

DEPARTMENT OF STATISTICS

END SEMISTERE EXAMINATION OF SEMISTER-VI,2019

PROJECT WORK ON

"A COMPARISION STUDY OF CYBER CRIMES
IN INDIA, STATISTICAL INVESTIGATION"

WBMITED BY-

ROUL: MC/UG/S-VI/19 NO: 1520

REG. NO: 2016-255 OF 2016-2017

COURCE: UG SECTION: DAY

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my teacher *Mrs. Anindita Ghosal* who gave me the golden opportunity to do this wonderful project on the topic "*A COMPARISON STUDY OF CYBER CRIMES IN INDIA – A STATISTICAL INVESTIGATION*", which also helped me to pursue my project work and I came to know about so many new things. I am really thankful to her. I also heartily express my gratitude to all the teachers of this department for their constant support and guidance.

Secondly, I would also like to thank my parents and friends who helped me a lot in finishing this project within the limited time. I am making this project not only for marks but to also increase my knowledge. Thanks again to all who helped me.

> Ranadip Kar Dept. of Statistics,

Midnapore College (Autonomous).

TO WHOM IT MAY CONCERN

This is to certify that the 6^{th} semester student of BSC(Honours) in Statistics with Roll: MC/UG/S-VI/19 NO: 1320, Reg. NO: 2016-255 of 2016-2017, has completed the project work (Academic session: 2019) entitled "A COMPARISON STUDY OF CYBER CRIMES IN INDIA—A STATISTICAL INVESTIGATION" from the department of Statistics, Midnapore College(Autonomous) under the supervision of the faculties of the department.

Aspiring for every success in life, thanking you.

Mrs. AninditaGhosa
Midnapore College(Autonomous)

CONTENTS

- > INTRODUCTION
- ➢ OBJECTIVE
- > METHODOLOGY
- > DESCRIPTION OF DATA
- > PLOTTING OF GRAPHS
- > RESULTS
- **CONCLUSION**
- **BIBLIOGRAPHY**

INTRODUCTION

The usage of internet services in India is growing rapidly. It has given rise to new opportunities in every field we can think of-be it entertainment, business, sports or education. There are some pros and cons of some new types of technology which are been involved or discovered. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spam's and software piracy and so on, which invade our privacy and offend our senses. Criminal activities in the cyberspace are on the rise.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyber-terrorism are also of significant concern. Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

- Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DOS) attacks.
- Crimes that use computer networks to advance other criminal activities. These types of crimes include cyber-stalking, phishing and fraud or identity theft.

CYBER CRIME IN INDIA

As India become the fourth highest number of internet user in the world, cyber crimes in India has also increased 50% in 2016 over the previous years. According to the information technology (IT) Act, the majority of offenders were under 30 years of age.

Around 46% of cyber crimes were related to incidents of cyber pornography, followed by hacking. According to recent published 'crime in 2016 report', published by the national crime record bureau (NCRB), in over 60% of these cases, offenders were between 18 and 30. These cyber crimes are punishable under two categories; the IT Act 2000 and the Indian penal code (IPC). In order to tackle with cyber crime, Delhi police have trained 100 of its officers in handling cyber crime and placed them in its economic offences wing.

DIFFERENT TYPES OF CYBER CRIMES

Cyber Crimes can be categorized in two ways:

- 1. The crimes in which the computer is the target. Examples of such crimes are hacking, virus attacks, DOS attack etc.
- 2. The crime-sin which the computer is used as a weapon. These types of crimes include cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc.

DIFFERENT KINDS OF CYBER CRIMES

The different kinds of cyber crimes are:

1. Unauthorized Access and Hacking:

Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

2. Web Hijacking:

Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

3. Pornography:

Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

4. Child Pornography:

The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet. Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes Pedophiles contact children in the chat rooms posing as teenagers or a child of similar age and then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money or falsely promising them good opportunities in life. The pedophiles then sexually exploit the

children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

5. Virus attacks:

Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available.

6. Software Piracy:

Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider's name so as to attract their users and get benefit from them.

