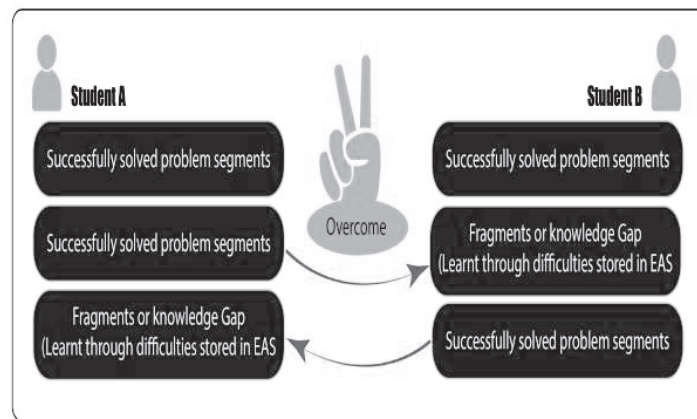


Figure 2: Gaining New Insights

3.5 Interaction Phase

In the interaction phase, students are allowed to perform peer interaction for individual development. Again, students can take aid from the EAS system to match their difficulties faced in a particular segmented problem with the other students. A review, either by the teacher or the peer groups is required for overcoming the knowledge gap or fragments. Considering previous equation, if we add the other student Y's problem solution for those segments which X could not solve and faced difficulties, we get,

$$X. \cup P_s + [\cup P_{s_i} - R] = Total(B_activity)_{Group} + [R] - \cup Y_i. \cup P_{s_i} + [\cup P_{s_i} - R] \quad (8)$$

This part $\sum_{i=1}^n P_{s_i} - R$ is called the review section after removing the common segments R of the particular segmented problem.

While students are interacting with their respective peer group, the teacher can view student's difficulties in EAS in order to provide more holistic solution. Additionally, the teacher can view difficulty pattern generated by the EAS system for more deep understanding. Note that we tried to identify each X's individual weakness through their faced difficulty set. The reason is, Gestalt principal of Closure quotes "Object grouped together is seen as a whole". We might compare the problem segment's solution as objects described in the principal. All of these segments of a particular problem can only be solved if each segment's solution is grouped with others. Holistic solution can easily be found if the problems are identified through the difficulties faced by the students and different students with different solutions are grouped together. That is why, the interaction phase is valuable. In our whole model, a review either by peer group or by the teacher is needed the review is indicated by $\sum_{i=1}^n P_{si} - R$ the equation in the both sides. By doing this, X's fellow group mates shall be able to revise their particular solved problem P's solution. This equation has been stated to realize the effectiveness of peer interaction, overcome the knowledge gaps and revision for those who have actually solved the problem. That is in our system peer interaction is very much needed to overcome the knowledge gaps.

3.6 Gaining New Insights

After all the phases being completed, a student can gain insight through individual problem solving and group interactions. After gaining new insights student shall log in to their EAS account and store their individual insights under particular problem headers. This insight building capability storage shall help the model to get better at times. Gestalt theory of similarity [8] says about elements possessed of similar properties (e.g., concepts, texture, shapes, color etc) are more likely to group together than the elements distributed with dissimilarities. As a result, while peer discussions students might be able to find their similarities (in this case, the problem segment's solution label). If they can find the similarities, it is possible that they will be able to find that, how their solution and difficulties differ from the members of other peer groups. In order to gain new insights, these activities are very much required.

We can consider gaining new insight as a dependent variable of prior knowledge and solving a particular problem with brain activity.

The new insight can be depicted as NI ,

Where,

NI is the new insight,

Pr is the prior knowledge,

$$NI := Pr + Solve(Br_{activity}) \quad (9)$$

From Equation (1), if we substitute the values of $Br_{activity}$ to equation (9), we get,

$$NI := Pr + Solve((EngageBrain(I_a, C_r, M_o)_{env} + Feedback)) \quad (10)$$

Here, in our system gaining new insight has been depicted by the solve function and their prior knowledge. After the substitution Feedback has been added by their fellow groupmates to gain new insight.

4 THE SCHEMA OF EAS

The schema diagram of the EAS might possess following tables and fields according to figure 3. In the schema there are five tables (Difficulties, Problems, Account, Gained insights, Segments) including the primary key and foreign key. Each of the table can resemble a table in a database which can run parallel in accordance with the combination of different front end and back end programs.

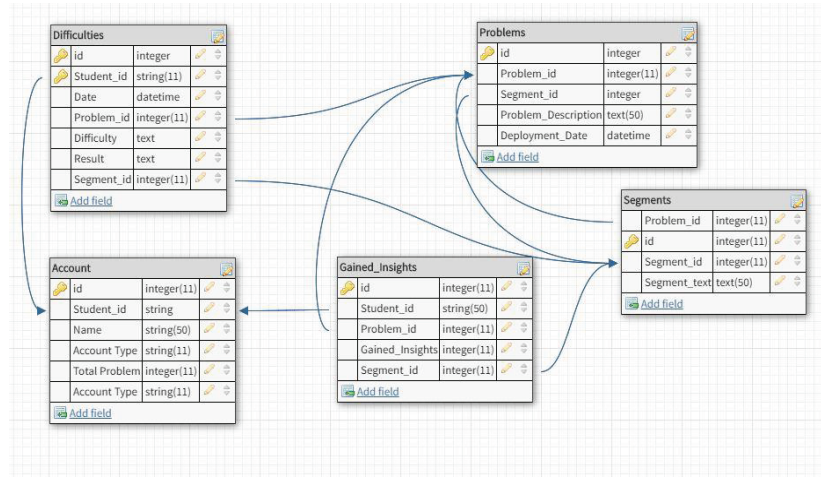


Figure 3: Schema of EAS System

5 SIGNIFICANCE

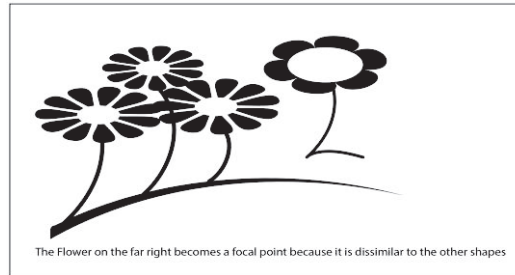


Figure 4: An illustration of the Gestalt theory of similarity

If you are using Word, use either the Microsoft Equation Editor or the MathType add-on (<http://www.mathtype.com>) for equations in your paper (Insert | Object | Create New | Microsoft Equation or MathType Equation). “Float over text” should not be selected.

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). First, use the equation editor to create the equation. Then, select the “Equation” markup style. Press the tab key and write the equation number in parentheses. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Use parentheses to avoid ambiguities in denominators. Punctuate equations when they are part of a sentence, as in

$$\int_0^{r_2} F(r, \varphi) dr d\varphi = [\sigma r_2 / (2\mu_0)] \cdot \int_0^\infty \exp(-\lambda |z_j - z_i|) \lambda^{-1} J_1(\lambda r_2) J_0(\lambda r_i) d\lambda. \quad (11)$$

Be sure that the symbols in your equation have been defined before the equation appears or immediately following. Italicize symbols (*T* might refer to temperature, but *T* is the unit tesla). Per IEEE Computer Society, please refer to “(1),” not “Eq. (1)” or “equation (1),” except at the beginning of a sentence: “Equation (1) shows ...” Also see *The Handbook of Writing for the Mathematical Sciences*, 1993. Published by the Society for Industrial and Applied Mathematics, this handbook provides some helpful information about math typography and other stylistic matters.

Please note that math equations might need to be reformatted from the original submission for page layout reasons. This includes the possibility that some in-line equations will be made display equations to create better flow in a paragraph. If display equations do not fit in the two-column format, they will also be reformatted. Authors are strongly encouraged to ensure that equations fit in the given column width.

6 A PRACTICAL EXAMPLE OF THE SCENARIO

Our model might create significant impact on both student’s individual and group wise development. While they are solving prob-

lem segments individually, they shall be able to connect their ideas, creativity and intelligence with their prior knowledge with the present challenge and build new insights. Again, by storing their difficulties regarding the segments while solving a particular problem in EAS, they shall be able to highlight their weakness by themselves. Afterwards, their weakness shall be greatly identified and purified in peer interaction phase. Moreover, students shall be able to gather their ideas as a whole by filling the gaps of their knowledge by peer interaction. Gestalt theory of similarity depicts that people often perceive the similar objects as a group and the group might create a pattern (Figure 4) [8]. On the contrast, an object can be however emphasized based on their dissimilar properties among all those objects which possess similar properties. Those dissimilar objects can become the focal point and easily identified. We call this anomaly [8].

Our model based on the Education Aid System (EAS), intends to emphasize on various difficulties faced by the students while solving the segments of a certain problem given by the instructor. For an example, M number of students within a group faced n numbers of difficulties while solving the problem segments. Among these n numbers of difficulties, supposedly y number of difficulties is similar to each other. Then, there shall be some difficulties $z = (n - y)$, which shall be dissimilar among all. We are assuming that, each and every student shall have at least one z which shall be highlighted easily. New insights can be built and stored inside the EAS for a particular problem set that might prove to be helpful in the future. According to another principle of Gestalt named Figure and Ground principle [8], shape can be naturally absorbed as figure (Object) while the surrounding area works as the ground (background). In total, the object can be emphasized enough to be visualized in the ground very easily by human eye (Figure 5).

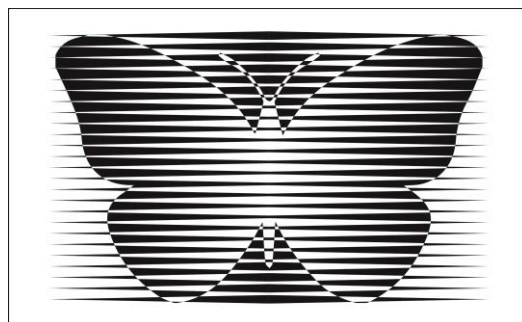


Figure 5: An illustration of Gestalt theory of Figure and Ground

Here in our model, the peers are working as the ground and the individual student as the figure or the object. Additionally, the problems tend to be given by the instructor shall be designed in such a way that holds continuation to the basis of the next problem. As Gestalt theory of continuation says that, our eyes tend to move through the objects which have continuous anchor (Figure 6).

