GLOBAL ACADEMIC RESEARCH INSTITUTE

COLOMBO, SRI LANKA

International Journal of Engineering Science

ISSN 2424-645X

Volume: 01 | Issue: 01

On 30th April 2023

GARI PUBLISHER

87/23A, KohilaKotuwa Road, Neelammahara,

Maharagama, Colombo, Sri Lanka

Tel: +94-112-849-268 / Fax: +94-112-849-426

Mobile: +94-773-940-838 / +94-715-279-696

For Paper Submission: editor@gariteam.com

For Help: helpdesk@gariteam.com

WhatsApp / Viber: +94-773-940-838

Skype: gari.conference

Web: https://www.research.lk/journal/list-of-journals

Journal Brief

International Journal of Engineering Science is an international peer-reviewed journal that publishes original and high-quality research papers in all areas of Engineering Science. An Open Access Double Blind Peer Reviewed Biannually Publish E-Journal, with a strong Editorial Board and a tested rapid peer review system. As an important academic exchange platform, scientists and researchers can know the most up-to-date academic trends and seek valuable primary sources for reference.

This E-journal publish 02 times per annually

DISCLAIMER

The responsibility for opinions expressed, in articles, studies and other contributions in this publication rests solely with their authors, and this publication does not constitute an endorsement by the Global Academic Research Institute of the opinions so expressed in them.

Volume: 01 | Issue: 01

ISSN 2424-645X

Edited by Global Academic Research Institute Publication Department

80 Pages

Publish by: Global Academic Research Institute Publication Department

Table of Contents

CASE STUDY ON ASSESSING STUDYING PATTERNS OF AERONAUTICAL ENGINEERING UNDERGRADUATES OF GENERAL SIR JOHN KOTELAWALA DEFENCE UNIVERSITY IN SRI LANKA

K. A. D. D. Kuruppu, C. J. Hettiarachchi

Department Aeronautical Engineering, Faculty of Engineering, General Sir John Kotelawala Defence University, Sri Lanka

ABSTRACT

Study patterns consider as one of the prominent factors in academic achievements. These studying patterns can be evaluated under several parameters such as regular study, study space, efficient in reading, listening to lectures, active participation for the lessons, doing homework, efficient writing of notes, preparation for exams and attending for exams. In this research, the sample consisted of all the undergraduates (29) studied in the Department of Aeronautical Engineering at their final year in 2015. The data related to studying patterns were collected using a self-administered questionnaire which includes 30 questions in the form of four point Likert. The objectives of this study were to evaluate the studying patterns of Aeronautical Engineering undergraduates who studied at their final year in the university and compare the influence of their studying patterns with their Academic class they obtained. A self-administered questionnaire was used to collect the data. Six studying pattern parameters were evaluated in this study. The Academic class achieved by the students who took part in this survey, were also considered for this study after they obtained their Final Grade Point Average (FGPA). The measured studying pattern parameters included reading text books, studying, memorizing, preparing for exams, time management and taking down notes. If the score relating to any study pattern parameter increases, the overall study pattern also increases. When the total points gathered from all study pattern parameters is high, the overall study pattern of that particular student is also getting higher. As per the statistics this scale reported the high level of reliability (internal consistency) as 0.604. In this research, internal consistency of the scale was found as 0.564. Descriptive statistics method was applied at this stage in order to analyze the study pattern of the students. Based on the responses given by the responders, the frequency levels for each question was tabulated in MS Excel worksheet. The Excel worksheet was uploaded to the IBM Statistical Package for the Social Sciences (SPSS) software and each study pattern parameter was evaluated.

It was found that only 31.7 % of the studied group effectively practice the habit of reading text books and only 39.3 % effectively engage in studying. 33.8 % from the whole population practice effective memorizing methods while 56.6 % of students prepare for exams well in advance. Moreover, only 26.9 % of students practices effective time management practices but only 32.4 % of students were good in effective note writing skills. As these studying skills are inefficiently used by majority of the students only 7% of the students from the total were obtained First Class degrees while the rest could get only general passes.

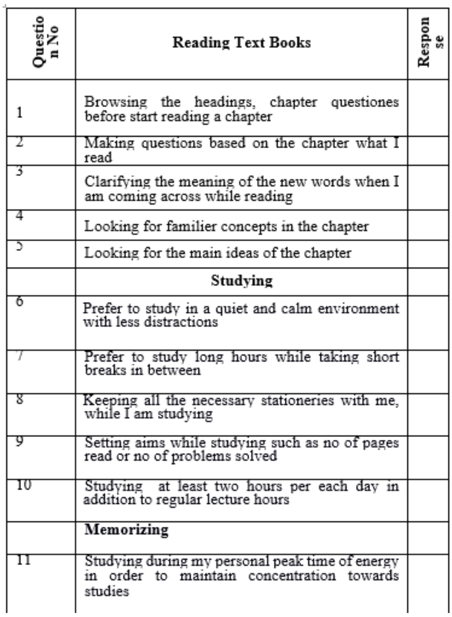
Keywords: Study patterns, Aeronautical Engineering, Undergraduates

INTRODUCTION

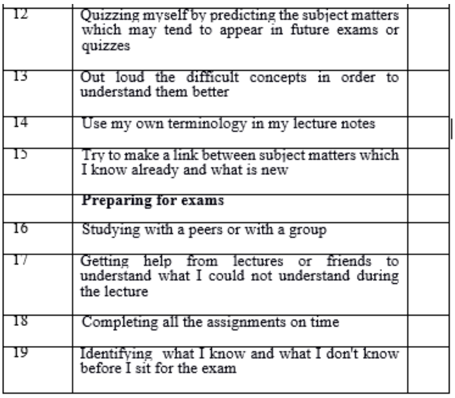
Researchers have recognized several factors of students which influence for their better performances in academic studies [1]. Some of these factors include students' perception about the teaching environment and the teaching strategies of the teacher [2]. One of the main reasons for student failures are due to inadequacy in the skills and attitudes towards their study [3]. Study patterns consider as one of the prominent factors in academic achievements [4, 5]. These studying patterns can be evaluated under several parameters such as regular study, study space, efficient in reading, listening to lectures, active participation for the lessons, doing homework, efficient writing of notes, preparation for exams and attending for exams [6, 7]. In addition, these efficient studying patterns can be explained under major three categories namely, motivation, time management and preparing for examinations [8]. Motivation plays a positive role in students' success academically by enabling them to manage time effectively. It was found that better time management skills lead to reach their goals at the end of the course [9]. Examinations plays an important role in the evaluation process of the students. Hence, effective studying strategies are vital to illustrate the real potential of the students [10]. As per the literature it is obvious that the contribution to enhance the students' effective studying patterns are mandatory in order to improve the university education system as a whole [2]. Further, there are many research articles where the researchers correlated the studying skills and academic achievements [11]. The objectives of this study were to evaluate the studying patterns of aeronautical engineering undergraduates who studied at their final year and compare the influence of their studying patterns for their Academic class they obtained.

METHODOLOGY

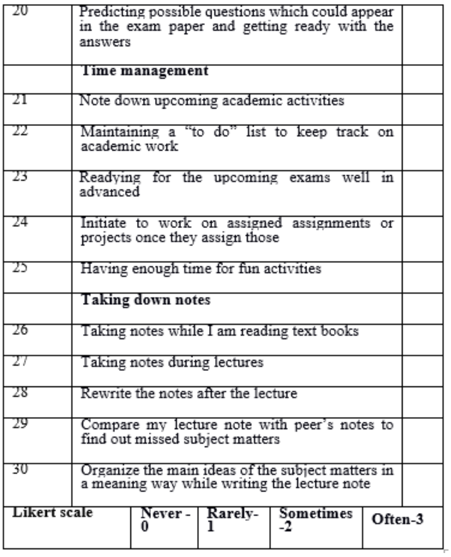
In this research, the sample consisted of all the undergraduates (29) studied in the Department of Aeronautical Engineering at their final year in 2015. The data related to studying patterns were collected using a self-administered questionnaire which includes 30 questions in the form of four point Likert. The 30 questions were divided for 6 sections. Each section consists of five questions and those five questions were related to one specific studying pattern parameter. Hence, there were 6 studying pattern parameters and collectively they described the overall studying pattern of undergraduates.



Question No	**Reading Text Books**	**Response**
1	Browsing the headings, chapter questiones before start reading a chapter	
2	Making questions based on the chapter what I read	
3	Clarifying the meaning of the new words when I am coming across while reading	
4	Looking for familier concepts in the chapter	
5	Looking for the main ideas of the chapter	
	Studying	
6	Prefer to study in a quiet and calm environment with less distractions	
7	Prefer to study long hours while taking short breaks in between	
8	Keeping all the necessary stationeries with me, while I am studying	
9	Setting aims while studying such as no of pages read or no of problems solved	
10	Studying at least two hours per each day in addition to regular lecture hours	
	Memorizing	
11	Studying during my personal peak time of energy in order to maintain concentration towards studies	



12	Quizzing myself by predicting the subject matters which may tend to appear in future exams or quizzes	
13	Out loud the difficult concepts in order to understand them better	
14	Use my own terminology in my lecture notes	
15	Try to make a link between subject matters which I know already and what is new	
	Preparing for exams	
16	Studying with a peers or with a group	
17	Getting help from lectures or friends to understand what I could not understand during the lecture	
18	Completing all the assignments on time	
19	Identifying what I know and what I don't know before I sit for the exam	

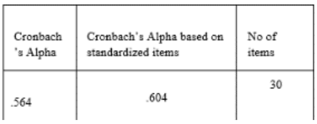


20	Predicting possible questions which could appear in the exam paper and getting ready with the answers	
	Time management	
21	Note down upcoming academic activities	
22	Maintaining a "to do" list to keep track on academic work	
23	Readying for the upcoming exams well in advanced	
24	Initiate to work on assigned assignments or projects once they assign those	
25	Having enough time for fun activities	
	Taking down notes	
26	Taking notes while I am reading text books	
27	Taking notes during lectures	
28	Rewrite the notes after the lecture	
29	Compare my lecture note with peer's notes to find out missed subject matters	
30	Organize the main ideas of the subject matters in a meaning way while writing the lecture note	

Likert scale	**Never - 0**	**Rarely- 1**	**Sometimes -2**	**Often-3**

The Academic class achieved by the students who took part in this survey, were also considered for this study after they obtained their Final Grade Point Average (FGPA). The measured studying pattern parameters were such as Reading text books, Studying, Memorizing, Preparing for exams, Time management and Taking down notes. If the score relating to any studying pattern parameter increases, the overall studying pattern also increases. The total points gathered from all studying pattern parameters is higher implies that the overall studying pattern of that particular student is high. This scale reported the high level of reliability (internal consistency) as .604. In this research, internal consistency of the scale was found as .564.

TABLE II. ERELIABI LITY STATISTICS



Cronbach 's Alpha	Cronbach's Alpha based on standardized items	No of items
.564	.604	30

Descriptive statistics method was applied at this stage in order to analyze the studying pattern of the students. Based on the responses given by the responders, the frequency levels for each question was tabulated in MS Excel worksheet. The Excel worksheet was uploaded to the IBM Statistical Package for the Social Sciences (SPSS) software and the each studying pattern parameter was evaluated.

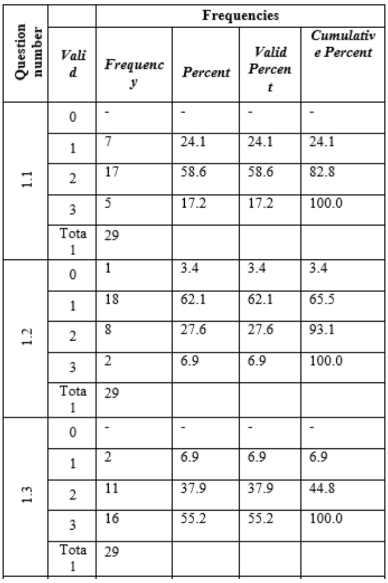
RESULTS AND DISCUSSION

The generated results for each studying pattern parameters were tabularized and analyzed as follows.

A. Responses related for Reading text book

TABLE III

READING TEXT BOOKS



Question number		**Frequencies**			
	Valid	***Frequency***	***Percent***	***Valid Percent***	***Cumulative Percent***
1.1	0	-	-	-	-
	1	7	24.1	24.1	24.1
	2	17	58.6	58.6	82.8
	3	5	17.2	17.2	100.0
	Total	29			
1.2	0	1	3.4	3.4	3.4
	1	18	62.1	62.1	65.5
	2	8	27.6	27.6	93.1
	3	2	6.9	6.9	100.0
	Total	29			
1.3	0	-	-	-	-
	1	2	6.9	6.9	6.9
	2	11	37.9	37.9	44.8
	3	16	55.2	55.2	100.0
	Total	29			

Question number	Valid	Frequencies			
		Frequency	Percent	Valid Percent	Cumulative Percent
1.4	0	-	-	-	-
	1	3	10.3	10.3	10.3
	2	14	48.3	48.3	58.6
	3	12	41.4	41.4	100.0
	Total	29			
1.5	0	1	3.4	3.4	3.4
	1	2	6.9	6.9	10.3
	2	15	51.7	51.7	62.1
	3	11	37.9	37.9	100.0
	Total	29			

Table III, represent the frequencies related to Reading Text Books of the selected sample. Out of 29 students in the sample, there are 7 students who rarely browse the headings, pictures and also the chapter questions before start reading the chapter and there are 17 students who do it sometimes. But there are 5 students, who browse the headings, pictures and chapter questions frequently prior to read the chapter. There is a student who never makes questions from the chapter and there are 18 students who rarely make questions from the read out chapter. Out of 29 students there are 8 students who make questions from the chapter sometimes in order to understand the content of the chapter properly, while there are 2 students who make questions frequently from the read out chapters. In addition, there are 2 students who rarely find out the meaning of new words while reading, where as there are 11 students who find out the meaning of new words sometimes. But there are 16 students who frequently find out the meaning of new words that they come across during reading. There are 3 students who rarely look for similar concepts that they knew already while reading the chapters and there are 14 students who look for familiar concepts in the chapters sometimes. Out of 29 students there are 12 students who frequently look for familiar concepts while reading new chapters. Further, there is a student who never looks for main idea in the chapter but there are 2 students who look for main idea of the chapter rarely while reading. There are 15 students who look for main idea of the chapter sometimes and there are 11 students who try to grab the main frequently out of 29 students.

B. Responses related for Studying

TABLE IV

STUDYING

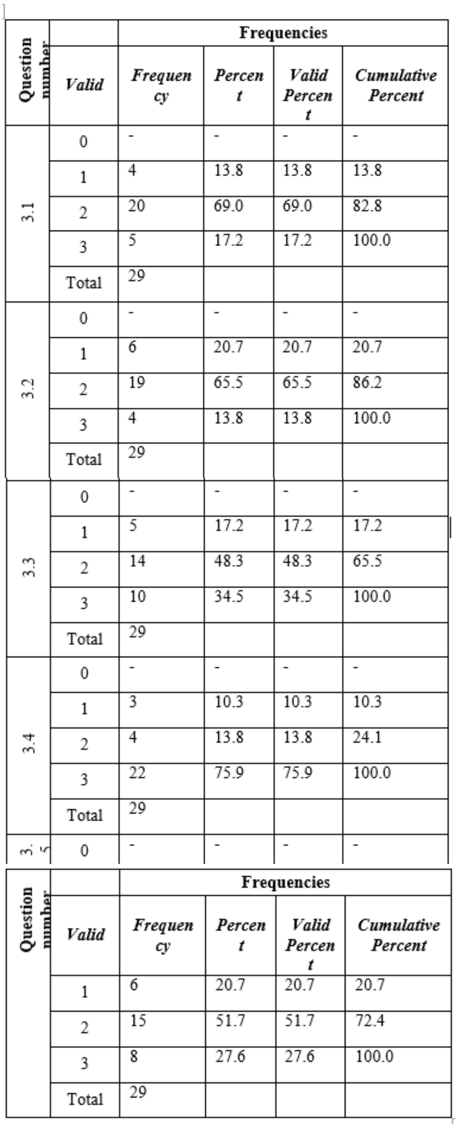
Question number	Valid	Frequencies			
		Frequency	Percent	Valid Percent	Cumulative Percent
2.1	0	1	3.4	3.4	3.4
	1	3	10.4	10.4	13.8
	2	13	44.8	44.8	58.6
	3	12	41.4	41.4	100.0
	Total	29			
2.2	0	1	3.4	3.4	3.4
	1	6	20.7	20.7	24.2
	2	9	31.0	31.0	55.2
	3	13	44.8	44.8	100.0
	Total	29			
2.3	0	1	3.4	3.4	3.4
	1	2	6.9	6.9	10.3
	2	4	13.8	13.8	24.1
	3	22	75.9	75.9	100.0
	Total	29			
2.4	0	1	3.4	3.4	3.4
	1	6	20.7	20.7	24.2
	2	17	58.6	58.6	82.8
	3	5	17.2	17.2	100.0
	Total	29			
2.5	0	1	3.4	3.4	3.4
	1	9	31.0	31.0	34.4
	2	14	48.3	48.3	82.8
	3	5	17.2	17.2	100.0
	Total	29			

As per the data given in Table IV, an out of 29 students there is a student who do not concern about the calmness of the surrounding environment during studying. But 3 students rarely concern about the distractions during studying and there are 13 students who concern about the quietness of the environment sometimes while studying, as well there are 12 students who often concern about the quietness and less distractions of the studying environment. Furthermore, there is a student who studies continuously for lengthy hours with no breaks and there are 6 students who rarely take short breaks during lengthy studying hours. There are 9 students who take short breaks sometimes during lengthy hours of studying. Out of 29 students, 13 students frequently get short breaks during lengthy hours studying. Moreover, there is a student who does not bother about having stationeries during studying and 2 students are rarely concern about having stationeries while studying and there are 4 students who sometimes concern about the having stationeries with them during studying period. In addition, there are 22 students who frequently concern about having stationeries during studying period. Further, there is a single student who never set an aim regarding no of pages to be completed or no of questions to be solved prior to start studying but there 6 students who set aims rarely regarding no of pages to be completed or no of questions to be solved. There are 17 students who set aims sometimes and also there are 5 students who often set aims for no of pages to be completed or no of questions to be completed prior to start studying. Also, there is a student who never studies at least two hours per day in addition to the regular lectures, but there are 9 students who rarely study at least two hours per day in addition to the regular lecture hours. Moreover, there are 14 students who study at least two hours per day sometimes and also there are 5 students who frequently study at least two hours per day in addition to the regular lecture series.

B. Responses related for Memorizing

TABLE V

MEMORIZING



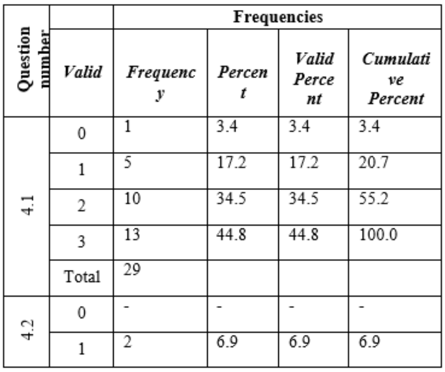
Question number	Valid	Frequencies			
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
3.1	0	-	-	-	-
	1	4	13.8	13.8	13.8
	2	20	69.0	69.0	82.8
	3	5	17.2	17.2	100.0
	Total	29			
3.2	0	-	-	-	-
	1	6	20.7	20.7	20.7
	2	19	65.5	65.5	86.2
	3	4	13.8	13.8	100.0
	Total	29			
3.3	0	-	-	-	-
	1	5	17.2	17.2	17.2
	2	14	48.3	48.3	65.5
	3	10	34.5	34.5	100.0
	Total	29			
3.4	0	-	-	-	-
	1	3	10.3	10.3	10.3
	2	4	13.8	13.8	24.1
	3	22	75.9	75.9	100.0
	Total	29			
3.5	0	-	-	-	-
	1	6	20.7	20.7	20.7
	2	15	51.7	51.7	72.4
	3	8	27.6	27.6	100.0
	Total	29			

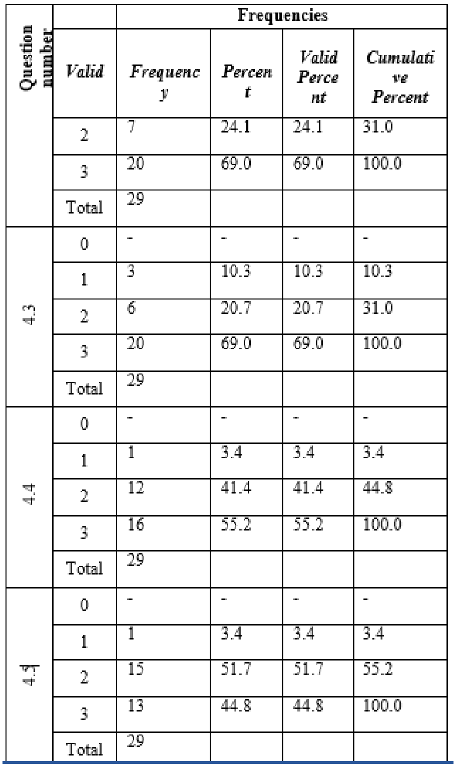
As given in Table V, there are 4 students, who rarely bother about their personal peak time of energy in order to maintain proper concentration level during studying. But there are 20 students who concern about their personal peak time of energy sometimes and try to study during that time. There are 5 students who often concern about their personal peak time of energy in order to memorize subject matters more effectively. There are 6 students who rarely quiz themselves regarding the possible subject matters which can appear in exam papers. In addition, there are 19 students who project quiz questions to themselves sometimes and the rest of 4 students who often project quiz to themselves which can appear in future exam papers. Additionally, there are 5 students who rarely out loud difficult concepts for better understanding while there are 14 students who out loud difficult concepts sometimes in order to understand them effectively. In addition, there are 10 students who frequently out loud difficult subject matters in order to understand them properly. Further, there are 3 students who use their own wordings in order to have a better lecture note while there are 4 students who use their own terminologies sometimes in their own lecture notes. But out of 29 students, 22 students use their own terminologies in their lecture notes for better understanding. Besides there are 6 students who rarely try to create an association between new subjects' matters and the subject matters they already know, while there are 15 students who try to create a link between subject matters sometimes. But there are 8 students who frequently try to create an association between new subject matters and subject matters they already know.

b Responses related for Preparing for exams

TABLE VI

PREPARING FOR EXAMS





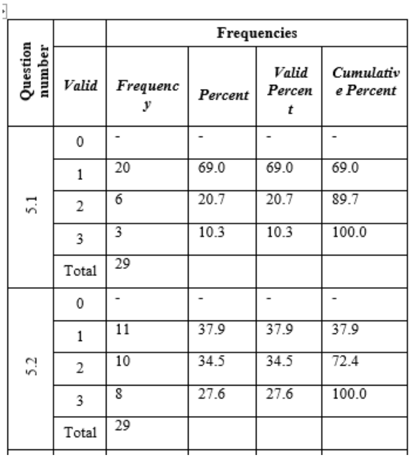
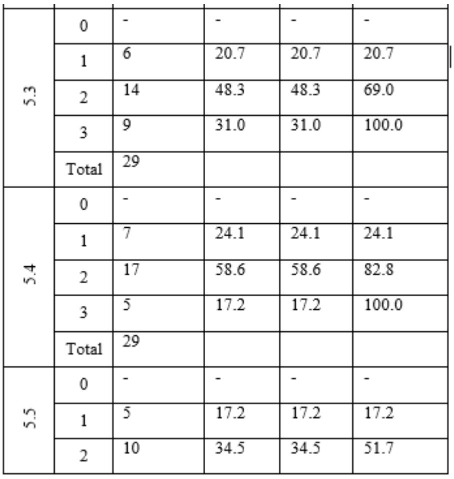
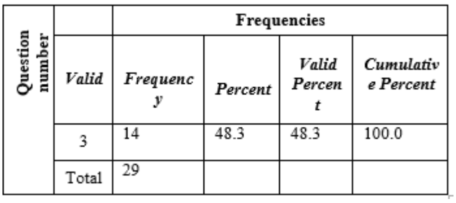
Question number	Valid	Frequencies			
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
4.1	0	1	3.4	3.4	3.4
	1	5	17.2	17.2	20.7
	2	10	34.5	34.5	55.2
	3	13	44.8	44.8	100.0
	Total	29			
4.2	0	-	-	-	-
	1	2	6.9	6.9	6.9
	2	7	24.1	24.1	31.0
	3	20	69.0	69.0	100.0
	Total	29			
4.3	0	-	-	-	-
	1	3	10.3	10.3	10.3
	2	6	20.7	20.7	31.0
	3	20	69.0	69.0	100.0
	Total	29			
4.4	0	-	-	-	-
	1	1	3.4	3.4	3.4
	2	12	41.4	41.4	44.8
	3	16	55.2	55.2	100.0
	Total	29			
4.5	0	-	-	-	-
	1	1	3.4	3.4	3.4
	2	15	51.7	51.7	55.2
	3	13	44.8	44.8	100.0
	Total	29			

As according to Table VI, there is a student who does only self-studies and there are 5 students who rarely study as a group with peers. Moreover, there are 10 students who study in a group sometimes and the rest 13 students study in a group frequently with peers. There are 2 students who rarely get the assistance from either lecturers or friends to clarify difficult subject matters while 7 students are sometimes get the help from lectures or friends to clarify unclear subject matters and the rest 20 students are frequently get the help from lectures or friends to understand subject matters more. Besides, there are 3 students who rarely complete the assignment on time while there are 6 students who complete their assignment sometimes on time. But out of 29 students, there are 20 students who complete their assignments on time. Further, there is a student who never concern about what knows and what does not know in subject matters before taking the exam. But there are 12 students who concern about what knows and what do not know in subject matters sometimes prior to the exam and the rest 16 students are frequently concern about what knows and what do not know before they take the exam. In addition, there is a student who rarely anticipates the possible questions which could appear in the question paper and prepare with the answers while there are 15 students who anticipate the probable questions in exam paper sometimes and prepare with the answers. The rest 13 students are frequently anticipating the possible questions which could appear in the exam paper and get ready with the answers.