7. Sale of illegal articles:

This category of cyber crimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

8. Online gambling:

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported.

9. Email spoofing:

Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

10. Cyber Defamation:

When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.

11. Theft of information contained in electronic form:

This includes theft of information stored in computer hard disks, removable storage media etc.

12. Email bombing:

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

13. Data diddling:

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

14. Internet time theft:

Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

15. Theft of computer system:

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

16. Physically damaging a computer system:

This crime is committed by physically damaging a computer or its peripherals.

17. E-commerce/ Investment Frauds:

An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

18. Cyber Terrorism:

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyber terrorism is an attractive option for modern terrorists for several reasons. The list of offenses given above is not exhaustive and would also include any other types of offenses that would be committed through a computer or against a computer in the future.

OBJECTIVE

The main objectives of this project are:

- ✓ Collecting data from the internet about cyber crime in India and divided them into six part by the six region of India.
- ✓ Comparison cyber crime of India for year 2007-2016 region wise (graphically).
- ✓ Drawing a multi diagram to do the comparison over all collected data about cyber crime in India (region & year wise).
- ✓ Comparison of percentages increase of cyber crime in India region wise.
- ✓ To know which zone among the six zones, viz: Northern region, Central region, Eastern region, North-Eastern region, Southern region, Western region are more cyber crime prone.

METHODOLOGY

• Analysis of two-way classified data with one observation per cell:

We can plan an experiment in such a way as to study the effects of two factors in, the same experiment. For each factor there will be a number of classes or levels. We shall first consider the case of one observation per cell (or combination). Let the factors be A and B and the levels A_1, A_2, \ldots, A_p and B_1, B_2, \ldots, B_q . Let Y_{ij} be the observation under the i^{th} level of A and the j^{th} level of B. The observations can be

TABLE OF OBSERVATIONS

	B ₁	B_2 B_j B_q	Total	Mean
A_1	Y ₁₁	$Y_{12} \dots \dots Y_{1j} \dots Y_{1q}$	T_{10}	Y_{10}
A ₂	Y_{21}	Y_{22} Y_{2j} Y_{2q}	T_{20}	Y_{20}
:				
:			T	V
A_i	Y_{i1}	Y_{i2} Y_{ij} Y_{iq}	T_{i0}	Y_{i0}
$A_{\mathbf{p}}$	Y_{p1}	Y_{p1} Y_{pj} Y_{pq}	T_{p0}	Y_{p0}
Total	T_{01}	T_{02} T_{0j} T_{0q}	T_{00}	
Mean	Y ₀₁	Y_{02} Y_{0j} Y_{0q}		Y ₀₀

Fixed-effects model

represented as follows:

Here the mathematical model may be written as:

$$Y_{ij} = \mu_{ij} + e_{ij}$$
, $i=1,2,....,p$; $j=1,2,....,q$

Where e_{ij} are independently normally distributed with common mean zero and common variance σ^2 . Corresponding to the above table of observations, we can form a table of expected values of observations. Here either these are the only levels of the two factors or we are interested only in these levels included in the experiment.

TABLE FOR EXPECTATIONS

	B_1	$B_2 \ldots B_j \ldots B_q$	Mean	Difference
A_1	μ_{11}	μ_{12} μ_{1j} μ_{1q}	μ_{10}	μ_{10} - μ = α_1
A ₂	μ_{21}	μ_{22} μ_{2j} μ_{2q}	μ_{20}	μ_{20} - μ = α_2
:				
A _i	μ_{i1}	μ_{i2} μ_{ij} μ_{iq}	μ_{i0}	μ_{i0} - μ = α_i
:				
Ap	μ_{p_1}	μ_{p1} μ_{pj} μ_{pq}	μ_{p0}	μ_{p0} - μ = α_p
Mean	μ_{01}	μ_{02} μ_{0j} μ_{0q}	μ	
Difference	μ_{01} - μ	μ_{02} - μ μ_{0j} - μ μ_{0q} - μ		
	β_1	$=\beta_2$ $=\beta_j$ $=\beta_q$		