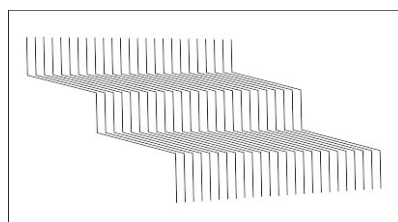


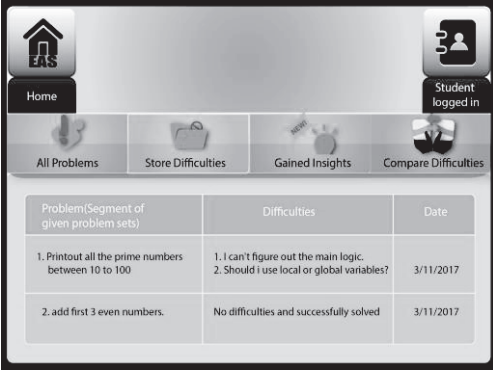
Figure 6: An illustration of Gestalt theory of Continuation

The EAS system of our model shall provide a way to do so. In total, students perceptual and concept development of their individual being has been done through peer interaction which might prove to be helpful for their future employability.

In case of dealing with various problems prevailing in students' future working environment, they might be able to build new insights (based on their present intellectual abilities which they have already developed in the class room) for solving problems in an efficient manner to ensure their better employability remains viable. Involvement of mind, intelligence and creativity aspects of the Gestalt theory gained by the students in their university environment would be pertinent assets for future career and continuous professional development. Therein, theory of proximity and continuity shall enlighten an individual with proper utilization of their mindfulness and create a tolerance of bearing a challenge further. The lessons of the theory of similarity shall create a focal point to highlight aspects of the future challenges towards employability and uphold the dedication level to some extent. Finally, individuals enlighten with the essence of Gestalt theory shall prove valuable in terms of conceptual, technical and creative skill set.

7 MODEL OVERVIEW IN PRACTICAL CLASSROOM

To demonstrate the model over a practical class room scenario, let us assume some programming related problems. Suppose teacher gave 10 programming problems under some time constraints. While solving their programming related problems students log in to their EAS account and adds what difficulties they are facing for solving a particular problem. It can be easily illustrated by figure 7.



Problem(Segment of given problem sets)	Difficulties	Date
1. Printout all the prime numbers between 10 to 100	1. I can't figure out the main logic. 2. Should I use local or global variables?	3/11/2017
2. add first 3 even numbers.	No difficulties and successfully solved	3/11/2017

Figure 7: Storing difficulties User Interface

Let us assume, one particular student solved 6 problems and stored the difficulties for the rest of the problems. The rest of the problems can be easily identified and solved by other group mates. In the interaction phase students in a group compares their difficulties with other group mates. We would do this kind of matching by comparing texts under difficulty tab in the back-end system and provide students with a result such that they shall eventually know his difficulty matches with which group mates. They might be able to check both individually with another student and in a total group.

They might be able to compare themselves with the other group mates by inserting their ids. However, teacher would be able to view all the students' difficulties and help each particular group to solve. If a particular problem have not solved by any of the students interacting within a particular group, then the teacher should come forward and try to solve. The comparing difficulties module should look like figure 8's illustration.

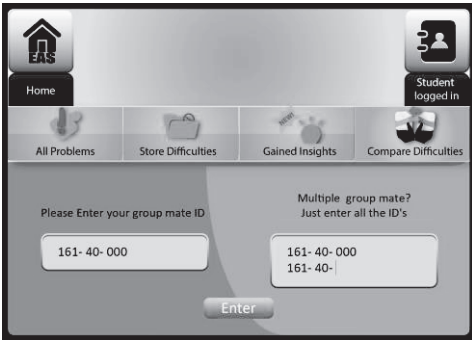


Figure 8: Comparing Difficulties User Interface

They might be able to compare themselves with the other group mates by inserting their ids. However, teacher would be able to view all the students' difficulties and help each particular group to solve. If a particular problem have not solved by any of the students interacting within a particular group, then the teacher should come forward and try to solve. The comparing difficulties module should look like the figure 9.

Problem	Your difficulties	group mate 1	Group mate 2	Group mate n
1. find the prime nu...	Logic, Loop, condition	Logic	loop	solved
2. Add first 2 even nu...	Solved Successfully	Loop condition	solved	solved

Figure 9: Comparing Difficulties with others User Interface

8 CONCLUSION

There is no doubt that the Gestalt theory of learning has a lot of practical application in an educational setting regardless of the grade levels. In this paper, students' problem solving abilities and development of insights as per the lessons learned from the theory have been incorporated within a computer supported learning environment called 'Education Aid System (EAS)' which may be regarded as an innovative approach of the Gestalt theory of learning. This problem solving model defines the role of a class room teacher who introduces and discusses the topic and assigned the task (problem) to the students and the responsibilities of the students for solving the problem in a holistic approach. The EAS provides an opportunity for interaction amongst the participating students for comparing thoughts, critical thinking abilities and development of insights of the group members. So, sharing experience in the form of interaction is another innovation of this model, which we have already shown in figure 1 and figure 2. The complete learning activities of the students in different phases in EAS environment such as, engage brain, intellectual abilities, creativity, motivation, interaction, distortion etc. are shown using mathematical equations. It is claimed here that the intellectual abilities gained by the students from EAP may contribute to deal with different problematic situation during their professional life. A Schema Diagram of the EAS learning environment is also presented for broader understanding and future work. Development of the proposed Education Aid System is left for the future effort. In addition, application of the system in a teaching-learning environment would reflect the worthiness of the model.

REFERENCES

- [1] J Todorovic, D. Gestalt Principles, Scholarpedia, 3(12):5345, retrieved on... from http://www.scholarpedia.org/article/Gestalt_principles(2008).
- [2] Pappes, C. "Instructional Design Models and Theories: Gestalt Theory", *eLearning Industry*... retrieved on... from <https://elearningindustry.com/gestalt-theory>.(2014).
- [3] Lai, F., Luo, R., Zhang, L., Huang, X., & Rozelle, S. "Does computer-assisted learning improve learning outcomes? Evidence from a randomized experiment in migrant schools in Beijing". *Economics Of Education Review* (2015).
- [4] Altintas, T., Gunes, A., & Sayan, H. "A peer-assisted learning experience in computer programming language learning and developing computer programming skills". *Innovations in Education & Teaching International* 53(3), 329-337. (2016).
- [5] De Witte, K., Haelermans, C., & Rogge, N. "The effectiveness of a computer-assisted math learning program". *Journal of Computer Assisted Learning*, 31(4), 314-329. (2015).
- [6] Agustianto, K., Permanasari, A. E. , Kusumawardani, S. S. , & Hidayah, I. "Design adaptive learning system using metacognitive strategy path for learning in classroom and intelligent tutoring systems", *AIP Conference Proceedings* (2016).
- [7] Lin, W., & Lien, Y. "The Different Role of Working Memory in Open-Ended Versus Closed-Ended Creative Problem Solving: A Dual-Process Theory Account". *Creativity Research Journal*, 25(1), 85-96. (2013)
- [8] Barrett, J. D., Mumford, M. D., Hester, K. S., Robledo, I. C., Peterson, D. R., Day, E. A., & Hougen, D. P. "Mental Models and Creative Problem Solving: The Relationship of Objective and Subjective Model Attributes". *PsycEXTRA Dataset*. (n.d.).

Mirza Mohtashim Alam is a Lecturer of Multimedia and Creative Technology Department of Daffodil International University. He completed his bachelor's degree in Computer Science from Department of Computer Science and Engineering of BRAC University. He achieved Vice Chancellors Gold Medal of holding the first position in his undergraduate program. Moreover, he has been in Vice Chancellor's list for academic excellence. Before Joining Daffodil International University, he as been appointed as a student tutor in BRAC University while studying

in undergraduate level. His research area is Machine Learning, Computer Vision and Software Engineering.

Md Kabirul Islam is a Professor of Multimedia and Creative Technology Department of Daffodil International University, Dhaka, Bangladesh. Prior to this position, he had been a teacher of Computer Science and Engineering (CSE) Department of this university. He holds a PhD degree from an Australian University in 2003. Dr Islam has a good number of publications in the area of E-learning, E-commerce, Multimedia Technology and Collaborative Learning in both online and face to face situations.

Md Samaun Hasan is a Lecturer of Multimedia and Creative Technology Department of Daffodil International University. He has completed his undergrauation in Fine Arts from Rajshahi University and Masters from Visva Bharati. He is currently enrolled in PHD in Janhangirnagar University. His research area is image processing, art, paintings and cultures. He has been in numerous exhibitions in national and international level. Moreover, he is a Gold Medalist from India for his excellency in painting. He got lots of awards and achievement for his academic excellence.

Mizanur Rahman is a Lecturer of Multimedia and Creative Technology Department of Daffodil International University. He has completed his undergrauation in Graphic Design from Dhaka University and Masters in Graphic Design from Dhaka University. His research area is image processing, typography, art, education, and animation. He had worked in advertising agency before joining as a lecturer. He currently holds numerous awards and achievement in graphic design.