B Responses related for Time management

TABLE VI I

TIME MANAGEMENT

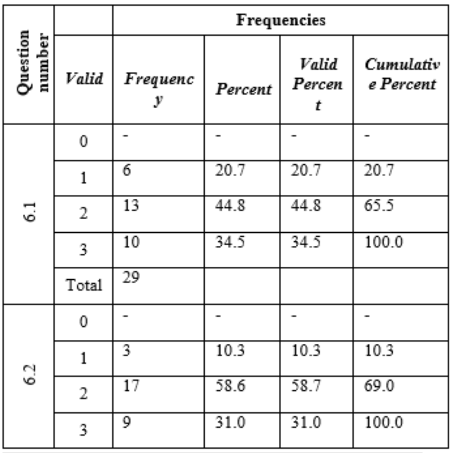
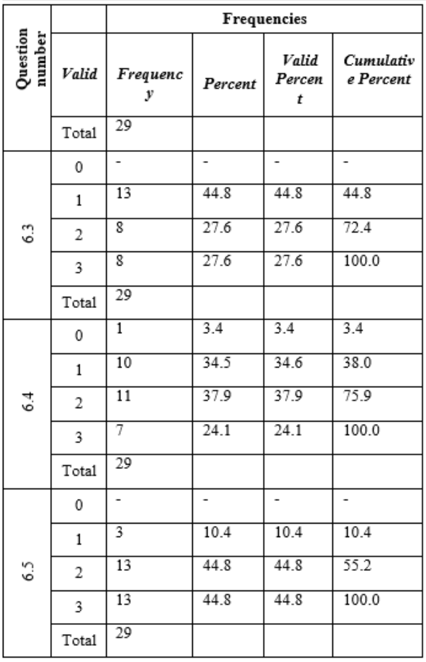
Question number		Frequencies			
	Valid	*Frequency*	*Percent*	*Valid Percent*	*Cumulative Percent*
5.1	0	-	-	-	-
	1	20	69.0	69.0	69.0
	2	6	20.7	20.7	89.7
	3	3	10.3	10.3	100.0
	Total	29			
5.2	0	-	-	-	-
	1	11	37.9	37.9	37.9
	2	10	34.5	34.5	72.4
	3	8	27.6	27.6	100.0
	Total	29			
5.3	0	-	-	-	-
	1	6	20.7	20.7	20.7
	2	14	48.3	48.3	69.0
	3	9	31.0	31.0	100.0
	Total	29			
5.4	0	-	-	-	-
	1	7	24.1	24.1	24.1
	2	17	58.6	58.6	82.8
	3	5	17.2	17.2	100.0
	Total	29			
5.5	0	-	-	-	-
	1	5	17.2	17.2	17.2
	2	10	34.5	34.5	51.7
	3	14	48.3	48.3	100.0
	Total	29			

As according to Table VII, there are 20 students who rarely note down upcoming academic activities while there are 6 students who note down the upcoming academic activities sometimes. In addition, there are 3 students who often write down upcoming academic activities. There are 11 students who rarely maintain a “to do” list to keep track on academic work, while there are 10 students sometimes use a “to do” list to keep tracks on those. There are 8 students who frequently use a “to do” list in order to keep record on academic work. Furthermore, there are 6 students who rarely start studying for the upcoming tests in well in advanced, while there are 14 students who start studying for upcoming tests sometimes in well in advanced. Out of 29 students only 9 students frequently get ready for the upcoming tests in advanced. There are 7 students who rarely start assignments or projects once they have assigned while there are 17 students who sometimes start assignments or projects just after they have assigned those. Besides, there are 5 students who often start the assignments or projects once they assigned those. Furthermore, 5 students responded that they rarely get time for fun while another 10 students sometimes get time for fun. But there are 14 students who get time for fun frequently.

B Responses related for Taking down notes

TABLE VI II

TAKING DOWN NOTES

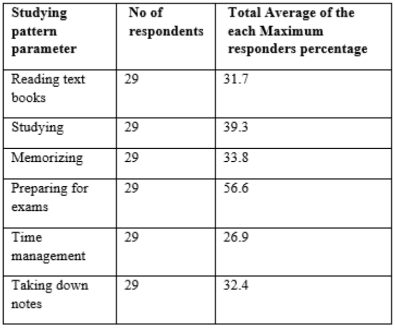
Question number	Valid	Frequencies Frequency	Percent	Valid Percent	Cumulative Percent
6.1	0	-	-	-	-
	1	6	20.7	20.7	20.7
	2	13	44.8	44.8	65.5
	3	10	34.5	34.5	100.0
	Total	29			
6.2	0	-	-	-	-
	1	3	10.3	10.3	10.3
	2	17	58.6	58.7	69.0
	3	9	31.0	31.0	100.0
	Total	29			
6.3	0	-	-	-	-
	1	13	44.8	44.8	44.8
	2	8	27.6	27.6	72.4
	3	8	27.6	27.6	100.0
	Total	29			
6.4	0	1	3.4	3.4	3.4
	1	10	34.5	34.6	38.0
	2	11	37.9	37.9	75.9
	3	7	24.1	24.1	100.0
	Total	29			
6.5	0	-	-	-	-
	1	3	10.4	10.4	10.4
	2	13	44.8	44.8	55.2
	3	13	44.8	44.8	100.0
	Total	29			

As given in Table VIII, there are 6 students who rarely taking down notes while they are reading text books and 13 students responded that sometimes they are taking down notes while reading the text books. Out of 29 students, 10 students responded that they use to taking down notes frequently, when they read text books. In addition, there are 3 students who rarely taking notes during lectures and there are 17 students who use to taking down notes at the lecture. But there are 9 students who frequently write down notes when they are in the lecture. Moreover, there are 13 students who rarely rewrite their notes after the lecture and there are 8 students in each category where they rewrite their lecture notes sometimes and more often. Besides, there is a student who never compares the lecture notes with peer's notes to find out missed subject matters, while there are 10 students who do so rarely. But there are 11 students who compare their lecture notes with peers sometimes and there are 7 students who compare their lecture notes with peers more often in order to have a complete lecture note. Furthermore, there are 3 students who rarely organize the main ideas of the subject matters in a meaning way while writing the lecture note. But there are 13 students in each category where they organize the main ideas of the subject matters in a meaning way while writing the lecture note sometimes and more frequently.

B. Responses related for achieved Academic Class

TABLE IX

TOTAL AVERAGE OF THE EACH MAXIMUM RESPONDERS PERCENTAGE FOR EACH TESTED STUDYING PATTERN PARAMETER



Studying pattern parameter	No of respondents	Total Average of the each Maximum responders percentage
Reading text books	29	31.7
Studying	29	39.3
Memorizing	29	33.8
Preparing for exams	29	56.6
Time management	29	26.9
Taking down notes	29	32.4

As according to the Table IX, only 31.7 % of the responders practices Reading text books and only 39.3 % practice effective studying methods. Besides, only 33.8 % of the respondents use effective memorizing techniques while only 56.6 % prepare for exams in an effective way. Proper time management techniques practice by 26.9 % from the studied group and only 32.4 % of students taking down notes in effective manner.

C. Responses related for achieved Academic Class

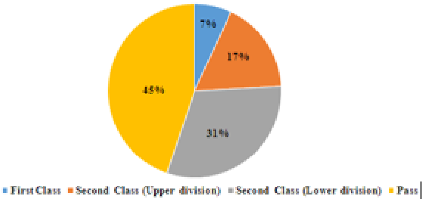


Fig. 1.Academic Class achieved by the responders

As shown in Fig.1, from the studied group of students only 7 % could obtained First Class and only 17 % of students could obatined Second Class (Upper division) as their academic achievements. Further, 31 % of the students from this sample could achieved Second Class (Lower division) while the rest 45 % of students could achieved Pass as their academic performances.

CONCLUSIONS

Based on the results of this study, it is clear that only 31.7 % from the studied group had followed most effective studying pattern in Reading text books while only 39.3 % from the studied group followed most effective study pattern for Studying. Out of the whole population, only 33.8 % were used proper memorizing methods and only 56.6 % of students followed most effective methods when it comes for preparing for exams. But from the studied group only 7 % could achieved First Class while another 17 % could achieved Second Class (Upper division). The most effective time management techniques were followed only by 26.9 % of the students and only 32.4 % were effectively take down notes. Hence, 31 % from the studied group could obtained Second Class (Lower division). The studied group of students were practicing ineffective studying patterns which led them to obtained lower grades. Hence, the majority of the students could obtain Pass grade as their final academic achievement. The poor academic performances of the students coincide due to practicing of ineffective studying patterns. Hence, it is important to encourage students to practice most effective studying pattern in order to obtain highest academic performances.

Acknowledgment

The authors would like to thank for all the undergraduate students who took part in this survey and spending their time and experiences with us to carry out this study successfully.

REFERENCES

Zhou, Y. Graham, L and West, C. (2016) "The relationship between study strategies and academic performance," J. Medical Education, vol. 7, pp. 324-332.

Bulent, A. Hakan, K. and Aydin, B. (2015) "An analysis of undergraduates' study skills," J. Procedia-Social and Behavioral Sciences, vol. 197, pp. 1355-1362.

Kucukahmet, L. (2000) Planning and evaluation in teaching, 11th ed., Ankara: Nobel Publications.

Aquino, L. B. (2011) "Study habits and attitudes of freshmen students: Implications for academic intervention programs," J. Language Teaching and Research, vol. 2, pp. 1116-1121.

Yu, D. D. (2011) "How much do study habits, skills and attitudes affect student performance in introductory college *accounting courses?," J. New Horizons in Education, vol. 59, pp. 1-15.*

Dodge, J. (1994) The study skills handbook: More than 75 strategies for better learning. New York: Scholastic Inc.

Yıldırım, I. (2000) "Loneliness, test anxiety and social support as predictors of academic success," J. Hacettepe, University Faculty of Education, vol. 18, pp. 167-176.

Kartika, A. (2007) "Study skills training: Is It an Answer to the Lack of College Students' Study Skills?," J. Learning, vol. 14, pp. 35-43.

Alay S. and Kocak, S. (2003) "The relationship between time management and academic achievement of university students," J. Theory and Practice in Education, vol. 35, pp. 326-335.

Koruklu, N. O. (2010) Educational guidance. Psychological counseling and guidance (Edt: M. Guven). Ankara: Anı Publishing, pp. 87-130.

Jones, C. H. Green, A. E. Mahan K. D. and Slate, J. R. (1993) "College Students' Learning Styles, Academic Achievement, and Study Behaviors," J. Louisiana Education Research, vol. 19, pp. 40-48.

“PRO-EYE” - A VIRTUAL ASSISTANT TO FACILITATE VISUALLY IMPAIRED INDIVIDUAL

Yogalingam Senthuran, Pushpakumare T.P.I.S, Amaranayake W.P.K, De Silva H.L.T., Dr. Anuradha Jayakody, Shashika Lokuliyana

Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Sri Lanka

ABSTRACT

Human senses play a crucial role in everyday life. Senses proactively let the brain knows about the environment, protects by alerting of any dangers. Out of the five senses, humans have ‘sight’ is the most dominant sense. More than 80% of what we perceive comes through our eyesight. In a fast-paced world to acquire knowledge and to survive independency has become a significant factor, but for a visually impaired person this independency is a critical question. As per studies visual loss a double the risks of depression as well as they can also develop many other mental disorders. Each day to do even routine tasks a visually impaired person needs the assistance of another person which makes the impaired person a dependent personality. Decision-making is a key factor that keeps a human’s life intact. Even though some technologies and devices are advanced enough to help vision-impaired they are either not affordable by most or complex in interaction. The proposed system compromises state-of-the-art technologies at low cost to aid visually impaired personalities in outdoor navigation, image recognition, text recognition using human alike conversations, providing effortless interactions. This improves the visual perception and the awareness of an ambiguous environment. This system analyzes the data and categorizes it into sections using Machine learning and Artificial Intelligence technologies to provide clear guidance to the user. The Proposed System includes a text recognition system which classifies text, tables, and graph in the material separately, and convert them to “life like speech” format, which can help visually impaired persons to read printed materials that are not available in braille format. Furthermore, the proposed solution provides outdoor navigation functionality for the visually impaired which integrates with the global navigation system to guide the user to a particular designation and avoiding static obstacles in the path. The proposed solution computes the optimized routes based on user preference, temporal constraints such as traffic congestion, road closings using real-time processing. The system constantly guides the blind user to navigate based on static and dynamic data. Users can interact using voice and the Assistant will be able to understand it using natural language processing.

Keywords: Virtual Assistant, Object Recognition, Intelligent Character Recognition, Natural Language Processing, Inference Engine, Expert System.

INTRODUCTION

Blindness, the most extreme type of visual disability, can diminish individuals' capacity to perform day-by-day tasks, and move about independently. Great quality restoration permits individuals with various degrees of visual impairment to completely benefit from life, accomplish their objectives to be active and productive in the present society.

An Artificially Intelligent assistant will be the core of the Pro-Eye which bridges the gap between the user and the other provided services such as navigation, environment identification (Image identification, Object tracking), and text recognition (Symbols, Charts). The assistant will proactively interact with the user and will guide him as well as help him by understanding his/her requirements. Users can interact using voice and the Assistant will be able to understand it using natural language processing. Pro-Eye acts like a human-like guider when the user steps to the outside environment. Navigational Functionality is a combination of two sub functionalities, which guide the user globally with geographical routes and guide the user to walk in the path considering physical temporal data. The proposed system is also capable of tracking obstacles in the walking lane and providing a user with navigational rules to avoid obstacles by understanding user requirements.

LITERATURE REVIEW

A key problem in the current developed assistive technologies in the market does not provide centralized control to perceive various functionalities of the system and most developed technologies provide only limited capabilities such as text reading. Implications of a survey done under “Needs of Visually Impaired Users and Requirements for a Virtual Assistant in Ambient Assisted Living” [1] states that for a visual impaired to study he would at least require Audiobooks or Braille Books, talking newspapers, and other assistive technologies to facilitate their education, this also implies the impaired person will also require helpers to provide help to utilize these tools available to them which are not efficient.

An electronic travel aid was introduced to provide enhanced navigational functionalities over the traditional white cane. This electronic travel aid is based on a set of sensors to provide the capabilities. An ultrasonic sensor for discovering obstacles, limiting detection range is achieved by coupling a gyro sensor and inclinometer, and to identify the color of the obstacles a color is used. When an obstacle is detected a vibrator is used to inform the user [2]. “The Guide Cane – Applying Mobile Robot Technologies to Assist the Visually Impaired” [3] elaborates about a device designed to help the visually impaired navigate locally using ultrasonic sensors. Even though the local navigation is provided by the proposed solution the user is unable to get a brief idea about the surroundings. The paper also suggests that there is a requirement to use computer vision to assist the user in ways that a traditional sensor-based navigation assistive technology unable to cater. Visual Pal a mobile device that provides object recognition functionalities via a hybrid algorithm combining both Artificial neural networks and Euclidean distance measures. The hybrid use of algorithms provides more accuracy and the colors are classified according to brightness and robustness [4]. This paper suggests providing a touch-free interaction to users for future improvements.

METHODOLOGY

Smartphone adaption now is immense, this also can be seen common among the visually impaired as well. The major reasons for the adaption are accessibility and mobility.

In Pro-Eye, we propose a system that provides key assistive functionalities to the visual impaired to carry out their day-to-day activities. An application specifically designed as an assistive technology running based on a smartphone regardless of the hardware can be very beneficial and reachable to the visual impaired.

Images are automatically taken by the application itself periodically to identify the environment and pro-actively assist the user. Taken images are pre-processed to make sure its in minimal resolution and processed in decouple manner to recognize objects and text parallel to increase efficiency and response time. The visual impaired can directly interact with the application via voice and get the required assistance which is outdoor navigation, object recognition, and text reading the application assists with voice communication as well. As Fig. 1 illustrates the system compromises decoupled modules provide the functionalities without stressing the whole system.

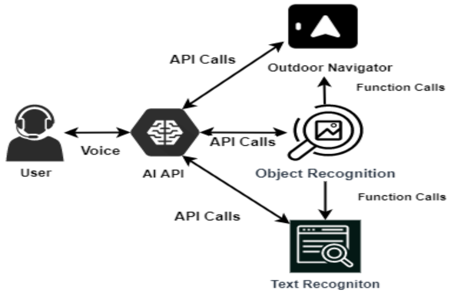


Figure 1: Logical View of the System

I.User interaction using NLP

The approach of handling the user interaction is one of the core concerns since when a vision-impaired user progressively uses any assistive technology its preferable to have a human-like companion which can bring randomness into responses as well as understanding random user queries rather than having a set of rules which predicates the user to remember the questions or patterns that can be requested from the assistant.

The system uses no SQL database to store user details and uses Redis cache to improve performance. When the mobile application is invoked by the user a docker container will be triggered by a lambda function that will serve the requests. The goal is to identify the question or the query of the user into subcategories on which the assistant can provide services. Spacy and open-source library for advanced natural language processing is optimized to classify the queries as specified above [5]. Using convolutional neural networks on named entity recognition to identify and classify the class of the query.

Pro-eye is trained on sentence based NER and entity label representation as follows,

Table 1: NER Entity Labels of Pro-Eye

Entity Label	Query Objective
NVG	Assist on navigation
TXT	Assist on Reading
OBJ	Assistant on recognition

In addition to the above mentions, entity labels pro-eye also include other labels which are based on the model English multi-task CNN trained on Onto Notes [6] the pre-trained model that is trained to understand the above entities.

Pro-eye uses the efficient implementation of word embedding strategy using subword features and Bloom embeddings, where the named entity parsing is handled through a deep convolutional neural network with persisting interrelation. Being trained on a new entity label the model will initially predict the unlabeled text and since we know the correct answer the feedback of the prediction made by the model can be given in the form of error gradient of the loss function which is a contrasting prediction expected value and output. The NER is trained with a hinge-loss objective which is used for the identification of loss function [7].

The application uses the trained model in the live scenario when a query comes in to classify, done by predicting the text by converting it into a spacy type of document. These entities are objectified as ents in the document type of the space. Once the query is classified it uses the parts of speech tagging to identify the object the user requires from the assistant to achieve for example if the user has questioned the assistant as “How can I go to library?” the NER model identification will identify as “NVG” which represents navigation which is the objective hence the object will be library to identify the object POS tagging [8] is used. Tokenization the process of chopping a unit of the document into pieces which are called tokens. The tokens are a set of series of characters that can be used in semantic processing. Once the tokenization of the document is completed pro-eye uses spacy to parse and tag a provided document in this case a query. The parsed document of the “How can I go to library?” query is shown in Fig. 2.

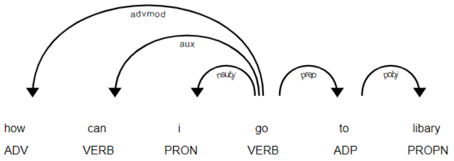


Figure 2: Semantic Relations in a sentence

Using the Parts of speech tagging the actual meaning of the text can be understood and the object the user trying to achieve can marked as library hence the final output of natural language processing component of the pro-eye will be both action and the object in the format of action as NVG and object as library.

After the action and object identification is completed pro-eye will use the artificial linguistic internet computer entity to generate random responses for the user while triggering the assistive service, in this case the navigation service.

II. Object Detection and Color Detection

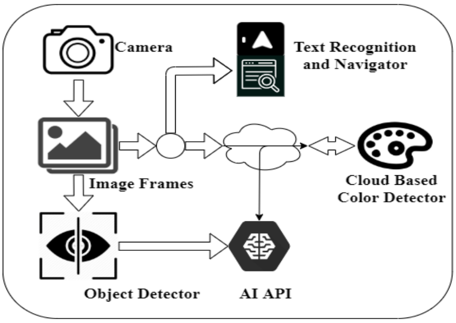


Figure 3: System Diagram of Camera and Object detection

As illustrated in Fig. 3. this function has several steps. AI API interacts with the user and provides the relevant instruction to the other components. To access the camera and take the image frames, CameraX API has been used [9]. Since the users are visually impaired It does not have a preview layout. All the functions have been automated due to these special users. When image frames are saved in the storage, those are converted into bitmap objects to work on object detection. Object detection has been built on the device. TensorFlow Lite interpreter has been applied to work on object detectors because it helps developers run TensorFlow models on mobile, embedded, and IoT devices and It enables on-device machine learning inference with low latency and small binary size [10]. A model for object detection is trained to detect the presence and location of various groups of objects

III. Outdoor Navigation

Walking securely in the outside environment is one of the main needs for visual impairers. The proposed method for outdoor navigation in Pro-Eye includes mainly three stages: supply user with directions from user location to the destination [11], identify two edges in the walking lane to navigate user inside the lane, generate navigation rules for the user to help the user avoid collisions [12].

Directions are supplied to the user using Google Directions API. And the lane line edge detection functionality has been mainly implemented using three steps.

1. Find and define the ROI (Region of Interest)
2. Image masking
3. Apply Hough Line Transform technique

Pro-Eye uses Hough Line Transform Algorithm to identify the final output or the straight lines which are road edges. The Hough Transform is an algorithm that was initially implemented to perceive complex lines in photos. To improve the accuracy in this lane edge detection functionality, Pro-Eye has used background subtraction and filtering.

The system uses CLIPS ide to develop the expert system for the navigation rule generation purpose. An expert system is a computer system that emulates the decision-making ability of a human expert [13]. The overview diagram of the expert system is illustrated in Fig. 4.

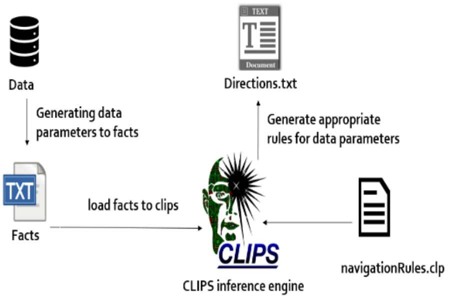


Figure 4: Overview of generating navigational rules

The data parameters use in Pro-Eye inference engine is presented in Table II.

Table 2: Description of the data parameters

Parameter Name	Description
FrameNo - A	Number of the video frame of the relevant video stream
StreetWidth - B	Starting width of the lane in the relevant frame
EndWidth - C	Ending width of the lane in the relevant frame
ObjectWidth - D	Width of the object
ObjectHeight - E	Height of the object
ObjectDepthFromBeginning - F	Object depth from the beginning of the lane
ObjectToLeftBoarder - G	Length to the left edge of the lane from the object
ObjectToRightBoarder - H	Length to the right edge of the lane from the object
FramePoint - I	Depth to the frame pointer from the beginning of the frame (normally, frame point is in ½ of lane width and ¼ of lane height)

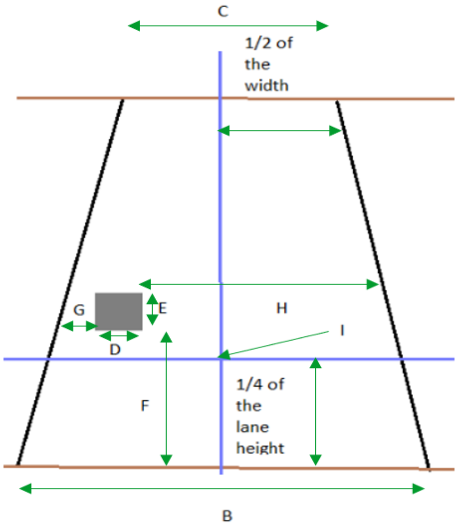


Figure 5: Data parameters preview

As illustrated in Fig. 5. the data parameters are taken by the system.

CLIPS ide can represent data using rules and facts formats. Therefore, the application transforms these data parameters to the facts format. Pro-Eye has stored navigational rules inside CLIPS ide working memory and the relevant rule will be triggered according to the variations of facts or the data parameters.

Finally, the inference engine creates an extra slot in facts which is the output that is used to navigate the blind person. Rules have been implemented in a manner to guide the user in situations encountered by a person while moving in an outdoor walking lane, and the actions that a person has to take to avoid walking away from road edges as well as to avoid collisions with obstacles. Each example rule consisting input elements such as the distances of the obstacles to left, to right, and in front of the person and the output element giving the change in the walking direction of the person being required in response to the input data. The first rule in the inference engine has been built so, if the length to object from the beginning is greater than 1m and the frame point is near to the left border, which is less than 0.5m, a rule will be created as a guide to the right. This is just a basic rule.

IV. Text Detection and Graph Reading

When the user requests a material to be read using voice the AI API framework will invoke the test recognition functionality which uses the outputs of the object recognition to recognize text. The pro-processed image frames will be taken as the input to the trained models in the application which will be then processed. It will give the text and description of the image in JSON format. The text-to-speech (TTS) system will convert the text in digital format to an audio format which the user will be able to listen to using headphones. The text reading system is implemented under two major categories.

- Text and symbols recognition.
- Graph reading.

Since the real-life, text is more sophisticated, the system uses an ML kit on java which uses a detection feature on TensorFlow conventional ML approach. To help the computer understand and match the character, a detection feature needs to be introduced. The detection feature runs through neural networks of inferences hence, detection feature or intelligent character recognition (ICR) is used to identify characters' traits [14]. It searches for letters that meet the specified requirements.

For example: If the system recognizes a longer vertical line meeting a shorter horizontal line at a right angle, that is the letter "L". These angles and lines are recognized as mentioned above.

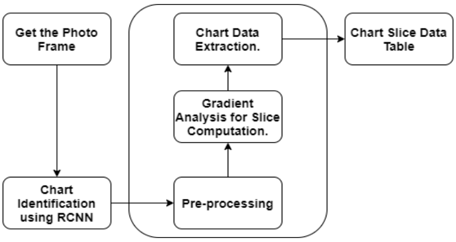


Figure 6: Graph reading system

Fig. 6. illustrates the steps carried out in detecting charts in the frame, if the diagram picture containing the border of the pie chart and specific borders of various neighboring slices is acquired, the next step is to classify each pie chart slice [15]. For that, invert the image. Then all the slices of the pie chart get separated. But the method of inversion added another dimension that exists outside the boundary of the pie chart and always touches the boundary of the image [16]. For automatic data extraction from a pie chart, boundary touching components should be removed. Therefore, Connected Component Analysis (CCA) is used to recognize the boundaries of the pie chart [17]. CCA removes the boundaries and contains only the chart slices as illustrated in Fig. 7.

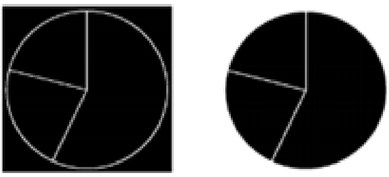


Figure 7: CCN converted chart.

For data extraction, CCN carries out the total number of pixels in all the slices. And CCN provides the number of pixels in each slice.

Let us assume,

Total number of pixels in the pie chart = X

Number of pixels in a slice = Y

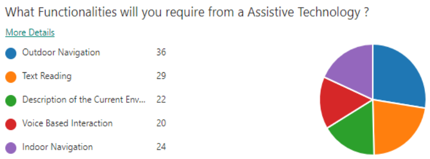
Therefore, we can compute the percentage of the slice as:

$$\text{Percentage of the slice} = Y/X \times 100\ \% \qquad (1)$$

Using the above algorithm, this system will be able to fetch the percentages of slices when providing a photo of a pie chart. After fetching data from the pie chart, the data packets will send to the cluster as illustrated in Fig. 8.

Research discussion and results

A survey was carried out among 44 visually impaired personalities to measure the usage and effectiveness of an Assistive Technology.



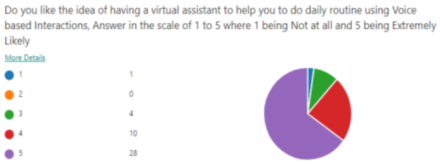
What Functionalities will you require from a Assistive Technology ?