Now, we can think $\boldsymbol{\mu}_{ii}$ as being composed of the following parts :

$$\begin{split} \mu_{ij} = & \mu + (\mu_{i0} - \mu) + (\ \mu_{0j} - \mu) + (\ \mu_{ij} - \mu_{i0} - \mu_{0j} + \mu) \\ = & \mu + \alpha_i + \beta_j + \gamma_{ij} \ , \, \text{say} \end{split}$$

Where μ is a constant general effect, present in all the observations;

$$\alpha_i = \mu_{i0} - \mu$$

is an effect due to the i^{th} level of the factor A, which is common to all the observations belonging to this level of A;

$$\beta_i = \mu_{0i} - \mu$$

is an effect due to the j^{th} level of the factor B, which is common to all the observations belonging to this level of B; and

$$\gamma_{ij} = \mu_{ij} - \mu_{i0} - \mu_{0j} + \mu$$

is called the interaction between the i^{th} level of A and the j^{th} level of B. It is an effect peculiar to the combination (A_i, B_j) . It is not present in the i^{th} level of A or in the j^{th} level of B if not taken together. If the joint effect of A_i and B_j is different from the sum of the effects due to A_i and B_j taken individually, then we say that there is interaction and it is measured by γ_{ii} .

From the table of expected value for the fixed-effects model, it is clear that-

$$\sum_{i} \alpha_{i} = 0,$$
 $\sum_{j} \beta_{j} = 0,$ $\sum_{i} \gamma_{ij} = 0,$ $\sum_{j} \gamma_{ij} = 0$

The observation γ_{ij} is the (i, j) th cell may thus be expressed as-

 γ_{ij} = a constant general effect (μ)+ an effect due to the i^{th} level of A (α_i)+ an effect due to the j^{th} level of B (β_j)+ interaction between A_i and B_j (γ_{ii})+ error (e_{ij})

In the case of two-way classified data with one observation per cell, the interaction (γ_{ij}) cannot be estimated, and we shall assume for the fixed-effects model that there is no interaction, i.e. γ_{ii} =0 for all I and j. So the model reduces to-

$$Y_{ij} = \mu + \alpha_i + \beta_j + e_{ij}$$

With $\sum_i \alpha_i = \sum_j \beta_j = 0$ and e_{ij} being independently normally distributed with common mean zero and common variance σ_e^2 .

The least-square estimators, obtained by minimising

$$\sum_i \sum_j (Y_{ij} - \mu - \alpha_i - \beta_j)^2$$
, are $\hat{\mu}$ = Y_{00} , $\hat{\alpha_i}$ = Y_{i0} - Y_{00} and $\hat{\beta_i}$ = Y_{0j} - Y_{00}

In the model, each observation is the sum of four components, and the analysis of variance partitions the raw SS, $\sum_i \sum_j Y_{ij}^2$, also into four components—SS due to general effect, SS due to factor A, SS due to factor B and SS due to error—as follows:

$$Y_{ij} = Y_{00} + (Y_{i0} - Y_{00}) + (Y_{0j} - Y_{00}) + (Y_{ij} - Y_{i0} - Y_{0j} + Y_{00})$$

Squaring both sides and summing over I and j, we get

$$\sum_{i}^{1} \sum_{j} (Y_{ij} - Y_{00})^{2} = q \sum_{i} (Y_{i0} - Y_{00})^{2} + p \sum_{j} (Y_{0j} - Y_{00})^{2} + \sum_{i} \sum_{j} (Y_{ij} - Y_{i0} - Y_{0j} + Y_{00})^{2}$$

In words,

total SS= SS due to factor A + SS due to factor B + SS due to error, or, in short,

$$total SS = SSA + SSB + SSE$$

The corresponding partitioning of the total df is as follows:

Dividing an SS by its df, we get the corresponding MS.