Importance of Generic Construction of Block-Cipher Based Compression Function

¹ Rashed Mazumder, ² Mohammad Shahriar Rahman, ¹ Muhammad Shahin Uddin, ¹ Mohammad Badrul Alam Miah

¹ Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Santosh, Tangail, 1902

Email: rakhu345@yahoo.com, shahin.mbstu@gmail.com, badrul_ict05@yahoo.com

² Department of Computer Science & Engineering, University of Liberal Arts Bangladesh, Dhaka-1209
Email: md.shahriar@gmail.com

Abstract

A cryptographic hash function is an algorithm that receives input data in an arbitrary size and produces data in fixed size. In addition, this algorithm is infeasible to invert. There are many applications in the field of cryptographic hashing, including digital signatures, message authentication-code, password verification, and file identifier. In general, using a blockcipher-based compression function to build a cryptographic hash function is preferable than that of the scratch, because a blockcipher function is easier to implement than an encryption function. Typically, three variants of blockcipher are available under the double block-length (DBL), namely (n, n) , $(n, 2n)$ and lightweight-cipher. Interestingly, many schemes have been proposed independently based on these blockcipher types. However, there is a lack of suitable scheme that can support all blockcipher types under a unique platform. Therefore, we address that a generalized blockcipher based compression function is important under the different kinds of communication platform.

Keywords— Blockcipher, Lightweight-cipher, Ideal Cipher Model, Collision resistance

University of Liberal Arts Bangladesh
All rights reserved.

Manuscript received on (date will be inserted) and accepted for publication on (date will be inserted).

1 INTRODUCTION

A cryptographic hash (CH) function is defined as a one-way function, i.e. it is infeasible to invert [1], [2]. The CH is one of the prominent tools in modern cryptography [1], [2]. Usually, a message and a chaining value are defined as the input of a CH [1]–[3]. In addition, the output of a CH is called a message-digest [2], [3]–[5]. A CH has many applications in the field of information security, including digital signatures, message authentication codes, password verification, and file/data identifier [1]–[2], [3]–[5], [6]–[7]. It is also used as ordinary hash functions for indexing data in hash tables [1], [3]–[5]. In certain cases, a CH is used for storing the encryption value of fingerprints, identifying duplicate data, and detecting accidental data corruption [1]–[3], [6], [7].

In general, a CH is built by a compression function [6], [8], [9]. Furthermore, the compression function has two prototypes, namely scratch and blockcipher (Fig. 1) [2]–[6]. Using a blockcipher-based compression function to build a cryptographic hash function is preferable to building one from scratch, because the blockcipher function can be directly implement as the encryption function [3], [6], [9]. According to internal construction, the blockcipher-based compression function has two types such as single block-length (SBL) and double block-length (DBL) [8]–[10], [11], [12], [13]. However, because of birthday attacks, SBL is no longer secure [13]–[14]. According to Stam's conjecture [8], the DBL compression function comes under various pretexts. In principle, the DBL has three variants: (n, n) , $(n, 2n)$ and lightweight-cipher [14]–[15]. In the (n, n) blockcipher, the block-length and key-length are equal. Under the $(n, 2n)$ blockcipher, the key-length is twice the block-length. Generally, AES and DES are used under the (n, n) and $(n, 2n)$ blockciphers. Moreover, the latter is a lightweight-cipher based compression function. In addition, the lightweight-cipher based compression function depends on size and characteristics of lightweight ciphers such as Present, KATAN, TWINE, and Lblock [16]–[18].

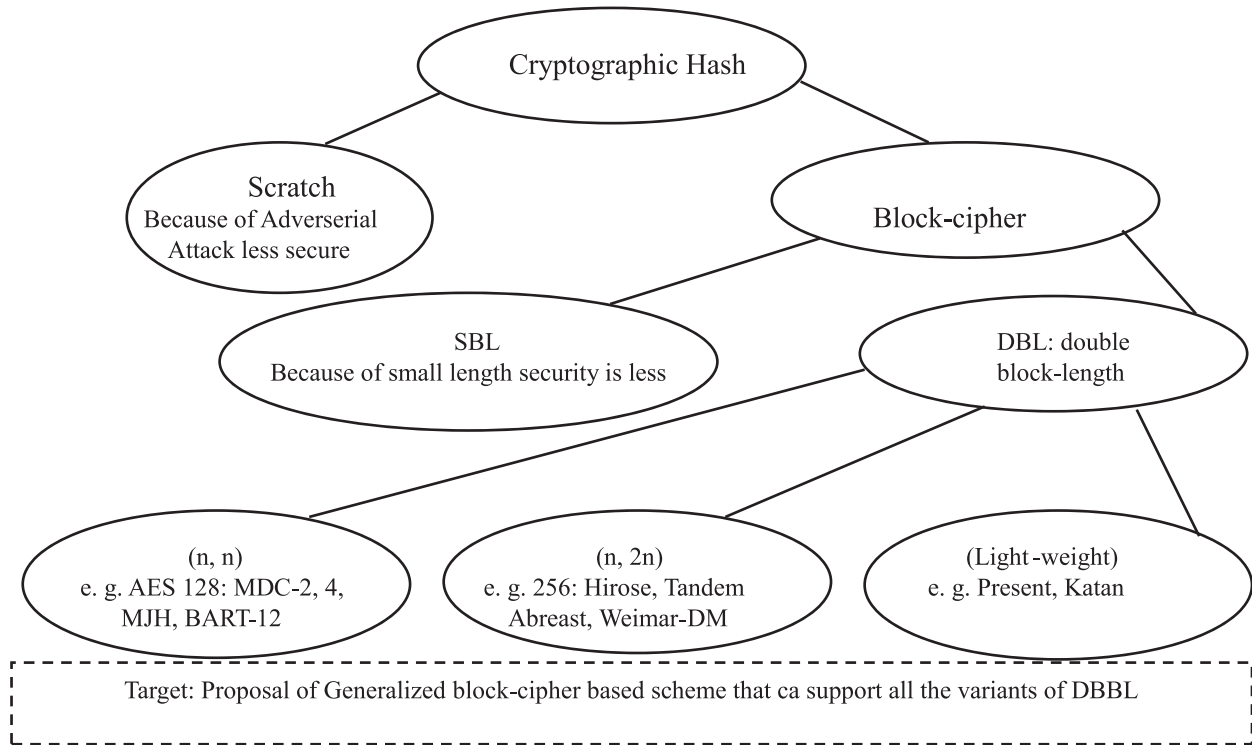


Figure 1: Basic of Cryptographic hash and Motivation [6], [8], [10], [11]-[12]

Motivations. Currently, many DBL-based schemes are available. The schemes of Weimar, MR, Hirose, Tandem, Abreast, Nandi, ISA-09, and CA are related to the $(n, 2n)$ blockcipher [6]-[12]. The MDC-2, MDC-4, MJH, BART, MSR, and CIDM schemes are associated with the (n, n) blockcipher [19]-[21]. Furthermore, SH-L1 [16] and SH-L2 [17] schemes satisfy the lightweight-cipher based compression function. Interestingly, there is a lack of a construction that can support all the variants of DBL through a single platform.

TABLE 1
CURRENT STATUS OF DBL BLOCKCIPHER BASED COMPRESSION FUNCTION AND OUR CONCEPT

	Scheme Name	Security in CR	Efficiency	#E
(n, 2n) block-cipher based compression function	MR	$O(2^n)$	$\frac{1}{2}$	2
	Weimar	$O(2^n)$	$\frac{1}{2}$	2
	Hirose	$O(2^n)$	$\frac{1}{2}$	2
	Tandem	$O(2^n)$	$\frac{1}{2}$	2
	Abreast	$O(2^n)$	$\frac{1}{2}$	2
	ISA-09	$O(2^n)$	$\frac{2}{3}$	3
	Nandi	$O(2^n)$	$\frac{2}{3}$	3
(n, n) block-cipher based compression function	MDC-2	$O(2^{n/2})$	$\frac{1}{2}$	2
	MDC-4	$O(2^{5n/8})$	$\frac{1}{4}$	4
	MJH	$O(2^{n/2})$	1	1
	BART	$O(2^{2n})$	$\frac{1}{3}$	3
	MSR	$O(2^{tn})$	t	2
	SKS	$O(2^{tn}), O(2^{tn/2})$	t, t/3	2, 3
Light-weight cipher based compression function	SH-L1	$O(2^n)$	$\frac{1}{2}$	2
	SH-L2	$O(2^n)$	$\frac{1}{2}$	2

In addition, current communication networks are very complex [1], [26]–[29]. In communication channels, one of the most prominent areas is the Internet of Things (IoT) [26]–[29]. IoT networks are undergoing a rapid rate of growth. There are various types of devices connected to IoT networks, grid networks, and cloud networks [1]–[3], [26]–[30]. These devices have different properties to consider, such as resource-limitations, keyfactors, power-factors, memory-factors, and operational cost factors [18]–[19], [20]–[27]. Under these circumstances, these devices should satisfy better security and efficiency. As a security tool, cryptographic hashing blockcipher compression function plays an important role. However, there is no common platform based solution for implementing a blockcipher-based compression function (Fig. 1, Table 1). More specifically, there is a lack of a generalized construction for blockcipher (DBL) based compression function.

Related Work. Actually, the MR, Weimar, Hirose, Tandem, Abreast, Nandi, ISA-09, and CA-16 schemes are related to the $(n, 2n)$ blockcipher-based compression function (Fig. 2) [6], [14]–[19], [22]. Furthermore, MR, Weimar, Hirose, Tandem, and Abreast provide an upper security bound [6], [14]–[19]. In addition, the Nandi and ISA-09 satisfy better efficiency [6], [14]–[19]. Interestingly, the CA scheme [7] is suitable for both higher efficiency and satisfactory security bounds. However, owing to their designs, the above constructions are not suitable for (n, n) and lightweight-cipher blockcipher based compression function. On the contrary, the MDC-2, MDC-4, MJH, MSR, BART, CIDM, and SKS constructions support (n, n) blockcipher based compression functions [19]–[23]. Although, these schemes have satisfactory security margin and upper efficiency, these schemes are not appropriate for $(n, 2n)$ blockcipher based compression function. Moreover, these schemes cannot support lightweight-cipher because of their internal construction. Most recently, two more schemes have been proposed by Hirose and Kuwakado such as SH-L1 [16] and SH-L2 [17]. These two constructions are suitable for lightweight-cipher based compression functions.