More Details

● Outdoor Navigation	36
● Text Reading	29
● Description of the Current Env...	22
● Voice Based Interaction	20
● Indoor Navigation	24

Figure 8: Survey Result 1

Fig. 8, Shows that almost 50% of the response included all the functionalities provided by the proposed system.



Do you like the idea of having a virtual assistant to help you to do daily routine using Voice based Interactions, Answer in the scale of 1 to 5 where 1 being Not at all and 5 being Extremely Likely

More Details

● 1	1
● 2	0
● 3	4
● 4	10
● 5	28

Figure 9: Survey Result 2

Fig. 9 illustrates that most of the participants are extremely likely to use a voice-based virtual assistant to help to do daily routines.

Results of the Outdoor navigation functionality provide the directions to the destination from the user's current location from the JSON format and Identified edges of the lane. Which is converted to voice and conveyed to the user in a human-understandable format.

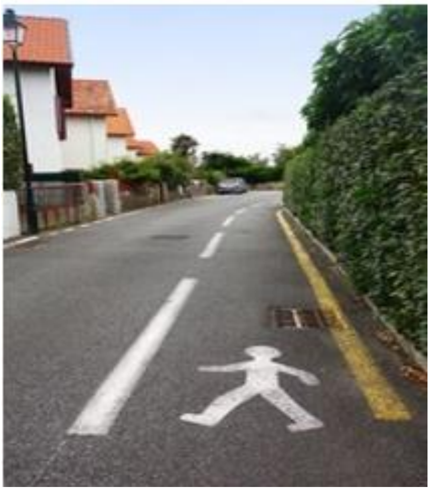


Figure 10: Input frame

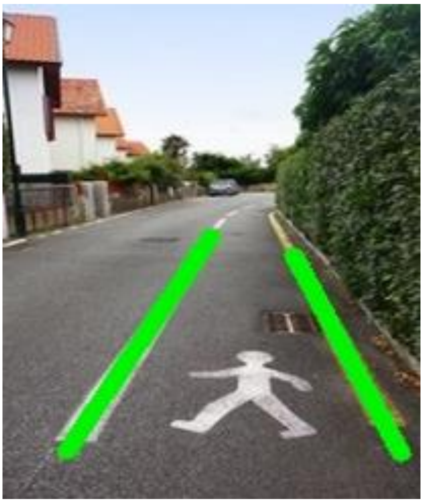
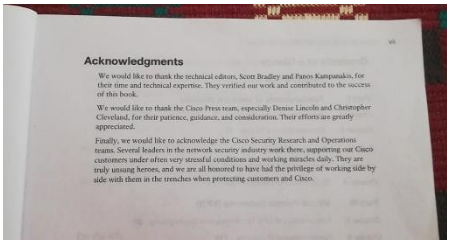


Figure 11: Output frame

As illustrated in Fig. 10. and Fig. 11. the input frames and the output frame after the application identified the lane edges. When the user is 0.5m near to a lane edge, the application generates a beep sound, so the user knows he is near to the lane edge. And then all the data parameters used in the training phase to generate navigation rules must be received to the application in real-time to generate rules using the inference engine. To that, coordinates of the obstacles and the road must be tracked using sensors. The more accurate the coordinates are, the more trustworthy rules become. That is the major limitation of the outdoor navigation functionality.



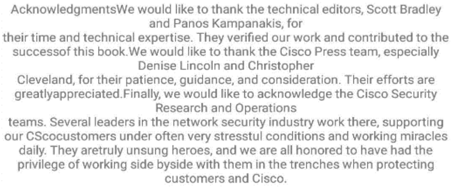
Acknowledgments

We would like to thank the technical editors, Scott Bradley and Panos Kampanakis, for their time and technical expertise. They verified our work and contributed to the success of this book.

We would like to thank the Cisco Press team, especially Denise Lincoln and Christopher Cleveland, for their patience, guidance, and consideration. Their efforts are greatly appreciated.

Finally, we would like to acknowledge the Cisco Security Research and Operations teams. Several leaders in the network security industry work there, supporting our Cisco customers under often very stressful conditions and working miracles daily. They are truly unsung heroes, and we are all honored to have had the privilege of working side by side with them in the trenches when protecting customers and Cisco.

Figure 12: Text in a Tangible Material



```
AcknowledgmentsWe would like to thank the technical editors, Scott Bradley
and Panos Kampanakis, for
their time and technical expertise. They verified our work and contributed to the
successof this book.We would like to thank the Cisco Press team, especially
Denise Lincoln and Christopher
Cleveland, for their patience, guidance, and consideration. Their efforts are
greatlyappreciated.Finally, we would like to acknowledge the Cisco Security
Research and Operations
teams. Several leaders in the network security industry work there, supporting
our CScocustomers under often very stresstul conditions and working miracles
daily. They aretruly unsung heroes, and we are all honored to have had the
privilege of working side byside with them in the trenches when protecting
customers and Cisco.
```

Figure 13: Text Recognized by the system

The system was able to recognize the text on a printed material shown in Fig. 11 using ICR and the output produced is illustrated in Fig. 13. Furthermore, the accuracy of the recognized text was evaluated by providing 50 text materials with different levels of font sizes and calculated the word-level accuracy.

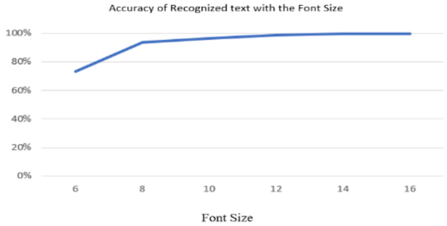


Figure 14: Accuracy of text recognition on various font sizes

As shown in Fig. 14. the result proved the trend accuracy of the system increases exponentially when the font size is above 8.

Table 3 shows a feature comparison between GuideCane [3], VisualPal [4], DAVID [18], and Pro-Eye, with this comparison we can derive that the proposed system accommodates more assistance than others.

Table 3: Feature Comparison

Feature	DAVID	Guide Cane	Visual Pal	Pro-Eye
Outdoor Navigation	✗	✓	✗	✓
Text and Graph Recognition	✓	✗	✗	✓
Object Recognition	✗	✗	✓	✓
Voice Interaction	✓	✗	✓	✓

CONCLUSION

Efficient and effective decision-making comes through independence, there is a strong gravitational pull the decision will impact when the decision was made independently. The person who is always dependent on someone will tend to make decisions from the input from others which is in the case of the visually impaired is a pretty much-affecting factor. Even to take minor decisions a visually impaired personality will have hesitation, which can rank them behind a visual health person. Pro-Eye will be a Virtual Assistant which helps users to navigate, understand the environment and to read texts using a collection various component located on the device.

Acknowledgment

It is a great appreciation that we convey our gratitude to the Sri Lanka Institute of Information Technology (SLIIT) for providing us an opportunity and appropriate environment to complete this research.

REFERENCES

Mahawariya, K., 2019. A Study of Needs and Requirements of Visually Impaired Students of University of Delhi. International Journal of Information Dissemination and Technology, 9(2), p.83.

Laehyun Kim, Sehyung Park, Sooyong Lee, Sungdo Ha "An electronic traveler aid for the blind using multiple range sensors" IEICE Electronics Express Vol. 6, No. 11, pp. 794-799, 2009.

Iwan Ulrich, Johann Borenstein "The GuideCane - Applying mobile robot technologies to assist the visually impaired" IEEE Trans. on Systems, Man, and Cybernetics, Part A: Systems and Humans, Vol. 31, pp. 131-136, 2001.

Shagufta Md. Rafique Bagwan, L. J. Sankpal, 'VisualPal: A mobile app for object recognition for the visually impaired', [Online] Available: https://ieeexplore.ieee.org/document/7375665 .

Spacy.io, 'Training spaCy's Statistical Models, [Online] Available: https://spacy.io/usage/training.

Anaconda.org, 'CNN trained on OntoNote, with Glove vectors', [Online] Available: https://anaconda.org/conda-forge/spacy-model-en_core_web_lg.

Hanieh Poostchi, Massimo Piccardi, 'A multi-constraint structured hinge loss for named-entity recognition' Australasian Language Technology Association 2019, [Online] Available: https://www.aclweb.org/anthology/U19-1006.pdf.

Giuseppe Ciaburro and Prateek Joshi, Python Machine Learning Cookbook. Birmingham: Packt Publishing Ltd, 2019.

"CameraX overview | Android Developers", Android Developers, 2020. [Online]. Available: https://developer.android.com/training/camerax. [Accessed: 12- Jul-2020].

TensorFlow. 2020. Object Detection | Tensorflow Lite. [online] Available at: https://www.tensorflow.org/lite/models/object_detection/overview [Accessed 10 July 2020].

SAGE Journals. 2020. Navigation Application Programming Interface Route Fuel Saving Opportunity Assessment on Large-Scale Real-World Travel Data for Conventional Vehicles And Hybrid Electric Vehicles - Lei Zhu, Jacob R. Holden, Jeffrey D. Gonder, 2018. [online] Available at: https://journals.sagepub.com/doi/abs/10.1177/0361198118797805

Balani, Y., Narayanan, D., Parande, S., Birari, A. and Yeole, A., 2019. Drishti – A Smartphone Application for Visually Impaired. SSRN Electronic Journal.

J. Pothal and D. Parhi, "Navigation of multiple mobile robots in a highly clutter terrains using adaptive neuro-fuzzy inference system", Robotics and Autonomous Systems, vol. 72, pp. 48-

58, 2015. Available: 10.1016/j.robot.2015.04.007.

"Simple OCR implementation on Android with Google's ML Kit | TSH.io", The Software House, 2020. [Online]. Available: https://tsh.io/blog/simple-ocr-implementation-on-android-with-googles-ml-kit/. [Accessed: 17- April- 2020].

W. Huang, R. Liu, and C. L. Tan. Extraction of vectorized graphical information from scientific chart images. In Proc. of the 9th Interna-tional Conference on Document Analysis and Recognition (ICDAR'07), pp. 521–525, 2007. [Accessed: 17- June-2020].

J. Gao, Y. Zhou, and K.E. Barner. View: Visual information extraction widget for improving chart images accessibly. In Proc. of the 19th IEEE International Conference on Image Processing (ICIP'12), pp. 2865–2868, 2012. [Accessed: 17- June-2020]

"Automatic Data Extraction from 2D and 3D Pie Chart Images - IEEE Conference Publication", Ieeexplore.ieee.org, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8692104. [Accessed: 17- April-2020]

Marvin, E., 2020. Digital Assistant for The Visually Impaired - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/9065191 [Accessed 12 September 2020].

IMPLEMENTATION OF DOUBLE ENCRYPTION USING ELGAMAL AND KNAPSACK ALGORITHM ON FPGA FOR NODES IN WIRELESS SENSOR NETWORKS

[1]Leelavathi G, [2]Dr.Shaila K, [3]Dr.Venugopal K R
[1,2]VTU-Research Centre, [3]University Visvesvaraya College of Engineering, India.

ABSTRACT

The primary objective of this proposed work is to implement elliptical curve cryptography with matrix mapping techniques and knapsack algorithm for information encryption and decryption in nodes of Wireless Sensor Networks. In this paper through mapping method there is complication to guess the phrases as it does not show any regularity and knapsack algorithm avoids brute drive attack by growing confusions. The modules are integrated to perform matrix mapping, Knapsack encryption, knapsack decryption and de mapping. Verilog language is used for coding and simulation is completing on Xilinx ISE 13.4 and Spartan 6, Kintex 5 and Artix 7 FPGAs are used as the hardware. The complete crypto process is executed with frequency of 503.702MHz. No Maximum combinational path delay is found in the implementation of modules. In comparison with previous works the area utilization in this work is very less, thus satisfying the resource constraints' of wireless sensor nodes.

Keywords: Elliptic Curve Cryptography, FPGA, Knapsack Algorithm, Matrix Mapping, Wireless Sensor Networks.

INTRODUCTION

The problem of securing Wireless Sensor Networks (WSNs) has been one of the challenging research areas in the field of network security. In Embedded system market, WSNs applications have greater share with promising future. WSNs are deployed in many real-world applications, including Ambient Intelligence and Ubiquitous Computing. Owing to scarcity of energy, unsecure channel and intensive mathematical operations of asymmetric cryptographic primitives, it is difficult to realize secure WSNs. Due to these exclusive challenges, security of WSNs become a very important topic in the research area. Many mechanisms are explored to provide security for WSNs [1] [2] [3].

Security of the information is significant issue; cryptography takes an important place in exchanging of information by secure way. There have been numerous efforts to secure applications efficiently, engaging a various choice of security techniques. The resource constrained nodes are subjected to issues with, latency, power consumption, and processor usage and memory requirements. There is continuously a resource consumption trade-off exists when flexibility in the levels of security is invoked for different applications [4]- [11].

Consequently, a fundamental of effective cryptography scheme is designing system with less key size. Size of the parameter is the chief advantage over RSA, because ECC delivers high computational protection than RSA in small number of bits only.

Static and dynamic mapping are two methods in Mapping of character into points on the curve. Static mapping accomplishes, for the same x-y coordinates it maps the same characters of the different words, the points generated is also same when encrypted. With the use of trial and error process third person interpret the message in this technique. With this technique secret of message transformation is low.

The dynamic mapping performs, for the different points of curve maps the different characters. This methodology is composite for a hacker to find out which point is taken for which character. However mapping process making use of matrix process in this work ensures the security for the data. Due to the fact this process avoids the regularity within the resulting encrypted textual content. Therefore this method strengthens the cryptosystems and provides better efficiency.

Comparison of knapsack algorithm and RSA algorithm exhibits that, knapsack algorithm is improved because it is highly sophisticated and it is having high complexity. This algorithm diminishes brute force attack from a hacker by introducing confusions.

The advantages of using Reconfigurable Hardware FPGA for security algorithm implementations are Algorithm agility, Algorithm upload, Architecture efficiency, Resource efficiency, Algorithm modification, Throughput, Cost efficiency. Public Key Cryptography algorithms are the most promising schemes with respect to energy and time consumption, which makes it very suitable for data encryption in WSN. Conventional methods are measured to be too expensive for computational implementation in WSNs. To address this problem, there has been a lot of research into employing Public key infrastructures for WSNs. Given the deficiency of the resources for securing WSNs, attention was placed on the asymmetric key algorithms.

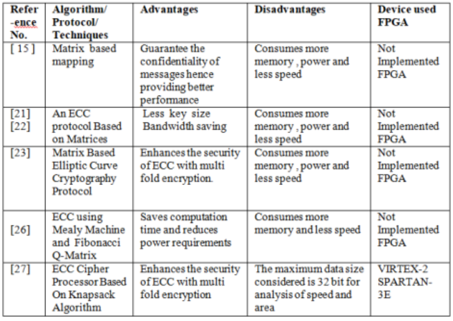
LITERATURE SURVEY

A key pre-distribution scheme for WSNs described in Shaila et al., [7]. Roy et al., [8] demonstrates appropriate scheduling for performing point addition and doubling in a pipelined data path of the ECSMA. Houssain et al., [9] delivers study of Elliptic Curve Cryptography (ECC) and hardware implementations with normal basis representation over GF (2m) in WSN. Rahuman et al., [10][11] offer Lopez-Dahab Elliptic Curve Point Multiplication algorithm. Hassan et al., [12-15] explore hardware/software co-design technique to understand a scalable Elliptic Curve Cryptography (ECC) processor.

Extreme safety of the Encrypted message is offered by a rapid mapping procedure i.e. matrix mapping. Encrypt and decrypt operation most effectively takes place on the curve but not using message in ECC. The points on elliptical curve are mapped by the character and by using Elgamal encryption algorithm perform encryption and decryption operation. Geetha et. al., [15] takes up only Elgamal encryption on FPGA.

In the finite field GF (p) alphabetic message is transformed into points on elliptical curve to perform encryption and decryption making use of knapsack algorithm. This method increases the security by avoiding the brute force attack by developing confusions to the third person [16] and the implementation is not carried out on FPGA.

Table 1.Comparison work previous works with proposed work



Refer -ence No.	Algorithm/ Protocol/ Techniques	Advantages	Disadvantages	Device used FPGA
[15]	Matrix based mapping	Guarantee the confidentiality of messages hence providing better performance	Consumes more memory , power and less speed	Not Implemented FPGA
[21] [22]	An ECC protocol Based on Matrices	Less key size Bandwidth saving	Consumes more memory , power and less speed	Not Implemented FPGA
[23]	Matrix Based Elliptic Curve Cryptography Protocol	Enhances the security of ECC with multi fold encryption.	Consumes more memory , power and less speed	Not Implemented FPGA
[26]	ECC using Mealy Machine and Fibonacci Q-Matrix	Saves computation time and reduces power requirements	Consumes more memory and less speed	Not Implemented FPGA
[27]	ECC Cipher Processor Based On Knapsack Algorithm	Enhances the security of ECC with multi fold encryption	The maximum data size considered is 32 bit for analysis of speed and area	VIRTEX-2 SPARTAN-3E

In [1] it is defined about how the ECC is better than RSA in security of the data. Relating to RSA, key enchantment of ECC is, in small number of bit also offers same level of protection, it decreases processing complexity. The point operations are appreciated in performing encryption and decryption operations [17]. Guarantee the confidentiality of the messages can be achieved by using the matrix mapping method. Strength of the cryptosystem is increased by this mapping system [18][19]. ECC in cellular Wi-Fi and other applications is an important public key cryptography [20].

PROBLEM FORMULATION

Today many of the ECC systems are prepared. All are prefer only the system that should consume less power. Many of ECC systems designed with microprocessor having there is no compatibility with the instruction set and data path of the microprocessor and the finite field of the ECC system. Our goal is to design the system that should consume less power, and minimum area and less in memory usage.

Static mapping performs, for the same x-y coordinates it maps the same characters of the different words, for these points generated is also same when encrypted. The dynamic mapping performs, for the different points of curve maps the different characters. This methodology is complex for a hacker to find out which point is taken for which character. This system avoids the regularity within the resultant encrypted message, strengthens the crypto system and offers better performance. Comparing with RSA, ECC has an advantages considering that it supplies equal degree of security even for a small key dimension. .

CONTRIBUTION

Utilization of shorter key length in ECC is highly suitable for the wireless sensor node by consuming less power, minimum area and minimum bandwidth. Because of its hardware realization and software efficiency ECC is more efficient than RSA. In this work, a matrix mapping methodology and knapsack algorithm is implemented. In matrix mapping procedure transfer of all alphabetic character into points on elliptic curve is defined. Encryption and decryption of mapping points is employed through knapsack algorithm. In this proposed work mapping method there is complicated to guess the phrases through it does no longer show any regularity and knapsack algorithm avoids brute drive attack by growing confusions. The language used to code these modules is Verilog. The modules are integrated to receive matrix mapping, Knapsack encryption, knapsack decryption and de mapping.

ELLIPTIC CURVE CRYPTOGR APHY

Elliptic Curve Cryptography (ECC) is a public-key cryptosystem that functions over points on an elliptic curve [20][21]. ECC operate directly on large integers. ECC is more efficient than other recognized public-key algorithms, due to its Elliptic Curve Discrete Logarithmic Problem (ECDLP). Equation (2) denotes to the general form of elliptic curve in Prime field GF (p). An elliptic curve group over real numbers contains the points on the equivalent elliptic curve, with O called the point at infinity.

$$4m^3+27b^2 \bmod p \neq 0 \qquad (1)$$

$$y^2=x^3+ax+b \bmod p \qquad (2)$$

Scalar point multiplication is the primary operation in ECC, in cryptographic terms, that is performed through a combination of point additions and point doublings.

Scalar point multiplication computes the Point Q(x, y):

$$Q(x, y)=k*P(x,y) \qquad (3)$$

Where a point *P(x, y),* an affine co-ordinate is multiplied by an integer k, which results in another point on the curve, *Q(x,y).* From ECDLP, given *P(x, y)* and *Q(x, y)* = k* *P(x, y)*, it is difficult to find *k*. A base point, *G(x, y)* generator point, is fixed for each curve. The random large integer, *k* acts as a private key; while multiplying *k* by the base point, *G(x, y)* results in corresponding public key. The best recognized technique for solving this problem is computationally infeasible for large values of k and the running time is completely exponential, in comparison with RSA or DSA, which have sub-exponential resolving speeds.

ECC POINT OPERATIONS

Point Inverse

If P = (x, y) Є E (Fp), then (x, y) + (x, – y) = ∞. The point (x, – y) Є E (Fp) and is called the inverse of J.

Given a point P(x1, y1) on an elliptic curve, -P(x1, y1) represents its inverse. The inverse of a given point can be computed using Equation 4.

$$-P(x1, y1)=P(x1, p- y1) \qquad (4)$$

Point Addition

The Addition operator is defined over E (Fp) and it can be seen that E (Fp) forms an abelian group under addition. The addition operation in E (Fp) is specified by Equation (5)

$$P + \infty = \infty + P = P, P Є E (Fp) \qquad (5)$$

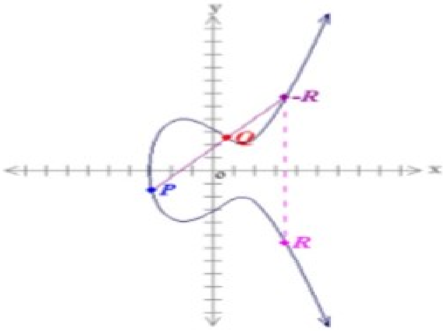


Fig 1. The addition of two points.

If P = (x1, y1) Є E (Fp) and K = (x2, y2) Є E (Fp) and P ≠ Q, then R= P + Q = (x3, y3) Є E (Fp). Given two points on an elliptic curve, P (x1, y1) and Q(x2, y2), then the addition of those points results in L(x3, y3) which lies on the same curve as shown in Figure 1. It is figured using Equation 6, Equation 7 and Equation 8 as given in [4] and [5].

$$\lambda= (y2-y1)/(x2-x1) \quad (6)$$

$$x3= \lambda^2-x1-x \quad (7)$$

$$y3= \lambda(x1-x3)-y1 \quad (8)$$

Point Doubling

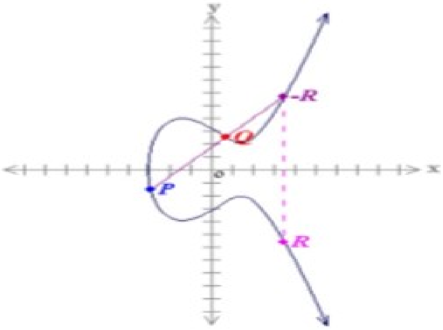


Fig.2 Doubling of a point

If P = (x1, y1) Є E (Fp), then R = 2 P = (x3, y3) Є E (Fp). Let J(x1, y1) be a point on the elliptic curve, then point doubling yields L(x3, y3) which lies on that curve as shown in Figure 2. It is computed using Equation 9, Equation 10 and Equation 11 as given in [4] and [5].

$$\lambda = (3x1^2+ a) / (2y1) \quad (9)$$

$$x3= \lambda^2-2x1 \quad (10)$$

$$y3=\lambda(x1-x3)-y1 \quad (11)$$

Scalar Multiplication

Given a point P(x1, y1) on the curve, to find k* P(x1, y1), where k is any integer, it needs repeated computations of point additions and point doublings. The reason for choosing prime fields is that distinct additive and multiplicative inverses exist for each number i.e. 0 to (P1) in the field of the prime number P.

In this proposed work, the operations point addition, point inverse, point subtraction, scalar multiplication are carried out on the points received from an elliptic curve equation (2) given in table 1.

ENCRYPTION AND DECRYP TION PROCESS

Figure 3 shows the Encryption block diagram which consists of three essential blocks, specifically point generation, matrix based mapping and knapsack encryption. While transmitting the information, both sender and receiver agree upon few conditions. Input is an undeniable text that can be converted into binary information. In that, undeniable textual content each and every letter is mapped as points on elliptical curve. This points are generatedd by using the chosen equation, this process is called as points generation. After the points are generated, in preliminary mapping points are mapped to alphabets. In matrix based mapping, storing all generated points into matrix form. Selecting one non singular matrix, multiply matrix points utilizing point addition and doubling approaches. Encyption process includes two methods i.e, ECC encryption and knapsack process. Knapsack process uses the knapsack vector to encrypt the ECC encrypted data resulting in binary representation of cipher textual content[15][16].

Figure 4 suggests the decryption block diagram. Decryption Block Diagram consists of three major blocks, namely knapsack decryption block, matrix situated de mapping block, inverse of point generation block, Encrypted cipher textual content can be decrypted through using knapsack decryption algorithm. It involves two steps one is restoration of bit pattern from the encrypted text by way of utilizing inverse knapsack method and an additional decrypted way of ECC decryption procedure. Computing an inverse of non-singular matrix, multiplying decrypted data points matrix, by making use of point addition and doubling elliptic curve generated points are obtained. Using inverse of point generation, change the points on elliptic curve to text. Then output will be the textual content [17][18][19].

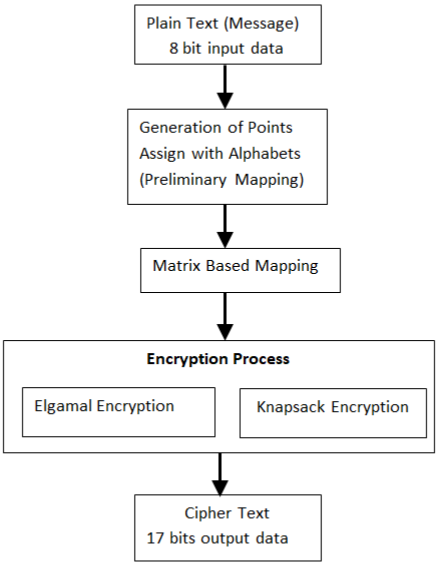


Fig 3. Flowchart of Encryption Process

At the beginning mapping and De mapping can be completed through using Matrix mapping methodology. Encryption and Decryption is applied utilizing Knapsack algorithm. Scalar multiplication is a main operation in ECC. All the modules are coded making use of Verilog language and simulation is completed on Xilinx ISE 13.2 and Spartan 6 , Kintex 5 and Artix 7 FPGA s are used as the hardware.

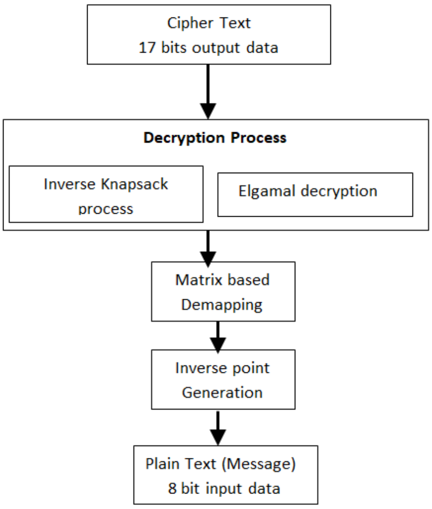


Fig 4. Flowchart of Decryption Process

ELLIPTIC CURVE POINT GEBERATION

In this proposed design the equation (2) of the elliptic curve is considered to generate the points on the curve. With this equation for simplicity, ‘a’ value is ‘1’; b value is ‘13’ and prime number p is ‘31’. All the operation takes place in the prime field and 34 points are generated. All this points are repeated after 34 points because these points are cyclic. Every generated point in a curve is having its inverse. First 26 points in a curve is considered as 26 alphabets and remaining points are considered as numbers are special characters.

