IJIRMPS

International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences

Multidisciplinary • Peer Reviewed • Online
Open Access • Widely Indexed • Bi-monthly International
Journal • Since 2013

VOLUME 8
ISSUE 3

May-June 2020

☞ ijirmps.org
✉ editor@ijirmps.org
✆ +91 87 585 383 22

E-ISSN 2349-7300
9 772349 730016

Vejalpur, Ahmedabad - 380051, Gujarat, India.

The **International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences** (**IJIRMPS**) is a **multidisciplinary, bi-monthly, online, peer reviewed, widely indexed, openly accessible international journal** and helping researches to share their research information **since 2013**.

Our aim is to explore advances in research pertaining to applied, theoretical and experimental technological studies. The goal is to promote scientific information interchange between researchers, developers, engineers, students and practitioners working all around the world. We provide an opportunity for practitioners and educators of all fields to exchange research evidence, models of best practice and innovative ideas.

Research Areas

As a multidisciplinary journal, we are accepting Research work from all branches of **Engineering**, all branches of **Ph.D.**, all fields of **Medical & Pharmacy**, all branches of **Business Administration (MBA)**, all disciplines of **Physical Sciences** and all streams of **Computer Applications (MCA)**.

Here is the wider list of all the disciplines:

- Engineering
- Medical / Pharmacy
- Business Administration
- Physical Science
- Computer Applications
- Arts
    - Drawing
    - Fashion
    - Movies / Music / TV
- Biology
    - Agriculture / Botany
    - Bio + Chemistry
    - Genetics / Molecular
    - Geology
    - Medical / Physiology
    - Zoology
- Chemistry
    - Petroleum
    - Pharmacy
- Computer
    - Artificial Intelligence / Simulation / Virtual Reality
    - Automation / Robotics
    - Data / Information
    - Design
    - Electronics
    - Logic
    - Network / Security
- Mathematics
    - Economy / Commerce
    - Logic
    - Maths + Physics
    - Statistics
- Sociology
    - Administration / Law / Management
    - Archaeology / History
    - Banking / Finance
    - Data / Information / Statistics
    - Economics
    - Education
    - Geology
    - Health
    - Home Science
    - Intelligence / Security
    - Journalism / Media
    - Linguistic / Literature
    - Philosophy / Psychology / Religion
    - Politics
    - Sports
    - Tourism / Transport
- Physics
    - Astronomy
    - Civil Engineering
    - Electric
    - Energy
    - Mechanical Engineering
    - Nano Technology / Nuclear

INDEX

Effect on productivity of silk *(Antheraea mylitta*) due to changes Environmental Factors in Ambikapur Surguja District CG

[1]Meena Singh, [2]Dr.Manoj Singh

Kalinga University Kotani,
New Raipur, 492002, Chhattisgarh, India

***Abstract*: Ambikapur is a city is surguja district of Chhattisgarh. The oldest districts of the Indian state of Chhattisgarh in the east.Central Indian Ambikapur is also the divisional headquarters of surguja district which consists of the five districts of surguja, koriya, balrampur, surajpur and jashpur. Ambikapur is located at 23^{0} 37' 25"to 24^{0} 6' 17"North latitude and 81^{0} 34'40"to 84^{0} 4' 40" east longitude, 244.62 km long east to westand 167.37 broad north to south. This land has as area of about 16359 sqkm. Ambikapur Tasar silkworm areas of 10 hectares in Arjuna plants culture. In current issue changing global climate seems to be one of the major hindrance in the effect on productivity of silkworm *Antheraea mylitta.* Various climatic factors such as temperature, humidity, light, air, wind etc. The present experimental analysis conducted in environment factors the role and influence of temperature and humidity in the growth of pupa from larvae of silkworm Antheraea mylitta.It is also observed that weight of pupa and shell reared at temperature 22-26 ^{0}c and 80-85% realative humidity are more.The present observation of the effect on productivity of silk due to environmental factors in Ambikapur district surguja.The study includes the steps to be taken for the management of condition and improved quality and quality of silk production in future.**

***Keywords:* Abiotic factors, temperature, humidity, rainfall, wind, diseases, pest.**

- Corresponding Author
- Name:Meena Singh
- Phone:9131090344
- Email: nevaan.ambikapur@gmail.com

Introduction

Sericulture is the Cultivation of silk through rearing of silkworm.It is an agro-based industry.sericulture also includes the practical aspects such as increasing productivity of land as well as labour,stabilization of cocoon production improvement of silk,fabric and generating profitable income for rural poor people.The discovered in china between 2600 and 2700 BC.Today china and India are two main producer with more than 60% of the worlds.Annual production India is the second largest producer of silk in world and contributes 18% of the total world raw silk production.In India silk is available with varieties such as Mulberry,Eri,tasar and munga.Tasar silkworm are reared traditionally by the tribes of Madhya Pradesh,Bihar,and Orissa;Munga and eri silk are produced exclusively in Assam.Mulberry silk is produced extensively in the states of Karnataka,West Bengal,Jammu & Kashmir.Sericulture or silk production is the breeding and management of silkworms for the commercial production of silk.It is an Economically important insect being a primary producer of silk.All the section of sericulture Industry viz; cultivation silkworm seed production,silk rearing,reeling and weaving of the silk and collection of by products and its processing provide a large scale employment there by a source of livelihood for the rural and tribal peopal(Gregory 1914 and srivastava 2003). Chhattisgarh state is a very high quality kosa silk production.silk way of life in Chhattisgarh has become an in separable part of Indian culture and tradition should be considered for rural management and development(Dewangan etal;2011).Presently in chhattisgarh three types of silk viz; Mulberry,Tasar culture furthermore it is practiced especially in trible belts of surguja,Raigarh,Bilaspur,Korba,Bastar district of the Chhattisgarh state Keeping in view of the above facts into consideration.The silk is preferred over all other types of fibres due to its remarkable properties like water absorbency heat ressistance dying efficiency and luster.Factor mainly influence the physiology of insects are temperature and humidity.The adaptability is quite different from those of wild silkworm;Temperature,humidity,light,wind Rainy effect on the physiology of silkworm depending upon the combination of factors and development stages affecting growth development productivity and quality of silk.The present study of silk production effect on due to changeable environmental factors is possible at the outdoor condition culture also climax included future strategies to be taken for the management best successful silk production by best environmental factor conditions.

Research Methodology:-

Fig 1: Terminalia arjuna food plant

Systematic position

- Kingdom - Planatae
- Phylum - Magnoliophyta
- Class - Magnoliopsida
- Order - Myrtales
- Family - Combretaceae
- Genus - *Terminalia*
- Species - *arjuna*

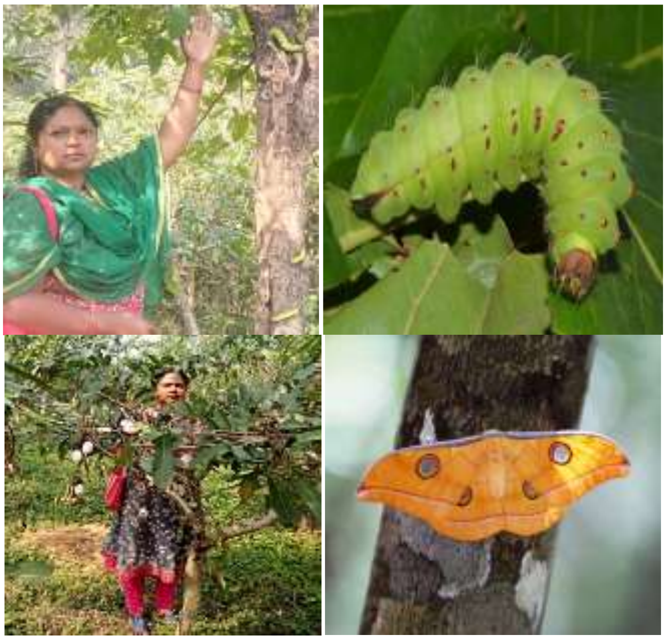


Fig 2: *Antheraea Mylitta* –Fifth Instar Larva, cocoon, Silkmonth

Systematic Classification:

- Kingdom - Animalia
- Phylum - Anthropoda
- Class - Insecta
- Order - Lepidoptera
- Family - Saturniidae
- Genus - *Antheraea*
- Species - *Mylitta*

The present work was sericulture center of Ambikapur Surguja district during 2018-2019.The Chhattisgarh state represented by climate is tropical.It is hot and humid because of its proximity to the tropic of cancer and its dependence on the man soons for rains.Summer temperature can reach up 45^0c(113'F).The man soon season is from late June to October and is a welcome respite from the head.The average rainfall of Chhattisgarh is 1292mm.Winter is from November to January and is a good time to visit

Chhattisgarh winters are pleasant with low temperature and less humidity.Temperature increases from march to June but by the end of June,the temperature decreases as the mansoon moved.In July Temperature remain about 27 ^{0}c -27 ^{0}c,there is no variation in the temperature in the month of September and October,but in the most of September and October,when the sky is clear,there is a slight increase in the temperature.There are 3 seasons in the Chhattisgarh.

1.**Hot season** - this season starts from march and goes up to mid june.In the month of June when the sun shines vertically over the tropic of cancer; due to high temperature.The pressure decreases and temperature rises to as much as 42 ^{0} 5’c in some parts of the state.

2**.Rainy season** - From mid June to September Ambikapur,Bilaspur and Bastar experiences rain more than 100 c.m.

3**.Winter season** – It starts from November to January.It September Temperature starts decreasing this is caused due to rainfall and humidity and winter arrives in November.

The Surguja district enjoy tropical climate which characterized by a hot summer and well distributed rainfall.The present work was in Ambikapur Tasar Silkworm host plant Terminalia arjuna was selected for the study.The period of sampling will collected from sericulture center of Ambikapur was 1st week of July 2018,total areas covered under Tasar fields is about 10 hecters through effective area is about 8 hecters and selected to 1st crop 50 Trees (2 plot) in Terminalia arjuna.Each plots consisted of approximately 25 trees. At First Tasar silkworm eggs has been taken at 10 dfl after that having keeping it in tray,then larves began to come out. After being observation of environmental factors,temperature,humidity,speed of wind.Then processes of making of cocoon is observed.After that doing analysis of cocoons production is done.After this crop is totally prepared.All the eggs have been taken in equal quantity.In these three crops 2018-2019,the whole process is completed.After obserningof these one year we know the maximum production of silk.All these environmental factor effects of production capacity and they determine the quantity of silk

1st Crop - Rearing Performance

3-Jul-18	12-Aug-18	**Meteorological Data (Day-wise) at Ambikapur Antheraea mylitta Feed in Arjuna Plant 2018-19**									
	Date	**T.MAX**	**T.MIN**	**R Fall (mm)**	**RH-I**	**RH-II**	**W SPEED**	**Rainy Day**	**No. of larva**	**Mor.No.**	**Mor.%**
	1-Jul-18	31.2	24.2	0.0	83	58	4.7				
	2-Jul-18	31.4	21.2	61.0	98	72	4.5	1			
1st crop	3-Jul-18	30.0	21.4	4.8	90	74	4.2	1			
	4-Jul-18	29.2	21.1	10.3	95	73	6.8	1			
	5-Jul-18	29.5	23.5	0.0	84	67	7.3				
	6-Jul-18	30.5	23.6	0.0	84	52	3.7				
	7-Jul-18	34.0	21.5	39.4	98	59	3.5	1			
	8-Jul-18	33.0	25.0	0.0	85	59	1.6				
	9-Jul-18	33.5	24.5	0.0	88	74	2.9				
1st larva*	10-Jul-18	31.2	22.9	44.0	98	68	2.8	1	1800	140	7.8
	11-Jul-18	31.2	23.7	0.0	92	66	2.3				
	12-Jul-18	31.7	24.7	0.4	94	84	2.7				
	13-Jul-18	29.5	24.5	2.3	94	76	1.4				
	14-Jul-18	30.2	23.2	15.3	95	77	2.7	1			
	15-Jul-18	29.0	24.4	4.2	94	66	1.7	1			
2ndlarva*	16-Jul-18	31.7	23.8	6.2	97	70	3.9	1	1660	125	7.5
	17-Jul-18	30.5	23.5	23.7	95	91	4.4	1			
	18-Jul-18	27.5	23.5	44.8	98	98	4.3	1			
	19-Jul-18	25.0	22.6	24.7	98	84	3.7	1			
	20-Jul-18	28.0	23.2	30.0	98	71	1.9	1			
3rd larva*	21-Jul-18	31.6	21.5	19.8	98	80	3.2	1	1535	60	3.9
	22-Jul-18	30.3	23.0	0.2	93	100	3.2				
	23-Jul-18	25.0	23.0	39.6	98	87	4.5	1			
	24-Jul-18	26.5	22.6	0.0	92	79	11.0				
	25-Jul-18	27.6	22.5	15.4	97	92	9.8	1			
	26-Jul-18	25.2	22.1	32.4	100	98	7.9	1			
4th larva*	27-Jul-18	24.6	21.0	6.6	98	89	3.6	1	1475	52	3.5
	28-Jul-18	26.0	22.2	4.4	90	73	7.4	1			

	29-Jul-18	28.5	22.2	3.7	98	98	4.7	1			
	30-Jul-18	25.0	22.1	22.2	95	75	3.6	1			
	31-Jul-18	28.5	22.5	0.0	86	87	4.4				
	1-Aug-18	26.0	21.4	0.4	92	86	6.6				
	2-Aug-18	25.2	20.8	10.0	98	86	7.9	1			
5th larva*	3-Aug-18	26.0	23.2	0.1	86	79	4.5		1423	11	0.8
	4-Aug-18	27.6	22.5	0.0	89	67	3.4				
	5-Aug-18	30.5	23.5	5.0	87	57	2.6	1			
	6-Aug-18	30.0	23.2	0.0	93	78	1.8				
	7-Aug-18	27.5	21.5	23.8	98	100	2.2	1			
	8-Aug-18	25.5	22.5	19.4	92	65	2.2	1			
	9-Aug-18	30.2	22.6	1.2	83	89	5.7				
	10-Aug-18	27.6	23.5	1.0	97	80	2.4				
	11-Aug-18	29.3	22.5	11.6	97	80	2.2	1			
	12-Aug-18	29.6	23.0	0.0	92	73	2.0				
Total									1412	388	
Prod.%									78.44%		