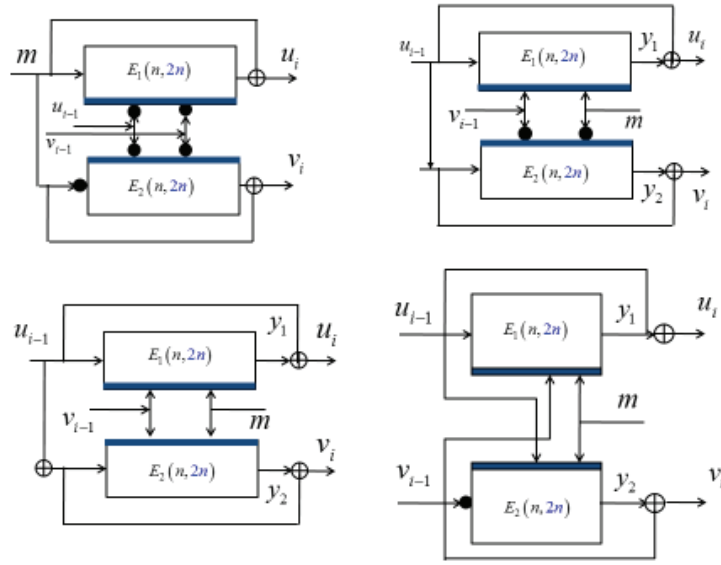


Figure 2: Certain well-known schemes of blockcipher compression function under $(n, 2n)$ [11], [12], [13], [14], [20]

Our Contributions. In this paper, we address the issue of generalization of the DBL-based blockcipher compression function. Usually, a blockcipher-based compression function is an important tool for creating cryptographic hashes. However, there are several blockcipher variants such as (n, n) , $(n, 2n)$ and lightweight-cipher under the DBL. Hence, the compression function also varies based on the properties of the blockcipher. Interestingly, there is a lack of a common scheme of compression function that can support all blockcipher variants of the DBL. Therefore, we address that there is a need of generalized constructions of blockcipher based compression function. In addition, we propose a concept or idea of constructing a generic blockcipher based compression function.

2 NOTATIONS AND PRELIMINARIES

We define certain notations such as H, f_E . For example, H is defined as hash function. In addition, f_E is noted as compression function.

Ideal Cipher Model (ICM). A blockcipher obtains two paired algorithms, the first provides encryption (E) and the second handles decryption (D) [12]–[13]. Both algorithms can accept two inputs such as block size n' , key size k' and return n -bit output. Typically, D is called as inverse of E ($E=D^{-1}$). Mathematically, the encryption and decryption algorithms are defined as $E(K, P) = C$; $D = E^{-1}(K, C) = P$ (Fig. 4), where P and C stands for plaintext and ciphertext. For example, a blockcipher encryption algorithm can receive 128 bits of plaintext as input and get back 128-bits of ciphertext. The transformation is controlled by the second input secret key. Decryption operates similarly do encryption but in reverse. For each key K , E^K is a permutation over the set of input blocks. Each key selects one permutation from the possible set of 2^n . In the ideal cipher model, the complexity of an attack is measured by adversary's total number of optimal queries to oracle E/E^{-1} [12], [13], [14]. The concept is depicted in Fig. 3.

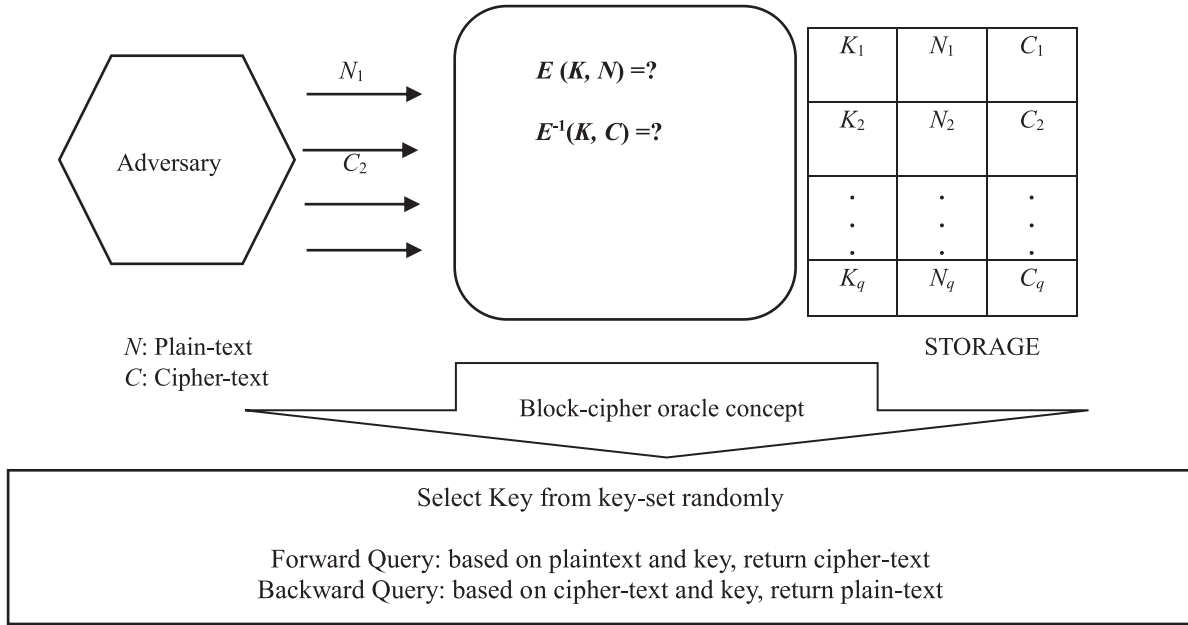


Figure 3: Concept of ICM and Query Method [6], [8]-[11]

Security Definition . An adversary, A is computationally unbounded -but always halts when a collision has occurred. Generally, A has access to an oracle E Block (K, N) for performing query through E and $D = E^{-1}$. This ensures that there is no chance of executing of duplicate query.

Collision resistance for hash function. Adversary A has access to blockcipher oracle. Let H is a hash function that is blockcipher-based. Adversary A has the advantage of finding a collision through Hash function (H), which is defined as Fig. 4.

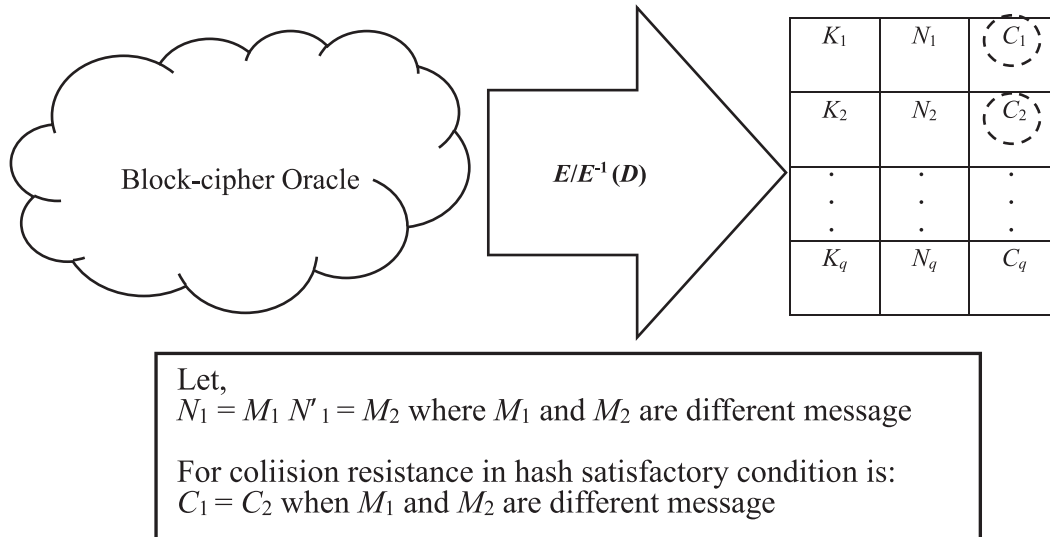


Figure 4: Concept of Collision Resistance [6], [8], [10]-[12]

3 CONCEPTS OF DESIGN

Our concept of design is to satisfy the generic construction of blockcipher based compression function. The main principle is supporting of variable size of key. Generally, the key size is fixed under the (n, n) , $(n, 2n)$, and lightweight-cipher based blockcipher ompression function. Hence, the construction principle is static. Under this circumstances, the construction principle should be dynamic. However, we mention an idea for creating this kind of construction by black-box model. Under this blac-box model, it can take two (02) input of message and key. Finally, in every iteration it produces two (02) chaining output values.

Our black-box is defined as $\mathbf{B}$ (Fig. 5), where we use input of x_1 and x_2 . In addition, the output are o_1 and o_2 . The condition is $x_1 + x_2 > o_1 + o_2$, where the size of key (k) is variable but less than message (m) size ($k < m$).

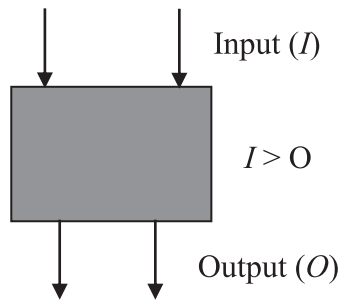


Figure 5: Concepts of design using black-box

4 CONCLUSION

In this paper, we describe using a blockcipher-based compression function as a cryptographic hash tool. The DBL blockcipher has three variants: (n, n) , $(n, 2n)$ and lightweight-cipher. There are certain schemes based on these three variants including, MR, Weimar, Tandem, Abreast, Nandi, ISA-09, MDC-2, MDC-4, MJH, Bart, MSR, SKS, SH-L1, and Sh-L2. However, there is a lack of a construction that can support the three variants listed above. In addition, generally, the communication networks are very complex and it depends on various types of devices. Furthermore, numerous devices are worked under IoT, cloud networks, and grid networks. These devices also have different properties such as resource-limitation, lightweightproperty, processing power and resource-adequate. Therefore, security solution schemes for these devices should be platform independent and generalized. Under these circumstances, we address the cracking issue of generalized construction of blockcipher based compression function. In future, we propose a specific design of blockcipher based compression function that will supports the characteristic of generalization.