By partitioning the total SS and the total *df* into three components each. we shall be able to test the following two hypotheses-

$$H_A: \alpha_1 = \alpha_2 = \dots = \alpha_P = 0$$

Vs $H_B: \beta_1 = \beta_2 = \dots = \beta_q = 0$

for the equality of the effects of the different levels of A and of the different levels of B, respectively. To derive appropriate tests for the hypotheses, we find the expectations of the mean squares. It can be shown that

E(MSA)=
$$\sigma_e^2 + q\sum_i \alpha_i^2/(p-1)$$

E(MSB)= $\sigma_e^2 + P\sum_J \beta_J^2/(q-1)$
And E(MSE)= σ_e^2

If H_A : $\alpha_1 = \alpha_2 = \dots = \alpha_P = 0$ is true, E(MSA)=E(MSE), and hence $F_0 = \text{MSA/MSE}$ will give the test of H_A . So a test for the hypothesis of equality of the effects of the different levels A Is provided by this F_0 , which follows the F-distribution with df = (P - 1), (p - 1) (q - 1). This results obtained by an application of the theorem of importance in Model-I analysis. Thus the null hypothesis Will be rejected at the 100a% level if (and only if)-

$$F_0 = \frac{MSA}{MSE} > F_{\alpha,(P-1),(p-1)(q-1)}$$

The alternative hypothesis in this case is H'_A : α 's are not equal.

Similarly, H_B : $\beta_1 = \beta_2 = \dots = \beta_q = 0$, for equality of the effects of the different levels of B, is rejected at the 1000% level if

$$F_0 = \frac{MSB}{MSE} > F_{\alpha,(q-1),(p-1)(q-1)}$$

The alternative hypothesis in this case is $H_{B}^{'}$: β 's are not all equal.

These calculations are shown in the following analysis of variance Table. After performing the F-test, we can test for the equality of the means of any pair of A-classes or any pair of B-classes with the help of the t-test. Here A be the region and B be the year.

ANALYSIS OF VARIANCEFOR TWO-WAY CLASSIFIED DATA WITH ONE OBSERVATION PER CELL

Source of	df	SS	MS	$\boldsymbol{F_0}$	F at le	vel
variation					1%	5%
Between	P-1	$q\sum_{i}(Y_{i0} -$	SSA/(p-1)=MSA	MSA		
the levels		$Y_{00})^2 = SSA$		MSE	-1)	-1)
of A				1465	- b)	- b)
	q-1		SSB/(q-1)=MSB	MSB	- 1)	- 1) - 1)
Between		$p\sum_{j}(Y_{0j} -$		MSE	1),(p - 1),(p -	1),(p - 1),(p -
the levels of B	(p-1)(q-1)	$(Y_{00})^2 = SSB$	$\frac{SSE}{(p-1)(q-1)} = MSE$			1 1
Error		$\sum_{i} \sum_{j} (Y_{ij} - Y_{i0} - Y_{0j} + Y_{00})^{2} = SSE$			F.01	$F_{.05:(\mathrm{P}}$
TOTAL	Pq-1	$\sum_{i} \sum_{j} (Y_{ij} - Y_{00})^2$				