2nd Crop - Rearing Performance

3-Sep-18	9-Oct-18	**Meteorological Data (Day-wise) at Ambikapur Antheraea mylitta Feed in Arjuna Plant 2018-19**									
	Date	**T.MAX**	**T.MIN**	**R Fall (mm)**	**RH-I**	**RH-II**	**W SPEED**	**Rainy Day**	**No. of larva**	**Mor.No.**	**Mor. %**
2nd crop	3-Sep-18	29.2	21.2	17.6	93	86	4.2	1			
	4-Sep-18	25.5	22.5	0.0	92	74	4.7				
	5-Sep-18	28.8	21.6	11.0	98	90	4.6	1			
	6-Sep-18	25.5	22.2	22.6	98	73	6.8	1			
	7-Sep-18	29.0	21.5	26.2	100	97	2.0	1			
	8-Sep-18	24.2	20.7	11.4	93	75	3.4	1			
	9-Sep-18	27.0	21.9	0.0	95	84	3.7				
1st larva*	10-Sep-18	28.5	23.0	0.8	97	64	3.0		1500	90	6
	11-Sep-18	29.5	22.4	0.0	87	61	2.1				
	12-Sep-18	30.4	21.8	0.0	84	64	2.3				
	13-Sep-18	29.5	22.3	0.4	92	72	3.0				
	14-Sep-18	28.8	21.5	6.7	93	60	2.9	1			
2nd larva*	15-Sep-18	31.0	22.5	0.0	89	58	2.6		1410	25	1.8
	16-Sep-18	30.8	21.6	0.0	92	62	1.6				
	17-Sep-18	31.0	22.0	0.0	92	62	2.0				
	18-Sep-18	29.8	21.9	0.0	92	54	1.6				
3rd larva*	19-Sep-18	32.0	21.5	0.0	92	55	1.4		1385	18	1.3
	20-Sep-18	31.3	19.8	0.0	93	61	2.0				
	21-Sep-18	29.8	20.5	1.6	93	77	4.2				
	22-Sep-18	27.2	20.7	0.0	84	67	6.9				
	23-Sep-18	29.6	20.6	0.0	80	60	4.7				
4th larva*	24-Sep-18	30.2	20.5	0.0	88	63	3.0		1367	10	0.7
	25-Sep-18	32.0	22.0	0.0	90	56	3.7				
	26-Sep-18	32.0	20.7	0.0	92	48	2.9				

	27-Sep-18	31.6	21.0	0.0	90	47	3.5				
	28-Sep-18	33.0	20.7	0.0	84	43	3.4				
	29-Sep-18	33.2	19.0	0.0	77	49	1.4				
5th larva*	30-Sep-18	32.0	19.7	0.0	85	49	1.6		1357	7	0.5
	1-Oct-18	32.0	18.6	0.0	80	39	1.5				
	2-Oct-18	33.2	19.2	0.0	71	38	1.7				
	3-Oct-18	33.2	18.7	0.0	69	37	1.8				
	4-Oct-18	33.0	18.0	0.0	71	36	1.8				
	5-Oct-18	33.0	19.0	0.0	81	37	1.2				
	6-Oct-18	33.2	18.1	0.0	88	37	1.6				
	7-Oct-18	32.6	17.8	0.0	87	32	1.3				
	8-Oct-18	32.0	17.0	0.0	75	37	1.0				
	9-Oct-18	32.5	15.5	0.0	76	34	0.6				
Total									1350	150	
Prod.%									90.00%		

3rd Crop –Rearing Performance

5-Nov-18	31-Jan-19	**Meteorological Data (Day-wise) at Ambikapur Antheraea mylitta Feed in Arjuna Plant 2018-19**									
	Date	**T.MAX**	**T.MIN**	**R Fall (mm)**	**RH-I**	**RH-II**	**W SPEED**	**Rainy Day**	**No. of larva**	**Mor. No.**	**Mor.%**
3rd Crop	5-Nov-18	30.0	15.6	0.0	90	45	3.1				
	6-Nov-18	30.8	17.6	0.0	93	42	2.1				
	7-Nov-18	30.2	12.4	0.0	62	30	1.4				
	8-Nov-18	30.5	10.0	0.0	93	29	1.6				
	9-Nov-18	28.4	9.0	0.0	84	28	1.3				
	10-Nov-18	28.6	9.0	0.0	95	34	1.6				
	11-Nov-18	27.8	9.1	0.0	95	34	1.4				
	12-Nov-18	26.9	9.0	0.0	95	31	1.4				
	13-Nov-18	27.0	10.5	0.0	86	29	2.0				
	14-Nov-18	28.5	11.0	0.0	89	26	1.6				
	15-Nov-18	30.0	12.5	0.0	81	31	1.7				
	16-Nov-18	29.8	13.3	0.0	74	29	2.0				
	17-Nov-18	29.5	12.3	0.0	91	33	3.1				
	18-Nov-18	27.2	10.5	0.0	86	26	1.6				
	19-Nov-18	28.0	10.0	0.0	91	35	1.3				
	20-Nov-18	29.0	11.0	0.0	87	25	1.5				
1st larva*	21-Nov-18	29.8	10.5	0.0	91	30	1.0		1680	300	17.85
	22-Nov-18	29.0	9.9	0.0	91	32	1.9				
	23-Nov-18	27.0	7.8	0.0	90	32	1.9				
	24-Nov-18	27.2	8.0	0.0	93	31	1.6				
	25-Nov-18	25.0	7.0	0.0	95	34	1.6				
	26-Nov-18	25.5	7.3	0.0	92	32	1.8				
	27-Nov-18	25.3	8.3	0.0	93	38	1.2				
	28-Nov-18	27.0	11.3	0.0	87	44	1.2				
	29-Nov-18	26.5	10.8	0.0	93	43	1.5				
	30-Nov-18	26.2	10.0	0.0	89	43	1.2				
	1-Dec-18	25.5	9.2	0.0	93	34	1.0				
	2-Dec-18	24.1	7.6	0.0	97	40	1.1				
	3-Dec-18	24.2	8.5	0.0	98	34	1.0				
	4-Dec-18	25.0	8.6	0.0	93	41	0.9				
	5-Dec-18	24.1	10.0	0.0	85	43	1.0				

	6-Dec-18	23.9	8.0	0.0	98	38	0.7				
	7-Dec-18	25.0	7.7	0.0	93	32	1.4				
	8-Dec-18	24.2	8.7	0.0	72	39	1.6				
	9-Dec-18	24.9	6.0	0.0	92	30	1.1				
2nd larva*	10-Dec-18	25.5	9.0	0.0	86	49	1.0		1380	195	14.13
	11-Dec-18	25.5	13.1	1.2	83	58	1.4				
	12-Dec-18	25.0	11.0	0.0	89	49	1.1				
	13-Dec-18	24.2	9.2	0.0	91	32	0.8				
	14-Dec-18	25.8	12.0	0.0	93	33	1.1				
	15-Dec-18	23.8	7.0	0.0	95	39	2.2				
	16-Dec-18	22.0	6.0	0.0	93	36	1.8				
	17-Dec-18	22.0	11.6	0.5	95	98	1.6				
	18-Dec-18	15.0	11.0	40.8	93	88	3.5	1			
	19-Dec-18	16.0	7.5	0.0	87	57	1.0				
	20-Dec-18	20.0	6.6	0.0	92	44	1.2				
	21-Dec-18	21.0	5.3	0.0	84	39	1.1				
	22-Dec-18	20.0	3.0	0.0	91	30	1.2				
	23-Dec-18	20.5	4.6	0.0	94	33	1.2				
3rd larva*	24-Dec-18	21.5	5.4	0.0	91	39	1.0		1195	196	16.54
	25-Dec-18	21.0	5.7	0.0	89	29	1.0				
	26-Dec-18	20.5	5.2	0.0	94	36	1.4				
	27-Dec-18	21.6	7.6	0.0	90	36	1.0				
	28-Dec-18	22.0	5.2	0.0	89	28	1.9				
	29-Dec-18	19.5	4.2	0.0	97	25	1.6				
	30-Dec-18	20.0	2.6	0.0	84	29	1.1				
	31-Dec-18	19.5	2.0	0.0	97	38	1.0				
Week No.	January										
1	4th larva*	23.2	5.1	**0**	93.0	29.7	1.1	**0**	989	79	7.98
2		22.7	6.8	0.0	93.0	41.0	1.6	0.0			
3	5th larva*	23.3	5.7	0.0	87.7	23.6	1.2	0.0	910	10	1.09
4		22.8	11.5	16.2	85.3	59.7	2.6	2.0			
5		22.8	7.6	0.0	85.9	31.0	1.7	0.0			
	Total								900	780	
	Prod.%								53.57%		

Fig 3. Spinning cocoon and cocoon,Silkmonth(Tasar silkworm)

1st,2nd ,3rd Crop- Cocoon weight, table (1,2,3)

Table 1

Set. No.	Terminalia arjuna plant Cocoon Wt. in gram	
	Female	Male
1	12.17	11.08
2	10.87	8.55
3	11.71	7.28
Total	35.29	26.91
Mean	11.76	8.97
SD	0.751	1.579
SE	0.433	0.911

Table 2

Set. No.	Terminalia arjuna plant Cocoon Wt. in gram	
	Female	Male
1	11.70	10.8
2	12.83	9.07
3	12.71	9.12
Total	37.24	28.99
Mean	12.41	9.66
SD	0.506	0.806
SE	0.292	0.465

Table 3

Set. No.	Terminalia arjuna plant Cocoon Wt. in gram	
	Female	Male
1	10.16	7.69
2	10.38	8.58
3	10.22	8.6
Total	30.76	24.87
Mean	10.25	8.29
SD	0.092	0.424
SE	0.053	0.244

Table 1,2,3 : Total mean of Female and Male Cocoon weight of 5th instar in the arjuna food plant.In the **table 1**. Female cocoon mean weight 11.76gm,male mean weight 8.97gm.Table 3.Female cocoon mean weight 12.4 gm and male cocoon mean weight 9.6gm. In the **Table -2.** mean weight of female cocoon from Arjuna plant is 12.41gm and the mean of male cocoon of Arjuna plant is 9.66 gm. **table 3**. We observed that mean weight of Female cocoon from Arjuna plant is 10.25gm and the mean of Male cocoon of Arjuna plant is 8.29gm**,**

1st ,2nd ,3rd Crop-Pupa weight, table (4,5,6)

Table 4

Set. No.	Terminalia arjuna plant Pupa Wt. in gram	
	Female	Male
1	11.17	9.70
2	9.48	7.33
3	10.19	6.11
Total	30.84	23.14
Mean	10.28	7.71
SD	0.692	1.49
SE	0.399	0.86

Table 5

Set. No.	Terminalia arjuna plant Pupa Wt. in gram	
	Female	Male
1	10.06	9.01
2	11.23	8.03
3	11.13	8.01
Total	32.42	25.05
Mean	10.81	8.35
SD	0.529	0.405
SE	0.305	0.233

Table 6

Set. No.	Terminalia arjuna plant Pupa Wt. in gram	
	Female	Male
1	9.15	6.6
2	9.21	7.5
3	9.2	7.5
Total	27.56	21.6
Mean	9.19	7.2
SD	0.09	0.04
SE	0.052	0.244

In the **Table 4** ,5,6. Total mean of Female and Male pupa weight of 5th instar in the arjuna food plant. **Table -4.** mean weight of female pupa from Arjuna plant is 10.28gm and the mean of male pupa of Arjuna plant is 7.71gm In the **Table -5.** mean weight of female pupa from Arjuna plant is 10.81gm and the mean of male pupal of Arjuna plant is 8.35gm. **Table 6.** We observed that mean weight of female pupa from Arjuna plant is 9.19 gm and the mean of male pupa of Arjuna plant is 7.2gm. In the

1st ,2nd ,3rd Crop- Shell weight, table (7,8,9)

Table 7

Set. No.	Terminalia arjuna plant Shell Wt. in gram	
	Female	Male
1	1.54	1.26
2	1.39	1.1
3	1.52	1.08
Total	4.45	3.44
Mean	1.48	1.14
SD	0.066	0.072
SE	0.038	0.041

Table 8

Set. No.	Terminalia arjuna plant Shell Wt. in gram	
	Female	Male
1	1.64	1.07
2	1.6	1.04
3	1.5	1.15
Total	4.74	3.26
Mean	1.58	1.09
SD	0.098	0.097
SE	0.056	0.056

Table 9

Set. No.	Terminalia arjuna plant Shell Wt. in gram	
	Female	Male
1	1.01	1.09
2	1.17	1.08
3	1.02	1.1
Total	3.2	3.27
Mean	1.06	1.09
SD	0.073	2.581
SE	0.042	1.49

.In the Table 7,8,9 .Total mean of Female and Male Shell weight of 5th instar in the arjuna food plant. In the **Table -7** mean weight of female shell from Arjuna plant is 1.48gm and the mean of male shell of Arjun plant is 1.14 gm. In the **Table –8** mean weight of female shell from Arjuna plant is 1.58gm and the mean of male shell of Arjuna plant is 1.09. **Table -9**. We observed that mean weight of female shell from Arjuna plant is 1.06gm and the mean of male shell of Arjuna plant is 1.09gm.