REFERENCES

- [1] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, "Hash Functions and RFID Tags: Mind the Gap," LNCS, CHES, vol. 5154, pp. 283-299, 2008.
- [2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, 5th edition, CRC Press, 2001.
- [3] J. P. Kaps, B. Sunar, "Energy Comparison of AES and SHA-1 for Ubiquitous Computing," LNCS, Emerging Directions in Embedded and Ubiquitous Computing, vol. 4097, pp. 372-381, 2006.
- [4] X. Wang, X. Lai, D. Feng, H. Chen, X. Yu, "Cryptanalysis of the Hash Functions MD4 and RIPEMD," LNCS, EUROCRYPT, vol. 3494, pp. 1-18, 2005.
- [5] J. A. Black, P. Rogaway, T. Shrimpton, "Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV," LNCS, CRYPTO, vol. 2442, pp. 320-335, 2002.
- [6] E. Fleischmann, C. Forler, S. Lucks, J. Wenzel, "Weimar-DM: A Highly Secure Double-Length Compression Function," LNCS, ACISP, vol. 7372, pp. 152-165, 2012.
- [7] O. Ozen, M. Stam, "Another Glance at Double-Length Hashing," LNCS, Cryptography and Coding, vol. 5291, pp. 176-201, 2009.
- [8] F. Armknecht, E. Fleischmann, M. Krause, J. Lee, M. Stam, J. Steinberger, "The Preimage Security of Double-Block-Length Compression Functions," LNCS, ASIACRYPT, vol. 7073, pp. 233-251, 2011.
- [9] M. Nandi, W. Lee, K. Sakurai, S. Lee, "Security Analysis of a 2/3 Rate Double Length Compression Function in the Black-Box Model," LNCS, FSE, vol. 3557, pp. 243-254, 2005.
- [10] J. Lee, S. Hong, J. Sung, H. Park, "A New Double-Block-Length Hash Function Using Feistel Structure," LNCS, ISA, vol. 5576, pp. 11-20, 2009.
- [11] J. Lee, D. Kwon, "The Security of Abreast-DM in the Ideal Cipher Model," IEICE Transactions, vol. 94-A (1), pp. 104-109, 2011.
- [12] J. Lee, M. Stam, J. Steinberger, "The Collision Security of Tandem-DM in the Ideal Cipher Model," LNCS, CRYPTO, vol. 6841, pp. 561577, 2011.
- [13] S. Hirose, "Some Plausible Constructions of Double-Block-Length Hash Functions," LNCS, FSE, vol. 4047, pp. 210-225, 2006.
- [14] S. Hirose, H. Kuwakado, "Collision Resistance of Hash Functions in a Weak Ideal Cipher Model," IEICE Transactions, vol. 95 A (1), pp. 251-255, 2012.
- [15] J. Lee, M. Stam, "MJH: A Faster Alternative to MDC-2," LNCS, CTRSA, vol. 6558, pp. 213-236, 2011.
- [16] H. Kuwakado, S. Hirose, "Hashing Mode Using a Lightweight blockcipher," LNCS, Cryptography and Coding, vol. 8308, pages 213-231, 2012.

- [17] H. Kuwakado, S. Hirose, "A Block-Cipher-Based Hash Function Using an MMO-Type Double-Block Compression Function," LNCS, Provsec, vol. 8782, pages 71-86, 2014.
- [18] A. Miyaji, M. Rashed, S. Tsuyoshi "A new (n, n) Blockcipher based Hash Function for Short Messages," IEEE, ASIAJCIS, 978-1-47995733, pp. 56-63, 2014.
- [19] E. Fleischmann, C. Forler, and S. Lucks "The Collision Security of MDC-4, LNCS, Africacrypt, vol. 7374, pp. 252-269, 2012.
- [20] J. Lee, M. Stam, "MJH: A Faster Alternative to MDC-2," CT-RSA, vol. 6558, 213-236, 2011.
- [21] J. Coron, Y. Dodis, C. Malinaud, P. Puniya, "Merkle-Damgard Revisited: How to Construct a Hash Function," LNCS, CRYPTO, vol. 3621, pp. 430-448, 2005.
- [22] A. Joux, "Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions," LNCS, CRYPTO, vol. 3152, pp. 306-316, 2004.
- [23] P. Gauravaram, J. Kelsey, "Linear-XOR and Additive Checksums Protect Damgrd-Merkle Hashes from Generic Attacks," LNCS, CT-RSA, vol. 4964, pp. 36-51, 2008.
- [24] X. Lai, X. Massey, L. J., "Hash function based on block ciphers," LNCS, EUROCRYPT, vol. 658, pp. 55-70, 1993.
- [25] B. Mennink, "Optimal Collision Security in Double Block Length Hashing with Single Length Key," LNCS, ASIACRYPT, vol. 7658, pp. 526-543, 2012.
- [26] L. Barreto, A. Celesti, M. Villari, M. Fazio, A. Puliato, "An Authentication Model for IoT Clouds", IEEE, ASONAM, pp. 1032 -1035, 2015.
- [27] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, A. Iera, "A systemic and cognitive approach for IoT security", IEEE explore, ICNC, pp. 183-188, 2014.
- [28] J. Y. Lee, Y. H. Huang, "A lightweight authentication protocol for Internet of Things", IEEE explore, ISNE, pp. 1-2, 2014.
- [29] H. Yoshida "On the standardization of cryptographic application techniques for IoT devices in ITU techniques for IoT devices in ITU-T and ISO/IEC JTC 1 T and ISO/IEC JTC1, <https://www.ietf.org/proceedings/94/slides/slides-94-saag-2.pdf>, 2015
- [30] G. S. Matharu, P. Upadhyay, "The Internet of Things: Challenges and security issues," IEEE ex., ICET, 978-1-4799-6088-0, pp. 54-59, 2014.

Rashed Mazumder He received his Bachelor's degree from University of Dhaka, Bangladesh in the field of Computer Science and Engineering. In 2010, he joined as a faculty of Mawlana Bhashani Science and Technology University (MBSTU), Bangladesh. He completed a Master's degree from the University of Japan Advanced Institute of Science and Technology (JAIST), Japan in 2014. After successful completion of master degree he finished his Ph.D degree under the school of Information Science of JAIST. Now he is serving as an Assistant Professor at the department of Information and Communication Technology (ICT) in MBSTU, Bangladesh.

Mohammad Shahriar Rahman He is currently an associate professor at the University of Liberal Arts Bangladesh. Earlier, he worked as associate professor at University of Asia Pacific, Bangladesh, and senior researcher at the Information Security group of KDDI Research, Japan. He received his Ph.D. and M.S. degrees in information science from Japan Advanced Institute of Science and Technology (JAIST), in 2012 and 2009 respectively, and B.Sc. in computer science and engineering from University of Dhaka, Bangladesh, in 2006. His research interests include secure protocol construction, privacy-preserving computation and security modeling. He is a member of International Association for Cryptologic Research (IACR).

Muhammad Shahin Uddin He received his B.Sc. Engineering degree in Electrical and Electronic Engineering from Rajshahi University of Engineering and Technology (RUET), Bangladesh and M.Sc. Engineering degrees in Electronics Engineering from Kookmin University, South Korea. He received the doctoral degree from the University of New South Wales, Australia. He worked for American International University Bangladesh (AIUB) and, Chittagong University of Engineering & Technology (CUET), Bangladesh. Since 2006, he has been with the department of Information and Communication Technology, Mawlana Bhashani Science and Technology University (MBSTU). He received the University Gold Medal from Rajshahi University of Engineering and Technology (RUET), Bangladesh. His research interests include, Visible Light Communication (VLC), LED-ID system, optical fiber, Bio-photonics and digital image processing.

Mohammad Badrul Alam Miah He received his BSc (Engg.) in Information and Communication Technology under the department of Information and Communication Technology (ICT) of Mawlana Bhashani Science and Technology University (MBSTU). He received the Masters degree from the University of MBSTU, Tangail, Bangladesh. He is now serving as an Associate Professor in the department of ICT. His research interests are Neural Network, Digital Image Processing, Data Mining, Network security, Computer Vision.

Numerical Study on Advection Diffusion Equation for Human Lung Model Channel

Mahtab U. Ahmmed and Monika Khatun

Department of Mathematics, Jahangirnagar University, Dhaka-1342, Bangladesh

E-mail:mahtab_ahmmed@yahoo.com

Abstract

An advection-diffusion equation (AD) based on lumped parameter model for O_2 transportation along human lung channel is presented and solved numerically with three explicit finite difference schemes FTFSCS (forward time forward space and centered space), FTBSCS (forward time backward space and centered space) and FTCSCS (forward time centered space in first order and second order). The stability conditions are obtained and implemented in numerical solution to present the AD effects entire the flow experiment. The role of inductive time constant within $t_L \in [0.01, 0.1]$ is investigated which dominates the rate of diffusion in the flow. Error comparisons with analytical solutions of ADE are also presented graphically to show the accuracy of the schemes.

Keywords— Lumped model, Lung model channel, Inductive time constant, Advection-diffusion equation, Finite difference scheme.

© University of Liberal Arts Bangladesh

All rights reserved.

Manuscript received on 31 August 2017 and accepted for publication on 1 November 2017.