DATA

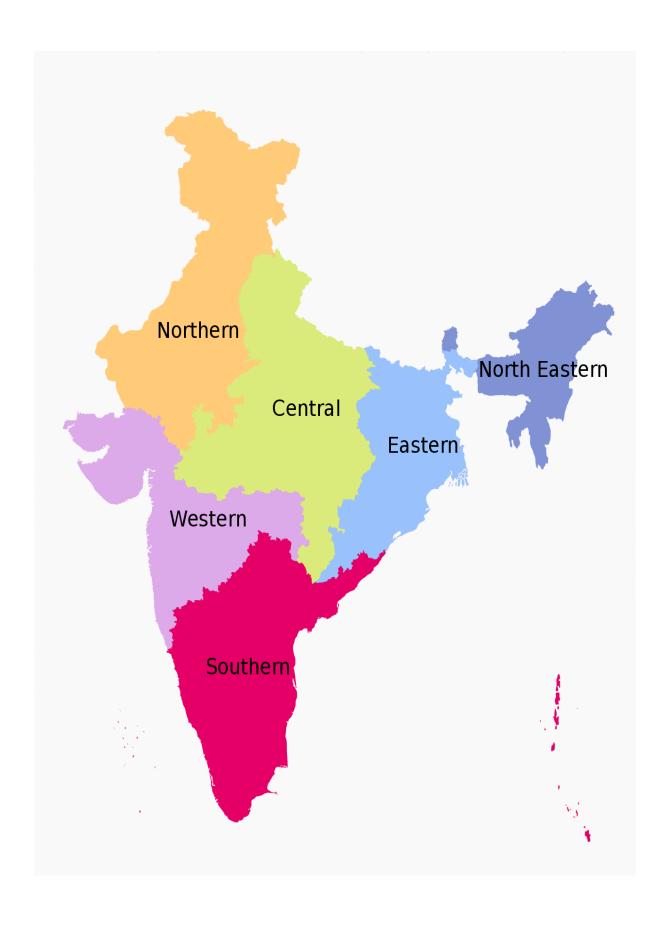
Cyber Crimes in India between 2007-20016

	Cases Reported under Total Cyber Crimes											
S. NO.	State/UT	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	
1	Andhra Pradesh	16	25	30	105	349	429	651	282	536	616	
2	Arunachal Pradesh	0	0	1	3	13	12	10	18	6	4	
3	Assam	0	1	2	18	31	28	154	379	483	696	
4	Bihar	0	0	0	2	25	23	139	114	242	309	
5	Chhattisgarh	5	1	4	4	2	49	101	123	103	90	
6	Goa	3	6	8	15	16	30	58	62	17	31	
7	Gujarat	1	17	20	35	52	68	77	227	242	362	
8	Haryana	0	0	0	1	42	66	323	151	224	401	
9	Himachal Pradesh	0	6	6	17	12	20	28	38	50	31	
10	Jammu & Kashmir	0	0	0	5	14	35	46	37	34	28	
11	Jharkhand	0	0	0	0	8	10	26	93	180	259	
12	Karnataka	40	57	97	153	151	412	533	1020	1447	1101	
13	Kerala	38	65	64	148	227	269	383	450	290	283	
14	Madhya Pradesh	6	9	16	148	90	142	342	289	231	258	
15	Maharashtra	49	37	53	142	306	471	907	1879	2195	2380	
16	Manipur	0	0	1	0	0	0	1	13	6	11	
17	Meghalaya	0	0	0	0	6	6	17	60	56	39	
18	Mizoram	0	0	0	1	3	0	0	22	8	1	
19	Nagaland	0	0	0	0	0	0	0	0	0	2	
20	Odisha	0	3	2	7	7	14	104	124	386	317	
21	Punjab	14	11	28	41	59	72	156	226	149	102	
22	Rajasthan	16	4	27	52	122	147	297	697	949	941	
23	Sikkim	0	0	0	0	3	0	0	4	1	1	
24	Tamil Nadu	10	21	18	52	37	39	90	172	142	144	
25	Telangana	0	0	0	0	0	0	0	703	687	593	
26	Tripura	0	0	0	0	0	14	14	5	13	8	
27	Uttar Pradesh	5	2	14	32	101	205	682	1737	2208	2639	
28	Uttarakhand	1	2	7	10	6	4	27	42	48	62	

29	West Bengal	2	0	13	49	43	196	342	355	398	478
30	A & N Islands	0	0	0	0	0	2	18	13	6	3
31	Chandigarh	1	8	4	3	10	33	11	55	77	26
32	D&N Haveli	0	0	0	0	3	0	0	3	0	1
33	Daman & Diu	0	0	0	0	1	0	1	1	1	0
34	Delhi UT	10	12	5	41	50	76	150	226	177	98
35	Lakshadweep	0	0	0	0	0	0	0	1	0	0
36	Puducherry	0	1	0	0	2	4	5	1	0	2
	TOTAL ALL INDIA	217	288	420	966	1725	2761	5693	9622	11592	12317