Table 1. Data showing I,II and III crop on Terminalia arjuna,cocoon weight(g),Pupa weight(g),shell weight(g) of Antheraea mylitta (male)Values are mean+_SE (N=3)

crop	Cocoon Weight (g)	Pupa weight (g)	Shell weight (g)
I	8.97±0.91 (3)	7.71±0.86 (3)	1.14±0.04 (3)
II	9.60±0.46 (3)	8.30±0.23 (3)	1.00±0.05 (3)
III	8.29 ±0.24 (3)	7.20 ±0.24 (3)	1.09±1.49 (3)

Xp< 1.49 in respect to I crop

Table 2. Data showing I,II and III crop on Terminalia arjuna,cocoon weight(g),Pupa weight(g),shell weight(g) of Antheraea mylitta (Female)Values are mean±SE (N=3)

crop	Cocoon Weight (g)	Pupa weight (g)	Shell weight (g)
I	11.76±0.43 (3)	10.28±0.39 (3)	1.48±0.03 (3)
II	12.40±0.29 (3)	10.80±0.30 (3)	1.50±0.05 (3)
III	10.25 ±0.05 (3)	9.10 ±0.05 (3)	1.06±0.04 (3)

Xp<0.04 in respect to I crop

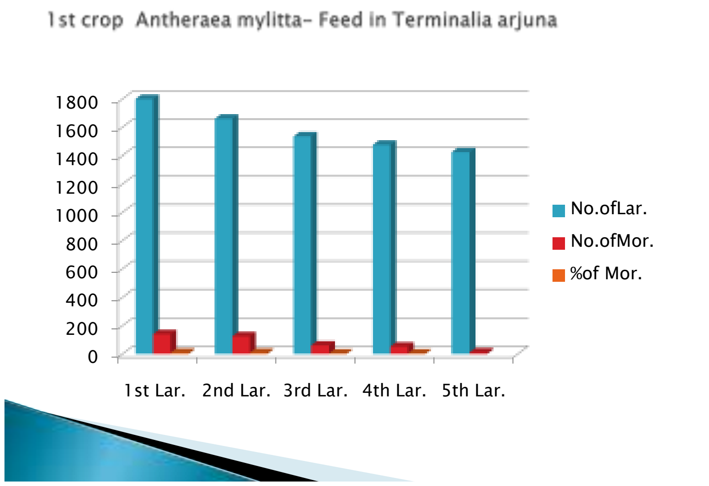


Fig 1 : Graph showing :Effective Rate of Rearing(No.of Larvae 0-1800)and effective mortality rate

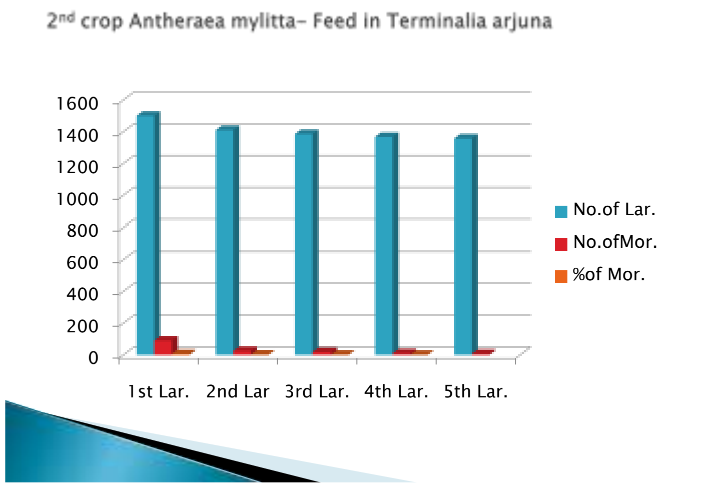


Fig 2 : Graph showing :Effective Rate of Rearing(No.of Larvae 0-1600)and effective mortality rat

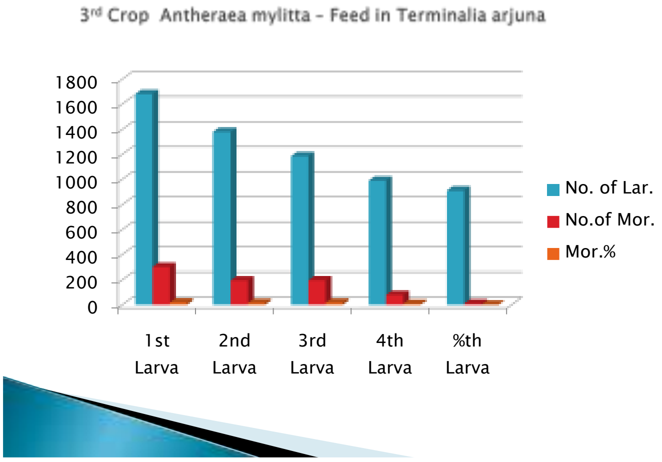


Fig 3: Graph Showing:Effective Rate of Rearing(No.of Larvae 0-1800 and Mortality Rate)

Results and discussion –

The result of the present study gives insight on the role of different environmental factors on the survivability of Tasar silkworm larvae in different stages in Ambikapur sericulture department.The larval mortality due to bacteria,verious,pestes was recorded in different larval stages in plot.The data analysis that larval mortality rate increases with fluctuation in the temperature and relative humidity existing in the previous two or three days.the environmental factor which exists during 4 days earlier plays a major role in deciding the survivability of the larvae outdoor condition. The results of the present study confirms that more larval mortality was noticed in depend favorable or non favorable environmental condition responses for spread of the diseases.Then main responses of silk production of environmental reasons.After study of doing analysis to find how much contribution of male is in the production of Tasar silkworm.How much contribution of female is also shown in the study report.In theproduction of silk how much directly or indirectly between.The both male and female is concerned is also mentioned is the report.Hence for more silk production depends upon suitable seasons.As a result of production of cocoon can be increased and more and more income can be earned in the production of Tasar silk.

References

1.chandrakanth N; Moorthy SM.Kariyapa,Ponnuvel KM,Sivaprasad V. Reeling performances of F2 and back cross populations under high Temperature conditions Journal of Entomology and zoology studies 2015;3(6):219-222.

2.RanjanA,Poddar A, Roy Sp, Environmental controlling factors of Tasar silkworm Antheraea mylitta Drury(Lepidoptera:Saturnide),our nature 2012;10:115-118.

3. V.K. Rahmathulla;"Management of climatic factors during silkworm rearing the textile Industry and trade Journal pp.25-26;1999.

4. T.Singh,M.M.Bhat,and M.K.Ashraf,"Insect adaptations to changing Environments temperature and humidity."International Journal of Industrial Entomology,Vol;19 no.1 pp.'55-165'2009.

5. Dewangan, SK, Sahu, KR and Soni,SK (2012).Breaking of poverty though sericulture among the tribe –A.Socio-Economic study of Dharmjaigarh blok of Raigarh Dist.C.G. India:Research Journal of Recent science,1:371 – 374.

6. Yadav,G.S.(2000)Studies on the association and interation of temperature.Relative humidity and rainfall in Tasar ecosystem of Vidarbha,Bull.Ind.Acad.Ser.,4(1):20-30.

7. Gregory,S. 1914, Rural Labour and sericulture:Typology Stretegies and prospects,Indian J.Ind.Relat 1,365-376.

8. Singh,C.1993, An Economic Analysis of sericulture production in Raigarh district of Madhya Pradesh,Agricultural Economics Research Review,6,52-53.

9. Srivastava, S.Kapoor, R.Thathola, A. Srivastava, R.P. 2003.Mulberry (momsalba) Leaves as human food,a new dimension of sericulture. Int.J.Food Sci.Nutr.54,411-416.

10. Sheela Patel,R.K.Singh and Shweta Sao(2016) Comparative studies of two silkworm species in Raigarh district for high quality yield.International Journal of Development Research Vol.6,10509-10514.

INDIA AND CYBERTERRORISM

Colonel B S Nagial (Retd)

Director: Academy of Proficiency & Training,
SCO-743, Tricity Trade Tower
Zirakpur Punjab-140603

Abstract: **To live peacefully in this world of danger and uncertainty, courage is prerequisite. There are two way to meet the danger: one, remain indifference to danger and two, prepare and motivate yourselves through knowledge and training and face the danger head-on. Technology is a double-edged weapon, which can used for both constructive as well as destructive work. Cyberterrorism is the fine example of destructive use of technology, which is posing threat to humanity. To defeat your enemy, first you know your enemy well. So, the aim of this paper is to understand the concept of cyberterrorism, its effect on the world community including India and how to counter this menace. Digital world is being exploited by the terrorist' organisations for radicalisation, recruitment, propaganda, fundraising, training, etc. These organisations use the darknet to carry out terrorist activities so not visible on the public platform. Time plays the biggest role in any combat and certainly it has greater significance when countering cyberterrorism wherein technology is changing very fast. This paper will also discuss the possible defences available against the cyberterrorism.**

Keywords: **Terrorism, Cyberterrorism, Cyberattacks, Radicalisation, Digital Infrastructure, Use of Internet by terrorists and other criminals.**

Introduction

Terrorism is an unlawful use of violence and threat especially against civilians for achieving the political goals. Terrorism is as old as the human history itself. After Sept 11, 2001 terrorists' attack on United State of America, the world community has come together to solve the problem of International Terrorism. It is pertinent to mention that there are different types of terrorism so profiling is not an easy task. Since different terrorist' organisations have different ideologies therefore operate differently, even individual terrorist work differently. Terrorism is very dynamic in nature, changing its strategies very fast and always look for weak target/targets to strike. These targets may include power stations, military assets, banking industry, air-traffic controls, radio and television stations, etc. Digital world is providing many opportunities and new battlegrounds to these terrorist' organisations. Through digital infrastructure these terrorists are targeting people for radicalisation, recruitment, fundraising, propaganda, training and other nefarious activities. As world is evolving and becoming dependent on technology more and more, threat posed is no longer physical but extended to digital world also. Like conventional warfare we can secure our digital infrastructure and any intrusion by inimical elements can be checked, pursued and destroyed. Awareness among the people is very essential.

What is terrorism?

For formulating any kind of strategy, especially when doing so for addressing the security threat such as terrorism, it is important that threat be minutely examined and defined. In fact, defining terrorism is a war on terrorism itself so we shouldn't be wrong. Beauty and terrorism both are as far as their definitions are concerned not easy to describe. As beauty lies in the eyes of beholder so the concept of terrorism lies with the nation/nations which have faced it. Let us examine a few definitions of terrorism to under the basic concept of terrorism.

"Terrorism is a form of violent struggle in which violence is deliberately used against civilians in order to achieve the political goals (nationalistic, socioeconomic, ideological, religious, etc)." [1]

The United Nations General Assembly adopted the resolution 49/60(Measures to eliminate the International Terrorism) on December 9, 1994 which states 'terrorism' as the criminal acts intended or calculated to provoke a state of terror in the general public or a group of persons or particular persons for political purposes are in any circumstances unjustifiable, whatever the considerations of political, philosophical, ideological, racial, ethnic, religious, or any other nature that may be invoked to justify them.

United Nation Security Council Resolution 1566(2004) gives a definition of terrorism: "Criminal acts including civilians, committed with the intent to cause death or serious bodily injury or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a govt or international organisation to do so or to abstain from doing any act." Further improving up on the definition of 'terrorism' a United panel, on March 17, 2005 stated that terrorism is an act "intended to cause death or seriously bodily harm to civilians or non-combatants with the purpose of intimidation a population or compelling a govt or international organisation to do so or abstain from doing any act."

FBI (Federal Bureau of Investigation), U.S.A, terrorism as under:

"**International Terrorism**: violent criminal acts committed by individuals and/ or groups who are inspired by or associated with, designated foreign terrorist organisation or nations (state sponsored)."

"**Domestic terrorism:** violent, criminal acts committed by individuals and/ or groups to further ideological goals stemming from domestic influences, such as those of political, religious, social, racial, environmental nature."

In India, Terrorism as an offence doesn't figure in the Indian Penal Code of 1860 which was amended from time to time. For the first time the term terrorism was described in Terrorist and Disruptive (Prevention) Act, 1987 but this act was repealed in 1993. Again, the word 'terrorism' found its place in Prevention of Terrorist Act, 2002. This act also got repealed in 2004. Finally, on Aug 02, 2019 Unlawful Activities (Prevention) Act, 1967 was amended and passed which contains the definition of terrorist act. "Under this Act, the Central government may designate an organisation as a terrorist organisation if it:

- Commits or participate in act terrorism or
- Prepares for terrorism or
- Promotes terrorism or
- Otherwise involved in terrorism.

The act additionally empowers to designate individuals as terrorists on the above mention grounds."

It is very essential to define the word 'terrorism' because it will help us to understand the problem of terrorism and make strategy to eliminate such blot from the face of humanity. It is very surprising that so far, we haven't reached at the consensus of defining terrorism. Basically, this is because of two main reasons: one, a terrorist in one country is a 'freedom fighter' for other country and two, some nation sates carry out clandestine operations against another country through terrorist' organisations. The fact is terrorism is a terrorism irrespective of its shape, size or form. There can't be 'good-terrorism' or 'bad-terrorism'. Terrorism is a crime against the humanity. All actions of terrorism should be considered as illegitimate irrespective of nature and goal/goals. And I think the most appropriate definition of the terrorism proposed so far is: "An act of terrorism=Peacetime Equivalent of War Crime" This short but most appropriate definition was proposed by Alex. P Schmid to United Nation Crime Branch in 1992.[2]

Cyberterrorism

Cyberterrorism is a genuine danger, which is spreading its roots in society very fast. There is an urgent requirement of world attention and action to contain this menace. The potential targets of the cyberterrorism are the frameworks which control country's resistance and provide resilience. Internet dependency has increased significantly and also the horizons of security threat have expanded. The traditional concepts and methods of terrorism are giving-in to new opportunities provided by the digital world. In this age of information most of the terrorist' organisations have developed a deadly combination of weapons and technology. Information Technology is a double-edged weapon, which can be used for constructive as well as destructive work. Awareness among the people is the only answer to this problem. It is an hour of need to formulate the safety networks in anticipation of invisible threats of terrorists' organisations. Cyberterrorists may win the war without firing a shot by crushing the fundamental foundation, which is mainly dependent on the use of data science. Definitely, a society without protection in the form of 'self-help', in this era of technology can't be imagined. Internet doesn't respect the boundaries created by nation states hence attackers can attack at will all over the world. If it is not tackled sooner than later then definitely it would become irreversible and catastrophic in nature worldwide.

As compared to other terrorist' activities, cyberterrorism is new phenomenon. Since there is no common acceptability to the term terrorism therefore consensus on the definition of cyberterrorism can't be reached. Cyberterrorism is the convergence of technology and terrorism. It is an unlawful attack or threat of attack against computers, networks and other paraphernalia and carried to intimidate or coerce a govt or the people for furtherance of their cause their (terrorist' organisations) goals and objectives. Let's examine a few definitions available to understand the concept of cyberterrorism.