1 INTRODUCTION

Most of the transportation of fluid in physical problem to biological system occur in advection and diffusion process according to the model $q_t + uq_x = Dq_{xx}$, where $q(x, t)$ = flux, D = the rate of diffusion and u = the mean flow velocity. Water pollution in oceans, rivers, lakes or ground water and pollution in atmosphere take place continually in surroundings. It is essential to know the contaminant or temperature distribution in the water for safety of the environment [1]. This type of problem describes transport and diffusion process can be modeled using one dimensional advection diffusion equation (ADE). ADE illustrates many quantities such as mass, velocity, heat and energy [2]. Many authors are involved in solving ADE by using finite difference method (FDM). The mathematical model of water pollution is solved using implicit centered difference scheme in space and forward difference method in time by [3]. Aral and Liao [4] solved for two-dimensional transport equation with time dependent dispersion coefficients analytically. Kumar et al. [5] presented analytical solution of one dimensional ADE with variable coefficients in a finite domain using Laplace transformation. The ADE has been used as a model equation in many engineering problems such as dispersion of tracers in porous media [6,7], pollutant transport in rivers and streams [8], thermal pollution in river systems [9]. Stability analysis of finite difference scheme for solving ADE is studied by [10-13]. As stated above, most of the works has been done for open channel. But ADE has wide applications in other disciplines too, like biosciences, soil physics, petroleum engineering and chemical engineering. In vivo, fluid (liquid or gas) moves along closed channel and flow might be transported to downstream by advection or spread out by diffusion when unidirectional flow is weaken. For example, a complete cycle of respiration in human lung channel is a consequence of oscillatory flow (advection) and stagnation in transition (diffusion) in nature. A patient who is unable to perform respiration, artificial high frequency oscillatory ventilation (HFOV) helps to survive in the world. HFOV controls the constant oscillatory flow along human lung channel and flows in lung channel faces resistance and compliance effects. Oscillatory flow and mass transport was studied along model channel of human lung by [14, 15]. They simulated governing equations with boundary conditions to show effective diffusion along straight tube. Laminar, turbulent and oscillatory dispersion along a circular channel is calculated by [16]. He established a relation between channel radius and diffusion coefficient. Tanaka et al. [17] examined that a secondary flow during HFOV method ensures effective diffusion in bent and bifurcated tubes than in straight tube. A lumped-parameter model has been developed to study airflow distribution by Elad et al. [18]. The authors also derived the modified time-dependent expressions of resistance and compliance of a single compartment. Numerical analysis of air flow along

lung channel with asymmetric compliance was examined experimentally and numerically by Hirahara et al. [19]. We found that the flow for inhomogeneous compliance ratio leads to irreversible flow along lung model. This type of flow effect might be the result of diffusion.

With the above discussions, in this paper, a transport equation of lung model channel is produced from lumped parameter model [18]. The numerical study on stability with FTFSCS, FTBSCS and FTCSCS techniques are discussed for solving the AD problem. A relation between inductive time constant and the rate of diffusion is introduced. The AD effect and relative errors for numerical solutions are presented graphically. The variations of relative error of lung model equation for each scheme are also presented graphically.

2 MATHEMATICAL MODEL

A lumped parameter model with resistance (R), inertance (L) and Compliance (C) for incompressible fluid flow in absence of driving force along human lung model channel may be modeled from

$$L \frac{dq}{dt} + Rq + \frac{1}{C} \int q dt = 0 \quad (1)$$

where $q = q(t)$ is the flow rate of fluid to

$$\frac{\partial q}{\partial t} + u \frac{\partial q}{\partial x} = \frac{Lu^2}{R} \frac{\partial^2 q}{\partial x^2} \quad (2)$$

where $q = q(x, t)$ is the flux. This is an advection-diffusion equation (ADE) of lung model. Using Fourier transform, convolution theorem and Dirac delta function, the analytic solution of Eqn.(2) is [20]

$$q(x, t) = \frac{M}{A_{yz} \sqrt{4\pi Dt}} \exp -\frac{(x-ut)^2}{4Dt} \quad (3)$$

Where, $D = Lu^2 / R \Rightarrow D \propto t_L$ and the inductive time constant, $t_L = L / R$

Where, u is the constant velocity, M is the mass volume along the model channel, and $q(x, 0) = M\delta(x)$ is the initial condition of IBVP.

3 NUMERICAL TECHNIQUE FOR MODEL EQUATION

The unsteady incompressible flow along a rigid channel without driving force and compliance effect is an ADE (2) for physical domain of channel length ($0 \leq x \leq l$), is

$$\begin{aligned} q_t + uq_x &= Dq_{xx} \\ q(x, 0) &= q_0(x), \quad 0 \leq x \leq l \\ q(0, t) &= g(t), \quad q(l, t) = h(t), \quad 0 < t \leq T \end{aligned} \quad (4)$$

In order to develop the computational scheme by finite difference method (FDM), we discretize the x - t plane with mesh size $\Delta x \times \Delta t$. Grid width and time step are taken equal individually. The spatial and temporal coordinate at the grid point $q(x_i, t_j)$ is defined as

$$\begin{aligned} x_i &= x_0 + i\Delta x; \quad i = 0, 1, 2, \dots, m \\ t_j &= t_0 + j\Delta t; \quad j = 0, 1, 2, \dots, n \end{aligned}$$

The approximate solution at grid points $q(x_i, t_j)$ is $q_{i,j} \in R^n$ so that $q_{i,j} \approx q(x_i, t_j)$.

The forward time (FT) difference formula

$$\frac{\partial q}{\partial t} \approx \frac{q_i^{j+1} - q_i^j}{\Delta t} \quad (5)$$

The forward space (FS) difference formula

$$\frac{\partial q}{\partial x} \approx \frac{q_{i+1}^j - q_i^j}{\Delta x} \quad (6)$$

The backward space (BS) difference formula

$$\frac{\partial q}{\partial x} \approx \frac{q_i^j - q_{i-1}^j}{\Delta x} \quad (7)$$

The first order centered space difference formula

$$\frac{\partial q}{\partial x} \approx \frac{q_{i+1}^j - q_{i-1}^j}{2\Delta x} \quad (8)$$

The second order centered space difference formula

$$\frac{\partial^2 q}{\partial x^2} \approx \frac{q_{i+1}^j - 2q_i^j + q_{i-1}^j}{(\Delta x)^2} \quad (9)$$

are employed to have the following computational schemes.

3.1 Explicit Scheme by FTFSCS Techniques

Substituting (5), (6) and (9) into (4) and rearranging according to the time level, implies to

$$q_i^{j+1} = \lambda q_{i-1}^j + (1 - 2\lambda + \gamma) q_i^j + (\lambda - \gamma) q_{i+1}^j \quad (10)$$

3.2 Explicit Scheme by FTBSCS Techniques

Inserting (5), (7) and (9) into (4) and rearranging, the scheme implies to

$$q_i^{j+1} = (\lambda + \gamma) q_{i-1}^j + (1 - 2\lambda - \gamma) q_i^j + \lambda q_{i+1}^j \quad (11)$$

3.3 Explicit Scheme by FTCSCS Techniques

Finally (5), (8) and (9) into (4) becomes

$$q_i^{j+1} = \left(\lambda + \frac{\gamma}{2}\right) q_{i-1}^j + (1 - 2\lambda) q_i^j + \left(\lambda - \frac{\gamma}{2}\right) q_{i+1}^j \quad (12)$$

Where (3.1 to 3.3), $\lambda = \frac{D\Delta t}{(\Delta x)^2}$, $\gamma = \frac{u\Delta t}{\Delta x}$

3.4 Stability Conditions

Stability is a property that concerns the growth or decay of errors introduced at any stage during the computation and strongly governs the numerical solution. The von Neumann stability condition may be developed by $e^{a\Delta t} \leq \cos(k_m \Delta x) - i\gamma \sin k_m \Delta x \leq 1$, where a is a constant, k_m is the wave number and γ is the CFL condition. We develop simultaneous stability condition for the schemes (10) to (12) and perform numerical simulation by implementing the schemes for various parameters. The stability conditions are Shown in Table 1.

TABLE 1
STABILITY CONDITIONS FOR THE VARIOUS SCHEMES

Conditions for the schemes	
Explicit Schemes	Stability Conditions
FTFSCS	$\frac{1}{2} \leq \lambda \leq 1$ and $2\lambda - 1 \leq \gamma \leq \lambda$
FTBSCS	$0 \leq \lambda \leq 1$ and $-\lambda \leq \gamma \leq 1 - 2\lambda$
FTCSCS	$0 \leq \lambda \leq \frac{1}{2}$ and $-2\lambda \leq \gamma \leq 2(1 - \lambda)$

4 NUMERICAL RESULTS AND DISCUSSIONS

4.1 Problem Description

An incompressible fluid flow along human lung model channel of length, $l=4$ mm is passed for fluid velocity, $u=60$ mm/s on a second. The inductive time constant, $t_L = 0.1$ is calculated from lab experimental value of L and R so that the inductive time constant based diffusion rate is $D=3600$ mm²/s. The computed time step and grid width are $\Delta t = 2 \times 10^{-4}$ and $\Delta x = 0.04$.

Solutions:

The numerical experiment for the problem is investigated for the schemes FTFSCS in Fig.1, FTBSCS in Fig.2 and FTCSCS in Fig.3 for several distinct times within the experimental time. The time constant, $t_L = 0.1$ is taken for the entire simulation where the accepted value for $t_L \in [0.01, 0.1]$ is found within the stability condition. The effect of advection-diffusion (AD) is compared at a time, $t = T/50$ for all three schemes. It is seen that AD effect is minimum for FTFSCS scheme and maximum for FTBSCS scheme and moderate for FTCSCS.

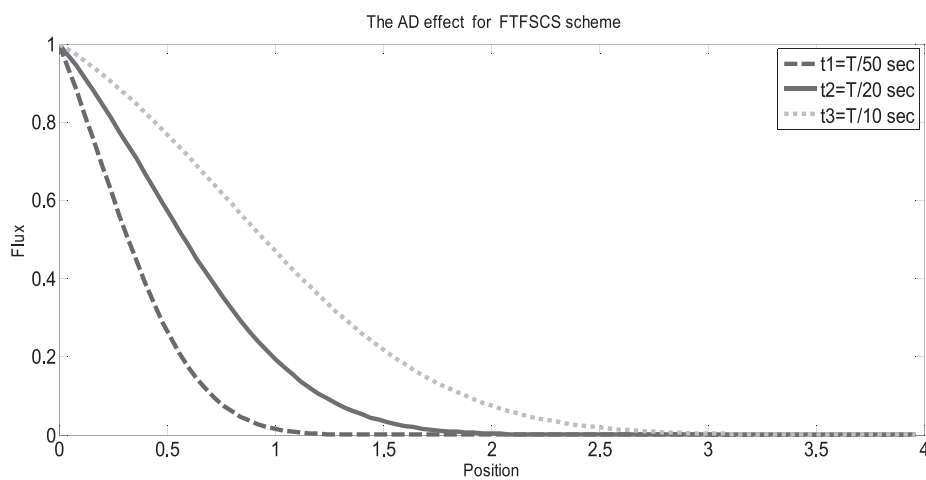


Figure 1: AD effect for FTFSCS Scheme.