In point generation module instead of ASCII value, input is text data and output is the *x* and *y* mapping points on elliptic curve. For Example *"99"* is the ASCII value of the character 'c' whose mapping points on elliptic curve is *p(23,19),* where *x=23, y=19*. This type of mapping is called preliminary mapping. This preliminary mapping output points is input to the matrix based mapping. Figure 5 is the point generation RTL schematic and Figure 6 the point generation simulation result. Generated points are shown in table 1.

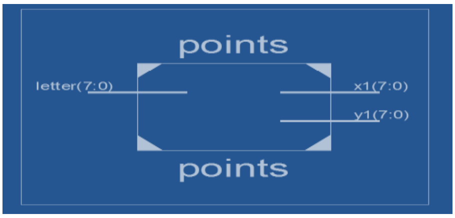


Fig 5. Generation of Points

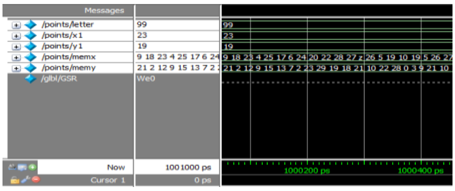
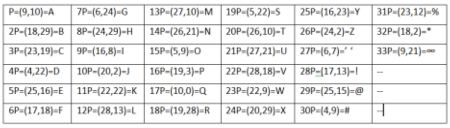


Fig 6. Timing Waveform of Elliptic Curve Points



P=(9,10)=A	7P=(6,24)=G	13P=(27,10)=M	19P=(5,22)=S	25P=(16,23)=Y	31P=(23,12)=%
2P=(18,29)=B	8P=(24,29)=H	14P=(26,21)=N	20P=(26,10)=T	26P=(24,2)=Z	32P=(18,2)=*
3P=(23,19)=C	9P=(16,8)=I	15P=(5,9)=O	21P=(27,21)=U	27P=(6,7)=' '	33P=(9,21)=∞
4P=(4,22)=D	10P=(20,2)=J	16P=(19,3)=P	22P=(28,18)=V	28P=(17,13)=!	--
5P=(25,16)=E	11P=(22,22)=K	17P=(10,0)=Q	23P=(22,9)=W	29P=(25,15)=@	--
6P=(17,18)=F	12P=(28,13)=L	18P=(19,28)=R	24P=(20,29)=X	30P=(4,9)=#	--

Table 2. Generated points of Elliptic curve

MATRIX MAPPING AND DE MAPPING METHOD

Both the sender and receiver agree upon few unique interactions between them that includes the elliptic curve equation, (*G (Fp)*) Set of elliptic curve points, (*P(x, y)*) Base (Generator) point of the elliptic curve, (*A*) Alphabets and special characters set, (*T*) Mapping points set, (*X* and X^{1}) Non-singular matrix and its Inverse with only integer values, (*k*) Private key of Receiver, (*g*) Secret key of Sender. If A (sender) wishes to transmit a message *"CRYPTOGRAPHY"* to B (receiver). The generator point *P = (9, 10),* with *a = 1*, and *b = 13*. Then, representing the above message into a stream of points as follows: *{(23, 19), (19, 28), (16, 23), (19, 3), (26, 10), (5, 9), (6, 24), (19, 28), (9, 10), (19, 3), (24, 29), (16, 23)}*.

Matrix mapping method is the conversion of generated points in to another set of points in the elliptical curve. This is nothing but multiplication of generated points and non-singular matrix.

After generating, the points, using matrix based mapping approach these points are further mapped to gain high security. The matrix mapping module has 12 inputs and 12 outputs. Inputs to these matrix mapping points are *(23,19),(19,28), (16,23), (19,3), (26,10), (5,9), (6,24),(19,28),(9,10),(19,3),(24,29),(16,23).* The output points getting from these matrix mapping module are *(22,4), (16,18), (9,4) ,(2,25) ,(15,24), (29,2) ,(12,24) , (5,27) ,(7,4) ,(0,30) ,(7,0) (8,25).*

Procedure for Matrix Mapping of Points on Curve

```
1: Convert given message into points on elliptic curve (P)
2: Form Matrix P with mapped points on elliptic curve
3: Compute Q by multiplying P with non-singular matrix (A)
4: Treat resultant values as matrix mapped points (M)
```

P=

$$\begin{bmatrix} P1 & P2 & P3 & \dots & Pw \\ Pw+1 & Pw+2 & Pw+3 & \dots & Ph \\ Ph+1 & Ph+2 & Ph+3 & \dots & Pd \end{bmatrix}$$

$$A=\begin{bmatrix} \boldsymbol{x11} & \boldsymbol{x12} & \boldsymbol{x13} \\ \boldsymbol{x21} & \boldsymbol{x22} & \boldsymbol{x23} \\ \boldsymbol{x31} & \boldsymbol{x32} & \boldsymbol{x33} \end{bmatrix} = \begin{bmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{bmatrix}$$

In step 4, the Multiplication of matrix P and matrix A is performed with addition and doubling of points. M = A*P. This results in another set of points M = [m_1,m_2…..m_n]. Figures 7, Figure 8, Figure 9 and Figure 10 shows the RTL Schematic of Implementation of point addition and doubling to perform scalar point multiplication.

The complete mapping and conversion of points are shown in table 4. The matrix de mapping method is same as the matrix mapping method. This method is performed by Multiplication of mapped data with inverse of non-singular matrix. This method retrieves the mapping inputs.

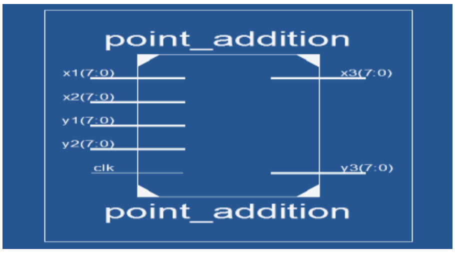
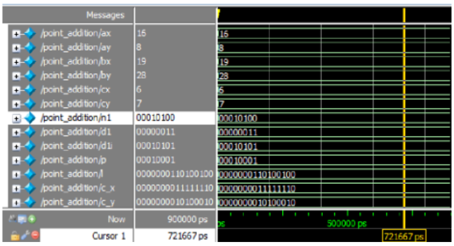


Fig.7 Point Addition



```
Messages
/point_addition/ax    16                   16
/point_addition/ay    8                    8
/point_addition/bx    19                   19
/point_addition/by    28                   28
/point_addition/cx    6                    6
/point_addition/cy    7                    7
/point_addition/n1    00010100             00010100
/point_addition/d1    00000011             00000011
/point_addition/d1i   00010101             00010101
/point_addition/p     00010001             00010001
/point_addition/l     0000000110100100     0000000110100100
/point_addition/c_x   0000000011111110     0000000011111110
/point_addition/c_y   0000000010100010     0000000010100010
Now                   900000 ps            ps    500000 ps
Cursor 1              721667 ps            721667 ps
```

Fig.8 Simulation output of Point Addition

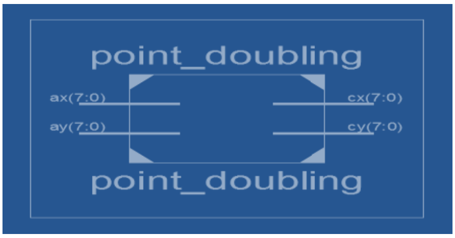
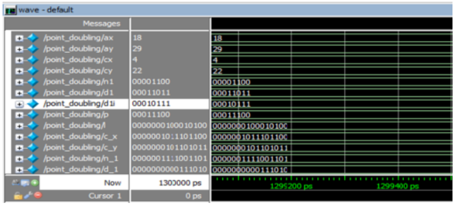


Fig 9. Point Doubling



```
wave - default
Messages
/point_doubling/ax    18                   18
/point_doubling/ay    29                   29
/point_doubling/cx    4                    4
/point_doubling/cy    22                   22
/point_doubling/n1    00001100             00001100
/point_doubling/d1    00011011             00011011
/point_doubling/d1i   00010111             00010111
/point_doubling/p     00011100             00011100
/point_doubling/l     0000000100010100     000000010001010C
/point_doubling/c_x   0000001011101100     000000101110110C
/point_doubling/c_y   0000000101101011     0000000101101011
/point_doubling/n_1   0000001111001101     0000001111001101
/point_doubling/d_1   0000000000111010     000000000011101C
Now                   1300000 ps           1295200 ps    1299400 ps
Cursor 1              0 ps
```

Fig.10 Simulation output of Point Doubling

ELGAMAL ALGORITHM

Elgamal Encryption

With sender's key g = 20 and receiver's key k = 16, the encrypted pair of points [C1, C2] are calculated as follows. To find the encrypted points for *'U'*=(25, 15) = $\boldsymbol{Q_i}$ =29*P*.

Encrypted pair of points = ***[C1, C2]*** *=>[(gP),* Q_i *+k*gP], [20P,* Q_i*+16*20P] =>* ***[20P, Qi+14P]****=> [(26, 10), Qi + (14P)]=>* ***[20P, 9P] => [(26, 10), (16, 8)]***

Elgamal Decryption

While message decrypting , receiver determines *k(gP)* from the first fragment of the encrypted couple of points, then subtract it from the second portion to acquire, $Q_i + g(kP) - k(gP) = Q_i + gkP - glP = Q_i$. By using the equation $D = (C_2 - kC_1)$ decrypted points can be discovered. To find the decrypted point for *'X'*, *i.e.,* the decrypted point is ***[D7] =>*** $\boldsymbol{(C_2\text{-}kC_1)}$ ***=> [(18P – 16(20P)] => [(18P – 14P] => 4P => (4, 22)***.

KNAPSACK ALGORITHM

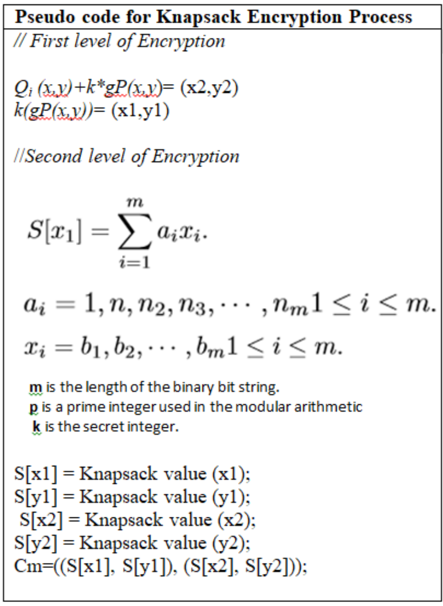
This algorithm is the most efficient algorithm for the security of the data transmission over an internet. Knapsack cryptography is an important class of public-key cryptosystems in the area of public-key cryptography. It involves no expensive modular exponentiations, which makes the encryption and decryption much more efficient than discrete logarithm based and factorization based cryptosystems. For a long time, knapsack-type cryptosystems were considered to be the most attractive and the most promising due to their high speed of encryption and decryption and NP-completeness nature. Many knapsack type cryptosystems were developed in the history of knapsack public-key cryptography especially in the 1980s, and the cryptographic applications of some variants of the knapsack problem were also investigated [16].

The **Pseudo code for** knapsack algorithm is written below.

Knapsack algorithm consisting of two steps one is ECC encryption with Elgamal algorithm and second one is knapsack process on ECC encrypted data.

Pseudo code for Knapsack Decryption Process consisting of ECC decryption with Elgamal algorithm, followed by knapsack process on ECC encrypted data is given in Table 2.

Table 2.Knapsack Encryption Process



Pseudo code for Knapsack Encryption Process

```
// First level of Encryption

$Q_i$ (x,y)+k*gP(x,y)= (x2,y2)
k(gP(x,y))= (x1,y1)

//Second level of Encryption

$S[x_1] = \sum_{i=1}^{m} a_i x_i.$

$a_i = 1, n, n_2, n_3, \cdots, n_m 1 \leq i \leq m.$
$x_i = b_1, b_2, \cdots, b_m 1 \leq i \leq m.$

m is the length of the binary bit string.
p is a prime integer used in the modular arithmetic
k is the secret integer.

S[x1] = Knapsack value (x1);
S[y1] = Knapsack value (y1);
S[x2] = Knapsack value (x2);
S[y2] = Knapsack value (y2);
Cm=((S[x1], S[y1]), (S[x2], S[y2]));
```

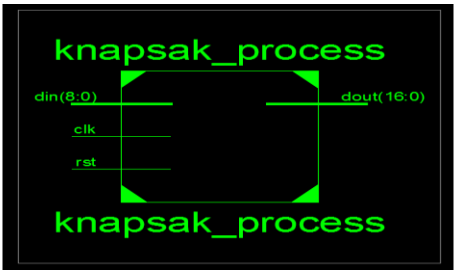
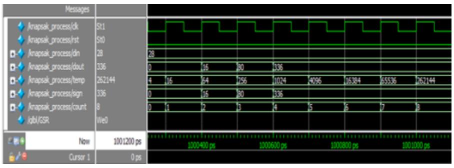


Fig.11 RTL Schematic of Knapsack Process

The plain text input to the knapsack module is 8 bit data as given in Figure 11 and Figure 12. The output is 17 bits, which is taken as input to the Inverse knapsack module as shown in Figure 11 and the process is explained in Table 3.



Messages	
/knapsak_process/clk	St1
/knapsak_process/rst	St0
/knapsak_process/din	28
/knapsak_process/dout	336
/knapsak_process/temp	262144
/knapsak_process/sign	336
/knapsak_process/count	8
/glbl/GSR	We0
Now	1001200 ps
Cursor 1	0 ps

Fig.12 Knapsack process result

Table 3.Knapsack Decryption Process

Pseudo code for Knapsack Decryption Process

// First level of Decryption with Inverse Knapsack Process
$S[x_1] - n^m.$
N[x1] – n^m, is +ve, binary bit is assigned to 1.
N[x1] - $n^m > 0$, binary bit is assigned to 1.
N[x1] - $n^m < 0$, is –ve , binary bit is assigned to 0.
x1 = Inverse Knapsack value (S[x1]);
y1 = Inverse Knapsack value (S[y1]);
x2 = Inverse Knapsack value (S[x2]);
y2 = Inverse Knapsack value (S[y2]);
// Second level of Decryption
*l*P(x,y) = (x1,y1);*
$Q_i + l*(k*P(x,y) - k*(l*P(x,y)) = (x2,y2);$

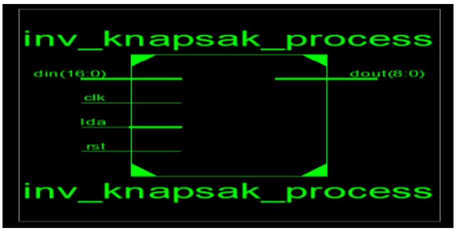
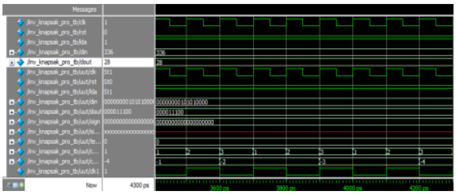


Fig.13 RTL Schematic of Inverse Knapsack Process

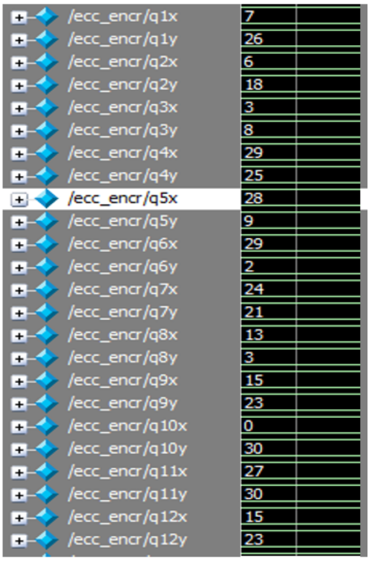
The 17 bit cipher text input to the Inverse knapsack module as given in Figure 13 and Figure 14. The output is 8 bits and the process is explained in Table 3.



Messages	
/inv_knapsak_pro_tb/clk	1
/inv_knapsak_pro_tb/rst	0
/inv_knapsak_pro_tb/lda	1
/inv_knapsak_pro_tb/din	336
/inv_knapsak_pro_tb/dout	28
/inv_knapsak_pro_tb/uut/clk	St1
/inv_knapsak_pro_tb/uut/rst	St0
/inv_knapsak_pro_tb/uut/lda	St1
/inv_knapsak_pro_tb/uut/din	00000000101010000
/inv_knapsak_pro_tb/uut/dout	000011100
/inv_knapsak_pro_tb/uut/sign	00000000000000000
/inv_knapsak_pro_tb/uut/si...	xxxxxxxxxxxxxxxxx
/inv_knapsak_pro_tb/uut/te...	0
/inv_knapsak_pro_tb/uut/c...	1
/inv_knapsak_pro_tb/uut/c...	-4
/inv_knapsak_pro_tb/uut/clk1	1
Now	4300 ps

Fig.14 The inverse knapsack process result

COMPUTATIONAL AND IMPLEMENTATION DETAILS



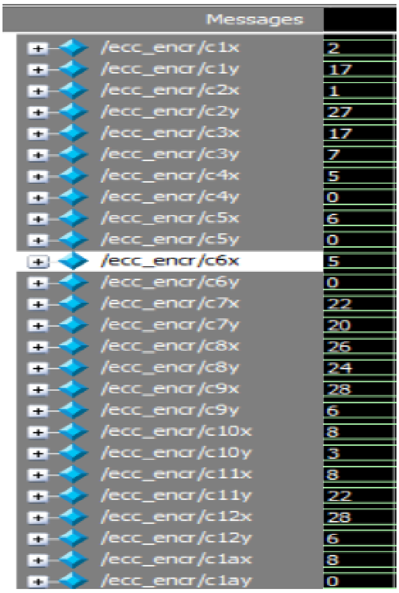
/ecc_encr/q1x	7
/ecc_encr/q1y	26
/ecc_encr/q2x	6
/ecc_encr/q2y	18
/ecc_encr/q3x	3
/ecc_encr/q3y	8
/ecc_encr/q4x	29
/ecc_encr/q4y	25
/ecc_encr/q5x	28
/ecc_encr/q5y	9
/ecc_encr/q6x	29
/ecc_encr/q6y	2
/ecc_encr/q7x	24
/ecc_encr/q7y	21
/ecc_encr/q8x	13
/ecc_encr/q8y	3
/ecc_encr/q9x	15
/ecc_encr/q9y	23
/ecc_encr/q10x	0
/ecc_encr/q10y	30
/ecc_encr/q11x	27
/ecc_encr/q11y	30
/ecc_encr/q12x	15
/ecc_encr/q12y	23

Fig 15. Elgamal Encryption inputs

The outputs shown in Figure 15 and Figure 16, consists of two co- ordinates (x1,y1) = (cax , cay) and (x2,y2) = (cx, cy). (cx,cy) has 12 outputs for 12 characters and (cax,cay) is same output for all the 12 characters. (cax, cay) = (8,0) and (cx,cy) = (2,17) ,(1,27), (17,7), (5,0), (6,0), (5,0), (22,20), (26,24), (28,6), (8,3), (8,22), (28,6).

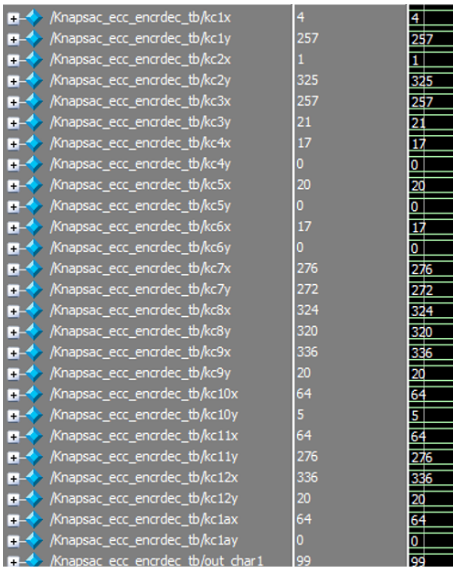
The Figure 17 and Figure 18 show the output of integrated module. It consists of point generation module, matrix based mapping module, knapsack encryption module, knapsack decryption module and matrix based de mapping, inverse point generation.

Input text is *"CRYPTOGRAHY"* that can be mapped into points on elliptical curve. Input is 8 bit encrypted data is 17 bit. *(cx, cy)* encrypted points are *(4,257) ,(1,325), (257,21), (17,0), (20,0), (17,0), (276,272) ,(324,320) ,(336,20), (64,5) ,(64,276) ,(336,20)* and *(c_{ax}, c_{ay})* points are *(64,0).*



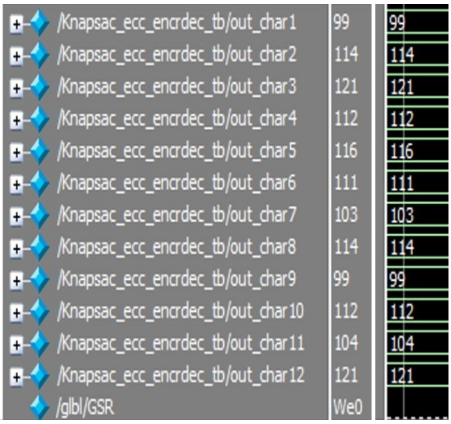
```
                Messages
/ecc_encr/c1x    2
/ecc_encr/c1y    17
/ecc_encr/c2x    1
/ecc_encr/c2y    27
/ecc_encr/c3x    17
/ecc_encr/c3y    7
/ecc_encr/c4x    5
/ecc_encr/c4y    0
/ecc_encr/c5x    6
/ecc_encr/c5y    0
/ecc_encr/c6x    5
/ecc_encr/c6y    0
/ecc_encr/c7x    22
/ecc_encr/c7y    20
/ecc_encr/c8x    26
/ecc_encr/c8y    24
/ecc_encr/c9x    28
/ecc_encr/c9y    6
/ecc_encr/c10x   8
/ecc_encr/c10y   3
/ecc_encr/c11x   8
/ecc_encr/c11y   22
/ecc_encr/c12x   28
/ecc_encr/c12y   6
/ecc_encr/c1ax   8
/ecc_encr/c1ay   0
```

Fig.16 Elgamal Encryption outputs



```
/Knapsac_ecc_encrdec_tb/kc1x        4      4
/Knapsac_ecc_encrdec_tb/kc1y        257    257
/Knapsac_ecc_encrdec_tb/kc2x        1      1
/Knapsac_ecc_encrdec_tb/kc2y        325    325
/Knapsac_ecc_encrdec_tb/kc3x        257    257
/Knapsac_ecc_encrdec_tb/kc3y        21     21
/Knapsac_ecc_encrdec_tb/kc4x        17     17
/Knapsac_ecc_encrdec_tb/kc4y        0      0
/Knapsac_ecc_encrdec_tb/kc5x        20     20
/Knapsac_ecc_encrdec_tb/kc5y        0      0
/Knapsac_ecc_encrdec_tb/kc6x        17     17
/Knapsac_ecc_encrdec_tb/kc6y        0      0
/Knapsac_ecc_encrdec_tb/kc7x        276    276
/Knapsac_ecc_encrdec_tb/kc7y        272    272
/Knapsac_ecc_encrdec_tb/kc8x        324    324
/Knapsac_ecc_encrdec_tb/kc8y        320    320
/Knapsac_ecc_encrdec_tb/kc9x        336    336
/Knapsac_ecc_encrdec_tb/kc9y        20     20
/Knapsac_ecc_encrdec_tb/kc10x       64     64
/Knapsac_ecc_encrdec_tb/kc10y       5      5
/Knapsac_ecc_encrdec_tb/kc11x       64     64
/Knapsac_ecc_encrdec_tb/kc11y       276    276
/Knapsac_ecc_encrdec_tb/kc12x       336    336
/Knapsac_ecc_encrdec_tb/kc12y       20     20
/Knapsac_ecc_encrdec_tb/kc1ax       64     64
/Knapsac_ecc_encrdec_tb/kc1ay       0      0
/Knapsac_ecc_encrdec_tb/out_char1   99     99
```

Fig 17. The Encrypted data's of Knapsack encryption and decryption top module



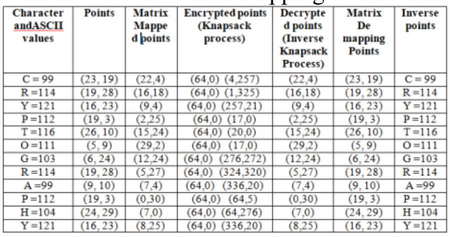
```
/Knapsac_ecc_encrdec_tb/out_char1    99    99
/Knapsac_ecc_encrdec_tb/out_char2    114   114
/Knapsac_ecc_encrdec_tb/out_char3    121   121
/Knapsac_ecc_encrdec_tb/out_char4    112   112
/Knapsac_ecc_encrdec_tb/out_char5    116   116
/Knapsac_ecc_encrdec_tb/out_char6    111   111
/Knapsac_ecc_encrdec_tb/out_char7    103   103
/Knapsac_ecc_encrdec_tb/out_char8    114   114
/Knapsac_ecc_encrdec_tb/out_char9    99    99
/Knapsac_ecc_encrdec_tb/out_char10   112   112
/Knapsac_ecc_encrdec_tb/out_char11   104   104
/Knapsac_ecc_encrdec_tb/out_char12   121   121
/glbl/GSR                            We0
```

Fig.18 The Knapsack encryption and decryption top module outputs

After decryption the original message "CRYPTOGRAPHY" is retrieved. Figure 11 gives Knapsack encryption and decryption module inputs. Figure 18 is Knapsack encryption and decryption module outputs.

Table 5 gives the device utilization for the different processes involved in the complete operations. In Spartan 3E FPGA device, the Xilinx application run out of memory and cannot simplify the operator module. The LUTs and Slice Registers utilization is very less in Artix and Kintex as compared to Spartan 6; this gives a choice to the application developer to choose the FPGA that provides more space to develop other applications on same FPGA. The time required for the processes are in terms of picoseconds that indicates very less computational time is required for the complete crypto processor compared to previous implementations given in table 1.