GROUPING THE STATES OF INDIA BY REGION

NORTHERN	1. Jammu & Kashmir 2. Punjab 3. Haryana 4. Rajasthan									
REGION	5. Himachal Pradesh 6. Delhi 7. Chandigarh									
CENTRAL	1. Chhattisgarh 2. Uttar Pradesh 3. Madhya Pradesh									
REGION	4. Uttarakhand									
EASTERN	1. West Bengal 2. Bihar 3. Odisha 4. Jharkhand									
REGION										
NORTH-EASTERN	Assam 2. Arunachal Pradesh 3. Manipur 4. Meghalaya									
REGION	5. Mizoram 6. Nagaland 7. Sikkim 8. Tripura									
WESTERN	1. Goa 2.Gujarat 3.Maharashtra 4.Daman & Diu									
REGION	5. D&N Haveli									
SOUTHERN	1. Andhra Pradesh 2.Karnataka 3.Kerala 4.Tamil Nadu									
REGION	5. Telangana 6. Puducherry 7. Lakshadweep 8. A & N									
	Islands									

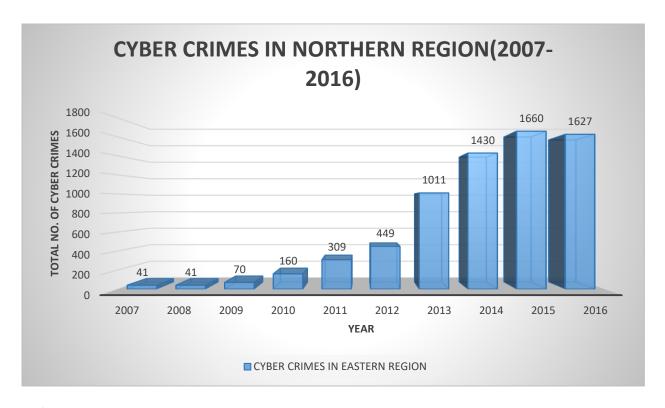


Dividing the Cyber Crimes in India between2007-20016 by six region

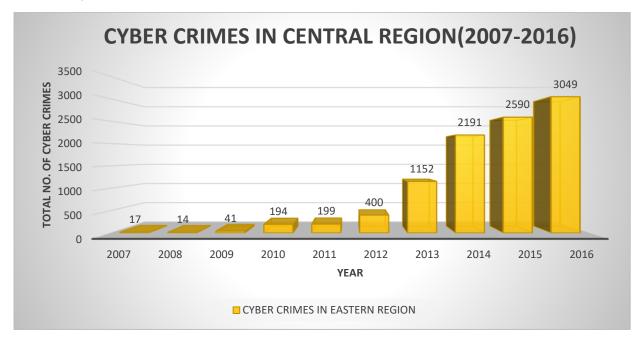
				Cases	Report	ed unde	er Total	Cyber (Crimes		
REGION	State/UT	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
	Jammu & Kashmir	0	0	0	5	14	35	46	37	34	28
	Punjab	14	11	28	41	59	72	156	226	149	102
	Haryana	0	0	0	1	42	66	323	151	224	401
NORTHERN	Rajasthan	16	4	27	52	122	147	297	697	949	941
REGION	Himachal Pradesh	0	6	6	17	12	20	28	38	50	31
	Delhi UT	10	12	5	41	50	76	150	226	177	98
	Chandigarh	1	8	4	3	10	33	11	55	77	26
	TOTAL	41	41	70	160	309	449	1011	1430	1660	1627
	Chhattisgarh	5	1	4	4	2	49	101	123	103	90
CENTRAL	Madhya Pradesh	6	9	16	148	90	142	342	289	231	258
CENTRAL REGION	Uttar Pradesh	5	2	14	32	101	205	682	1737	2208	2639
REGION	Uttarakhand	1	2	7	10	6	4	27	42	48	62