As per Lexicon-a US Dictionary powered by OXFORD, "Cyberterrorism is the politically motivated use of computers and information technology to cause severe disruption or widespread fear in the society".

"[G]et ready…… terrorists are preparing …...cyberspace-based attacks…." (John Arqiua, Waging War through Internet).

The term 'cyberterrorism' appeared for the first time in defence literature in1998 in U S Army War College.[3]

Prof. Dorothy Denning offered definition of terrorism in testimony before the House Armed Services Committee in May 2000 that has been widely cited:

"Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks and information stored therein when done to intimidate or coerce a govt or its people in furtherance of its political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property or at least cause enough harms to generate fear. Attack that leads to death or bodily injury, explosion, plane crashes, water contamination, or severe economic loss…... would be examples. Serious attacks against critical infrastructure could be acts of terrorism, depending on their impact. Attack that disrupt non-essential services or that are mainly costly nuisance would not." [4]

Federal Bureau of Investigation, a U S investigating agency define "cyberterrorism as a premediated, politically motivated, attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents." [5]

Bruce Hoffman defines terrorism as “the deliberate creation and exploitation of fear through violence or threat of violence in the pursuit of political change.” [6]

From above mentioned definitions certain activities which form part of the cyberterrorism are inciting, recruitment, radicalisation, financing, planning, communication, etc, these activities can be grouped under Enabling Cyber Terrorism (ECT). In general, we use the terms such as cyberwar, cyberterrorism, cybercrime, hacktivism, etc interchangeable but there are inbuilt insidious differences. The term cyber is generally used for computer but it could also include other information technology including people who have the capacity to interpret the information. Cyberspace is a global domain where interdependent network of information technology infrastructure including internet, telecommunication networks, computer system, etc exists. The aim of the terrorists using cyber destructive terrorism is to manipulate the computer code and corrupt the information networks to destroy or damage the virtual as well as physical national assets. The internet has allowed for exchange of vast exchange of information. Thus, created space for both criminals and terrorists to operate individually or collectively. It is very important to understand the motives behind such attacks this will facilitate to grasp the term cyberterrorism properly. While all cyberterrorism could be attributed to cybercrimes but all the activities of cybercrimes can’t be attributed to cyberterrorism. The threat of cyberattacks are continuous on rise and online users are vulnerable to such attacks. Our dependency on cyber-world is increasing day by day. In fact, it is impossible to think of life without internet. Different countries have developed various rules and regulations to combat cyberterrorism but at international level we lack coordination. Before agreeing up on the counter cyberterrorism measures first of all we must reach at an acceptable definition of Terrorism as well as Cyberterrorism.

Motives, Interests of Terrorists in Cyberattacks.

There could be many logical reasons of terrorist’ cyberattacks. The first and the foremost motive could be to gain visibility and influence people by creating fear among them. Destroying things and killing people could be the other reasons. [7] Other lesser goals could be in relation to the maintenance and upkeep activities such as fund raising, planning, recruitment, intelligence gathering, etc. The cyber domain provides various benefits which are enumerated as under:

- Anonymous communication with other terrorist’ organisations and own cadres within the organisations.
- Because of personal safety as compared to physical attacks
- Can access the target/targets easily
- It is a cost-effective as only PC or Mobile Hand Set with internet facilities is required.
- Availability of various attacking tools
- Vulnerable targets could be accessed through remotely connected networks.
- A person with an average skill can operate without much knowledge. Its user friendly.
- Propaganda can be spread worldwide with speed.

Terrorists can plan and coordinate cyberattacks and other physical attacks through covert use of communication networks. In asymmetrical warfare, even a small group of terrorists can carry out a largescale cyberattacks as well as physical attacks thus inflicting serious damage. Some thinkers and strategists think that the term “cyberterrorism” is not justified because a well-planned cyberattack may only produce annoyances, not the terror as a bomb or Improvised Explosive Devise (I ED) would have done. But according to other thinkers and strategists, since computer networks attack produces enough of disruption in economic activities, spread fear amongst the targeted population and may cause death to civilians and non-combatants thus qualifies as “terrorism”. Cyberterrorism could be considered as an act of terrorism if it fulfils the following criteria.

- Effects based event. Cyberterrorism exists when computer-based attacks result in the effects that are disruptive enough to produce fear in the minds of targeted people as compared to traditional acts of terrorism.
- Intent -based event. Cyberterrorism exits when unlawful or politically motivated computer attacks are done to intimidate or coerce a govt or organisation or section of people to achieve a political objective or inflict injuries or cause severe damage the assets of the targeted nation.

The uses of internet by terrorist for cyberterrorism.

“The Internet is a prime example of how terrorists can behave in a truly transitional way; in response, States need to think and function in an equally transitional manner.” (Ban Ki Moon, Ex Secretary-General of U N O).

Peter Flemming and Michel Stohi identify two components of Cyberterrorism.[8]

- Computer technology as a facilitator of terrorism: It is used for political propaganda, terrorist recruitment and financing, intra and inter-group communication and coordination, intelligence gathering, etc. This enables the terrorist’ groups to maintain anonymity in routine activities and tactical operations, and also carry out their operation in cost-effective manner.
- Computer technology as a specific component of terrorist weapons or targets: This includes computer technology-based attacks or threats or public utilities and transportation, commercial institutions, individuals, political or ethnic groups, security forces, nation-states or far that any ‘perceived enemy’.

It is well known fact that terrorists possess the knowledge about computers, internet and various other tools and their usages in furtherance of their cause of terrorism. Such causes could be anything ranging from social goals to political gaols. [9]

As per the United Nation Office of Drugs and Crime report, terrorists use the internet for following reasons:

- Spreading propaganda relating to institutions, explanations, justifications or promotion of terrorist' activities
- Incite violence
- Recruitment and radicalisation of individuals
- Fund raising through direct solicitation, e-commerce, online payment modes, charitable organisations, etc.
- Training for the followers for combat tactics, use of explosions and weapons

Objectives of cyberattacks.

There could be many objectives of inimical elements for carrying the cyberattacks such as intentional disruption in the digital infrastructure, to cause economic losses, destroying of military assets, luring people to join the terrorist' organisations, etc. Cyberattacks are defined as deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and /or transiting these systems or networks. [10]. Cyberattack is deliberate exploitation of computer systems, technology dependent enterprises and networks. As per U.S. Army Training and Doctrine Command, cyber operation and cyberterrorism Handbook No.102, Aug15, 2005, p-ii-1 and ii-3 following objectives may drive terrorists to carry out the cyberattacks.

- Loss of integrity- unauthorised changes made to the data or IT system can result in accuracy, fraud or error in decision making that bring the integrity of the system under suspicion.
- Loss of availability- an attack on mission or computer system makes it unavailable for the end users.
- Loss of confidentiality-the consequences of unauthorised discloser of information ranges from loss of public confidence to national security threats.
- Physical destruction- ability to create actual physical harm through computer hardware or IT Infrastructure.

A cyberattack, disrupts the integrity and authenticity of the data mainly through malicious code that alters the program system software, thus leading to disruptive or incorrect output. Whole internet network is scanned completely through security software manipulation. Once infected, the machine can be manipulated remotely via internet. Cyber-weapons and ammunitions are the subdivisions of computer/machine codes intended to be used with aim of terrorising people and disruption or destruction of cyber-infrastructure.

Cyberattacks have the ability to disrupt the way in which ordinary individuals live (e.g. the chaos that would arise if none of the automatic teller machines (ATMs in country were operational). The interconnectedness of global financial institutions, enabled by modern communication technology increase the risk. [11]

Cyberattacks weapons are easy to use and can produce results such as defacing of website to steal data and sensitive information, intellectual property, spying on targeted system and disruption of essential services. On the other hand, cyberattack as a mode of conflict raises many operation related issues, such as origin or roots of such attack, whether done by terrorist' organisations or any particular nation state. Very difficult to prove all this. But definitely cyberattacks can support military operations. They are capable to disrupt and destroy the target/targets Command, Control and Communication (C3). And can also support covert operations to influence government, group of people, any particular organisation, etc. Valuable information and state secret can be obtained through cyberespionage.

How cyberattacks work?

If we understand the different types of attacks and how they are carried out then certainly we can take preventive measures to safeguard our digital infrastructure and can take care of vital & essential resources. A cyber-attack is generally carried out by a trained handler and may consist of many stages. As per National Cyber Security Centre, United Kingdom, the cyber-attack could be grouped in two categories:

1. **Un-targeted cyber-attacks.** Under this category attackers indiscriminately target as many devices, services or users as possible. Victims are not identified. For such attacks they use the following techniques: -

- **Phishing-** sending emails to large numbers of people asking for sensitive personal information such as bank details, PAN, Aadhaar, etc.
- **Water holing-** setting up a fake website or compromising a legitimate one in order to exploit visitors to such website.
- **Ransomware-** which could include disseminating disk encrypting exploiting malware
- **Scanning-** attacking wide swathes of internet at random

2. **Targeted Cyber Attacks.** In such attacks target is identified and attacker has specific interest in such target. For this preparation may take for months even years. It is often more damaging than untargeted attacks. It is customised or tailormade for the specific target. These attacks may include:

- **Spear-phishing.** By sending emails to targeted individuals that could contain an attachment with malicious software or a link that downloads malicious software.
- **Deploying a botnet**. To deliver a DDOS (Distributed Denial of Service) attack.
- **Subverting the supply chain-** to attack equipment/ software being delivered to the organisation/target.

Stages of a cyber-attack.

In our cyberworld, cyberattacks are taking place almost daily in every organisation weather civil or military and to thwart such attacks such attacks we have to think and act like a military mind. These attacks occur at different stages depending upon the target and aim chosen by the terrorists. The term cyber Kill-Chain originally came from military environment, which is according to Joseph Raczynski a chain of stages leading to cyberattack [12]. A cyberattack takes place at 7 stages which are enumerated as under:

- **Reconnaissance.** Initially hackers begin with searching for the profile of the target, which include names, titles, e-mail addresses, telephone/mobile numbers, etc. They identify the target/targets and then plan the attack.
- **Weaponisation.** Hackers have the libraries of codes at their disposal which they use and tweak their attacks. They consider the networks, system software and operating system used by the victim/ victims. Then hackers customise their own codes and attack the unpatched software system.
- **Deliver.** Through research the hackers know the names of CEO and various other functionaries of the organisation. Get their particulars from the google search. And then lure the boss and other employees through various phishing tactics.
- **Exploitation**. The hackers send perfectly feasible emails to CEO and other employees with attachments.
- **Installation**. Maximum chances are there that boss and other employees of the organisation will click the e-mail with link provided therein. Once clicked malicious software takes the root.
- **Command and Control**. Once the malicious code has been established, it sends the messages to remotely computer station set-up by the hackers. Then hackers get activated extract the information and data as per their need and requirement.
- **Action on the objectives**. Finally, hackers are able to establish the contact with target/targets and carry out the desired operations.

Now, many proactive institutions are attempting to ‘break’ an opponent’s ‘kill-chain’ as a defence method. One of the leaders in this area of the concept of Information Security is Lodheed Martin. He suggests the following defence mechanism:

- **Survey**- investigation and analysis of available information about the target/targets. Also, vulnerabilities are identified at this stage.
- **Delivery**- getting to the point where vulnerability could be exploited.
- **Breach**- exploitation of vulnerabilities to gain an un-authorised access.
- **Affect**- carrying out the designated activities for desired results.

After attacking, the capable attacker would exit without leaving any source of evidence or attacker may create an access for future visits. On the other hand, other attackers may encash it and publicise widely, to garner more support in term of men and material.

Methods of cyberattacks.

Today, technology is changing very fast, this world is driven by social networks, online-transactions, cloud-computing and many other automated processes. Good and bad always progress at the same rates. On the one hand this technology has facilitated smoothness in our life, at the same time it has given birth to new types of threat in our life. If you have ever studied the history of battles in this world, then you will realise that no two battles employed the same tactics. But similar strategies and tactics have been used again and again in many battles because they are time-proven to be effective. Similarly, when terrorists and criminals carry out cyberattacks, they use different strategies and tactics to re-invent the wheel. Common types of cyberattacks are mentioned under:

- **Malware**. Attackers love to use malware to gain foothold in users’ computer networks and consequently the offices they work in. This type of attack is very effective. Malware is kind of harmful software which damage the digital infrastructure. Viruses, spyware, worms, ransomware are the popular examples. Malware is installed emails in attachments. Once malware is there in the computer it can cause the havoc beyond imagination. It silently steals the data from the computer system. Blocks the way to essential components of a network. Creates networks of other malicious software.
- **Phishing**. It is process of sending the fraudulent communication that appears to be come from reliable sources. It is generally sent through emails. The goal is to steal the confidential information or install malware on the victim’ computer. Advanced Persistent Threats (APTs) and ransomware often start with phishing.
- **Man-in-the-middle-attacks.** Also known as eves dropping attacks, occur when attackers insert themselves in a two-party-transaction. Once the attackers interrupt the traffic, they can filter and steal the data. They can basically enter through two routes. One, through free public Wi Fi and two, when malicious malware is installed. An attacker can install software to process the information and data.
- **Denial of service attack.** Through this they attack the floods systems, servers or networks with traffic to exhaust the resources and bandwidth. As a result, system is unable to fulfil the legitimate requests. Attackers can also malicious software and devices to block the genuine information to the user/users. This is also known as denial of information.
- **SQL Injection Attack.** A Structure Query Language (SQL) injection occurs when an attacker inserts the malicious code into a server that uses SQL and forces the server to reveal information it would not normally. This can be done through injection of malicious code in website search box.
- **DNS Tunnelling.** It utilises the DNS protocol to communicate to non-DNS traffic port number 53. It sends the HTTP and other traffic over the protocol. There are various reasons for using DNS Tunnelling. But there are different reasons use the malicious DNS Tunnelling VPN services. They are used to disguise the outbound traffic as DNS, concealing data through internet connection.

For malicious use DNS requests are manipulated to extract information from the compromised computer system. Through this process a command and control station could be established.