Table.4 Encryption and decryption of points with matrix mapping

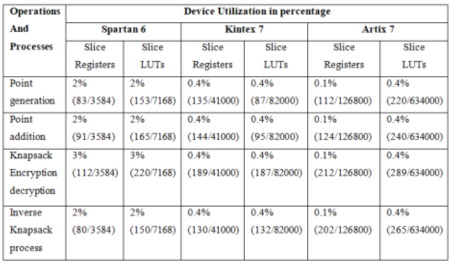


Character andASCII values	Points	Matrix Mapped points	Encrypted points (Knapsack process)	Decrypted points (Inverse Knapsack Process)	Matrix De mapping Points	Inverse points
C = 99	(23, 19)	(22,4)	(64,0) (4,257)	(22,4)	(23, 19)	C = 99
R =114	(19, 28)	(16,18)	(64,0) (1,325)	(16,18)	(19, 28)	R =114
Y =121	(16, 23)	(9,4)	(64,0) (257,21)	(9,4)	(16, 23)	Y =121
P =112	(19, 3)	(2,25)	(64,0) (17,0)	(2,25)	(19, 3)	P =112
T =116	(26, 10)	(15,24)	(64,0) (20,0)	(15,24)	(26, 10)	T =116
O =111	(5, 9)	(29,2)	(64,0) (17,0)	(29,2)	(5, 9)	O =111
G =103	(6, 24)	(12,24)	(64,0) (276,272)	(12,24)	(6, 24)	G =103
R =114	(19, 28)	(5,27)	(64,0) (324,320)	(5,27)	(19, 28)	R =114
A =99	(9, 10)	(7,4)	(64,0) (336,20)	(7,4)	(9, 10)	A =99
P =112	(19, 3)	(0,30)	(64,0) (64,5)	(0,30)	(19, 3)	P =112
H =104	(24, 29)	(7,0)	(64,0) (64,276)	(7,0)	(24, 29)	H =104
Y =121	(16, 23)	(8,25)	(64,0) (336,20)	(8,25)	(16, 23)	Y =121

PERFORMANCE EVALUATION AND DISCUSSIONS

Elliptic Curve Cryptography provides a secure means of exchanging keys among communicating hosts using the Diffie Hellman Key Exchange algorithm. Encryption and Decryption of texts and messages have also been attempted. This work presents the implementation of ECC by first transforming the message into an affine point on the EC, and then applying the knapsack algorithm on ECC encrypted message over the finite field *GF (p)*. In ECC we normally start with an affine point called *Pm(x, y)*. This point lies on the elliptic curve. In this work we have illustrated encryption/decryption involving the ASCII value of the characters constituting the message, and then subjecting it to the knapsack algorithm. We compare our proposed algorithm with RSA algorithm and show that our algorithm is better due to the high degree of sophistication and complexity involved. It is almost infeasible to attempt a brute force attack. Moreover only one parameter, namely the Knapsack vector a_i alone needs to be kept secret. On the contrary in RSA, three parameters such as the modulus n, its factors *p* and *q* need to be kept secret.

Table.5 Device Utilization for Knapsack process and Point inverse on Spartan 6



Operations And Processes	Device Utilization in percentage					
	Spartan 6		Kintex 7		Artix 7	
	Slice Registers	Slice LUTs	Slice Registers	Slice LUTs	Slice Registers	Slice LUTs
Point generation	2% (83/3584)	2% (153/7168)	0.4% (135/41000)	0.4% (87/82000)	0.1% (112/126800)	0.4% (220/634000)
Point addition	2% (91/3584)	2% (165/7168)	0.4% (144/41000)	0.4% (95/82000)	0.1% (124/126800)	0.4% (240/634000)
Knapsack Encryption decryption	3% (112/3584)	3% (220/7168)	0.4% (189/41000)	0.4% (187/82000)	0.1% (212/126800)	0.4% (289/634000)
Inverse Knapsack process	2% (80/3584)	2% (150/7168)	0.4% (130/41000)	0.4% (132/82000)	0.1% (202/126800)	0.4% (265/634000)

Table 6. Timing details

Minimum Period	1.985 ηseconds
Maximum Frequency	503.702MHz
Minimum input arrival time	1.872 ηseconds
Maximum output required time	0.511 ηseconds
Maximum combinational path delay	**No path delay found**

The arrival of this development environment has addressed a number of the widespread concerns relating to WSNs [28][29][30][31]:

Strength of Security: The architecture that has been implemented is on a par with previous implementations with respect to area, delay and speed.

Scalability: Key management has been of great concern in WSNs. The mechanism of ECC reduces concerns regarding key management.

Resource Consumption: Considering the ideals of WSNs in relation to one-use devices, this is within the bounds of acceptability. There is provision for improvement in the area.

Speed/Efficiency: There is no combinational path delay; however this may differ with larger data and key size.

The input data of smaller size is used to check for suitability for Wireless Sensor Nodes and since the matrix calculation requires more computation time. The implementation of LUT in coding design becomes complex. As the bit size increases; memory requirement becomes more as affects the energy utilization in networks, thereby network lifetime. We can manipulate data with dissimilar representation to provide protection along with knapsack.

CONCLUSIONS

Utilization of shorter key length in ECC is highly suitable for the user by consuming less power, minimum area and minimum bandwidth. Because of its hardware realization and software efficiency ECC is more efficient than RSA. In this work, a matrix mapping methodology and knapsack algorithms are implemented. In matrix mapping procedure transfer all alphabetic character into points on elliptic curve is defined. Encryption and decryption of mapping points is employed through knapsack algorithm. In mapping method there is complicated to guess the words through it does no longer show any regularity and knapsack algorithm avoids brute force attack by growing confusions. The language used to code these modules is Verilog. The modules are integrated to receive matrix mapping, Knapsack encryption, knapsack decryption and de mapping. The complete crypto process is executed with frequency of 503.702MHz. No Maximum combinational path delay is found in the implementation of modules. In comparison with previous works the area utilization and computational time required in this work is very less, thus satisfying the resource constraints' of wireless sensor nodes.

REFERENCES

Ian, F., Akylidiz, Weilian Su, Yogesh Sankarasubramaniam and E Cayirci.(2002), "Wireless Sensor Network : A Survey on Sensor Networks," *in IEEE Communication Magazine,* ISSN:0163-6804, vol. 40, no. 8, pp. 102-114.

William Stallings. (2011), "Cryptography and network security principles and practices", Prentice Hall, 5th Edition.

Darrel R. Hankerson, A. Menezes and A. Vanstone.(2004), "Guide to Elliptic Curve Cryptography" Springer.

Leif Uhsadel, Markus Ullrich, Amitabh Das, Dusko Karaklajic, Josep Balasch, Ingrid Verbauwhede, Wim Dehaene, "Teaching HW/SW Co-Design With a Public Key Cryptography Application," in IEEE Transactions in Education, 56(4):478-483, 2013.

Thomas Newe. (2008), "The Impact of Java and Public Key Cryptography in Wireless Sensor Networking", 2008 The Fourth International Conference on Wireless and Mobile Communications, 07/2008.

Antonio de la Piedra, An Braeken, AbdellahTouhafi.(2012), "Sensor Systems Based on FPGAs and their Applications: A Survey," in Journal of Sensors, DOI:10.3390/s 120912235, 12(0):12235-12264, 2012.

Shaila K, S H Manjula, Thriveni J, Venugopal K R and L M Patnaik.(2011), "Resilience Against Node Capture Attack using Asymmetric Matrices in Key Predistribution Scheme in Wireless Sensor Networks ," *in International Journal on Computer Science and Engineering,* ISSN:0975- 3397, vol. 11, no. 3, pp. 31-41.

Lata B T, Vidya Rao, Sivasankari H, Tejaswi V, Shaila K, Venugopal K R, L M Patnaik.(2015), "SEAD: Source Encrypted Authentic Data for Wireless Sensor Networks," *in International Journal of Engineering Research and Development,* e-ISSN: 2278-067X, p-ISSN: 2278-800X, vol. 11, no. 3, pp. 01-16.

Sujoy Sinha Roy and Chester Rebeiro.(2013), " Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* ISSN:1063-8210, vol. 21, no. 5, pp. 901-909.

Hilal Houssain, Mohamad Badra and Turki F Al-Somani.(2012), " Comparative Study of Elliptic Curve Cryptography Hardware Implementations in Wireless Sensor Networks," *in International Journal of RFID Security and Cryptography (IJRFIDSC),* vol. 1, no. 1/2, pp. 67-74..

Kaleel Rahuman and G Athisha.(2010), "Reconfigurable Architecture for Elliptic Curve Cryptography," *in Proceedings of the IEEE International Conference on Communication and Computational Intelligence,* INSPEC Accession number 1188746, pp. 461-466.

A Kaleel Rahuman and G Athisha.(2013), "Reconfigurable Architecture for Elliptic Curve Cryptography using FPGA," *in Mathematical Problems in Engineering, Hindawi Publishing Corporation,* Article ID 675161, 8 pages.

Hassan M N and Benaissa M, "A Scalable Hardware/Software Codesign for Elliptic Curve Cryptography on PicoBlaze Microcontroller," in *Proceedings of 2010 Symposium on IEEE Circuits and Systems (ISCAS),* p-ISBN:978-1-4244-5308-5, pp. 2111-2114, Paris, 2010.

Xining Cui and Jingwei Yang , "An FPGA Based Processor for Elliptic Curve Cryptography," *in Proc. of International Conference on Computer Science and Information Processing (CSIP),* p-ISBN:978-1-46733-1410- 7, pp. 343-350, Xian, China 2012.

Geetha G, Padmaja Jain (2014.), "Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography", International Journal of Computer Applications Technology and Research Volume 3, Issue 5, 312 – 317.

Jitendra Sharma and Prashant Shukla(2013), "ECC Cipher Processor Based On Knapsack Algorithm",National Conference on Emerging Trends in Electrical, Instrumentation &Communication Engineering Vol.3, No.2, pp 67-71.

O.Srinivasa Rao, Prof. S. Pallam Setty.(2010), "Efficient Mapping methods for Elliptic Curve Cryptosystems" , International Journal of Engineering Science and Technology, 2010

F. Amounas and E.H. El Kinani. (2012), "Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography," International Journal of Information & Network Security (IJINS), Vol.1, No.2, pp. 54~59, ISSN: 2089- 3299.

Kamalakannan, V., and S. Tamilselvan. (2015), "Security Enhancement of Text Message Based on Matrix Approach Using Elliptical Curve Cryptosystem", Procedia Materials Science.

G. Chen, G. Bai, and H. Chen.(2007)," A High-performance elliptic curve cryptographic processor for general curves over GF(p) based on a systolic arithmetic unit," IEEE Transactions on Circuits System- II,vol.54,no.5,pp.412-416.

.

E. El Kinani.(2012), "Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography*"*, in International Journal of Information and Network Security (IJINS*)*, vol. 1, no. 2. pp.45-53.

F. Amounas and E.H. El Kinani.(2012), "An Efficient Elliptic Curve Cryptography protocol Based on Matrices", International Journal of Engineering Inventions.

Balamurugan, R., V. Kamalakannan, Ganth D. Rahul, and S. Tamilselvan. "Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography", 2014 International Conference on Contemporary Computing and Informatics (IC3I), 2014.

Brian King, "Mapping an Arbitrary Message to an Elliptic Curve When Defined Over GF (2^n)," in International Journal of Network Security, 8(2):169-176, 2009.

Anjan K, Abhijith C, Arun Raj, Deekshith, Jibi Abraham, "Design and Mathematical Model of Hybrid Cryptographic Algorithm-A3D Algorithm," in International Journal of Advanced Research in Computer and Communication Engineering, 3(6):6988-6901, 2014.

Fatima Amounas, El Hassan El Kinani, Moha Hajar," A Matrix Approach for Information Security Based ECC using Mealy Machine and Fibonacci Q-Matrix," in International Journal of Engineering and Innovative Technology (IJEIT) Volume 3(1):500-504, 2013..

Jitendra Sharma, Prashant Shukla," ECC Cipher Processor Based On Knapsack Algorithm", in journal of control systems and Informatics, ISSN 2224-5774 (print) ISSN 2225-0492 (online) ,3(2):53-57, No.2, 2013.

Leelavathi G, Shaila K, Venugopal K R, “Elliptic Curve Cryptography Implementation on FPGA using Montgomery Multiplication for Equal Key and Data size over GF(2m) for Wireless Sensor Networks,” in Proceedings of the International Conference on 2016 IEEE Region 10 Conference (TENCON), DOI: 978-1-5090-2597-8/16, pp.469-473, Singapore,2016..

Leelavathi G, Shaila K, Venugopal K R, “Implementation of ECC on FPGA using Scalable Architecture With equal Data and Key for WSN,” in International Journal of Engineering and Technology (IJET), ISSN (Print): 2319-8613, ISSN(Online):0975-4024, DOI: 10.21817/ijet/2017/v9i2/170902063, 9(2):773-796, 2017.

Mostafa.I.Soliman, Ghada.Y.Abozaid, “ FPGA Implementation and Performance Evaluation of a high throughput Crypto Processor”, Elsevier Journal of Parallel and Distributed Computing, 71(2011)1075-1084..

Md Selim Hossain1 , Yinan Kong1, Ehsan Saeedi1, Niras C. Vayalil1, “High-performance elliptic curve cryptography processor over NIST prime fields”, IET Journal Computers & Digital Techniques ,2017, Vol. 11 Iss. 1, pp. 33-42.

STUDY ON WOMEN'S PERSPECTIVE TOWARDS AVIATION CAREERS IN SRI LANKA

K. A. D. D. Kuruppu, C. J. Hettiarachchi

Department Aeronautical Engineering, Faculty of Engineering, General Sir John Kotelawala Defence University, Sri Lanka

.

ABSTRACT

The aviation sector is very important to Sri Lanka both in terms of contribution to employment as well as for the growth in Gross Domestic Product. The aviation sector is dominated by men rather than women. As according to the literature, one of the major issues that women have to face is lonesomeness while other factors including public opinions and political pressure. Besides, the women who were seek to enter for aviation related jobs have under gone challengers related to educational and occupational stereotypes in physical, cognitive and psychological abilities. It is imperative to understand the underrepresentation of women in other sectors in aviation other than in flight crew which induce professionalism to women in aviation. The purpose of this study was to identify the women's perspective towards aviation sector jobs in Sri Lanka. 10 in- depth semi structured face-to-face interviews were conducted with females who were selected as embedded - single case design method as per in statistics to order to represent different divisions in aviation. Prior to conduct in-depth semi structured face-to-face interviews, the questions were predetermined. 10 females from different divisions in a same organization was considered for the interview. The responders (10 women) were selected based on embedded - single case design and all the face-to-face interviews were conducted at the same day. Individual interviews were carried out to collect unbiased information from the responders. The research objectives were briefed to each interviewee prior to the interview. The snowball sampling method was enabled the interviewees to introduce the research for other responders who were in the target population. The results revels that there are several issues that women should overcome if they select aviation sector as their long term career path. In-flexible work schedules, lack of training opportunities, and also male work culture were identified as the major factors that influence of their work capacity. The gender imbalance can be rectified by implementing employer level and national policies which nurture more women in aviation. Majority of the women who are in the aviation sector jobs like to see more female representation in aviation sector jobs. Hence, as per this study reveals, it is mandatory to address the difficulties pertaining with in-flexible working hours for women in order to retain more women in aviation sector jobs.

Keywords: Aviation, Sri Lanka, Careers, Women

INTRODUCTION

The aviation sector is very important to Sri Lanka both in terms of contribution to employment as well as for the growth in Gross Domestic Product. The aviation sector is dominated by men rather than women [1]. Hence, there have been very low number of empirical studies carried out about women in aviation [2,6]. However, it is obvious that the majority of cabin crew and ticketing staff are women, while the behind the locked door of the cockpit, the situation is quite different [4]. By the change of social environmental situation occurred in 1970s, more feminine movement could be seen in aviation sector which were traditionally dominated by male [5]. As according to literature [3], one of the major issue a woman has to face is lonesomeness while other factors including public opinion and political pressure. Besides, the women who were seek to enter for aviation related jobs have under gone challengers namely educational and occupational stereotypes related to physical, cognitive and psychological abilities [6]. It is imperative to understand the underrepresentation of women in other sectors in aviation other than in flight crew which induce professionalism to women in aviation. The purpose of this study is to identify incentives and barriers which attract or limit women in general aviation sector in Sri Lanka.

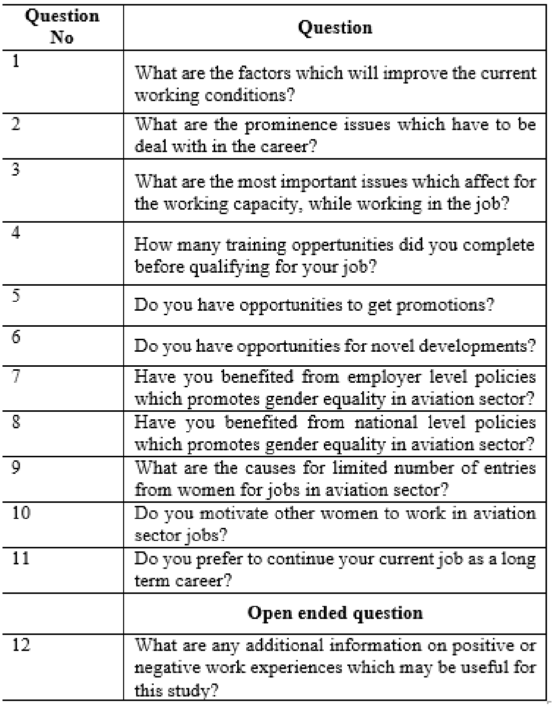
METHODOLOGY

Prior to conduct in-depth semi structured face-to-face interviews, the questions were predetermined. 10 females from different divisions in a same commercial airline based in Sri Lanka was considered for the interview. The responders (10 women) were selected based on embedded - single case design and all the face-to-face interviews were conducted at the same day. This approach produces healthy empirical qualitative data and it was allowed the respondents to discuss their opinions in explicit manner [7]. Individual interviews were carried out to gather unbiased information from the responders. The research objectives were briefed to each interviewee prior to the interview. The snowball sampling method was enabled the interviewees to introduce the research for other responders who were in the target population. The emails were sent for few members in the target population and these individuals were told to provide contact details of the other members in the same airline. Ultimately, it was ended up with 10 interviewees for the interview.

All the semi – structured interviews were carried out by a single interviewer in a day. A part from age, job profile and experience, 12 questions (Table I) were piloted with two aircraft technicians.

TABLE I. NTERVIEW SCHEDULE

TABLE I. INTERVIEW SCHEDULE



Question No	Question
1	What are the factors which will improve the current working conditions?
2	What are the prominence issues which have to be deal with in the career?
3	What are the most important issues which affect for the working capacity, while working in the job?
4	How many training oppertunities did you complete before qualifying for your job?
5	Do you have opportunities to get promotions?
6	Do you have opportunities for novel developments?
7	Have you benefited from employer level policies which promotes gender equality in aviation sector?
8	Have you benefited from national level policies which promotes gender equality in aviation sector?
9	What are the causes for limited number of entries from women for jobs in aviation sector?
10	Do you motivate other women to work in aviation sector jobs?
11	Do you prefer to continue your current job as a long term career?
	Open ended question
12	What are any additional information on positive or negative work experiences which may be useful for this study?

The interview process was started by inquiring the age, job profile and experience at the current job profile (Table II) from each responder.

TABLE II. LIST OF RESPONDENTS

Respondent	From Introductory questions		
	Age	Job profile	Experience (years)
1	26-35	Aircraft Technician	6-10
2	26-35	Ticketing	0-5
3	15-25	Management	0-5
4	15-25	Ground Handling	0-5
5	26-35	Information System Analysis	0-5
6	15-25	Aircraft Technician	0-5
7	15-25	Aircraft Technician	0-5
8	15-25	Management	0-5
9	15-25	Aircraft Technician	0-5
10	26-35	Ground Handling	11-15

The rest other questions were related to identify the issues and challengers pertaining to limit women in aviation as given in Table I. Each interview was carried out 30 - 40 minutes. The responses were recorded separately. Prior to conduct this pilot study all participants noted that the questions did not make them to feel discomfort, hence they answered honestly. The interview was concluded with an open ended question which allowed the responders to give any additional information on positive or negative work experiences for women in aviation sector.

RESULTS AND DISCUSSION

The 10 interviewees had an average age range of 15-25 and all of them have average range of experience from 0-5 years at the current designation. All the responders were females and out of that there were 2 females who are working as Aircraft Technicians, 2 as Ground Handling staff, 2 as Management staff and also 2 from Ticketing and 2 from Information System Analysis staff.

A. Responses related for factors which affect to improve the current working conditions

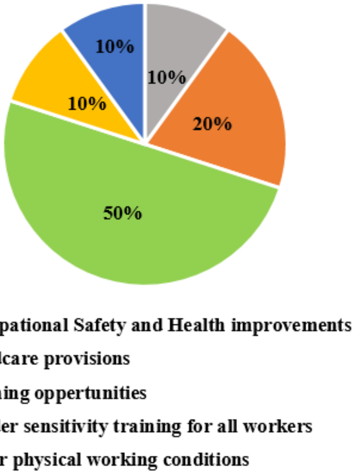


Fig. 1.Factors affect to improve the current working conditions

As shown in Fig. 1, half from the responders believe that providing the training oppertunities will improve the working conditions of the employees, while 10% from the responders believe that gender sensitivity training for all workers, better physicl working conditions and also improvements in occupational safety and health improvements will affect to enhance the present working conditions among female employees in aviation. Further, the rest 20% responded that Childcare provisions also influence to improve the current working condiitons.

B. Responses related for the prominence issues which have to be deal with in the career

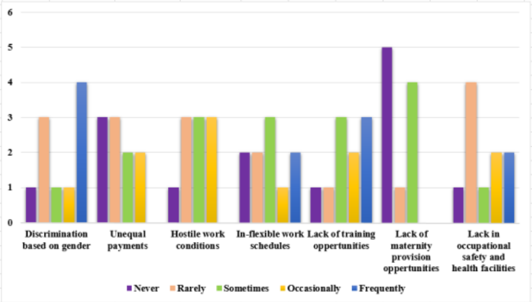


Fig. 2.Factors for the prominence issues which have to deal with in the career

As according to Fig. 2, seven parameters were identified which are directly relevant for the prominenet issues that the females under go during their career. As according to the responders only one mentioned that she has not gone through any sort of discrimination based on gender, while there are four females who have under gone discriminations due to femininity during their career. There were three females who experienced gender discrimination rarely during their career while other two females were experienced gender discrimination somethimes and occationally. Unequal payments were experienced rarely by three female emplyees, while another three never experienced such. Another two females were experinced unequal payments sometimes and another two by occasionally. But none of them experienced unequal payments frequently. As per the responders view there was one female who never experienced unfrienly working conditions while there were another three females for each who experienced hostile work conditions rarely, sometimes and occasionally. But there were non of the females who experienced unfriendly working conditions frequently. As per the information given by the responders, two of the responders have never under gone in-flexible work schedule while another two have frequently under gone through the in-flexible work schedules. There were three of the females who have experienced in-flexible work schedules sometimes. In addition there was one emplyee who experienced in-flexible work conditions occasionally while another two experienced in-flexible working conditions rarely. Three of the female responders mentioned that they have experienced lack of tarining oppertunities frequently while another three experienced lack of training oppertinities sometimes. One employee stated that she never experienced lack of training oppertinites and another one rarely experienced lack of training oppertunites. But two of the responders mentioned that they have experienced lack of training opperunities occasionally. Half of the respondents mentioned that they have never experienced lack in maternity provision oppertunities while another four respondents sometimes experienced lack in maternity provision oppertinities. One has expeirenced lack in maternity provisions oppertunities rarely but none of them experience lack in maternity provision oppertunities frequently. Four of the respondents have rarely under gone lack in occupational safety and health facilities while another one never experienced lack in occuptonal safety and health facilities. Another two females experienced lack in occuptonal safety and health facilities occasionally and other two experienced it frequenty. In addition there was a single respondent who experienced lack in occuptonal safety and health facilities sometimes.

C. Responses related for the most important issues which affect for the working capacity, while doing in the job

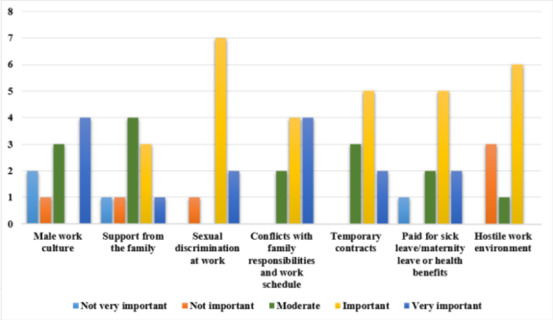


Fig. 3.Factors which affect for the working capacity

As given in Fig. 3, six factors were identified which have the influence on the working capacity of female employees. Four respondents mentioned that the male work culture is very important and two females mentioned that male working condition is not very important of their working capacity. Three of the employees mentioned that male work culture is moderately influence for females working capacity while none of them mentioned it as important factor of their working capacity. But there was one respondent who mentioned that male work culture is not imporatnt for her working capapcity. Four of the respondents mentioned that support from the family moderatly influences for the working capacity and another three mentioned that support from the family effect for the working capacity importantly. One of the respondents mentioned that family support is not very important for the working capacity for her while each one mentioned that support from the family is not important for the working capacity and the remaining one stated that support from the family is a very important factor for her working capacity. Seven of the responders stated that the sexual discrimination at working place importantly influence for the working capacity and two of the respondents mentioned that sexual discrimination is a very importantly influence for the working capacity. Only one respondent mentioned that sexual discrimination at the working place is not important for the working capacity of her. Four of the responders mentioned that conflicts with family responsibilities and work schedule moderately influence for the working capacity while another four stated that conflicts with family responsibilities and work schedule very importantly influence on their working capacity. The rest of the responders mentioned that conflicts with family responsibilities and work schedule moderately affect for their working capacity. Five from the total respondents mentioned that by being in temporary contract in job importantly influence for the working capacity while three of the responders stated that being in temporary contracts moderately influence for the woking capacity. The rest of the responders stated that being in temporary contract plays a very important role in working capacity of them. Five respondents mentioned that paid for sick/ maternity leave or health benefits are important for working capacity while two respondents mentioned that paid for sick/ maternity leave or health benefits are very important for working capacity. Another two respondents stated that paid for sick/ maternity leave or health benefits are moderately important for the working capacity while one respondent mentioned that paid for sick/ maternity leave or health benefits are not important for her working capacity. Six respondents mentioned that hostile work environment is importantly influence for the working capacity and one mentioned that hostile work environment is moderately influence on working capacity for her. The rest of the respondents mentioned that hostile work environment is not very important factor to influence their working capacity.

D. Responses related for training oppertunities before qualifying for the specific job

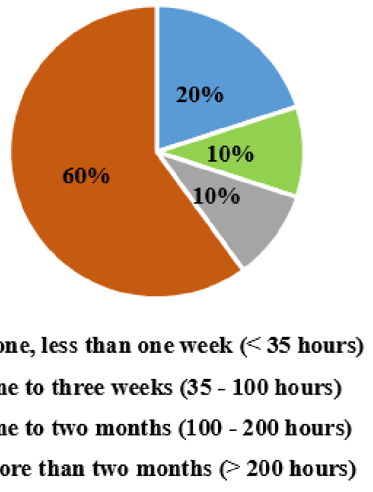


Fig. 4.Training oppertunities prior to job

As shown in Fig. 4, 60 % from the respondents have gone through a training for more than two months before they start the specific job and 20 % of the females have gone through none or less than one week training programme. There were 10 % from the respondents for each who have done the training for one to three weeks and one to two months respectively.