	TOTAL	17	14	41	194	199	400	1152	2191	2590	3049
	West Bengal	2	0	13	49	43	196	342	355	398	478
FACTERN	Bihar	0	0	0	2	25	23	139	114	242	309
EASTERN REGION	Jharkhand	0	0	0	0	8	10	26	93	180	259
REGION	Odisha	0	3	2	7	7	14	104	124	386	317
	TOTAL	2	3	15	58	83	243	611	686	1206	1363
	Arunachal Pradesh	0	0	1	3	13	12	10	18	6	4
	Assam	0	1	2	18	31	28	154	379	483	696
	Manipur	0	0	1	0	0	0	1	13	6	11
NORTH-	Meghalaya	0	0	0	0	6	6	17	60	56	39
EASTERN	Mizoram	0	0	0	1	3	0	0	22	8	1
REGION	Nagaland	0	0	0	0	0	0	0	0	0	2
	Sikkim	0	0	0	0	3	0	0	4	1	1
	Tripura	0	0	0	0	0	14	14	5	13	8
	TOTAL	0	1	4	22	56	60	196	501	573	762
	Maharashtra	49	37	53	142	306	471	907	1879	2195	2380
	Goa	3	6	8	15	16	30	58	62	17	31
WESTERN	Gujarat	1	17	20	35	52	68	77	227	242	362
REGION	D&N Haveli	0	0	0	0	3	0	0	3	0	1
	Daman & Diu	0	0	0	0	1	0	1	1	1	0
	TOTAL	53	60	81	192	378	569	1043	2172	2455	2774
	Andhra Pradesh	16	25	30	105	349	429	651	282	536	616
	Karnataka	40	57	97	153	151	412	533	1020	1447	1101
SOUTHERN	Kerala	38	65	64	148	227	269	383	450	290	283
REGION	Tamil Nadu	10	21	18	52	37	39	90	172	142	144
	Telangana	0	0	0	0	0	0	0	703	687	593
	Lakshadweep	0	0	0	0	0	0	0	1	0	0

Puducherry A & N Islands										
TOTAL	104	169	209	458	766	1155	1680	2642	3108	2742

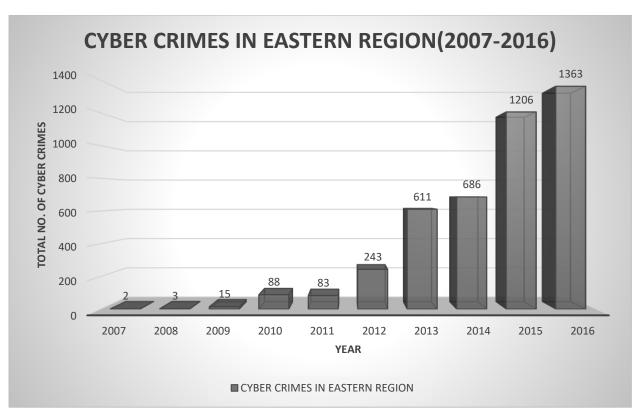
PLOTTING OF GRAPHS



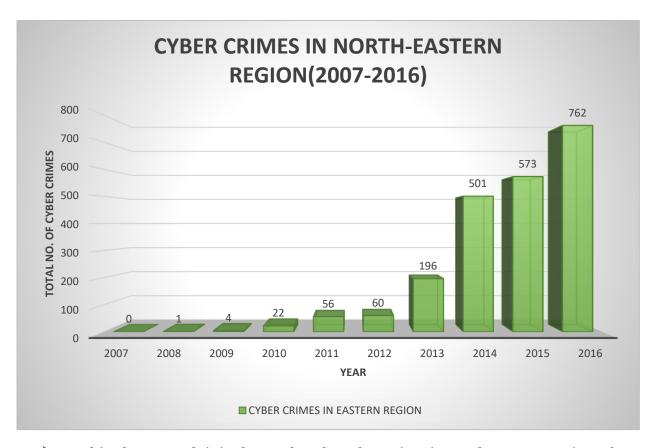
In this above graph it is shown that the increasing of cyber crime is highest for year 2015 for northern region of India. Here we can see that the total no. of cyber crimes are increasing from year 2007-2015 in northern region but it is little bit decreased in the year 2016.