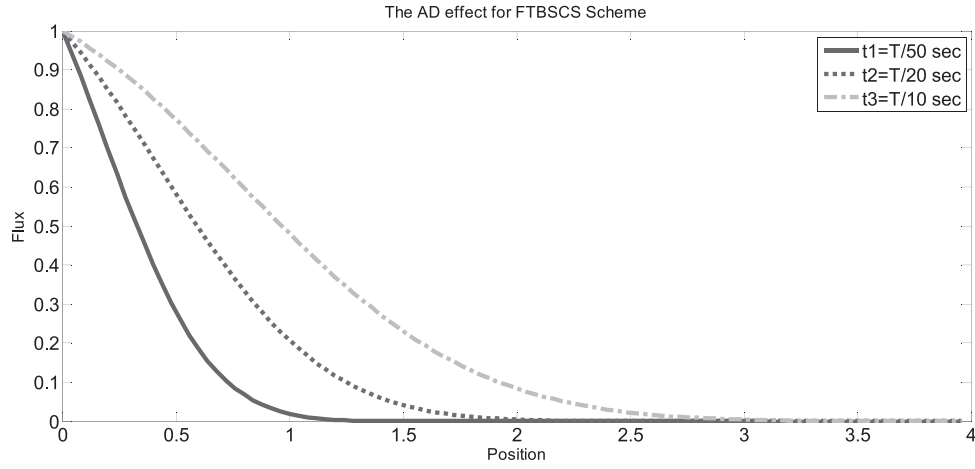


Figure 2: AD effect for FTBSCS Scheme.

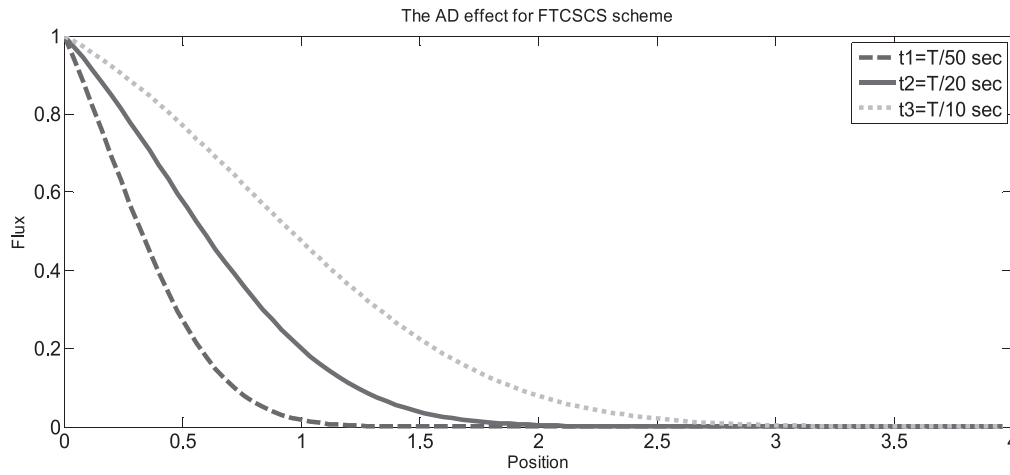


Figure 3: AD effect for FTCSCS Scheme.

4.2 Error Estimation and Convergence

The explicit finite difference schemes FTFSCS, FTBSCS and FTCSCS is employed to compute the results of the model

problem for $t=1s$. The relative error estimated in L_1 -norm is defined by $err = \frac{\|q_e - q_a\|_1}{\|q_e\|}$

Where q_e is the exact and q_a is the approximate solution computed for $t \in [0,1]s$.

As depicted in Fig.5, the curves marked by dot line (red) shows the relative error for the FTFSCS scheme, the solid line (green) shows the relative error for the FTBSCS scheme and the dash line (blue) shows the relative error for the FTCSCS scheme in the same numerical conditions. It is evident that FTBSCS has minimum relative error in comparison with FTFSCS and FTCSCS scheme.

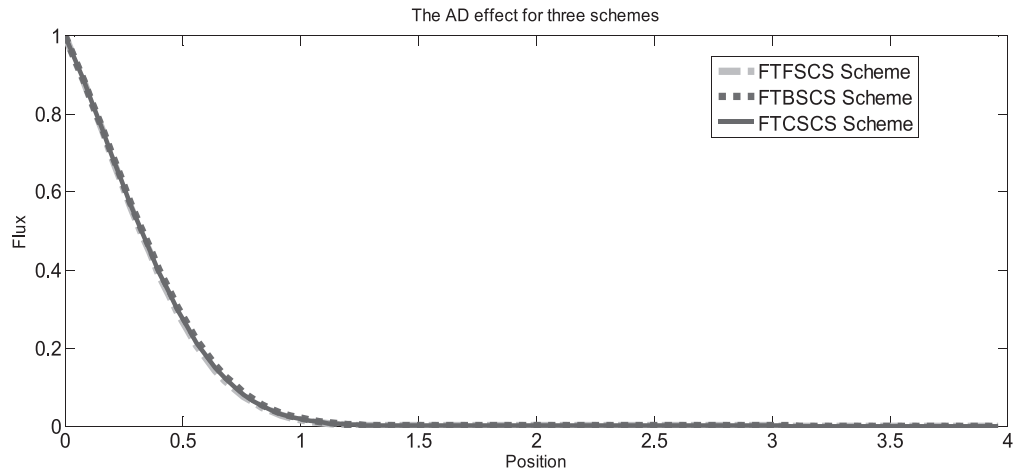


Figure 4: AD effect for FTFSCS, FTBSCS and FTCSCS scheme in time $t = T/50$ s

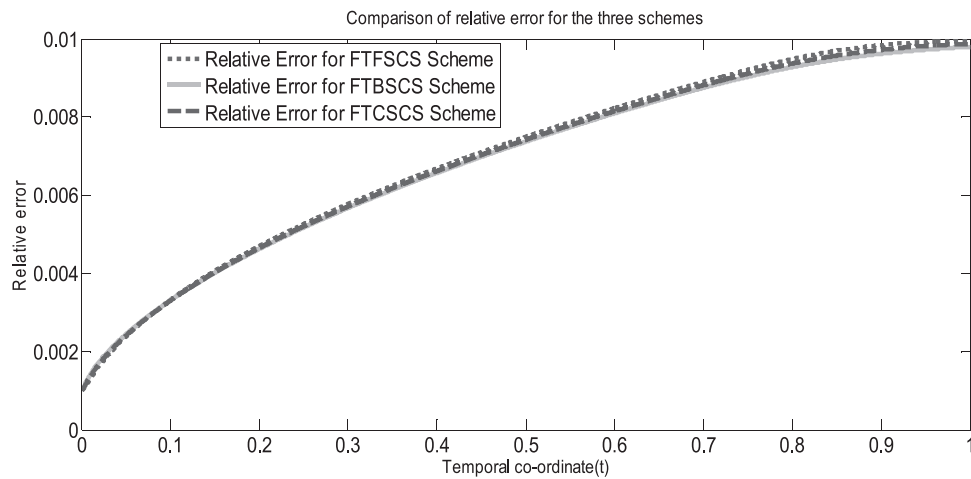


Figure 5: Comparison of relative error for the schemes.

Now, it demands for showing convergence of the solution due to the change of grid size variations. The convergence of relative error for the FTBSCS scheme is taken for time step $\Delta t = 0.0002$ s, velocity $u = 6$ cm/s at several positions, $\Delta x = 0.1, 0.3, 0.5$ as shown in Fig.6. It is clear that the variation of error is related to the value of Δx . If $\Delta x = 0.5$ then the relative error is maximum compared with other values of space increment which is shown by dot line (green). It is concluded that the larger value shows the larger error and vice versa within a certain time fractions for all schemes.

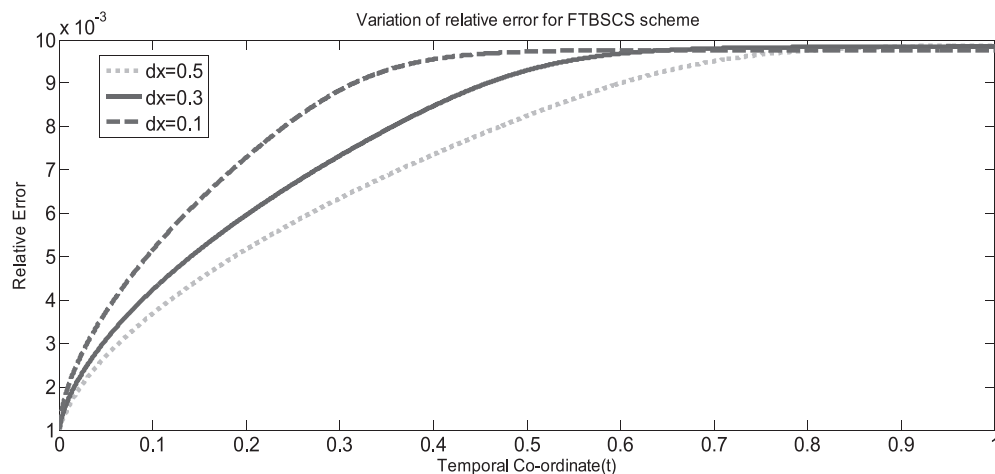


Figure 6: Variation of relative error for FTBSCS scheme.