- **Zero-day exploit.** Attackers do this when a compromise is established and patching work or remedial measures are initiated. They exploit the vulnerabilities during time available.
- **Cross-Site Scripting (XSS).** Under these malicious scripts are injected in otherwise benign or trusted websites. Attackers use web application to send malicious code, generally in the form of browser side script, for different end using.

Cyberattacks in India.

Cyberattacks exploit reported vulnerabilities in the system and its users. Indian telecom service providers offer the lowest data rates in the world. India has the population more than 1.3 billion, internet users would increase definitely and the vulnerabilities would also increase in future.

As per the information provided by Computer Emergency Response Team (CERT), 50,362 cases of cyberattacks were reported in the year 2016. The number increased to 53,117 in the year 2017 and rose drastically in the year 2018 with 2,08,456 cases. Till Oct 2019, the number of cases reported are 3,18, 649, which is the highest in last four year. Major incidents of cyberattacks happened in India are enumerated in succeeding paras:

“The Indian Army has faced 23 attempted cyberattacks so far, this year or 2 cyberattacks every month. The number of attempts were sustainably higher than witnessed last year.” [13]

“In 2016, it was found that cybercrooks stole thousands of files that reveal the compatibility of Indian scorpene class submarine fleet. It was around 22,400 pages.” [14]

“On May 23rd 2017, a SUKHOI 30 aircraft which was meant for air warfare crashed on Indo-China border under mysterious conditions. The wreckage of the plane was discovered three days after crash and an analysis of the crash was carried out by Indian Air Force (IAF). The internal inquiry made by IAF led to believe that flying aircraft was cyberattacked by when it was airborne.” [15]

Union Bank of India heist. Through a phishing e-mail was sent to an employee, hackers accessed the credentials to execute fund transfer, swindling Union Bank of India $ 171 million, but prompt action helped the bank to recover almost the entire amount. In June 2017Petya Ransomware, this made its impact felt across the world, including India, where container handling functions at terminal operated by the Danish firm A P Moller Maersk at Mumbai Jawaharlal Nehru Port Trust got affected.

“Kundankulam Nuclear Power Plant (KNPP) came under cyberattack in the last week of Oct, 2019. The damage was in the form of data theft, the same data can used to enhance future attacks. Even ISRO faced attacks prior to Chandrayan-2 mission.” [16].

In late Feb 2019, Pakistan based threat actor Green Havildar (a.k.a Goron Group) used to lure related to airstrikes conducted by Indian Military within, Pakistan, airspace, allegedly targeting a Jaish-e-Mohammad training camp. The lure document delivered crimson RAT payload to victims. [17]

Rise in sophisticated attacks, botnet works, attacks on critical infrastructure using evolved malware dominated the threat landscape in 2019 as reported by Subex-a internet and telecommunication analytics company based at Bengaluru, its report Dated Feb 27, 2020. The report was prepared using threat intelligence gathered from Subex global honeypot network operational in 62 cities globally. The report highlighted that malware complexity and sophistication on rising, increasing reconnaissance capabilities of hackers, increasing common attacks on Internet of Things (IOT) devices, critical infrastructure as areas require tremendous actions. Major cities which were attacked globally in 2019 are New York, New Delhi, Atlanta, London, Kyiv. Recently there have increased incidents in South Asia, in Middle East and North America.

Countering Cyberattacks in India.

As per Dr V K Saraswat, member, NITTI Aayog, the state cyberattacks and cyber security are enumerated as under:

- India ranks 3rd in forms of the highest number of internet users in the world after USA and China, the number has grown six-fold from 2012-2017 which is compounded 44% annually.
- India secures a spot amongst the top 10 spam-sending countries in the world alongside USA.
- India was ranked among top five countries to be affected by cybercrime, according to 22 October report online security firm “Symantec Corp”.

Major players in cybercrimes usually belongs to organised criminal groups, criminal societies, criminal’ organisations operational both at national and international level. Almost all countries of the world recognise the inherent criminal liabilities of the terrorist’ organisations. After terrorists’ attack on USA on Sept 11, 2001, the fight against terrorism was hardened worldwide. Terrorism is considered as a threat to humanity. Many countries amended their existing laws and some brought new legislations to weed out the terrorism from the society. India has been suffering mainly due to state-sponsored terrorism since 1947. India has been tough on terrorism and to counter cyberterrorism she brought out the amendments in Information Technology Act 2000 in the year 2008.

66F. Punishment for cyber terrorism (1) Whoever, - (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource;

or (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access;

or (iii) introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70,

or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly 26 relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Various agencies in India which are working in tandem with another to meet the challenges thrown by cyberterrorism.

1. **Indian-Computer Emergency Response**. It was established in 2004 and placed under the Ministry of Electronics and Information Technology. It is nodal agency to deal with cybersecurity threats like hacking, malware, spam, phishing, etc and strengthen the security related defence of India Internet Domain.
2. **National Cyber Coordination Centre.** It received an in-principle approval in 2013 and would come under National Information Board. It is an operational cybersecurity and e-surveillance agency in India. It is intended to screen communication metadata and coordinate other intelligence gathering activities of other agencies.
3. **Cyber and Information Security Division**. It forms part of Ministry of Home Affairs of India and deals with matter related to cybersecurity, cybercrime, National Information Security and Policy & Guidance, NATGRID, etc. Also acts as a nodal agency to fight against cybercrime. To prevent the misuse of cyberspace for furthering the extremists and terrorists.
4. **National Technical Research Organisation.** It was established in 2004 under National Security Adviser in Prime Minister's office, India. It also included the National Institute Of Cryptology Research and Development, which is first of its kind in Asia. It is a national intelligence agency.
5. **Defence Intelligence Agency (India).** It was established in 2002, and is responsible for providing and coordinating military intelligence for Indian Defence Forces. It also deals with technical assets of our defence forces. Generally, handles the information warfare including psychological operation, cyber-war, electronic interception, etc.
6. **National Crime Records Bureau.** It was set-up in 1986 to function as a repository of Information on crimes and criminals so as to help the investigating agencies in linking crime to the preparators. It is responsible for monitoring, coordinating and implementing the crimes and criminal tracking networks & systems.
7. **Defence Cyber Agency.** It was established in 2018 as a tri-services agency of Indian Defence Forces. It would have the capacity and capability to hack into networks, mount surveillance operations, lay honey-pot, recover deleted data from the hard disks and other hardware, break into encrypted communication channel, etc. When fully functional will definitely become a force-multiplier.
8. **Defence Space Agency.** It was established in the year 2018, entrusted with responsibility of operating and maintaining Space Warfare Assets of the country. Months before coming into being DSA conducted and Anti-Satellite Weapon (ASAT) Test in Mar 2019. Test was conducted demonstrate the India's anti-satellite capabilities. This was in response to Ballistic Missiles System of China and Pakistan. With launching of ASAT, India has become 5th country in the world to have such capability.

International Collaboration.

- The commonwealth countries have unanimously agreed to take action in the field of cybersecurity by 2020. Nations agreed to work closely to evaluate and strengthen their cybersecurity frameworks and response mechanism.

- As governments the world over deliberate over how to tackle growing nation-state cyber-attacks and protect sensitive data, a top Microsoft official said on Tuesday that collaborations between the governments, tech companies and third-party cybersecurity agencies can help address the growing menace. According to Rob Lefferts, CVP-Program Management M365 Security at Microsoft, the company takes nation-state cyber-attacks very seriously. [18]
- In the third Indo-French cyber dialogue which was held in Paris on 20 June 2019, India and France have joined hands to work closely in the areas of cybersecurity.
- India and Japan have decided to collaborate in the areas of cybersecurity and outer space as part of their growing security partnership in the Indo-Pacific region, a development that comes in the backdrop of increasing violation of social media platforms by extremists and India's successful Anti-Satellite Weapons (ASAT) test.[19]
- "It is not well known that cooperation on cyber issues constitute an important aspect of the India-UK security relationship. Opportunities to enhance cyber cooperation relating to threats, challenges, defence, crime, international law, diplomacy, governance and prosperity could ensure substantive bilateral security convergences post-Brexit. Both India and the UK share a common vision

and principles for cyberspace. These include a commitment to a free, open, peaceful and secure cyberspace; recognition of the importance of cooperation for combating cyber threats; promotion of cyber security; and a commitment to the multi-stakeholder approach to internet governance.” [20]

- India and USA have renewed their agreement to cooperate in the field of cyber security. On Wednesday, a MoU was signed between the Indian Computer Emergency Response Team (CERT- India) under the Ministry of Electronics and Information Technology and the Department of Homeland Security, Government of the United States of America. [21].
- India and Israel on Monday signed nine agreements, including in the areas of cyber security and oil and gas, following delegation-level talks headed by Prime Ministers Narendra Modi and Benjamin Netanyahu in Delhi. A memorandum of understanding (MoU) on cooperation in cyber security was signed. A second MoU was signed between the Ministry of Petroleum and Natural Gas and Israel's Ministry of Energy in oil and gas sector.[22]

Conclusion.

The topic of terrorism is both complex and emotive. It is complex because it involves many other subjects such as politics, psychology, philosophy, military strategy, history, etc. On the other hand, it is emotive because an act of terrorism (through any means) evoke sentiments/emotions from the various sections of the society. As and when such acts of terrorism are discussed evoke different feelings.

Terrorism poses a great threat to humanity. The aim of the terrorism is to create disruption and instil fear in the minds of people. Reasons for such drastic actions could be anything ranging from political motives to religious motives. History is full of evidences that some nation-states have also been involved in using physical violence against the other countries through preparators. Nation states and terrorist’ organisations who get involved in such activities, violate the laid down legal system of the established governments. Such countries and terrorist’ organisations then face the counter reactions both from within and from outside.

In the recent past many such organisations have come up in many parts of the world and posing great challenges. These terrorist’ organisations go against the grain of country pose a serious threat to security and integrity of the nations. When confronted with terrorism, the affected nation states have two options: one, they can yield to the demands of terrorists, two, face the challenges thrown by terrorists boldly and crush all such groups. Only weak nations could think of first option. On the hand, strong nations would crush such terrorist’ groups with carrot and stick policy. India is one of those countries which is facing the problem of terrorism for the last seven decades or so. Country faces the multifarious challenges in dealing with homeland security/ internal security. A stable and comprehensive ant-terrorism measures are required to be undertaken with adequate safety provisions for the public. Terrorists’ violence has to dealt with an iron hand. An effective, efficient and responsive administrative setup works as an antidote to terrorism. Outdated laws don’t help to fight terrorism so legislations should be updated regularly. No terrorism can survive without the support of local people hence along with tough laws to deal with terrorism we must formulate policy win the hearts and minds of the local people. Inclusive and sustainable developmental policies must be implemented to keep the people in the national mainstream. Violation of human rights is a big issue in fighting against terrorism so we must endeavour to safeguard the basic human rights of the people. Media should be encouraged to carry out self-regulated code of conduct to make people aware of terrorists’ violence.

Internet has grown, primarily unregulated & unstructured and it has given a new lease of life to terrorism There has been exponential growth in data transfer rates and volume. We face a new threat of cyber terror related activities not only from our adversaries only, but amateur hackers, disgruntle people within the society, unemployed youth etc. With the help of digital world terrorist’ organisations can reach to the targeted population with speed and volume of information. By using the digital infrastructure terrorists can spread their propaganda, carryout recruitment and training, lure young people to join their outfits and reach out to people for fund raising and launching pads. They collude with criminals for conception and implementation of clandestine operations which generally result in killing of people and destruction of resources. Criminal activities help these terrorists to hide their true identities and divert the attention of law enforcing agencies.

Knowledge and synchronisation of various agencies fighting cyberterrorism is very essential. But it is easier said than done, lot of efforts are required for such combined strategy. For centuries we thought that we could win the battle if we were to from the ground of tactical importance. Now that physical place has been shifted to digital space. There are many issues and intricacies involved in the studies of intelligence & terrorism, international security, cyberterrorism, internet security in India as well as world over which have been researched and discussed by the various social scientists and cybersecurity techies. Proper cyber hygiene for all organisations is essential with well-defined policies and protocols. Training to update on technology changes is another aspect which to be looked into. Cybersecurity should form part of any organisational culture. After addressing these, attention may be given to software developments to defeat the more cultured threats by invoking distracting tools such as honey traps & dummy sites for hackers, bounties to trap bugs, sandboxing to trap malware, and security holes. To tackle the cyberterrorism, we need to be proactive and to be ready and organised with a set of controls, trained personnel, and a well-established security policy, with defined legislations, rules, regulations, roles and responsibilities. Cybersecurity management policy should be based upon the principles of good Information Technology governance and be based upon recognizable standards that give assurance given to all stakeholders. There is a need of cooperation and coordination among the nations to defeat the cyberterrorism in totality.

Bibliography

1. Boaz Ganor Page-17, The Counter-Terrorism Puzzle, A Guide for Decision Makers, 2007 Transaction Publishers, New Brunswick (U.S.A) and London (U.K).

2. Source: Alex. P Schmid: http://en.wikipedia.org/wiki/Definition of Terrorism.

3. (While, Kenneth C 1998. Cyberterrorism: modern mayhem, US Army War College. Retrieved on 13 March 2015 by Wikipedia-The Free Encyclopaedia).

4. Dorothy Denning, "Cyberterrorism- Testimony before Special Oversight Panel on terrorism, Committee on Armed Services, US House of Representatives." Washington DC. US House of Representatives, May 23, 2000, available on www.stealth-iss.com/documents/pdf/cyberterrorism.pdf.

5. (Centre for Excellence, Defence Against Terrorism, ed. (2008) Responses to Cyber Terrorism, NATO science for peace and security series, Sub series E: human and societal dynamics, ISSN 1874-6276.34, Amsterdam: I O S press page 119).

6. Bruce Hoffman Inside Terrorism-New York: Columbia University Press, 2006, page no.40.

7. (G. Giacomello, "Bangs for the Buck: A cost Benefit Analysis of Cyberterrorism", studies in Conflict and Terrorism, vol27, 2004 page 387-408).