E. Responses related for the oppertunities for promotions

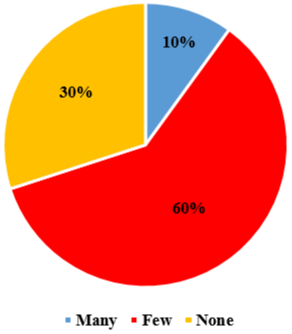


Fig. 5.Oppertunities for promotion

As according to Fig. 5, 60 % from the respondents have obatined few oppertunities for promtion while another 30 % from the respondents have obatined none of the oppertunities for promotion. The rest of the respondents obatined many oppertunities for promotion.

F. Responses related for oppertunities for new developments

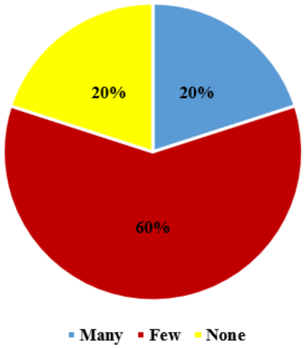


Fig. 6.Oppertunities for new developments

As shown in Fig. 6, 60 % from the respondents have got opportunities to do new development while 20 % have received many opportunities for new developments. The rest of the females never got an opportunity to do novel developments during their career so far.

G. Responses related for the impact of employer level policies which nurture women in aviation

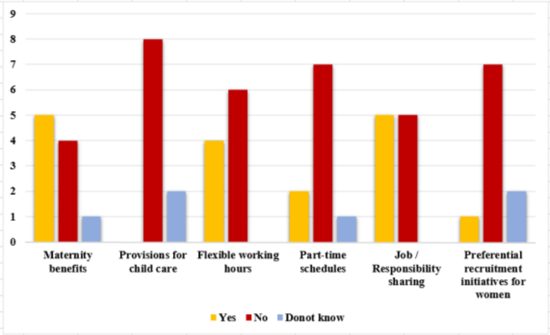


Fig. 7.Impact of employer level policies to promote women in aviation

As Fig. 7 illustrate the identified factors based on employer level policies which affect to nurture gender equality. Half of the respondents mentioned that providing maternity benefits has an influence on promoting female in aviation, while four respondent mentioned that they do not think that providing maternity benefits nurture women in aviation sector. In addition, one respondent stated that she did not have any idea about it. 8 of the respondents mentioned that provisions for child care do not have any influence on promoting women in aviation while the rest stated that they do not know about it. Six of the respondents mentioned that by providing only flexible working hours for ladies may not influence women in this sector and four of the females stated that providing flexible working hours may influence women in aviation sector jobs. Seven of the respondents mentioned that by providing part-time schedules will not nurture women in aviation and one responded against to it. Two respondents mentioned that by providing part-time schedules will lead to nurture women in aviation. 50 % of the respondents agreed that the feasibility of sharing responsibilities may nurture women in aviation while the rest of the respondents disagreed with it. Seven of the respondents mentioned by providing only preferential recruitment initiatives for women will not influence women in aviation while one was against to it. Two of the respondents mentioned that they did not have any idea about it.

H. Responses related for the impact of national level policies which nurture women in aviation

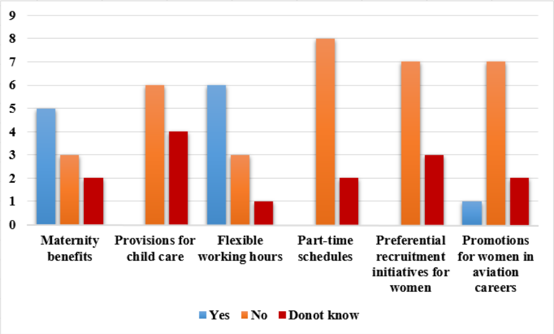


Fig. 8.Impact of national level policies to promote women in aviation

Based on the respondent's comments six factors were identified which have (Fig.8) the impact to nurture women in aviation in national level. Half of the respondents mentioned that national level policies for maternity level benefits may encourage to nurture women in aviation sector and three of them were not agreed with it, while the rest of the respondents mentioned that they did not have any idea about it. Six of the respondents stated that national policies of provisions for child care will not nurture women in aviation while the rest was against to it. Six respondents mentioned that national policies on flexible working hours will influence to have more females in aviation sector and three were disagree to it. But one of the respondents mentioned that she did not think that national level policies on flexible working hours may effect to enhance the number of women in aviation. Eight of the respondents mentioned that national level policies on part-time schedules will not nurture women in aviation while two respondents did not have any idea about it. Similar responses were obtained for the preferential recruitment initiatives for women as well, where seven respondents were agreeing with it and the rest was against to it. Seven respondents stated that national level policies on promotions will not nurture women in aviation while one was agreeing with the statement. There were two respondents who did not know about it.

I. Responses related for limited number of entries from women for jobs in aviation sector

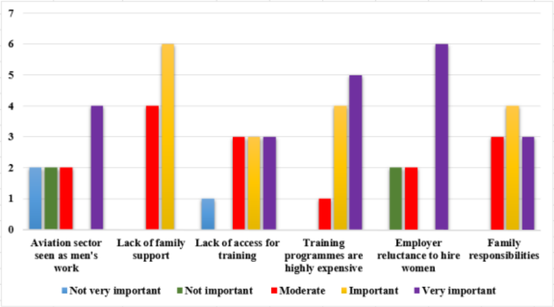


Fig. 9.Factors related for the limited number of women entries in aviation sector

Based on the respondent's comments six factors were identified (Fig 9) which influenced for the limited entries of women in aviation sector. Four respondents mentioned that very importantly they seek aviation as men's work sector while two were totally against to it. In addition, another two females moderately agree with the statement while another two did not think importantly that the aviation sector is only for men. Six from the respondents seen that lack of family support is one of the important factor for not choosing aviation sector jobs by women. The rest of the women had moderate consent on it. Three of the respondents mentioned that lack of access for training opportunities was very important factor which limit women entries in aviation sector jobs and three respondents were moderately agreed to it. But one respondent stated that lack of access for training was not very important factor for limited women in aviation sector jobs while the three of the respondents considered it as an important factor. Six of the respondents mentioned that employers are reluctance to hire women in aviation sector and as per them it was very important factor which limit women entries in aviation but three of the respondents did not think it as an important factor while the rest of the respondents think it as a moderate factor for women entries in aviation. Three respondents mentioned that family responsibilities play a very important role which lead to limits women entries in aviation and another three females were moderately agree to it, while the rest of the responders were considered it as an important factor which restrict women entries in aviation sector jobs.

J. Responses related for promoting aviation sector jobs among other women

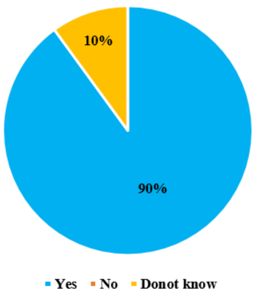


Fig. 10. Promoting aviation jobs among other women

As shown in Fig. 10, 90 % of the respondents have the consent to promote aviation sector jobs among other women while 10 % of them have no idea yet.

J. Responses related for aviation sector jobs as a long term career

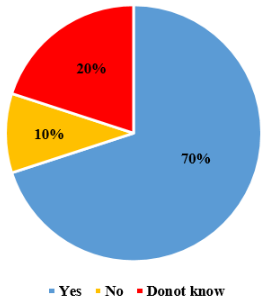
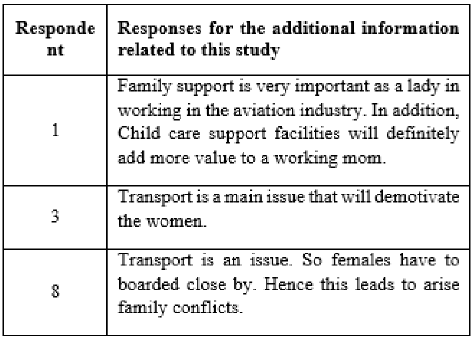


Fig. 11. Selection of aviation as a long term career

As given in Fig. 11, 70 % from the respondents stated that they select their present career as their long term career while 10% mentioned that their current job isnot their long term career. 20 % of the respondents mentioned that they have not decided yet whether their current job will be their long term career or not.

K. Responses related for any additional information on positive or negative work experiences for women in aviation sector

TABLE III. GENERAL COMMENTS BY RESPONDENTS



Respondent	Responses for the additional information related to this study
1	Family support is very important as a lady in working in the aviation industry. In addition, Child care support facilities will definitely add more value to a working mom.
3	Transport is a main issue that will demotivate the women.
8	Transport is an issue. So females have to boarded close by. Hence this leads to arise family conflicts.

Table III consist with the responses which were given by the respondents for the open ended question which was raised by the interviewer. 1st respondent mentioned that family support plays a major role for a woman who occupy in the aviation sector. Besides she mentioned that providing child care support facility is very important for a female who is working in the aviation sector. 3rd and 8th respondent mentioned that transport is one of the issues to demotivate ladies in the aviation sector. Further, 8th respondent stated that when they boarded away from their home, it leads to miss some of the day today responsibilities. It may lead to arise family conflicts as well.

CONCLUSIONS

It is evident that women who are in the aviation sector still believe that they have to overcome several hurdles than their peer males in the aviation sector. Majority of the respondents suggested that the current working conditions can be uplift by providing more training opportunities and also by providing more childcare provisions. The respondents mentioned that they are frequently undergone issues such as discrimination based on gender, in-flexible work schedules, lack of training opportunities and also lack in occupational safety and health facilities. Similar factors were identified by the literature [2, 8], as attributes which women concern when they select aviation sector as their career path. Majority of the respondents agreed that male work culture at the working place and conflicts with family responsibilities are major issues which effect for their working capacity. 60 % of the respondents have gone through training prior to their job. 60 % of the respondents got few opportunities to do new developments in their working place and also 60 % of the respondents got few opportunities to promote. As per the responses employer level and national level policies are very important to nurture women in the aviation sector. This is agreeing with the literature [6], which mentioned that policies and regulations should be brought to implement gender equality in aviation sector. In this study majority of the respondents seen aviation as men’s work which is contradictory with literature [8]. There were several factors were also identified which limit women entries to aviation such as lack of access for training, training programs are highly expensive and also employers are reluctant to recruit women for aviation jobs. In addition, higher family responsibilities in motherhood also limit more women entries in aviation, which is also coincide with the literature given in [1]. Most of the respondents like to promote aviation sector jobs among other women which is also similar with the research findings in literature [8]. Further, this study reveals that 70 % from the respondent would like to continue their present aviation sector job as their long term career, but they noted that they should able to balance their family life as well as career life due to being women, they have more responsibilities towards childcare and family life than men. Further in-depth research needs to be done with more number of respondents in order to generalize these findings through the populations.

Acknowledgment

The author would like to thank for all the interviewees for sharing their time and experiences with us to carry out this study successfully. Further, the author would like to express many special thanks to Mr. S. Jayasiri his assistance in this research.

REFERENCES

Germain, M. L. Herzog, M. J. R. and Hamilton, P. R. (2012) “Women employed in male-dominated industries: lessons learned from female aircraft pilots, pilots-in-training *and mixed-gender flight instructors," J. Human Resource Development International, vol. 15, pp. 435-453.*

Hynes, G. E. and Puckett, M. "Feminine leadership in commercial aviation: success stories of women pilots and captains," J. Aviation Management and Education, Feminine leadership, pp. 1-6.

Luedtke, J. R. (2011) Report at Forum on Public Policy. College of Aviation: Embry-Riddle Aeronautical University.

The Royal Aeronautical Society's women in aviation and aerospace committee, London: UK (2009) "The future for women in aviation and aerospace," A specialist report by, pp. 1-12.

Xiaoni, R. (2017) "Exploiting women's aesthetic labour to fly high in the chinese airlines industry," J. Gender in Management, vol. 32, pp. 386-403.

McCarthy, F. Budd L. and Ison, S. (2015) "Gender on the flightdeck: Experiences of women commercial airline pilots in the UK," J. Air Transport Management, vol. 47, pp. 32-38.

Bryman, A. (2012), Social research methods, 4th ed., Oxford University Press, Inc, New York.

Clark P. and Newcomer, J. (2015) "Overcoming gender barriers in aircraft maintenance: women's perceptions in the United States," J. Collegiate Aviation Review, vol. 33, pp. 66-84.

IDENTIFYING THE CHALLENGES OF BIG DATA USAGE IN THE EDUCATIONAL SECTOR OF SRI LANKA

Anuruddika Upul Bandara Ratnamalala

Faculty of Business Management

International College of Business and Technology (ICBT), Sri Lanka

ABSTRACT

The volume and velocity of data generated have increased substantially in the education sector of Sri Lanka. Although there is an increase, the majority of educational employees do not realize the importance or value of data and often discard without taking into consideration the numerous benefits big data can offer to students and educational institutions. The root causes that contribute to the lack of utilization of big data are mainly due to lack of infrastructure, trained workforce, standards of data usage, security issues, policies, and education of employees. The main objective of this study is to identify the challenges faced by the education sector of Sri Lanka when dealing with big data implementation and further recognize the incentives that encourage the use of big data to support the development, profitability, and decision-making capabilities of Sri Lanka. Qualitative data will be collected from interviews taken from managers, marketing professionals, accountants, and lecturers in various educational institutions across Sri Lanka using snowball and convenience sampling techniques. Furthermore, to establish how educational employees use big data, a survey will be distributed to various educational employees working in different regional educational institutions across Sri Lanka. SPSS is used to determine the correlation between independent variables (infrastructure, trained workforce, policies, education, security, and standards) and dependent variable (data usage). The findings of this research would help educational employees understand the value of big data. Moreover, this research would contribute to improving the profitability and standards of decision-making processes in the education sectors of Sri Lanka.

Keywords: Big data, data usage, education sector, Sri Lanka, data velocity

INTRODUCTION

In today's society, big data is a commonly discussed topic due to the availability and use of data for various purposes in different industries. Big data can be defined in simple terms as large volume of data which are organized and unorganized. Having ample amount of data does not matter for any industry, if there is lack of usage from it. Big data can be used to identify the market and create better strategic decisions that lead to competitive advantage of the business. An industry analyst called Laney (2001) identified three dimensions and properties of big data, namely Volume, Velocity and Variety. Volume is referred to as the amount of data that can be collected from variety of sources which include from daily business transactions, social media activities, data collected from sensor or from data transferred from one machine to another (Laney, 2001). In the past storing of these huge volume of data would be a great difficulty, but nowadays open source software like Apache hadoop have provided a software framework for storing ample amount of data conveniently. It is expected to increase the data storage by 300 times from 2005 to 2020 which is 43 trillion gigabytes. Most of the companies in the world have a storage capacity of more than 90 Tb of data nowadays.

Nevertheless, velocity can be referred to as data processing speed. It is unbelievable that the way sensors, radio frequency identification and smart metering devices capture information and process them at rapid pace. It is identified that New York stock exchange captures 1TB of trade information daily. Even a vehicle that runs on the road has more than 100 sensors to capture data and drive away from traffic efficiently (Laney, 2001). Finally, variety can be defined the amount of different data available. Data can come in different formats, for instance one format is unstructured data such as financial data, stock ticker, audio, video data and text documents whereas another format is structured data such as numeric data in traditional databases.

In addition to the above mentioned Dong Lanely data classification, two other data dimensions are identified recently. They are Variability and Complexity. Variability means that with the increase of amount of variety of data the data flow can differ by maybe having peaks or by falls (McNulty, 2016). For instance, seasonal data received in online shopping sites tend to differ significantly. Finally, Complexity refers to data that comes from different sources tend to be difficult to managed and linked (Khan et al, 2014). Most difficult task today is to identify the connection that is having certain type of data. Data analyst spend plenty of time sorting these data and making it meaningful to the relevant parties. Data types can be structured, semi structured and unstructured data. This has to be analyzed and sorted in order to make them meaningful.

With the volume, verity, velocity, variability and complexity of data it is difficult to understand what we are going to do with it (McNulty, 2016). Most of the companies in various industries have used these data to take advantages such as cost reduction, new product development, time reduction and smart decision-making, but ample amount of data go to waste without any usage. Although most industries use big data to receive comparative advantage, education sector of Sri Lanka tend to show a negative attitude towards big data usage. Education sector is where there is so many skilled professionals such as doctors, accountants, engineers, mechanics and businessman are made, but attention of big data use seems to be greatly less. In education industry, there is currently a regular interaction of students with the technology. As a result of regular interaction, most of the big data created in educational industry are student assignments records uploaded to the Moodle, teachers notes uploaded to the system, metric systems to monitor students’ attendance and performance, digital libraries to issue and return books as well as entrance and graduation records of students (Shacklock, 2016). Each of these mentioned data records is responsible for bringing in many students and developing the education sector in the economy. Big data usage can enable education institutes to retain students, improve the graduation rates, improving quality of the teaching and curriculum (Economist Report, 2008). Furthermore, big data would help to receive necessary funding to archive organizational efficiency (Petkovics et al, 2014). With all the above mentioned benefits, value of big data is not understood by the educational sector employees in Sri Lanka. They tend to discard and ignore the data available without getting proper usage of the data. By realizing that there is a problem to clarify and verify the availability of problem, pilot study was conducted with 20 employees in education sector of Sri Lanka. The study was done through telephone interview and discussion using convenient and snowball sampling where mostly open-ended questions were asked from participants.

From the Pilot study, it was identified one of the major root cause for ignoring big data is lack of infrastructure. Most of the places in Sri Lanka lacks telecommunication network to link and connect to the required networks to share information. Moreover, special servers and multiple processors are required to handle and store the educational data, but due to the cost factor most of the educational institutes in Sri Lanka cannot afford the servers and processors. Secondly, it was identified that in order to use big data, there should be trained and skilled workforce. These workforce should be aware of the current technological development and should process developer skill set. Not only IT knowledge they also should possess the ability to analyze data using statistics and mathematics. To find the appropriate skills required in the education industry is especially a huge challenge. Only few possess all round skill set and others even lacks ICT knowledge. Therefore, to adopt and use big data is a major challenge in the education industry.

Thirdly, ample amounts of data are captured regularly by the student databases but there is no proper standards of maintaining these data. All the data are stored in one place without any categorization of data. When a particular need arises educational administrators find it difficult to retrieve the data that is relevant to the issue. As a result most of educational administrators tend to discourage the use of big data. Additionally, security issues are a major challenge to the professionals in the educational industry. Mainly, because antivirus software that is need to protect data need regular updating and need up to date protection. If the data protection malfunction the whole system can bring down to a standstill position and hackers could use those information to their own advantage. To purchase and update these virus guards to protect the whole databases in education sector also cost so much money. Therefore, due to limited budget and complexity educational administrators consider maintain security as a challenge to the big data usage. Most of the policies implemented in Sri Lankan educational institutes does not support the big data usage. For instance, there is a policy that student exam records are kept on manual books for maximum 5 years, after that they are considered no longer useful. If a particular student require those details after 5 years destroyed data cannot be retrieved from the system.

Finally, ICT education literacy level of Sri Lanka is declining from 28.5% in 2017 to 27.5% in 2018 from overall population according to department of census of Sri Lanka (Census, 2018). Lack of computer literacy suggests that lesser education level to cope up with huge databases in the society. Therefore, due to lack of education in ICT is a challenge to the use and implementation of big data in education sector in Sri Lanka. It could be seen that there are many root causes that lead to major problem of lack of big data usage in education industry. Neglecting without taking any necessary precautions for improvement of big data usage would impact our standards of education with the world and also would make poor decisions in education industry. As a result, of poor decision making it will weaken the profitability of education services in Sri Lanka. Therefore, necessary corrective actions need to be implemented for improvement of big data usage.

This paper would recognize the importance of big data usage to education sector of Sri Lanka and also would highlight the need for actions to be taken to encourage big data usage. With the finding of this paper most of the professionals in education sector will realize the value of big data usage which in return improve the decision-making, profitability and the competiveness in the education sector of Sri Lanka. Primary objective of this paper is to determine the main challenges of big data usage in education sector Sri Lanka. Secondly, to evaluate and see weather identified Challenges have any correlation with the big data usage. Furthermore, to understand whether the realized challenges would continue to be challenges in future as well. Finally, to recognize the recommend actions to be implemented in order to encourage data usage.

With lack of big data usage becoming a major problem the research would identify what are the main challenges faced by education sector of Sri Lanka of big data implementation? Further, need to determine whether there is a relationship between the identified challenges and big data usage? Additionally, to predict whether identified challenges would contribute to the future big data usage? Finally, this research would try to recognize what are the appropriate recommend solutions in order to encourage big data usage in education industry Sri Lanka?

This paper mainly focuses on answering the above mentioned questions. The boundaries are set forth in order to achieve a more valid and accurate outcome. Research mainly uses managers, marketing professionals, accountants and lecturers in selected areas such as Kurunegala, Kandy and Colombo in Sri Lanka within 8-year time period (2010-2018).

LITERATURE REVIEW

There are various advantages of utilizing big data, however it can be seen that the implementation of big data is a major challenge for the different sectors in one’s economy. Hence, empirical evidences from various studies have highlighted the actual and perceived challenges of big data usage in diverse industries. According to Stephen Kaisler et al. (2014), there are numerous issues and challenges of moving forward with big data implementation for education sector as well as some other sectors. Some of the most common challenges that were highlighted are issues of storage, attitudes of management, affordability, issues of processing, not having tools to analyze and also not having powerful algorithms to sort the big data from their systems or processes.

Other different studies conducted by Daniel (2014); Shitut (2017); and Kernochan (2013) also emphasize certain challenges that act as barriers for the implementation of big data systems. Mainly, they have identified such challenges as difficulty of acceptance (most of the management are not willing to change from traditional systems of data analytics), difficulties in accessing relevant data (sorting from ample amount of data and obtaining required data is a problem), obtaining expertise knowledge to operate (lack of relevant skills is a problem) and barriers in the organization environment (linking all the departments for big data implementation is a problem).

Another study by Long and Siemens (2011) demonstrate that not accurate data, mismanagement of data, culture, privacy issues, lack of skills, not enough return on investment, lack of training and resources as well as difficulty in data standardization are major challenges in application of big data in the industry. Further, studies conducted by authors such as Dan and Roger (2010); Jayasree (2013); and Rachana and Guruprasad (2014) debate that security, reliability, data quality, cost, performance and data storage facilities are key issues in big data implementation in major economies. Some of the major challenges that are identified from different literatures have been discussed below for better understanding.

Privacy and security

Most of empirical studies have identified that when it comes to raw data and information, securing and the privacy of data are as a biggest threat for any industry and any organization. When ample amount of data are used for various purposes they should be securely stored in order to prevent it from usage of various third parties. Ferguson (2017) identifies that some data are valuable for making vital decisions in the organization, but there are possibility of targeted cybercrimes and hacking of such valuable data due to competitive edge and various other reasons. Eynon (2013) also suggests that fear of misuse of valuable data lead to lack of implementation of big data in most of the companies. Additionally, a comprehensive study conducted by Broeders et al. (2017) also state that misuse of sensitive data and information fraud is a major concern in big data utilization. Hence, it is evident that majority of organizations have fear of using big data due to the lack of privacy and security of valuable data and information.

Infrastructure

Infrastructure is a vital component in big data usage, especially in today's society. According to Barroso, Clidaras and Hölzle (2013) telecommunication is considered as a vital infrastructure or a factor for implementing big data projects. In order to connect with big data storage systems such as cloud systems, telecommunication systems are considered highly necessary for any organization. Furthermore, specially designed architecture is required to process millions of nodes with multiple of disks and processors at high internet connection speed (Shapiro and Varian, 2010). Moreover, maintaining all the infrastructure leads to number of side effects such as rise of huge costs and additional resources and support systems. Hence, only large companies have the necessary capacity to bear those costs and other required resources (Barroso, Clidaras, and Hölzle, 2013). Therefore, obtaining necessary infrastructure to implementing big data usage is a massive challenge in any industry.

Trained workforce

According to Hilbert (2013), proper adaptation is required to big data project implementation. For a proper adaptation of big data software, it is necessary to acquire trained workforce within the organization. He also suggests that if data is distributed in several clusters, expertise knowledge can be obtained from several communities as well. For instance, companies like Google and Facebook use open source software like Apache hadoop to distribute their data among several clusters and obtain necessary expertise knowledge (Hilbert, 2013). Hence, it can be seen that it is essential to have a trained workforce with some expertise knowledge in order to implement the big data systems and processes in organizations.

Education level of employees

According to Villars et al. (2011), it is crucial to acquire adequate knowledge of information technology and application developing skillset in order to effectively apply big data systems and processes. People who have the relevant knowledge are scares and difficult to acquire today in terms of information technology, especially when it comes to developing countries like Sri Lanka. Moreover, studies piloted by Manyika et al (2011) suggest that key subject areas such as statistics, mathematics and computer science are needed to be enhanced regularly by employees in order effectively integrate with big data implementation. His study prove that having lack of knowledge in the mentioned subject areas would make employees difficult to analyze and interrupt the big data and data would be meaningless to conduct the further business operations. Thus, in order to implement the big data systems successfully, organizations should have right skillset and knowledgeable employees who can be identified as difficult to acquire in today's job market.

Policies and standards of data usage

Majority of empirical evidences have identified another challenge of implementing big data systems which is lack of policies and standards of data utilization. Protecting data privacy in health services report (2000) stresses out the necessity of collecting data in a standard procedure, mainly because of big data projects are vulnerable for possible security threats. Report also elaborates that strategies should be implemented by companies as a part of their policy guidelines and code of conduct in order of methods data should be collected, how should be protected and the procedure they should be used. Moreover, the action plan needs to be constructed in order of how data should be managed in order to protect from possible security breaches and data losses. In addition, Campbell (2007) identifies regulatory framework is necessary to protect against possible data breaches and security losses and also would create trust among the users of big data, if there is proper regulatory procedures.

THEORETICAL FRAMEWORK OF BIG DATA USAGE

Technology Acceptance Model (TAM) which was developed by Davis in 1989. This theory determines that new technology is mainly accepted by users due to perceived usefulness and the ease of use. When people perceive that new technology is not beneficial for them and complicated to use they tend to neglect the acceptance of usage of new technology (Davis, 1989). Therefore, from this theory we can deduce that perceived usefulness and ease of use contribute to acceptance of big data usage and implementation in organizations.

Technology Task Fit Model (TTF) assumes that user require necessary technology that fit their working environment to increase employee performance as well as organizational performance. When user lacks the necessary equipment, they find it difficult to perform to the expected standards by the organization which creates a visible gap of expected performance and actual performance. So in that sense, the performance is heavily correlated with the appropriateness of technology (Goodhue, and Thompson, 1995). Therefore, it can be recognized from technology task fit model that employees require necessary equipment in order to boost their actual performance levels to be successfully implement the big data systems within their working environment. Theory of Planned Behavior (TPB) which was developed by Icek Ajzen in 1988 which predicts the behavioral intention of humans to make decisions. Main factors that lead to behavior intention are attitudes, subjective norms and perceived behavioral control. People tend to make positive decisions based on agreement of all the factors mentioned (Ajzen, 1988). For instance, if people have positive attitudes, cultural views tend to support and also if they believe it is easy to use, then people tend to accept new technologies, particularly like big data processes. Hence, it is vital to understand the perception and intention of management as well as employees when implementing the big data processes and systems in the organization.