5 CONCLUSION

In this work, we have presented numerical solution of 1D advection-diffusion transportation equation generated from lumped parameter model of human lung. Our model channel is very narrow and short in length. The AD effect is investigated for FTFSCS, FTBSCS and FTCSCS schemes numerically and presented graphically. The analytical result is used for code validation and for error comparison within the schemes. We found that the AD effect of the lung model equation (2) for the schemes are stable within the range of the inductive time constant, $t_L \in [0.01, 0.1]$. The inductive time constant introduced in this model plays a significant role in advection-diffusion effect. The FTBSCS scheme shows the maximum AD effect in comparison with FTCSCS and FTFSCS scheme in Fig.4. Also, FTBSCS scheme presents minimum relative error in comparison with FTCSCS and FTFSCS schemes as in Fig.5. Since FTBSCS scheme has minimum relative error, it is more suitable for our lung model problem. Moreover, we found that due to the increasing of the value of Δx for the schemes separately, the relative error is also increasing as in Fig. 6. This error reduction is due to a decrease in the influence of the initial data.

REFERENCES

- [1] C.G. Koutitas, 'Elements of computational hydraulics', Pentech Press, London, UK, 1983.
- [2] B.J. Noye, 'Numerical solution of partial differential equations' Lecture notes, 1990.
- [3] F.B. Agosto, O.M. Bamigbola, 'Numerical treatment of the mathematical models for water pollution', Research J. Appl. Sci. 2(5), 548-556, 2007.
- [4] M.M. Aral and B. Liao, 'Analytic solutions for two-dimensional transport equation with time dependent dispersion coefficients', J. Hydrol. Eng., 1(1), 20-32, 1996.
- [5] A. Kumar, D. Kumar and N. Kumar, 'Analytical solution of one dimensional advection diffusion equation with variable coefficients in a finite domain', J. Earth. Syst. Sci. 118(5), 539-549, 2009.
- [6] R.B. Banks and J. Ali, 'Dispersion and absorption in porous media flow', J. Hydraulic Div., 90, 13-31, 1964.
- [7] N. Kumar, 'Unsteady flow against dispersion in finite porous media', J. Hydrology, 63(3-4), 345-358, 1983.
- [8] P.C. Chatwin and C.M. Allen, 'Mathematical models of dispersion in rivers and estuaries', Annual Review of Fluid Mechanics, 17, 119-149, 1985.
- [9] M.H. Chaudhry, D.E. Cass and J.E. Edinger, 'Modeling of unsteady flow water temperatures', J. Hydraulic Eng. 109(5), 657-669, 1983.
- [10] K.W. Morton, 'Stability of finite difference approximations to a diffusion-convection equation', Int. J. Numerical Methods in Eng., 15(5), 677-683, 1980.
- [11] L.F. Leon, P.M., Austria, 'Stability criterion for explicit scheme on the solution of advection-diffusion equation', Mexican Institute of Water Technology.
- [12] T.M.A.K. Azad and L.S. Andallah, 'Stability analysis of finite difference schemes for an advection diffusion equation', Bangladesh J. Sci. Res. 29(2), 143-151, 2016.
- [13] H. Karahan, 'Unconditional stable explicit finite difference technique for the advection-diffusion equation using spread sheets', Advances in Eng. Software, 38(2), 80-86, 2007.
- [14] D.M. Eckmann, J.B. Grotberg, 'Oscillatory flow and mass transport in a curved tube', J. Fluid Mech., 188, 509- 527, 1988.
- [15] H. Fujioka, K. Oka, and K. Tanishita, 'Oscillatory flow and gas transport through a symmetrical bifurcation', J. Biomechanical. Eng., 123, 145-153, 2001.
- [16] H.K. Chang, 'Mechanisms of gas transport during ventilation by high-frequency oscillation', J. Appl. Physiology 56(3): 553-563.
- [17] G. Tanaka, T. Ogata, K. Oka, and K. Tanishita, 'Spatial and temporal variation of secondary flow during oscillatory flow in model human central airways', J. Biomechanical. Eng., 121, 565-573, 1999.
- [18] D. Elad, A. Shochat and R.J. Shiner, 'Computational model of oscillatory airflow in a bronchial bifurcation' Respiration Physiology, 112, 95-111, 1998.
- [19] H. Hirahara, K. Iwazaki, M.U. Ahmmed, M. Nakamura, 'Numerical analysis of air flow in dichotomous respiratory channel with asymmetric compliance under HFOV condition' Journal of Fluid Science and Technology, 6(6), 932-948, 2011.
- [20] S.G. Ahmed, 'A numerical algorithm for solving advection-diffusion equation with constant and variable coefficients', Dept. Eng. Physics and Mathematics, Faculty of Engg., Zagazig University, Egypt.

Mahtab Uddin Ahmmed awarded Ph.D on Mechanical Engineering and Science from Saitama University, Japan and M. Phil in Mathematics from Bangladesh University of Engineering & Technology (BUET), Dhaka. He also received M.Sc and B.Sc (Hons.) degrees from the department of Mathematics, Jahangirnagar University. Now, he has been working as an Associate Professor in the department of Mathematics, Jahangirnagar University. Prior to this, he served Dhaka University of Engineering & Technology (DUET), Bangladesh as a faculty from 2003 to 2011. He has published a number of papers in peer-reviewed international and national journals and presented original research articles in numerous international conferences. He received various scholarships, research and travel grants as recognition of his research works. He is a life member of Bangladesh Mathematical Society. His research is focused on computational fluid dynamics (CFD) especially in the field of biological flow and mathematical modeling.

Monika Khatun is appeared in M.S in the department of Mathematics, Jahangirnagar University. She also received B.Sc (Hons.) degree from the department of Mathematics, Jahangirnagar University. Her research interest is in numerical simulation of fluid dynamical problems.

ULAB JOURNAL OF SCIENCE AND ENGINEERING

ISSN 2079-4398 (Print), ISSN 2414-102X (Online)

A Note for Contributors

SCOPE

The ULAB Journal of Science and Engineering is published annually by the University of Liberal Arts Bangladesh. Its editorial board encourages submission of high quality original and unpublished research papers in all branches of Science and Engineering that are not being considered for publication in any other forums. This includes all traditional areas of both theoretical and practical applications of physics, mathematics, environmental science, electronics, computer science, information and communication engineering. Besides, the journal will gladly accept papers on emerging technologies and new areas related to the above fields.

SUBMISSION GUIDELINES

- The contribution must be written in English and describe original research, which is not published or currently under review by other journals or conferences.
- Authors are solely responsible for the factual accuracy of the contribution.
- All papers will be rigorously reviewed by a panel of reviewers.
- Paper Format: All manuscripts should follow our template, which is downloadable from our journal's website.
- We will copy edit all accepted papers for more clarity and readability by a professional copy editor. This is our final version.
- Authors will receive copy-edited final version just for making it camera-ready according to our template and return it within specified time. Please note that conformity with our template is a stringent requirement. No new matters should be inserted in the texts of this final version without the intimation to the editorial board.
- Manuscripts should be submitted electronically directly to the editor-in-chief <shorif.uddin@ulab.edu.bd> in pdf/doc format. It is mandatory for an accepted paper to submit a signed copyright transfer form.
- No publication charge is required for an accepted paper

CORRESPONDENCE

Editor-in-Chief, ULAB Journal of Science and Engineering,
School of Science and Engineering
University of Liberal Arts Bangladesh (ULAB)
Campus B, House 719/A, Road 7/A (Satmasjid Road)
Dhanmondi R/A, Dhaka 1209, Bangladesh
Tel: +880-2-9661255, Fax: +880-2-9670931, Cell: 01747615832
E-mail:shorif.uddin@ulab.edu.bd
<http://journals.ulab.edu.bd/jse/>

ULAB JOURNAL OF SCIENCE AND ENGINEERING

ISSN 2079-4398 (Print), ISSN 2414-102X (Online)

COPYRIGHT FORM

To ensure uniformity of treatment among all contributors, other forms may not be substituted for this form, nor may any wording of the form be changed. This form is intended for original material submitted to the ULAB Journal of Science and Engineering for publication. Please read the form carefully and keep a copy for your files.

TITLE OF PAPER (hereinafter, “the Work”):

COMPLETE LIST OF AUTHORS:

Copyright Transfer

The undersigned hereby assigns to the University of Liberal Arts Bangladesh (ULAB) all rights under copyright that may exist in and to the above Work, and any revised or expanded derivative works submitted to the ULAB Journal of Science and Engineering by the undersigned based on the Work. The undersigned hereby warrants that the Work is original and that he/she is the author of the Work; to the extent the Work incorporates text passages, figures, data or other material from the works of others, the undersigned has obtained any necessary permissions.

General Terms

- The undersigned represents that he/she has the power and authority to make and execute this assignment.
- The undersigned agrees to indemnify and hold harmless the ULAB from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.
- In the event the above work is not accepted and published by the ULAB or is withdrawn by the author(s) before acceptance, the foregoing copyright transfer shall become null and void and all materials embodying the Work submitted to the ULAB will be destroyed.
- For jointly authored Works, all joint authors should sign, or one of the authors should sign as authorized agent for the others.

Author/Authorized Agent for Joint Authors

Date

RETAINED RIGHTS/TERMS AND CONDITIONS

1. Authors/employers retain all proprietary rights in any process, procedure, or article of manufacture described in the Work.
2. Authors/employers may reproduce or authorize others to reproduce the Work, material extracted verbatim from the Work, or derivative works for the author’s personal use or for company use, provided that the source and the ULAB copyright notice are indicated, the copies are not used in any way that implies ULAB endorsement of a product or service of any employer, and the copies themselves are not offered for sale.
3. Authors/employers may make limited distribution of all or portions of the Work prior to publication if they inform the ULAB in advance of the nature and extent of such limited distribution.

PLEASE DIRECT ALL QUESTIONS ABOUT THIS FORM TO:

Editor-in-Chief, ULAB Journal of Science and Engineering, School of Science and Engineering, University of Liberal Arts
Bangladesh Campus B, House 719/A, Rd 7/A (Satmasjid Rd), Dhanmondi R/A, Dhaka 1209, Bangladesh
Phone: +880-2-9661255, Fax: +880-2-9670931, E-mail: shorif.uddin@ulab.edu.bd