8. (Flemming, Peter, Michel Stohi, " Myths and realities of Cyberterrorism" Available at http://www.comn.ucsb.edu/Research/Myths/Realities/Cyberterrorism.pdf as reflected in para 2.5.1.6.4 8th Report, Second Administrative Reform Commission, Combating Terrorism, Protecting by Righteousness, June 2008).

9. [P.Brunts, " Terrorism and Internet: New threats posed by cyberterrorism and terrorist using internet, " M. Wadea and A.Malijevic, eds, A war on Terror: The European Stance on a New Threat, Changing Laws and Human Rights Implications, New York: Springer 2010].

10. Data Security Council of India (D S C I), Promoting Data Protection.

11. Orman, L. 2013 "Technology at Risk", IEEE Technology and Society magazine, 23-31.

12. Killer Chain: The 7 stages of cyberattack, October 12, 2018, Thomson Reuters.

13. Amrita Nayak Dutta, The Print, India 25 Nov, 2019.

14. Economic Times CIO.com, 09 Dec, 2019.

15. Naveen Gaud, Cybersecurity Insiders, May 23, 2017.

16. Analytics India Magazine, Dec19, 2019.

17. Cyber Threats 2019: A year in Retrospective. Cyber threat operations Feb 2020 by PWC.

18. Outlook, India dt Jan 28, 2020.

19. The Economic Times, India dt July 02, 2019.

20. Rahul Roy Choudhary, Senior Fellow, South Asia, IISS dt Nov 22, 2019.

21. The Economic Times, Delhi, Jul 12, 2018.

22. The First Post, India, Jan 15, 2018.

DIALYSIS - AN OVERVIEW

Mrs. M. VEGUNA RANI,
Research Scholar, Medical Surgical Nursing, Vinayaka Missions Research Foundation (Deemed to be University), Salem.

Mrs. Dr.K.KAMALA,
Principal, Vinayaka Missions College of Nursing, Vinayaka Missions Research Foundation (Deemed to be University), Salem.

***Abstract*: People with failed or damaged kidneys may have difficulty eliminating waste and unwanted water from the blood. Dialysis is an artificial way of carrying out this process. Dialysis substitutes the natural work of the kidneys, so it is also known as renal replacement therapy (RRT).Healthy kidneys regulate the body's levels of water and minerals and remove waste. The kidneys also secrete certain products that are important in metabolism, but dialysis cannot do this. A person who has lost 85 to 90 % of their kidney function will be a likely candidate for dialysis.**

***Keywords:* Dialysis, Metabolism, Renal failure**

INTRODUCTION:

Dialysis is the process used to remove fluid and waste products from the body when the kidneys are unable to do so, because of impaired function or when toxins or poisons must be removed immediately, to prevent damage. Dialysis used in renal failure remove toxic substance and body wastes normally excreted by healthy kidneys.

DEFINITION:

Dialysis is the movement of fluid and molecules across a semi permeable membrane from one compartment to another.

PURPOSES:

- To remove the end products of protein metabolism such as urea and creatinine, from the blood.
- To maintain a safe concentration of serum electrolytes
- To correct acidosis and replenish the bloods bicarbonate levels
- To remove excess fluid from the blood

PRINCIPLES:

❖ DIFFUSION:

It is the movement of solutes from an area of greater concentration to an area of lesser concentration.

❖ OSMOSIS:

It is the movement of fluid an area of an area of lesser to an area of greater concentration of solutes.

❖ ULTRA FILTRATION:

It results were there is osmotic gradient or pressure gradient across the membrane. Excess fluid is removed by increasing the osmolarity of the dialysate with the addition of glucose.

TYPES OF DIALYSIS:

❖ Peritoneal dialysis
❖ hemo dialysis
❖

PERITONEAL DIALYSIS:
MEANING:

It involves repeated cycle of instilling dialysate in to the peritoneal cavity, allowing time for substance exchange and then removing the dialysate.

INDICATION:

❖ Renal failure
❖ Who are unable or unwilling to undergo hemo dialysis or renal transplantation
❖ Patient who are susceptible to the rapid fluid, electrolyte are metabolic changes that occur during hemo dialysis.
❖ Those who may be risk for side effects of systemic use of heparin.
❖ Severe hypertension, congestive heart failure and pulmonary oedema not responding to usual treatment regimen.

TYPES:

➢ Continuous ambulatory dialysis
➢ Automated peritoneal dialysis

CONTINUOUS AMBULATORY PERITONEAL DIALYSIS:

In the continuous type of peritoneal dialysis 1.5 to 3.0 L of dialysate is instilled into the abdomen and left in place for a prescribed period of time. The empty dialysate bag is folded up and carried in a pocket until it is time to drain the dialysate. The bag is then unfolds and placed lower than the insertion site so that fluid drains by gravity flow. When full, the bag is changed and new dialysate is instilled in to the abdomen as the process continues.

In CAPD usually four dialysis cycle used every 24 hours, including 8 hours dwell overnight.

AUTOMATED PERITONEAL DIALYSIS:

Automated peritoneal dialysis necessitates use of peritoneal cycling machine. This method can be performed as continuous cyclic, intermittent or nightly intermittent peritoneal dialysis.

CONTINUOUS CYCLIC PERITONEAL DIALYSIS:

In this variation, there are usually three cycles at night and a cycle with an 8 hour dwell in the morning. The advantage of this procedure is that the peritoneal catheter is opened only for the time of procedures, which reduce the risk of infection.

INTERMITTENT PERITONEAL DIALYSIS:

Dialysis is performed for 10 to 14 hours; 3 to 4 times a week by the same peritoneal cycling machine is a continuous cyclic peritoneal dialysis.

NIGHTLY INTERMITTENT PERITONEAL DIALYSIS:

Dialysis is performed for 8 to 12 hours each night with no day time dwells.

PREPARATION OF PATIENT PERITONEAL DIALYSIS:

✓ Explain the procedure to the patient and obtained a signed consent
✓ Baseline vital signs, weight and serum electrolyte levels are obtained and recorded
✓ Emptying the bladder and bowel may be indicated to minimize the risk of puncture of internal organs
✓ Assess the patient anxiety about the procedure and to provide support and instruction.

PREPARATION OF THE EQUIPMENT:

✓ Nurse consult with the physician to determine the concentration of dialysing to be used and the medications to be added to the dialysate and assemble the equipment
✓ Heparin may be added to prevent fibrin clot formation
✓ Potassium chloride may be prescribed to treat hyperkalemia
✓ Antibiotics may be added to treat peritonitis
✓ Warm the dialysate to body temperature
✓ The administration set and tubing are assembled
✓ The tube is filled with prepared dialysate fluid to reduce the air entering.

PERITONEAL CATHETER AND ITS INSERTION:

Soft catheters are inserted through the abdominal wall.

TENCKHOFF:

It is made of silicone rubber tubing. The catheter are about 60 cm long and have two Dacron cuffs on the subcutaneous and peritoneal portion of catheter that act as a anchors and prevent the migration of micro organisms down the shaft from the skin within a few weeks, fibrous tissue grown into the Dacron cuff holding the catheter in place and preventing bacterial penetration into the peritoneal cavity. There are two types of catheter used.

❖ Bent neck, curled catheters
❖ Disk catheters

TECHNIQUE:

The technique for catheter placement varies.

NON SURGICAL APPROACH:

An area approximately 2 cm below the umbilicus numbed with and local anaesthesia and a small stab wound is made.

➢ A catheter is inserted and abdomen is distended with dialysis solution
➢ A catheter place in to the peritoneal cavity

SURGICAL APPROACH:

A midline umbilical incision is made and a small puncture is made to one side of and below this incision.

- ➢ Distal end of the catheter is placed in the peritoneum and it is tunneled under the skin in to the puncture site
- ➢ After catheter is inserted the skin is cleaned with an antiseptic solution, and a sterile dressing is applied.
- ➢ A catheter is connected to a sterile tubing system and secure to the abdomen with tape
- ➢ A catheter is irrigated immediately with heparinised dialysate (500 ml) to clear it
- ➢ A the irrigation may continue for 12 to 24 hours using small volume of dialysate
- ➢ Before starting peritoneal dialysis it is preferable to allow a weighting period of 7 to 14 days for proper healing of catheter incision site and for tissue to grow into the cuffs.
- ➢ Once the catheter incision site is healed, clean a shower and then pat the catheter and exit the site dry

Daily catheter care includes application antiseptic solution and clean dressing as well as examination of catheter site for the signs of infection.

DIALYSIS SOLUTION:

One or two plastic bags (dianeal, inpersol) with glucose concentration of 1.5%, 2.5% and 4.25% the dialysate combination is similar to that of plasma. The dialysate solution is warmed to body temperature to increase peritoneal clearance, prevent hypothermia and enhance of comfort.

PHASES OF PERITONEAL CYCLE:

- Inflow
- Dwell
- Drain

INFLOW:

Solution is infused through the catheter over about 10 minutes. After the solution has been inferred the inflow clamp is closed before air enters the tubing.

DWELL:

The dwell phase or equilibrium, diffusion and osmosis occur between the patient’s blood and the peritoneal cavity. The duration of dwell time can lasts 20 to 30 minutes to 8 or more hours, depend on the method of peritoneal dialysis.

DRAIN:

Drain time may take 15 to 30 minutes and may be facilitated by gently massaging the abdomen or changing the position.

The cycle start again with the infusion a period of 30 to 50 minutes is required to complete and exchange.

COMPLICATIONS:

- ✓ Peritonitis
- ✓ Bleeding
- ✓ Respiratory difficult
- ✓ Abdominal pain
- ✓ Leakage
- ✓ Constipation
- ✓ Low serum albumin

HEMO DIALYSIS:

DEFINITION:

A synthetic semi permeable membrane replaces the renal glomeruli and tubercles act as filter of impaired kidneys.

VASCULAR ACCESS SITES:

1. FISTULA

Fistula is created surgically by connecting a joining an artery to vein either side or end side (AV Fistula). It takes 4-6 weeks to mature before needy to use.

2. GRAFT:

A graft is created by suturing a piece of bovine artery or vein, heterograft material or saphenous vein graft into the patient’s own vessel. Graft is placed in forearm, upper arm or upper thigh.

3. SHUNT:

The shunt consists of a U- shaped silastic tube divided at the midpoint and each of the two ends is placed in an artery and vein. External shunts were used in the past, but now rarely used due to numerous complications associated with them.

TEMPORARY VASCULAR ACCESS:

In some situations, immediate vascular access is required, percutaneous cannulation of the internal jugular or femoral vein is performed. A flexible Teflon, silicon rubber or poly urethane catheter is inserted into one of these large veins and provides access to circulation without surgery.

Temporary catheter in the jugular or subclavian veins can be left in place for 1 to 3 weeks, femoral vein cannulas can remain for up to 1 week.

HEMO DIALYSIS SYSTEM:

In hemo dialysis system, the blood is removed via a needle inserted in a fistula or via lumen catheter. It is propelled to the dialyzer by heparin pump. Heparin is infused either as blows before dialysis or through a heparin pump continuously to prevent clotting. Dialysate is pumped in and flows in to the opposite direction of the blood. The dialyzed blood is returned to the patient through the second needle on lumen catheter. Old dialysate and ultra filtration are drained and discarded.

TYPES OF HEMODIALYSIS:

- Home hemo dialysis
- Hemo dialysis
- Continuous Arteriovenous hemofiltration

DIALYZERS:

Dialyzers are a long plastic cartridge that contains thousands of parallel hallows tubes or fibres. The blood is pumped into the top of the cartridge and is dispersed into the top of the cartridge and is dispersed into all of the fibres.

HEMO DIALYSIS SCHEDULE:

It varies with the size of client, type of dialyzer used, the rate of blood flow, personal preference of the client and other factors.

THERAPEUTIC EFFECTS OF HEMO DIALYSIS:

- Clear the waste product from the body
- Restore the fluid and electrolyte balance

MANAGEMENT:

- During procedure promote patient comfort
- Meet the psychological considerations
- Dietary intake of electrolyte may be encouraged or restricted
- Restrict potassium
- Advice to continue the medications.

COMPLICATIONS:

- Disturbance of lipid and carbohydrate metabolism
- Congestive cardiac failure
- Coronary heart disease
- Stroke
- Peripheral vascular insufficiency
- Anaemia
- Diminished emotional and physical well being
- Back pain
- Hypotension
- Muscle cramps
- Loss of blood
- Hepatitis
- Sepsis

CURRENT TRENDS RECOMMENDATIONS FOR PROVIDING DIALYSIS TREATMENT TO PATIENTS WITH INFECTED DISEASE

The following recommendations take into consideration recent knowledge about update infection-control strategies for dialyzing patients with infected disease:

1. Procedures for environmental control and for disinfection and sterilization of hemo dialysis machines have been described. The hemo dialysis machine pumps dialysis fluid into the dialyzer (artificial kidney) where circulating blood from the patient is separated from the dialysis fluid by a membrane. The dialyzer, along with the associated blood lines, is disposable. Strategies for disinfecting the dialysis fluid pathways of the hemo dialysis machine are targeted to control bacterial contamination and generally consist of using about 500-750 ppm of sodium hypochlorite for 30-40 minutes or 1.5%-2.0% formaldehyde overnight. In addition, several chemical germicides

formulated to disinfect dialysis machines are commercially available. None of these protocols or procedures need to be altered after dialyzing patients infected with HTLV-III/LAV. Chemical germicides used for disinfection and sterilization of devices in the dialysis centre are effective against HTLV-III/LAV.

2. Patients infected with HTLV-III/LAV can be dialyzed by either hemo dialysis or peritoneal dialysis and do not need to be isolated from other patients. The type of dialysis treatment (i.e., hemo dialysis or peritoneal dialysis) should be based on the needs of the patient. The dialyzer may be discarded after each use. Alternatively, centers that have dialyzer-reuse programs, in which a specific dialyzer is issued to a specific patient, removed, cleaned, disinfected, and reused several times on the same patient only, may include HTLV-III/LAV-infected patients in the dialyzer-reuse program. An individual dialyzer must never be used on more than one patient.

3. Standard infection-control strategies that are used routinely in dialysis units for all dialysis patients and personnel should be used to prevent HTLV-III/LAV transmission. Specifically, these strategies include blood precautions and barrier techniques, such as the use of gloves, gowns, and hand washing techniques that have been described elsewhere.