Unified Theory of Acceptance and Use of Technology (UTAUT) is a developed theory that discusses the intention to use technology in any industry (Venkatesh et al, 2003). This theory identifies behavioral intention of people to use the different systems is mainly driven by expectancy of the performance of the system, amount of effort, influences by the society and conditions that support the system. Thus, a study by Venkatesh et al. (2003) state that people’s behavioral intention to use the system diminishes, if any of the conditions mentioned do not provide the necessary facilitation. Therefore, it can be identified that there has to be a clear and proper intention of implementing big data systems in every industry as well as the people who relates to it should be clearly understood these intentions to productively utilize the big data in their daily operational activities.

Motivation model (MM) theory was introduced in 1992 by Davis, Bagozzi and Warshaw in order to identify the adaptation and utilization of information and communication technology within an organizational environment. They stress out that usage is mainly depend on intrinsic and extrinsic motivators (Davis et al, 1992). Intrinsic motivators arises from person’s inner motive to perform a task, for example satisfaction received from the computer usage is an intrinsic motivator. Extrinsic motivator arises from outside of a person, for instance factors from the society, perceived benefits and usefulness encourages people to use technology (Davis et al, 1992). Therefore, it can be determined that according to this theory intrinsic and extrinsic factors motivates people to use and implement big data for their daily operations.

Model of PC Utilization discusses about leading factors that lead to utilization of technology. Main factors such as social factors, complexity, job fit, long term consequences, affect towards PC usage and fascinating conditions greatly affect technology usage (Thompson et al, 1991). According to this study by Thompson et al (1991), they believe that people tend to absorb and adopt technology based on certain factors such as; if the social factors support, technology is less complex to use, day-to-day tasks fit their working environment, less consequences of personal computer usage and there should be supporting conditions to use personal computers. Hence, it could be understood all these six factors can contribute the big data usage and implementation in an organization.

METHODOLOGY

Based on the analysis of literature review and pilot study conducted, this research investigates whether the identified challenges can impact the big data usage in the education sector of Sri Lanka. Consequently, big data usage in education sector in Sri Lanka is considered as dependent variable and lack of infrastructure, trained workforce, policies, ICT education and lack of security is identified as independent variables. The research mainly tests weather there is a relationship between the independent and dependent variables and also research tries to predict whether the particular identified connection would continue to the future using regression analysis.

Conceptual framework

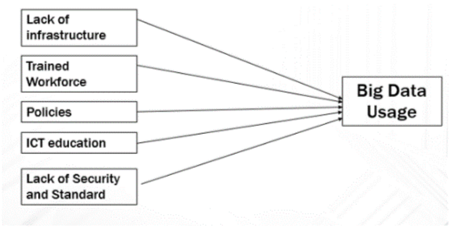


Figure 1 - Conceptual Framework

List of Hypothesis

H0: There is no relationship between Infrastructure and big data usage in Sri Lanka.

H1: There is relationship between Infrastructure and big data usage in Sri Lanka.

H0: There is no relationship between trained workforce and big data usage in Sri Lanka.

H2: There is a relationship between trained workforce and big data usage in Sri Lanka.

H0: There is no relationship between policies and big data usage in Sri Lanka.

H3: There is relationship between policies and big data usage in Sri Lanka.

H0: There is no relationship between ICT education and big data usage in Sri Lanka.

H4: There is a relationship between ICT education and big data usage in Sri Lanka.

H0: There is no relationship between security and standards and big data usage in SL.

H5: There is relationship between security and standards and big data usage in SL.

Population, Sample size and sample selection

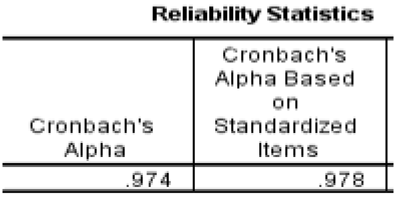
It was identified that approximately 120,000 private sector employees working in education sector in Sri Lanka. Managers, marketing professionals, accountants, and lecturers in various fields are considered to be working in educational industry in Sri Lanka. From the whole population, 130 employees working in different sectors are selected using simple random sampling technique. Areas such as Colombo, Kandy and Kurunegala are selected for the research depending on the convenience.

Data collection, Questionnaire type, time and Data analyzing technique

Data collection was done using an online questionnaire mainly because it could be easier to reach a widespread population. Selected all 130 employees have access to internet and they could answer the questions in their own spare time. Questionnaire was designed in a simple manner with mostly close-ended questions. Questions are setup using Likert scale that ranges from 1=strongly agree, 2= agree, 3=neither agree nor disagree, 4= disagree and 5=strongly disagree. Questionnaire is designed in a manner to derive at specific answer in the questionnaire. This research is conducted within time frame of 01st October 2018 to 28th February 2019. Data analysis is done using IBM SPSS software to facilitate correlation and regression.

Reliability test

Cronbach's Alpha reliability test was conducted in order to measure the complete stability of the outcomes of the statements in the questionnaire involving to the variables highlighted. It was found that more than 90% of data are reliable and satisfactory.



Reliability Statistics

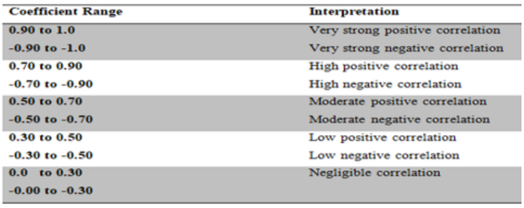
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items
.974	.978

Table 1 - Reliability Statistics

DATA ANALYSIS

Correlation analysis

Pearson Correlation is used to identify weather there is any relationship between independent and dependent variables. In Pearson correlation, coefficient range determines the type of relationship between variables which further depicts in the following table.



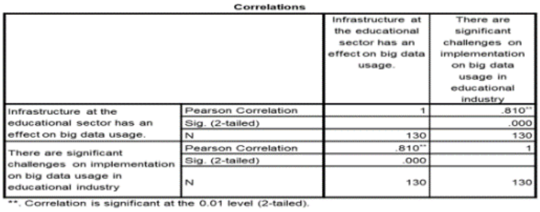
Coefficient Range	Interpretation
0.90 to 1.0	Very strong positive correlation
-0.90 to -1.0	Very strong negative correlation
0.70 to 0.90	High positive correlation
-0.70 to -0.90	High negative correlation
0.50 to 0.70	Moderate positive correlation
-0.50 to -0.70	Moderate negative correlation
0.30 to 0.50	Low positive correlation
-0.30 to -0.50	Low negative correlation
0.0 to 0.30 -0.00 to -0.30	Negligible correlation

Table 2 - Coefficient range for correlation

Regression analysis

Simple regression analysis examines when the value of dependent variable Y (big data usage) can be effectively predicted using the Independent variable X (Infrastructure, trained workforce, policies, ICT education and security and standard).

Relationship between Infrastructure on big data usage in Education sector Sri Lanka



Correlations

		Infrastructure at the educational sector has an effect on big data usage.	There are significant challenges on implementation on big data usage in educational industry
Infrastructure at the educational sector has an effect on big data usage.	Pearson Correlation	1	.810**
	Sig. (2-tailed)		.000
	N	130	130
There are significant challenges on implementation on big data usage in educational industry	Pearson Correlation	.810**	1
	Sig. (2-tailed)	.000	
	N	130	130

**. Correlation is significant at the 0.01 level (2-tailed).

Table 3 - Correlation between infrastructure and big data usagþ in Education sector

Based on the above analysis it indicates that Pearson correlation of r value is 0.810 which implies that there is a high positive correlation between variables. Moreover, Sig. (2-tailed) value is 0.000 which is less than 0.05 this means when one variable increase or decreases another variable also changes significantly. From the hypothesis, it can reject null hypothesis and accept H1: which shows there is a relationship between infrastructure and big data usage. Therefore, since there is a positive correlation, it suggests when there is lack of infrastructure there is lack of big data usage and also when people are provided with proper infrastructure, the big data usage tend to be high.

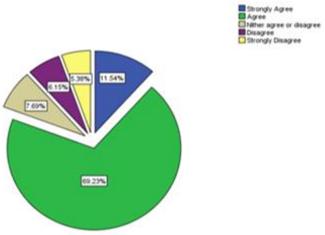
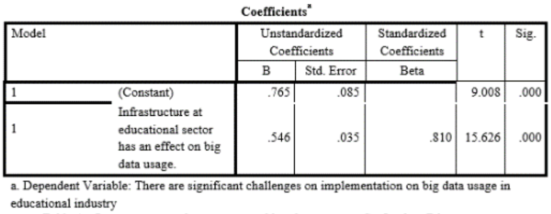


Figure 2 - Opinions about infrastructure and big data usage in Sri Lankan Education sector

According to the analysis of survey 69.23% agreed better infrastructure is required for higher big data usage in educational sector. Moreover, 11.53% of educational sector employees disagreed that infrastructure lead to improvement big data usage. Overall, majority agreed that infrastructure is a requirement in big data usage.

Regression analysis infrastructure on big data usage



Coefficients^a

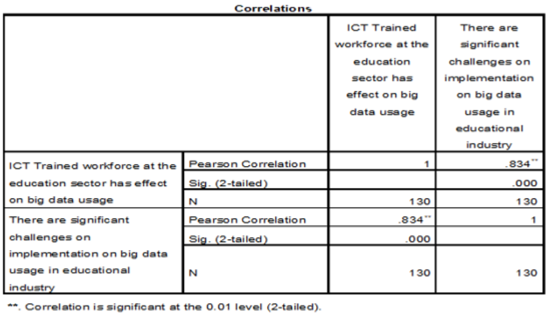
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.765	.085		9.008	.000
1	Infrastructure at educational sector has an effect on big data usage.	.546	.035	.810	15.626	.000

a. Dependent Variable: There are significant challenges on implementation on big data usage in educational industry

Table 4 – Regression on infrastructure and big data usage in Sri Lankan Education sector

Regression equation to determine Impact for big data usage from infrastructure is determined as follows: Y=0.546X+0.765. Where X is the people viewpoint of the need for infrastructure where Y is the change of big data usage. With the regression equation identified it could be determined that in future people believe proper infrastructure is necessary for big data adaptation.

Relationship between trained workforces on big data usage in education sector



Correlations

		ICT Trained workforce at the education sector has effect on big data usage	There are significant challenges on implementation on big data usage in educational industry
ICT Trained workforce at the education sector has effect on big data usage	Pearson Correlation	1	.834**
	Sig. (2-tailed)		.000
	N	130	130
There are significant challenges on implementation on big data usage in educational industry	Pearson Correlation	.834**	1
	Sig. (2-tailed)	.000	
	N	130	130

**. Correlation is significant at the 0.01 level (2-tailed).

Table 5 - Correlation between trained workforce and big data usage in Education sector

From the information Pearson R value is 0.834 which implies there is a high positive correlation. Additionally, Sig. (2-tailed) value is .000 which is less than 0.05 which suggest when one variable change other also changes positively. When we consider hypothesis, we can reject null hypothesis and accept H2: There is a relationship between trained workforce and big data usage in Sri Lanka. From all the information it could be determined that trained workforce is necessary for big data implementation.

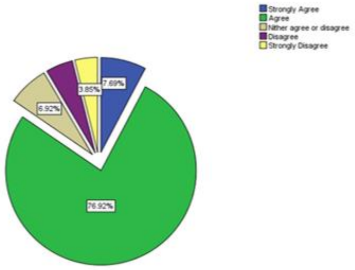
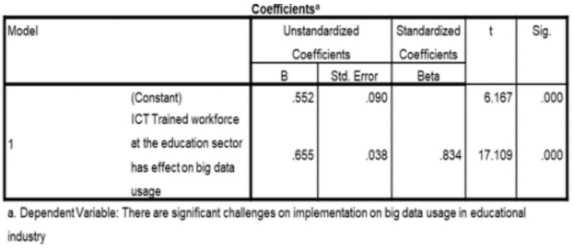


Figure 3 - Opinions about trained workforce and big data usage in Education sector

Information from the questionnaire suggest that 76.92% implies that training is required for big data adaptation. Furthermore, only 8.47% disagree that training is necessary for big data implementation. Majority agree that training is a vital for big data implementation.

Regression analysis trained workforce on big data usage



Coefficients[a]

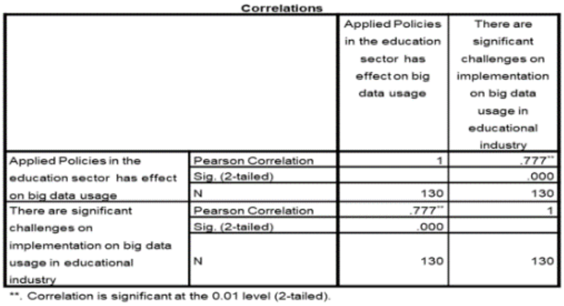
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.552	.090		6.167	.000
	ICT Trained workforce at the education sector has effect on big data usage	.655	.038	.834	17.109	.000

a. Dependent Variable: There are significant challenges on implementation on big data usage in educational industry

Table 6 – Regression on trained workforce and big data usage in Education sector

Regression equation to identify whether training is necessary in future for big data usage is determined as follows: Y=0.655X+0.552. From the equation it could be determined that even in the future people believe that trained workforce is necessary for big data usage.

Relationship between applied policies on big data usage in Sri Lankan education



Correlations

		Applied Policies in the education sector has effect on big data usage	There are significant challenges on implementation on big data usage in educational industry
Applied Policies in the education sector has effect on big data usage	Pearson Correlation	1	.777**
	Sig. (2-tailed)		.000
	N	130	130
There are significant challenges on implementation on big data usage in educational industry	Pearson Correlation	.777**	1
	Sig. (2-tailed)	.000	
	N	130	130

**. Correlation is significant at the 0.01 level (2-tailed).

Table 7 - Correlation between policies and big data usage in Sri Lankan Education sector

From the information it could be determined that Pearson R value is 0.777 which indicates that high positive correlation. Additionally, sig (2-tailed) value is .000 which is lesser than 0.05 this indicates when policies changes big data usage also changes relatively. Moreover, we can reject null hypothesis and accept H3: there is relationship between policies and big data usage in Sri Lanka. Further, it could be determined lack of policies leads to lack of big data usage and also better policies leads to higher big data usage.

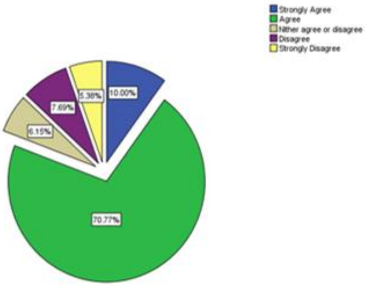
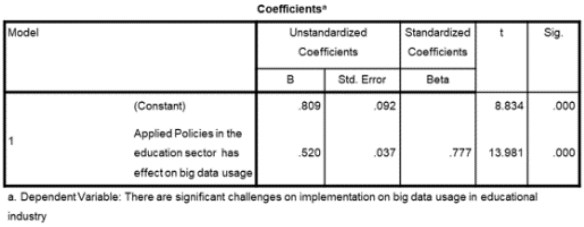


Figure 4 - Opinions about applied policies and big data usage in Education sector

Information obtained from the questioner suggest that 70.77% agree that proper policies should be implemented in order for effectively promote big data usage. Moreover, 13.07% disagree that proper policies are necessary for encourage big data usage. Overall, majority decides that proper policies are crucial to encourage big data usage.

Regression analysis policies on big data usage



Coefficients[a]

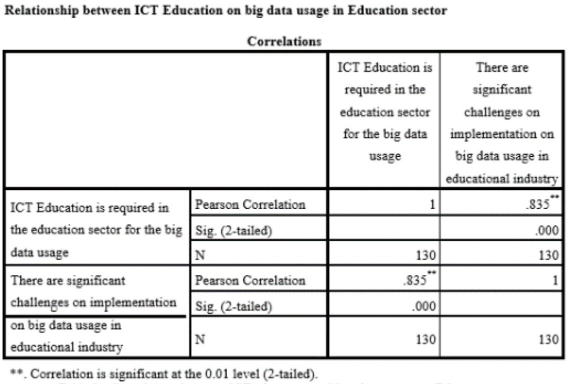
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.809	.092		8.834	.000
	Applied Policies in the education sector has effect on big data usage	.520	.037	.777	13.981	.000

a. Dependent Variable: There are significant challenges on implementation on big data usage in educational industry

Table 8 – Regression on policies and big data usage in Sri Lankan Education sector

From the table above we can arrive at the regression equation as follows: Y=0.520X+0. 809. This regression equation indicates that people believe when applied policies increases big data usage also increases. It also predicts that in future employees believe proper policies is necessary for improve big data adaptation.

Relationship between ICT Education on big data usage in Education sector



Relationship between ICT Education on big data usage in Education sector

Correlations

		ICT Education is required in the education sector for the big data usage	There are significant challenges on implementation on big data usage in educational industry
ICT Education is required in the education sector for the big data usage	Pearson Correlation	1	.835**
	Sig. (2-tailed)		.000
	N	130	130
There are significant challenges on implementation on big data usage in educational industry	Pearson Correlation	.835**	1
	Sig. (2-tailed)	.000	
	N	130	130

**. Correlation is significant at the 0.01 level (2-tailed).

Table 9 - Correlation between ICT education and big data usage in Education sector

Pearson R value 0.835 indicates high positive correlation between ICT education and big data usage. Additionally, Sig (2-tailed) value 0.000 is lesser than 0.05 suggests when changes in ICT education impacts on big data usage. It can reject null hypothesis and accept H4: there is relationship between ICT and big data usage. Overall, data indicates that lack of ICT education lead to lack of big data usage and vice-versa.

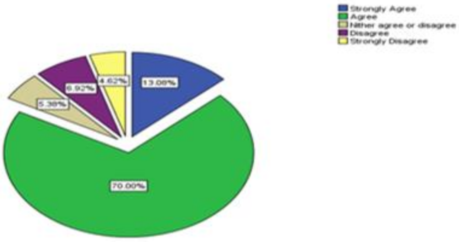
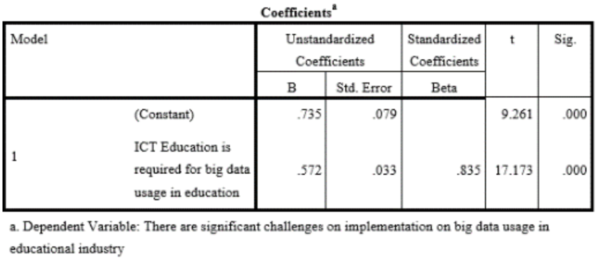


Figure 5 - Opinions about ICT education and big data usage in Education sector

70% of respondents agree that ICT education is required to improve big data usage in education sector in Sri Lanka whilst 11.54% disagree on that statement. Overall, majority accepts that education is a requirement for big data usage in Sri Lanka.

Regression analysis ICT education on big data usage



Coefficients^a

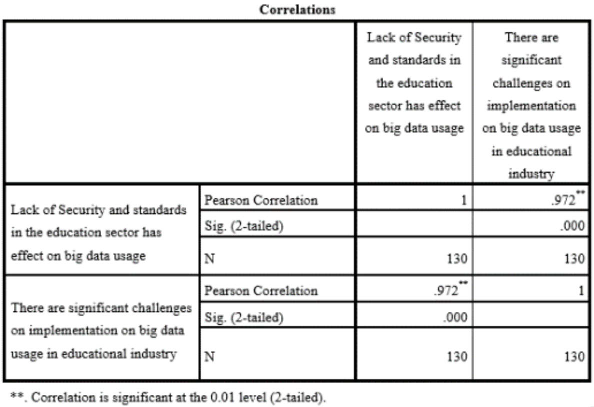
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.735	.079		9.261	.000
	ICT Education is required for big data usage in education	.572	.033	.835	17.173	.000

a. Dependent Variable: There are significant challenges on implementation on big data usage in educational industry

Table 10 - Regression on ICT education and big data usage in Education sector

From the regression analysis the equation that can be arrived is: Y=0.572X+0. 735. From the equation it can be predicted that people believe when ICT education increases the big data usage also increases.

Relationship between security and standards on big data usage in Sri Lankan Education sector



Correlations

		Lack of Security and standards in the education sector has effect on big data usage	There are significant challenges on implementation on big data usage in educational industry
Lack of Security and standards in the education sector has effect on big data usage	Pearson Correlation	1	.972**
	Sig. (2-tailed)		.000
	N	130	130
There are significant challenges on implementation on big data usage in educational industry	Pearson Correlation	.972**	1
	Sig. (2-tailed)	.000	
	N	130	130

**. Correlation is significant at the 0.01 level (2-tailed).

Table 11 - Correlation between security and standards on big data usage in Education sector

Pearson R value is 0.972 which indicates very strong positive correlation between security standards and big data usage. Additionally, Sig. (2-tailed) value is 0.000 which is lesser than 0.05 that suggest security standards improve big data usage also changes positively. Hence, we can reject null hypothesis and accept where H5: There is relationship between Security Standards and big data usage. Finally, analysis depicts lack of higher security and standards leads to Lack of big data usage and also high security and standards leads to higher big data usage.

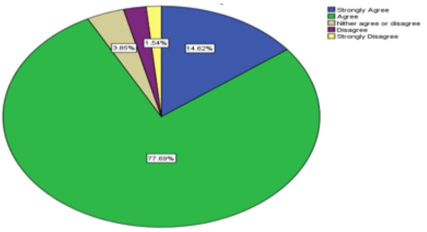
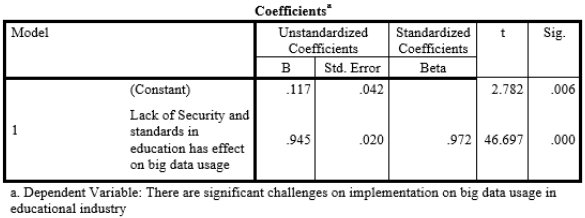


Figure 6 - Opinions about security and standards on big data usage in Education sector

Above pie chart illustrates 77.69% agreed that lack of security and standard in the education sector lead to lack of big data usage whereas only 3.84% disagreed that security and standards are essential for big data usage.

Regression analysis of security and standards on big data usage



Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.117	.042		2.782	.006
	Lack of Security and standards in education has effect on big data usage	.945	.020	.972	46.697	.000

a. Dependent Variable: There are significant challenges on implementation on big data usage in educational industry

Table 12 - Regression on security and standards on big data usage in Education sector

From the information we can derive at the equation Y=0.945X+0.117. It can be understood from the equation that employees in education sector Sri Lanka believe that in future they might consider security and standards as a necessity for big data usage.

DISCUSSION

This study clearly identified that infrastructure, trained workforce, security standards, policies and education of employees are required for big data utilization. Firstly, it is identified that ICT infrastructures such as computers, processors, storage facilities and network facilities are considered vital for education sector to use big data facilities. The data clearly supports that without proper infrastructure, big data implementation is difficult by indicating Pearson R value 0.810 and Sig.2 (tailed) value is 0.000 which is less than 0.5. Furthermore, education sector employees in Sri Lanka would consider that infrastructure is a necessity in future for big data usage according to regression equation: Y=0.546X+0.765. Secondly, it is understood that training the workforce in education sector of Sri Lanka is necessary in order to work with big data and also to encourage big data usage. When workers are trained properly, they will understand how to work with appropriate systems effectively without impacting the whole process. With the Pearson R value identified as 0.834 and sig(2-tailed) value 0.000 which is lesser than 0.5 this suggest that there is high positive correlation between train workforce and big data usage. Furthermore, with the regression equation Y=0.655X+0.552, it could be predicted that education sector employees in Sri Lanka feel that training workforce is a must to encourage big data usage. Thirdly, it is recognized that proper policies need to be implemented by government to encourage big data usage among education sector employees in Sri Lanka. For instance, simple rules and policies need to be implemented to data recording, storing, processing and accessing data so that education sector employees would be motivated to use data. From the data analyzed Pearson R value is identified as 0.777 and Sig (2-tailed) value 0.000 this implies that there is high positive correlation between policies and big data usage. Moreover, education sector employees believe that in future they need simple and supportive policies to encourage big data usage according to regression equation: Y=0.520X+0.809. Moreover, ICT knowledge and skills in Sri Lanka is considered at a lower level, hence it will heavily impact on managing big data. From the information analyzed Pearson R value is at 0.835 and Sig (2-tailed) value is 0.000 which suggest high correlation between ICT education and big data usage in Sri Lanka. This implies knowledge and skills are highly required to implement big data. Even for the future education sector employees will consider knowledge and skills as a requirement for them to implement big data. Finally, education sector employees in Sri Lanka believe that security and standards are a necessity and constantly need to be updated in protecting systems against harmful viruses to effectively implement big data usage. According to opinions given, there is tendency of stealing valuable data and also misuse of data so security and standards are considered highly important for big data usage in Sri Lanka. This is clearly suggesting that from the analyzed data where it shows Pearson R value 0.972 and Sig (2-tailed) value 0.000. Most importantly, according to the regression equation Y=0.945X+0.117 education sector employees perceive that security standards are necessary for big data usage in the future as well.

CONCLUSION

This research mainly focuses on identifying challenges that impact on big data usage in education sector in Sri Lanka. By referring to previous literatures, conceptual model was developed based on identified challenges of big data adaptation. To test whether these challenges essentially impact the big data usage, a quantitative analysis technique was used. To collect the data well-structured online questionnaire was distributed among 130 employees. Obtained information is analyzed through IBM SPSS software to find the correlation and regression. This analysis revealed that Sri Lankan authorities need to focus on infrastructure, trained workforce, security standards, policies and education of employees in order to improve the big data usage. If required actions are not taken to improve the identified challenges, there will be a future trend of lack of big data usage in education sector of Sri Lanka. Moreover, there will be further consequences such as lack of big data usage for decision-making and impact profitability of education sector in Sri Lanka. Additionally, world is becoming globalized rapidly and there will be so much competition from other educational institutes in the world. Thus, big data usage would allow them to effectively understand and adopt to the market changes. Nonetheless, failure to use big data would cause most of the educational institutes in Sri Lanka to drive away from the international market. Finally, Sri Lankan economy is heavily depended on education sector for generating knowledgeable workforce that would contribute to the economy. If proper attention is not given by authorities to improve big data usage, the efficiency and productivity of education sector would hinder. Therefore, it is highly advisable that effective big data usage should be encouraged by overcoming the challenges identified in the research.

RECOMMENDATION

Based on the findings and conclusion, infrastructure, training, policies, ICT education and security should be improved to encourage big data usage. Firstly, Infrastructure can be improved by use of software like Apache Hadoop which is a free open source software that could be used to store and process ample amount of data conveniently. Additionally, government should provide network facilities to all regional and rural areas. Government should also encourage local innovators by providing funding to develop analytic tools for data storing and processing. Moreover, government should develop a system where all educational institutes could purchase necessary infrastructure required for big data implementation at a lesser rate. Secondly, training of workers can be enhanced by providing a system where education sector employees could connect with industry professionals regularly to receive training about big data usage. Another way to increase big data usage is by training the amount of data scientist in the society. When amount of data scientist increases, other parties could obtain the guidance about the complex areas of big data usage. Thirdly, education institutes should enhance policies to encourage big data usage. Education system can change from manual systems to technological systems to record, store and analyze data. Technological systems would support big data usage. Next, Sri Lankan government should establish institute and regulatory frameworks to ensure the privacy and security of sensitive data due to the higher significance of big data utilization. Proper framework might gain trust among top managers of educational institutes to implement big data, mainly because they do not have to worry about the misuse of data and viruses that cause harm to sensitive data. Finally, education of employees needs to be enhanced to encourage use of big data. Government can incorporate computer science, statistics, and mathematics into Sri Lankan educational curriculum from ordinary level to university level. Moreover, implement strategic partnerships with private and public institutions with expertise in big data tools and techniques which allows to facilitate use of big data. Therefore, it could be highly understood necessary precautions and steps need to be taken earliest in order to encourage and motivate educational institutes in Sri Lanka to properly utilize big data in their daily operational activities.

REFERENCES

Ajzen, I. (1988). Attitudes, Personality, and Behavior. The Dorsey Press, Chicago.

Ali-ud-din Khan, M., Uddin, M.F. and Gupta, N. (2014). Seven Vs of Big Data: Understanding Big Data to extract Value. In 2014 Zone 1 Conference of the American Society for Engineering Education (ASEE Zone 1), pp. 3-5.

Barroso, L., Clidaras, J. and Hölzle, U. (2013). The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines, Second edition. Synthesis Lectures on Computer Architecture, 8 (3), pp. 1-154.

Broeders, D., Schrijvers, E., van der Sloot, B., van Brakel, R., de Hoog, J. and Hirsch Ballin, E. (2017). Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data. Computer Law & Security Review, 33 (3), pp. 309-323.

Campbell, A.V. (2007). The Ethical Challenges of Genetic Databases: Safeguarding Altruism and Trust. Kings Law, 18 (2), pp. 227–45.

Dan, S and Roger, C. (2010). Privacy and consumer risks in cloud computing. Computer Law and Security Review, Vol 26, pp. 391-397.

Daniel, B. (2014). Big Data and analytics in higher education: Opportunities and challenges. British Journal of Educational Technology, 46 (5), pp. 904-920.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13 (3), pp. 319.

Davis, F., Bagozzi, R., & Warshaw, P. (1992). Extrinsic and Intrinsic Motivation to Use Computers in the Workplace. Journal of Applied Social Psychology, 22 (14), pp. 1111–1132.

Department of Census and Statistics Sri Lanka. (2018). Computer Literacy Statistics – 2018 (First six months). pp. 1-4.

Economist Report (2008). The future of higher education: how technology will shape learning. A report from the Economist Intelligence Unit.

Eileen McNulty, E. (2016). Understanding Big Data: The Seven Vs. [online] Data Economy. Available at:

Eynon, R. (2013). The rise of Big Data: what does it mean for education, technology, and media research?. Learning, Media and Technology, 38 (3), pp. 237–240.

Ferguson, A. (2017). Policing Predictive Policing. Wash Univ Law Rev. pp. 211–68.

Goodhue, D. and Thompson, R. (1995). Task-Technology Fit and Individual Performance. MIS Quarterly, 19 (2), pp. 213.

Hilbert, M. (2013). Big Data for Development: From Information - to Knowledge Societies. SSRN Electronic Journal.

Jayasree, M. (2013). Data Mining: Exploring Big Data Using Hadoop and Map Reduce. International Journal of Engineering Science Research - IJESR, 04 (1).

Kaisler, S., Armour, F., Espinosa, J. A., Money, W. (2014). Big Data: Issues and Challenges Moving Forward. 46th Hawaii International Conference on System Sciences, 46 (1).

Kernochan W. (2013). 4 barriers to big data success and ways to overcome them. Enterprise Apps Today.

Laney D. (2001). 3D Data Management: Controlling Data Volume, Velocity, and Variety [Online]. META Group. Pp. 1-4.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., Angela Hung Byers, Mckinsey Global Institute and Al, E. (2011).

Petkovics, I., Tumbas, P., Matković, P. and Baracskai, Z. (2014). Cloud computing support to university business processes in external collaboration. 11 (3), pp. 181-200.

Protecting data privacy in health services research. (2000). Washington, D.C.: National Academy Press.

Shacklock, X. (2016). From Bricks to Clicks. The potential of data and analytics in higher education (Report). Higher Education Commission: UK.

Shapiro, C. and Varian, H.R. (2010). Information rules : a strategic guide to the network economy. Boston, Mass.: Harvard Business School Press.

Shitut, N. (2017). 5 Skills You Need to Know to Become a Big Data Analyst. [Online]

Thompson, R., Higgins, C., & Howell, J. (1991). Personal Computing: Toward a Conceptual Model of Utilization. MIS Quarterly, 15 (1), pp. 124–143.

UNIFIED DIGITAL AUDIO AND DIGITAL VIDEO BROADCASTING SYSTEM USING ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM) SYSTEM

Drakshayini M N, Dr. Arun Vikas Singh

ABSTRACT

The foremost objective of Digital Audio Broadcasting (DAB) is to provide high definition radio which offers very high audio quality and data services to the fixed and mobile receivers. Digital video broadcasting (DVB) is the set of standard for the broadcast transmission of digital television signal and DVB is the replacement for existing analogue television transmission. Orthogonal Frequency Division Multiplexing (OFDM) system is an efficient multicarrier digital modulation technique and which compromises high spectral efficiency. This paper presents the unified approach for DAB and DVB using OFDM system. Bit Error Rate (BER) performance analysis of DAB and DVB system is performed and also Bit Error Rate (BER) performance analysis of unified DAB and DVB is performed using OFDM system. Comparisons are made between the theoretical values and with the obtained results. Keywords: OFDM, DAB, DVB, QAM, BER, SNR.

INTRODUCTION

Present Wireless communication demands high spectral efficiency and high robustness. OFDM is an efficient digital multicarrier modulation technique which provides high spectral efficiency and high robustness [1]. Applications of OFDM are DAB, DVB, ADSL, LTE, Wireless LAN standards and Digital Radio Mondale etc [2-3]. This paper presents the unified approach for DAB and DVB using OFDM system. Bit Error Rate (BER) performance analysis of DAB and DVB system is performed and also Bit Error Rate (BER) performance analysis of unified DAB and DVB is performed using OFDM system. Comparisons are made between the theoretical values and with the obtained results. Unified system is developed using MATLAB programming and simulation results are observed, for the real time audio and video input, output is obtained with minimal bit error rate.

Orthogonal frequency division multiplexing

OFDM is a method of multicarrier digital modulation technique in which a signal is divided into several narrow band channels at different frequencies [4]. Every sub channels are modulated by using subcarriers of different frequencies. OFDM modulation is used in many applications because it provides high efficiency in combating multipath fading and also provides high data-rate transmission [5]. Hence efficient utilization of bandwidth is possible with OFDM when compared to conventional modulation schemes. In OFDM the subcarriers are chosen in such a way that they are orthogonal to each other so that cross talk among subcarriers can be eliminated. Equation (1) describes the orthogonally of two signals which are linearly independent.

$$\int_x^y X_p(t)\, X^*_q(t)\, dt = \begin{cases} K \; for \; p = q \\ 0 \; for \; p \neq q \end{cases} \qquad (1)$$

Where [x, y] is one symbol period.

OFDM symbol is defined mathematically in equation (2).

$$Y(n) = 1/N \sum_{k=0}^{N-1} y(k)\; e^{j2\pi kn/N} \qquad 0 \leq n \leq N - 1 \qquad (2)$$

Where N = FFT length, y(k) = Complex value data, k = kth element of the array.

Figure 1 illustrates the block diagram of the OFDM systems. symbol mapping block performs one to one mapping takes binary data input and each bit is mapped to complex valued number on the constellation. The various types of modulation can be used in this stage is Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), 16-Quadrature Amplitude Modulation (QAM), 64-Quadrature Amplitude Modulation, 128-Quadrature Amplitude Modulation and 256-Quadrature Amplitude Modulation. On the receiver, symbol de-mapping transforms the complex valued number into the binary data with respect to their phase and amplitude values. Serial symbol sequences are converted into parallel sequence in serial to parallel converter block and also sequence of data symbols are reorganized into a number of smaller sub–set of data symbols in this block. Across the receiver parallel to serial converter block are used to convert parallel data sequence into serial sequence of OFDM symbols and also used to reorganize the data symbol to its original form. In the pilot insertion block pilot carriers are interleaved into the OFDM Symbol. Pilot carrier is a non-information carrier and pilot carrier does not carry any information. Pilot carrier is the complex valued number and it is a point represented on the constellation. Basically pilot carriers are used to overcome the frequency and timing error and also in channel estimation stage pilot carriers are used for the estimation where exactly the OFDM symbol begins. Inverse Fast Fourier Transform (IFFT) block generates an OFDM symbol, These OFDM symbols are real valued and multiplexed subcarriers.

IFFT transforms frequency domain symbols into time domain waveform. IFFT produces the combined set of subcarriers which are multiplexed and are orthogonal to each other.

The guard interval insertion block affixes a cyclic prefix to the beginning of every OFDM which reduces the effects of Inter symbol Interference (ISI) and Inter carrier Interference (ICI) [6].

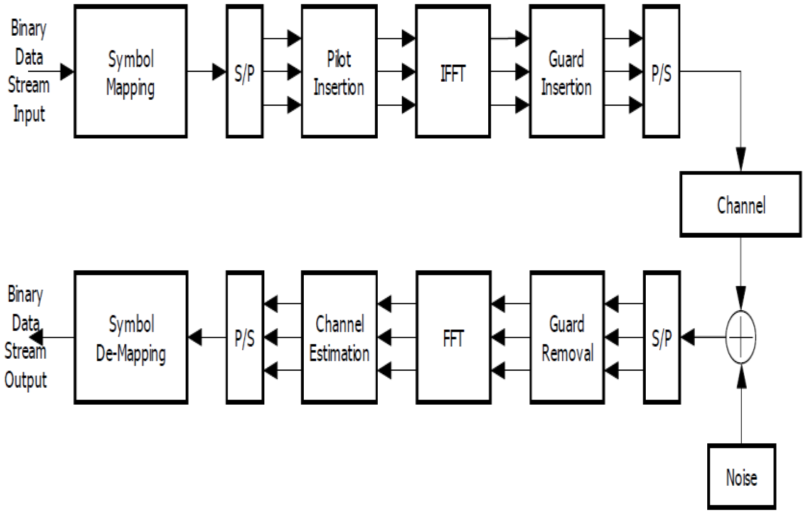


Figure 1: Block diagram of typical Orthogonal frequency division multiplexing System.

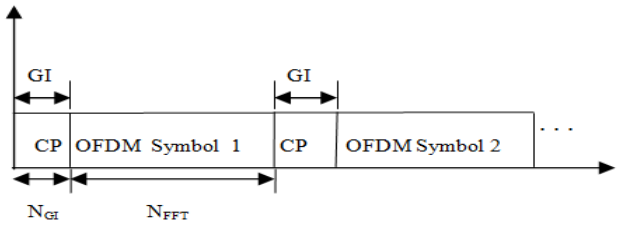


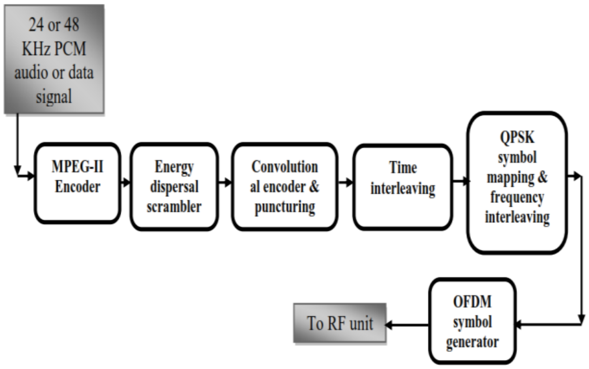
Figure 2: Time domain representation of a sequence of Orthogonal frequency division multiplexing symbols with cyclic prefix guard interval.

Figure 2 illustrates the OFDM symbol with cyclic prefix guard interval. In the receiver guard removal block eliminates the cyclic prefix from the OFDM symbol.

Parallel to serial conversion stage transforms the OFDM Symbols into the serial sequence of OFDM symbols which is real-valued base band OFDM waveform. At the receiver OFDM waveforms are converted back to parallel sequence.

The length of serial sequence OFDM is defined in equation (3)

$$Z_{len} = S\,[N_{GI} + N_{FFT}] \qquad (3)$$


24 or 48 KHz PCM audio or data signal
MPEG-II Encoder
Energy dispersal scrambler
Convolutional encoder & puncturing
Time interleaving
QPSK symbol mapping & frequency interleaving
OFDM symbol generator
To RF unit

where Zlen= OFDM frame length, S = Number of OFDM symbols, NFFT = Duration of OFDM symbol, NGI = Length of guard interval.

Review on digital audio broadcasting

FM has many advantages over AM but FM suffers from Multipath fading and ISI. FM is suitable for fixed reception than mobile reception since FM suffers from loss of broadcasting quality during mobile reception. These issues can be addressed in Digital Audio Broadcasting (DAB). DAB can be defined as digital radio or high definition radio which broadcasts wide ranges of radio services from studio to receiver. DAB is designed to obtain high quality digital audio programs and data services to fixed, mobile and handy devices. It was established in 1990s by Eureka 147 DAB.

Figure 3: DAB transmitter block diagram

Figure 3 illustrates the transmitter block diagram of the DAB system. The overall DAB transmission can be distributed to the number of functional blocks and these blocks process the input signal and produces the complete DAB signal. The audio signal or data signal is given as input to MPEG layer-2 encoder which generates the encoded data. In order to make sure that the appropriate energy dispersal in the transmitted signal, distinct inputs of the energy dispersal scramblers is to be scrambled with the help of modulo-2 addition and PRBS.

Punctured convolutional encoder does the forward error correction and convolutional encoding by taking the input scrambled bit stream. Interleaving block rearranges the coded bit-stream. Time interleaving increase the robustness of the transmitted data. Time interleaved data is then fed to QPSK modulation block which takes binary data stream input and each bit is represented as complex valued number on the constellation and performs one to one mapping. After the QPSK modulation symbols are given to OFDM block where final DAB transmission signals are generated [7].

Review on digital video broadcasting

Figure 4 illustrates the transmitter block diagram of the DVB system. Transmission and storage of audio, video and programs are performed by Source coding and MPEG2 and these are standard container format. Program stream (PS) is just a container format for audio, video and data and performs multiplexing of audio, video and data. Transport stream (TS) is a Container format for transmission as well as storage of audio, video and data. Example movie, news cart, sports news which displays on TV. Encoder block provides the first level of protection in the transmitter. Encoder block helps in detecting and correcting multiple symbol errors. The type of encoder used is the convolution encoder. Convolution encoders are used for error detection and error correction. Block inter leaver is also called random inter leaver which rearranges the data sequence to provide the robustness.

Mapper performs symbol mapping on one to one basis. QAM is the combination of both amplitude and phase modulation. 16 QAM refers to number of message points on the constellation, it is 4 bits per symbol(1/4 bit rate). Existing system uses QAM modulation so 16 constellation points are used [8].

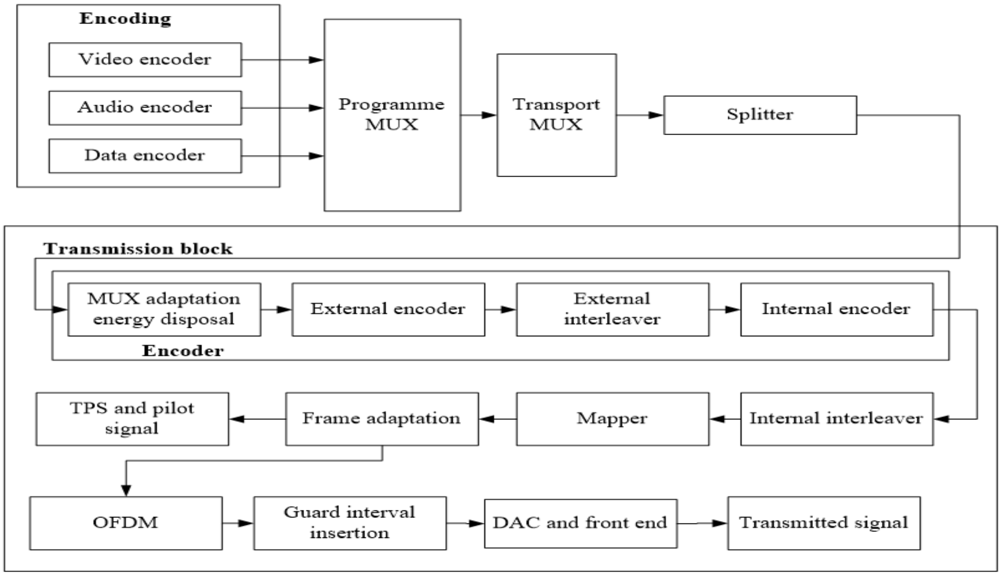


Figure 4: Block diagram of DVB

Performance analysis DAB system using MATLAB Simulation

DAB system is modeled and simulated using MATLAB programming. The objective of this simulation is to evaluate the BER and SNR of the DAB system using convolutional coding using puncturing method. Puncturing method lets the encoding and decoding of higher rate codes by standard rate ½ encoders and decoders. The simulation parameters for DAB mode II are listed in Table 1. Frame based processing is done in this simulation model under AWGN channel for the performance analysis. DAB frame structure is designed by using one synchronization channel for transmission frame synchronization and transmitter identification, three Fast Information Channel [FIC] used for quick access of information in the receiver and 72 Main Service Channel [MSC] used to convey audio and data services.

Table 1: Mode II Parameters of DAB system

Parameter	Value
Number of Subcarriers	384
Subcarrier Spacing	4 kHz
Transmission Frame duration	24 ms
Symbol duration	321 µs
Guard Interval	62 µs
Null Symbol duration	324 µs
OFDM symbols per transmission frame	76

OFDM Symbols with SC data	1
OFDM Symbols with FIC data	3
OFDM Symbols with MSC data	72

This section illustrates the simulation results of DAB system for AWGN channel. An audio input is given to the DAB system which is shown in figure 5. An audio signal is processed and transmitted under AWGN fading channel. Figure 6 illustrates BER vs. SNR for DAB system.

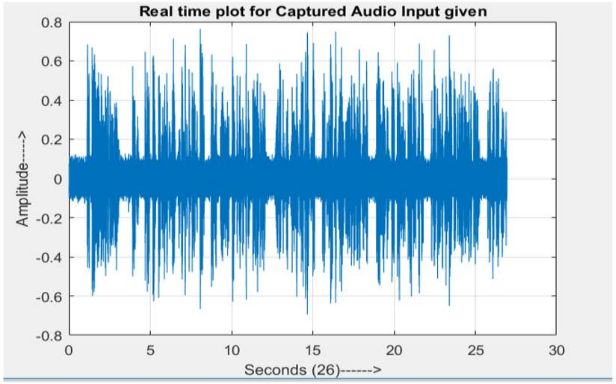


Figure 5: Audio input to DAB system

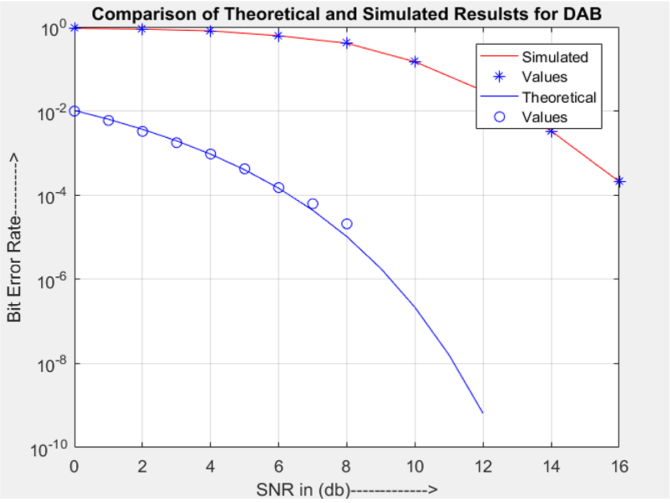


Figure 6: BER vs. SNR for DAB system under AWGN channel

DVB system using MATLAB Simulation

Block diagram of the DVB system is as shown in figure 4. Initially the video is captured which is divided into a finite number of frames. The frames are then converted from parallel to serial data.

Table 2: Mode II Parameters of DAB system

Parameter	Value
Number of Subcarriers	2K mode:1705 8K mode:6817
Subcarrier Spacing	2K mode:4464 8K mode:1116
Channel spacing B[MHZ]	6,7,8
Symbol length, Tu(µs)	2K mode:224 8K mode:896
Guard Interval	1/4, 1/8, 1/16, 1/32
Sub-carrier spacing Δf=1/ Tu Hz	2K mode:4464 8K mode:1116
Net bit Rate, R(Mbit/S)	4.98-31.67(typically 24.13)
FFT size [K=1024]	2K 8K
Sub-carrier modulation Scheme	QPSK 16QAM or 64QAM
Symbol length, Tu(µs)	2K mode:224 8K mode:896

The data is then encoded using the cyclic encoder which is then passed into an interleaver. Here for protection two levels of encoders are used which are external encoder and internal encoder. Two levels of interleaver are used here which are external interleaver and internal interleaver. The interleaved data is then passed into a modulation block. Modulation method chosen is 16 QAM. The modulated signal is then passed into an OFDM block which performs the modulation and multiplexing. The simulation parameters for DVB – T are listed in Table 2.

This section illustrates the simulation results of DVB system for AWGN channel. A video input is transmitted under AWGN channel. Figure 7 illustrates BER vs. SNR for DVB system.

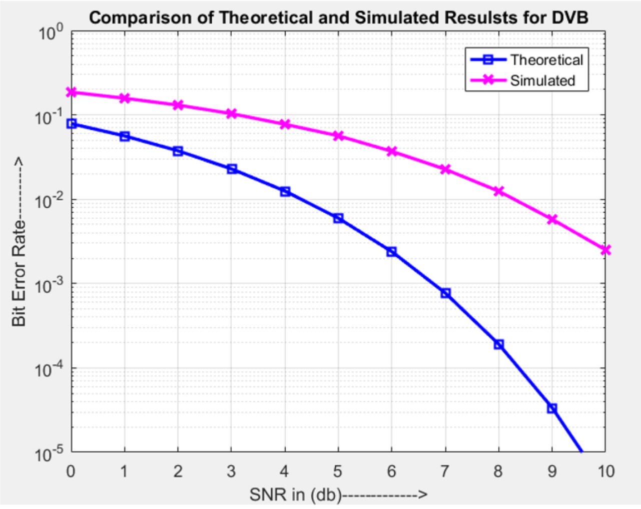


Figure 7. BER vs. SNR for DVB system under AWGN channel

Unified DAB and DVB system using MATLAB Simulation

This section illustrates the simulation results of Unified DAB and DVB system for AWGN channel. A video input is transmitted under AWGN channel. Figure 8 illustrates BER vs. SNR for Unified DAB and DVB system.

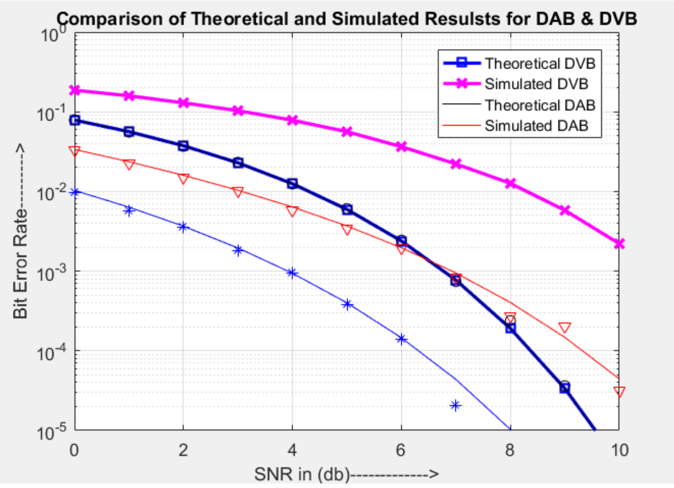


Figure 8. BER vs. SNR unified DAB and DVB system

CONCLUSION

A simulation based performance analysis of DAB and DVB system and also unified DAB and DVB system is presented in this paper. Many applications use OFDM system because of its high spectral efficiency. Outcome of the system will be confirmed by multiple and extended simulation based experiments in OFDM. The proposed system will reduce the design complexity, conserves design time, Power consumption, reduced cost as compared to multiple designs for different standards.

REFERENCES

T. Hwang, C. Yang, G. Wu, S. Li and G. Y. Li, "OFDM and Its Wireless Applications: A Survey," in IEEE Transactions on Vehicular Technology, vol. 58, no. 4, pp. 1673-1694, May 2009.

A. S. Bhosle and Z. Ahmed, "Modern tools and techniques for OFDM development and PAPR reduction," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 290-292.

R. Umar, F. Yang and S. Mughal, "BER performance of a polar coded OFDM over different channel models," 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, 2018, pp. 764-769.

N. LaSorte, W. J. Barnes and H. H. Refai, "The History of Orthogonal Frequency Division Multiplexing," Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, New Orleans, LO, 2008, pp. 1-5.doi: 10.1109/GLOCOM.2008.ECP.690 doi: 10.1109/TLA.2016.7430062

C. Yu, C. H. Sung, C. H. Kuo, M. H. Yen and S. J. Chen, "Design and implementation of a low-power OFDM receiver for wireless communications," in IEEE Transactions on Consumer Electronics, vol. 58, no. 3, pp. 739-745, August 2012. doi: 10.1109/TCE.2012.6311312

Drakshayini M N, Dr. Arun Vikas Singh, “A Review on Reconfigurable Orthogonal Frequency Division Multiplexing (OFDM) System for Wireless Communication”, 2nd InternationalConference on Applied and

Theoretical Computing and Communication Technology(iCATccT), 978-1-5090-2399-8/16/$31.00 c, 2016 IEEE.

Drakshayini M. N, Dr. Arun Vikas Singh "An Efficient Orthogonal Frequency Division Multiplexing (OFDM) System and Performance Analysis of Digital Audio Broadcasting (DAB) System", International Journal of Computer Applications (0975 – 8887) Volume 148 – No.8, August 2016.

Drakshayini M N, Arun Vikas Singh, Vyshanava Nandini S, "Performance Of Digital Video Broadcastingterrestrial (Dvb-T) Using Ofdm As System", IJRET: International Journal of Research in Engineering and Technology, eISSN: 2319-1163, pISSN: 2321-7308, Volume: 05 Special Issue: 04, ICESMART-2016, Ma