REFERENCES:

[1] Black M. Joyce and Jane Hokanson Hawks, (2005). **“Medical surgical nursing”,** (7th edition), Missouri: Saunders, Page No: 949 – 968.

[2] Lewis, et. al., (2007). **“Medical surgical nursing”,** (7th) edition), Missouri: Mosby, Page No: 1204 -1216.

[3] Phipps, Long and Woods, (1999). **“Shaffer’s Medical Surgical Nursing”,** (7th edition), New Delhi: B.I Publications Pvt. Ltd., Page No: 643-647.

[4] Smeltzer C. Suzanne and Bare G., Brenda, (2004). **“Brunner and suddarth’s text book of Medical surgical Nursing”,** (10th edition), Philadelphia :Lippincott Williams and Wilkins, Page No:1326-40

[5] htt/ptt/:www.dialysis.com

[6] htt/ptt/:emedicine.medscape.com

[7] http ://www.ncbi.nlm.nih.gov/pubmed

[8] http ://www. nlm. nib. gov/medcineplus

[9] http ://www.emedicine. medscape.com

[10] http ://www. Nephrology channel. Com

Smart Parking System Using IoT

Dr. K Madhavi[1], Naveen Kandulu[2], Ravada Mohan Rao[3], Susmitha Manimala Vandrasi[4], Gonthina Kumar Swamy[5]

Associate Professor, Department of Computer Science and Engineering, NSRIT, Visakhapatnam, India[1].
Student, Department of Computer Science and Engineering, NSRIT, Visakhapatnam, India[2,3,4,5]

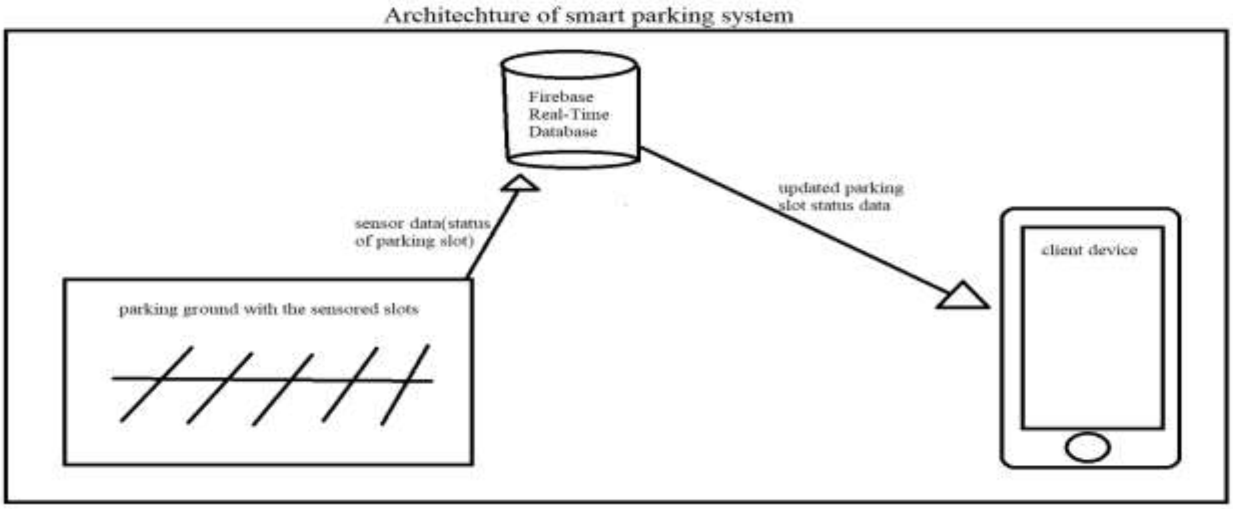
***Abstract*: Parking problems are very much common in most of the major cities of any country. The narrow accessibility of parking results in traffic blocking, air effluence as well as driver frustration. The price for parking extension is frequently unaffordable or enormously high. Recently investigators turned to apply technologies for effective parking administration. It is understood that this simple development could be applied to monitor vehicles in parking spaces can be executed. In this arrangement, the driver can get the position of the parking slot through the website. The system can then notify drivers for the number of accessible parking spaces. The system should be achieved over the less network circulation and diminish the database server disruptions preserving the organization in the client data fast and precise response. The system should apply to large and small areas. The system should provide reliable performance.**

***Keywords*: database, IoT, technologies, performance**

Introduction

Nowadays parking is a big problem in the major cities .the expansion of the parking slot is impossible an finding the free parking slots in open parking tougher. So there are many systems by using the technologies provided the efficient parking management but the existing systems use the brute force method to perform this activity. On a device will update the data int the database and the client device is continuously requesting the updated data on the database server which leads to the more amount of load on the database server. The network traffic increased and the data on the clients will not in the synchronized manner. For those problems, there is a solution called the firebase real-time database. The Firebase Realtime Database is cloud-hosted. Data is stored as JSON and synchronized in real-time to every connected client. There will be a module built out by node MCU and the ultrasonic sensor which is used to update the status of the parking slot to the firebase. When the change in the data of the Realtime Database, all of your clients share one Realtime Database instance and automatically receive updates with the newest data. In this model, the client device doesn't need to interrupt the database server continuously. When the change occurs the client will receive the data so less network usage. as the equipment is small as it provides a portable feature which supports to use in the open area parking. the devices are individual bodies so it supports use as our requirement those can be used for large and small scale areas.

Block diagram


Architechture of smart parking system
Firebase Real-Time Database
sensor data(status of parking slot)
updated parking slot status data
parking ground with the sensored slots
client device

Requirements

Hardware requirement

NodeMCU

NodeMCU V3 is an open source firmware & development kit that shows an important character in planning an IoT product with a few writing lines. Various GPIO pins on the board allows us to link the board with other peripherals. This capability to read the ultrasonic data with the help of the ESP8266 Wi-Fi SoC can connect with the internet and send the data to the firebase.

Ultrasonic sensor

An ultrasonic sensor is a power-driven device that procedures the distance of a goal element by discharging ultrasonic sound waves & interprets the reproduced sound into an electrical signal. Ultrasonic waves travel quicker than the rapidity of noticeable sound (the sound that individuals can catch). Ultrasonic sensors have mainly two workings: the spreader (which produces the sound via piezoelectric crystals) & the receiver (which run into the sound after it has traveled to & from the goal).

Software requirement

Firebase real-time database

The Firebase Realtime Database is cloud-hosted. Data is stored as JSON and synchronized in real-time to every connected client. When the change in the data of the Realtime Database, all of your customers share one Realtime Database occurrence & inevitably obtain updates with the latest data.

Key capabilities

Real-time

As an alternative of typical HTTP appeals, the Firebase Real time Database performs data association - every time data variations, any linked device obtains that apprise within no time. Provide concerted & immersive involvements without thinking about the interacting code.

Offline

Firebase apps endure approachable even whenever it is offline since the Firebase Real time Database SDK perseveres your statistics to disk. Once connectivity is reinvented, the client device attains any adjustments it lost, coordinating it with the current server state.

Accessible from Customer Devices

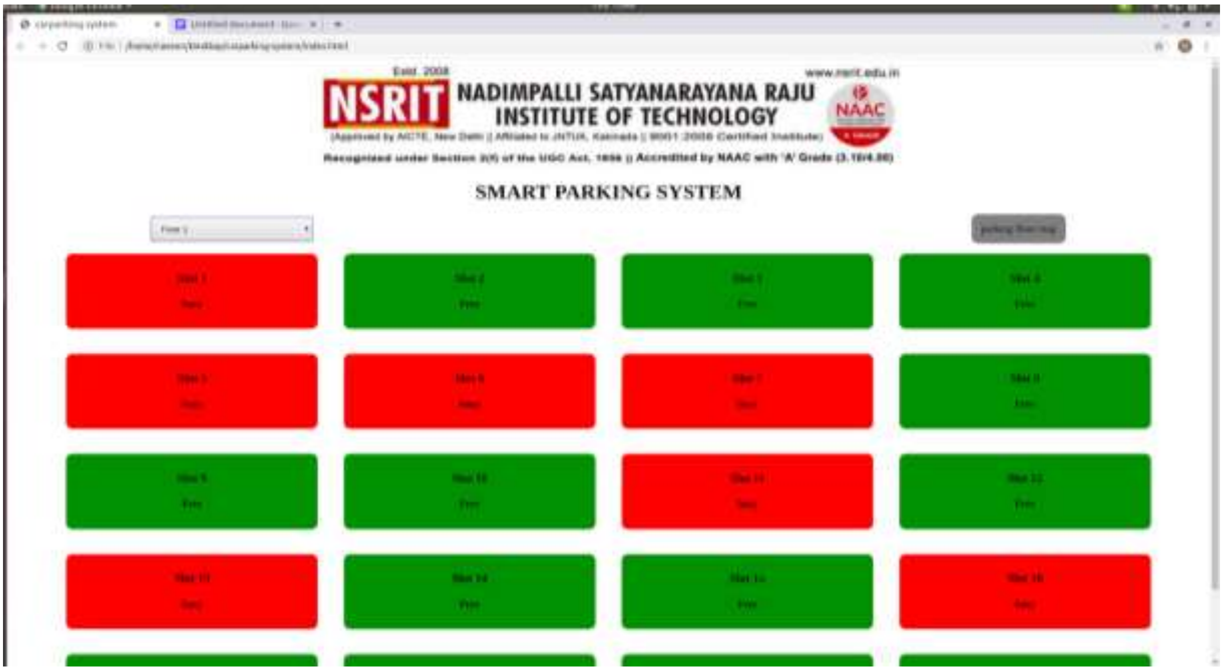
The Firebase Real time Database can be retrieved openly from any of the device or any of the web browser; there is no necessity for submission server. Security & data authentication are accessible over the Firebase Real time Database Safety Rules, expression-based instructions that are implemented when statistics is deliver or written

Web technologies

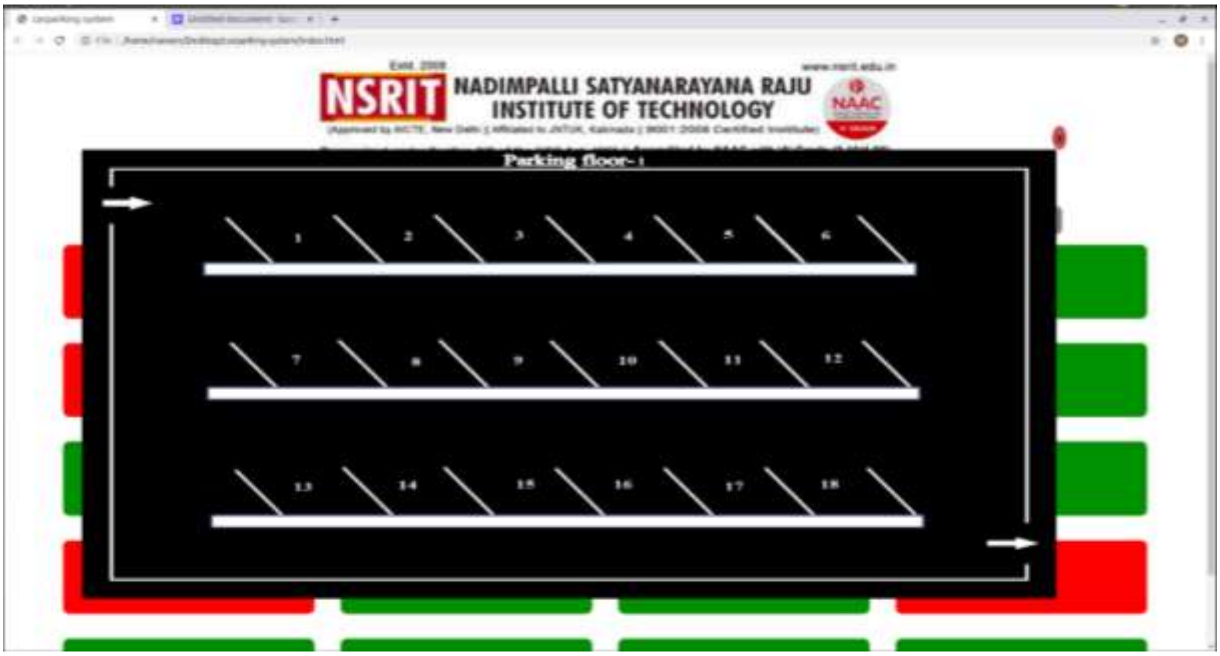
The programing knowledge required to build a webpage like HTML, CSS, JavaScript. Some knowledge on working with the JSON objects and JSON format data.

Results

Data of available slots



Map of slots



Conclusion

In this project, we are presented and advance improvements to the existing system the can be implemented right now with the technical advancement. in my project, I used a fire base real time database to send the data to the client when the parking slot is changed over the website. by that, the database server load will be reduced and network traffic is minimized. a reliable consistent system can be created.

Future Scope

In the future, we would like to add the slot reservation feature with the location-based system, and we will suggest the nearest and available slot for the driver if he ok with it he can reserve the solve and he will directly navigate to that slot.

References

[1] J. Rico, J. Sancho, B. Cendon, M. Camus, "Parking easier by using context information of a smart city: Enabling fast search and management of parking resources", Advanced Information Networking and Applications Workshops (WAINA) 2013 27th International Conference on, pp. 1380-1385, 2013, March.

[2] Y. Zheng, S. Rajasegarar, C. Leckie, "Parking availability prediction for sensor-enabled car parks in smart cities", Intelligent Sensors Sensor Networks and Information Processing (ISSNIP) 2015 IEEE Tenth International Conference on, pp. 1-6, 2015, April.

[3] F. Zhou, Q. Li, "Parking Guidance System Based on ZigBee and Geomagnetic Sensor Technology", Distributed Computing and Applications to Business Engineering and Science (DCABES) 2014 13th International Symposium on, pp. 268-271, 2014, November.

[4] A. Botta, W. De Donato, V. Persico, A. Pescapé, "On the Integration of Cloud Computing and Internet of Things", Future Internet of Things and Cloud (FiCloud) 2014 International Conference on, pp. 23-30, 2014, August.

[5] A. Zaslavsky, C. Perera, D. Georgakopoulos, "Sensing as a service and big data", arXiv preprint arXiv: 1301.0159, 2013.

[6] C. Doukas, L. Capra, F. Antonelli, E. Jaupaj, A. Tamilin, I. Carreras, "Providing generic support for IoT and M2M for mobile devices", Computing & Communication Technologies-Research Innovation and Vision for the Future (RIVF) 2015 IEEE RIVF International Conference on, pp. 192-197, 2015, January.

[7] C. Tsirmpas, A. Anastasiou, P. Bountris, D. Koutsouris, "A new method for profile generation in an Internet of Things environment: An application in ambient assisted living.

[8] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, V. Suciu, "Smart cities built on resilient cloud computing and secure internet of things", Control Systems and Computer Science (CSCS) 2013 19th International Conference on, pp. 513-518, 2013, May.

[9] S. K. Dash, S. Mohapatra, P. K. Pattnaik, "A survey on applications of wireless sensor network using cloud computing", International Journal of Computer science & Engineering Technologies (E-ISSN: 2044-6004), vol. 1, no. 4, pp. 50-55, 2010.

Author Details

	Dr. Madhavi Kolukuluri, working as Associate Professor in department of Computer Science and Engineering, Nadimpalli Satyanarayana Raju Institute of Technology, Visakhapatnam. She is having total 14 years of teaching experience. Her areas of interests are Data Mining, Software Engineering and Computer Networks. She Guided UG and PG students and having 4 papers published in international journals. **Dr . K . Madhavi** Associate Professor, NSRIT, Visakhapatnam, India kolukulurimadhavi@gmail.com
	Mr. Naveen kandula Student, CSE NSRIT, Visakhapatnam, India naveenkandula1002@gmail.com
	RAVADA MOHAN RAO Student, CSE NSRIT, Visakhapatnam, India Mohanravad666@gmail.com
	Susmitha Manimala Vandrasi Student, CSE NSRIT, Visakhapatnam, India susmithavandrasi27@gmail.com

	Gonthina kumar swamy Student, CSE NSRIT, Visakhapatnam, India Kumarswamy1616@gmail.com

Matrix method for determining Minimum Spanning Tree

Prof. Farhan Banu

Assistant Professor
Department of Mathematics,
University of Dhaka, Bangladesh

Abstract: **This paper is concerned with Minimum Spanning Tree problem, a fundamental problem of Network modeling. Here we have proposed a novel approach to determine minimum spanning tree of an undirected connected network which is also demonstrated with numerical example.**

Index Terms: **spanning tree, Network model, shortest length.**

I. Introduction

Minimum Spanning Tree (MST) problem: Given a connected graph G which has positive weights on each edge. The target is to find a set of edges with minimum weights that connects all of the vertices. A graph can have a number of different spanning trees. A Minimum Spanning Tree (MST) for a weighted, connected and undirected graph is a spanning tree with weight less than or equal to the weight of every other spanning tree. The weight of a spanning tree is the sum of weights given to each edge of the spanning tree. The minimum spanning tree may not be unique if the graph has two or more edges with equal weights.

In network modeling, determining Minimum Spanning Tree (MST) is a fundamental problem which has a variety of applications in different sectors such as: Network design: TV /computer cable, telephone, road, Travelling salesman problem, Taxonomy [1], Cluster analysis [2, 3], Circuit design[4] etc.

A number of algorithms are developed for solving MST. Among them some greedy algorithms are mainly used now a days. The very first algorithm [5, 6] for finding a minimum spanning tree was developed in 1926 by Otakar Borvka. After that Prim's algorithm which is mostly used was invented by Vojtch Jarnk in 1930 and rediscovered by Prim in 1957[7]. Kruskal's[8] algorithm and reverse-delete algorithm, which is the reverse of Kruskal's algorithm are also well known though reverse-delete algorithm are usually not in use.

Our approach is inspired by the idea of Prim's algorithm.

The rest of the paper is organized as follows:

In the next section we have discussed the basic idea of our proposed approach. We have explained the methodology in details in the following section. A numerical example is included in section 3. Finally we have concluded our work in section 4.

II. Methodology

The idea of Matrix method for MST is inspired by Prim's Algorithm described as follows:

Initial step: We start with the first node say a. Consider a connected set C whose first entry is the node a and let DC be the disconnected set which contains all other nodes in the network. We can start with any other node as well.

- Consider a matrix whose columns are labelled with the name of nodes and entries are the length of all adjacent nodes to node a in the respective column.
- Determine the minimum of all these distances from node a to all other nodes in the disconnected set . Select the node corresponding to the minimum length as the next node to enter the connected set

General steps: The newly selected node enters the connected set and leaves the disconnected set. We insert a new row to the matrix of connected set described in initial step whose entries are the lengths of all adjacent nodes to this newly selected node in the respective column.

Determine the minimum of all the lengths from the nodes of connected set to all the nodes in the disconnected set. Consider the node corresponding to the minimum length as the next node to enter the connected set. Cross out all the connection (length) between the nodes in the connected set to avoid cycle. At each iteration we include a node to the connected set. We continue the process until we get all the nodes in the connected set.

If in a network there are n nodes then we need $(n-1)$ iteration to complete the procedure.

III. Explanation:

Suppose we have a network of n nodes $1, 2, 3, \dots, n$. We define the disconnected set

$DC = \{1, 2, 3, \dots, n\}$ The distance matrix $D = [d_{ij}]$ where d_{ij} represents the distance from node i to node j is as follows:

	1	2	3	…	n
1	-	d_{12}	d_{13}	…	d_{1n}
2	d_{21}	-	d_{23}	…	d_{2n}
3	d_{31}	d_{32}	-	…	d_{3n}
⋮	⋮	⋮	⋮	⋮	⋮
n	d_{n1}	d_{n2}	d_{n3}	…	-

We start 1st iteration with node 1 and the corresponding table:

	1	2	3		k	…	n
1	-	d_{12}	d_{13}	…	d_{1k}	…	d_{1n}

Table 1: Iteration: 1

Suppose d_{1k} is the smallest length. At the 2nd iteration we include k to the connected set and the table at this stage is shown in Table 2.

	1	2	3	…	k	…	n
1	-	d_{12}	d_{13}	…	$d_{1k}{}^{*}$	…	d_{1n}
k	-	d_{k2}	d_{k3}	…	-	…	d_{1n}

Table 2: Iteration 2

Since 1 is in the connected set so in Table-2 we replaced d_{k1} with a bar $(-)$ to avoid cycle. In general, at any iteration if j is selected to enter the connected set with shortest distance d_{sj} from node s where s is in C and if i is any node in C, then at the next iteration we put bar $(-)$ for all the distance d_{ij} and d_{ji} except d_{sj} as shown in Table 3.

We continue the process until all the nodes of the graph are in the connected set C.

	1	2	3	…	k	…	s	…	j	…	N
1	−	d_{12}	d_{13}	…	$d_{1k}{}^*$	…	d_{1s}	…	−	…	d_{1n}
k	−	d_{k2}	d_{k3}	…	−	…	−	…	−	…	d_{kn}
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
s	−	d_{s2}	d_{s3}	…	−	…	−	…	$d_{sj}{}^*$	…	d_{sn}
j	−	d_{j2}	d_{j3}	…	−	…	−	…	−	…	d_{jn}

Table 3: At some Iteration: Here the connected set is $C = \{1, k, ..., s, j\}$.

IV. Numerical Experiment

To explain the algorithm with a numerical example, we choose a graph of 6 nodes shown in Figure 1 :

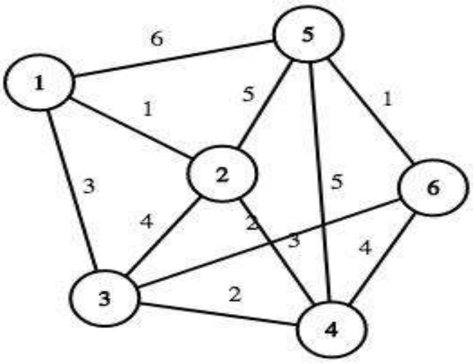


Figure 1: Undirected graph

The distance matrix D for the above graph is given by

Table 4

	1	2	3	4	5	6
1	−	1	3	−	6	−
2	1	−	4	3	5	−
3	3	4	−	2		2
4	−	3	2	−	5	4
5	6	5	−	5	−	1
6	−	−	2	4	1	−

.

Iteration 1 starts with node 1. We can choose any node to start with.

Table 5: Iteration 1: $C = \{1\},\ DC = \{2, 3, 4, 5, 6\}$.

	1	2	3	4	5	6
1	−	1	3	−	6	−

Here 1 is the smallest length from node 1 to node 2 so we select 2 as the next entering node in the connected set as shown in table 6.

Table 6: Iteration 2: $C = \{1, 2\},\ DC = \{3, 4, 5, 6\}$.

	1	2	3	4	5	6
1	−	1^*	3	−	6	−
2	−	−	4	3	5	−

At iteration 2, since node 1 is already in the connected set so we replace the length d_{21} with a bar $(-)$ which implies this length will be excluded for further consideration to avoid the generation of cycle. The minimum length from the nodes of connected set to all other nodes of disconnected set is 3 which appears in two cells d_{13} and d_{24}. We can choose any of them randomly and the resulting minimum length of the spanning tree will be same. First we choose the cells d_{24} and continue further iterations. Thus node 4 becomes the next entering node in the connected set. Alternatively we can select d_{13} which will be shown later.

Table 7: Iteration 3: $C = \{1, 2, 4\}, DC = \{3,\ 5,\ 6\}$.

	1	2	3	4	5	6
1	−	1^*	3	−	6	−
2	−	−	4	3^*	5	−
4	−	−	2	−	5	4

At iteration 3 we cross out the lengths d_{42} to avoid cycles. In general if a node is in the connected set then the column corresponding to that node will contain a single entry (the length for which it was selected to entre the connected set) at the final matrix.

The following iteration selects node 6 to entre the connected set. At the last iteration, node 5 enters the connected set and thus $DC = \{\ \}$. We get the minimum spanning tree with edges $E = \{(1,\ 2),\ (2, 4),\ (4,\ 3),\ (3,\ 6),\ (6,\ 5)\}$ and minimum length $ML = 9$.

Table 8: Iteration 4

$C = \{1, 2, 4, 3\}, DC = \{5, 6\}$

	1	2	3	4	5	6
1	−	1^*	−	−	6	−
2	−	−	−	3^*	5	−
4	−	−	2^*	−	5	4
3	−	−	−	−	−	2

Table 9: Iteration 5

$C = \{1, 2, 4, 3,\ 6\}, DC = \{5\}$

	1	2	3	4	5	6
1	−	1^*	−	−	6	−
2	−	−	−	3^*	5	−
4	−	−	2^*	−	5	−
3	−	−	−	−	−	2^*
6	−	−	−	−	1	−

Alternatively: if we choose d_{13} as the minimum length and select node 3 in iteration 2 as shown in table 6, we will have Table 10 and the successive iteration will be as follows.

Table 10: Iteration 2: $C = \{1, 2\}$

	1	2	3	4	5	6
1	–	1^*	3	–	6	–
2	–	–	4	3	5	–

Table 11: Iteration 3: $C = \{1, 2, 3\}$

	1	2	3	4	5	6
1	–	1^*	3^*	–	6	–
2	–	–	–	3	5	–
3	–	–	–	2	–	2

Thus we get a different spanning tree with edges $E = \{(1, 2), (1, 3), (3, 6), (6, 5), (3, 4)\}$ and minimum length $ML = 9$. We may have some other alternative minimum span- ning tree since we have several edges with equal lenght. The number of iteration required for determining these MST will be same

Table 12: Iteration 4: $C = \{1, 2, 3, 6\}$

	1	2	3	4	5	6
1	–	1^*	3^*	–	6	–
2	–	–	–	3	5	–
3	–	–	–	2	–	2^*
6	–	–	–	4	1	–

Table 13: Iteration 5: $C = \{1, 2, 3, 6, 5\}$

	1	2	3	4	5	6
1	–	1^*	3^*	–	6	–
2	–	–	–	3	5	–
3	–	–	–	2	–	2^*
6	–	–	–	4	1^*	–
5	–	–	–	5	–	–

V. Conclusion

In network modeling, Minimum Spanning Tree (MST) is a fundamental problem. A number of algorithms are developed for solving MST . Among them Prim's algorithm and Kruskal's algorithm are mainly in use. In this paper we have proposed a new approach which is inspired by the idea of Prim's algorithm. The advantage of our approach is that we do not need to work with graph at each iteration unlike Prim's and Kruskal's algorithms. We first determine the distance matrix and then solve the problem using the distances. Though the number of iteration required for our proposed approach is similar to that of Prim's and Kruskal's but working with matrix is a great advantage over that with graphs.

REFERENCES

[1] P.H.A. Sneath, The Application of Computers to Taxonomy. Journal of General Microbiology. 17 (1): 201226. doi:10.1099/00221287-17-1-201, 1957.

[2] S. Theodoridis and K. Koutroumbas, Pattern Recognition. Elsevier Inc., 2009.

[3] S. Theodoridis and K. Koutroumbas. An Introduction to Pattern Recognition, A MATLAB approach, Elsevier Inc., 2010.

[4] H. Ohlsson, Implementation of low complexity FIR filters using a minimum spanning tree. 12th IEEE Mediterranean Electrotechnical Conference (MELE- CON 2004). 1, 261264. doi:10.1109/MELCON.2004.1346826.

[5] Borvka, Otakar, O Jist´em Probl´emu Minim´aln lm. Pr´ace Moravsk´e Pˇr lrodovdeck´e Spoleˇcnosti III, 3 (1926): 3758.

[6] https://algowiki-project.org/en/Boruvka's algorithm# cite note-1 .

[7] R. C. Prim, Shortest Connection Networks and Some Generalizations, Bell System Technical Journal, 36(6), 13891401, 1957. doi:10.1002/j.1538- 7305.1957.tb01515.x.

[8] J. B. Kruskal, On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem, Proceedings of the American Mathematical Society, 7(1), 1956, 48-50. doi:10.1090/S0002-9939-1956-0078686-7.