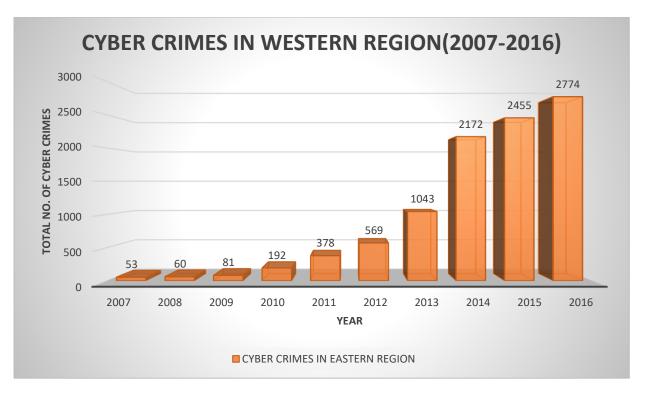
In this above graph it is shown that the cyber crime in central region of Indiabeen increased repeatedly from years 2007 to 2016.



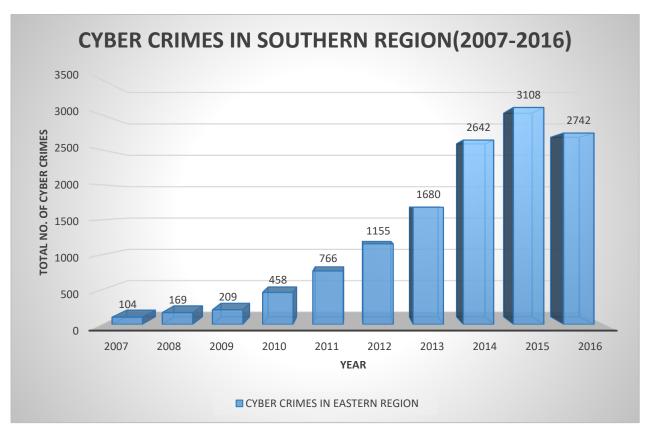
In this above graph it is shown that the cyber crime in eastern region of India been increased from years 2007 to 2016.



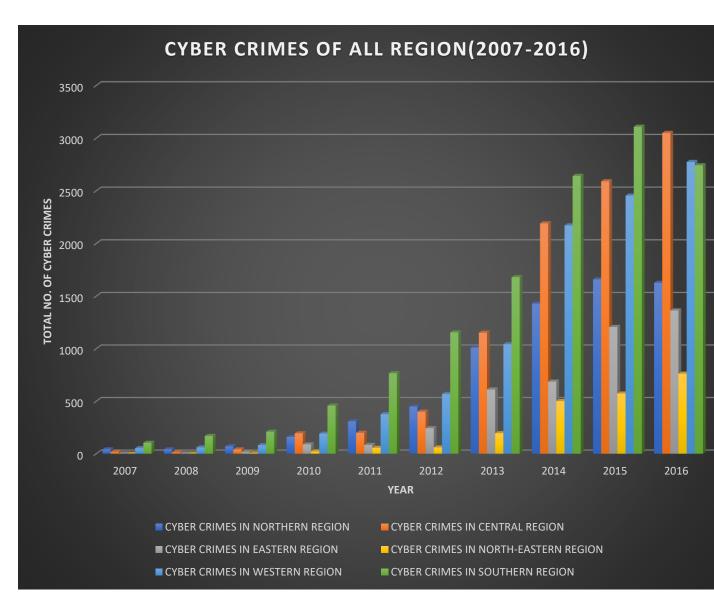
In this above graph it is shown that the cyber crime in north-eastern region of India been increased repeatedly from years 2007 to 2016.



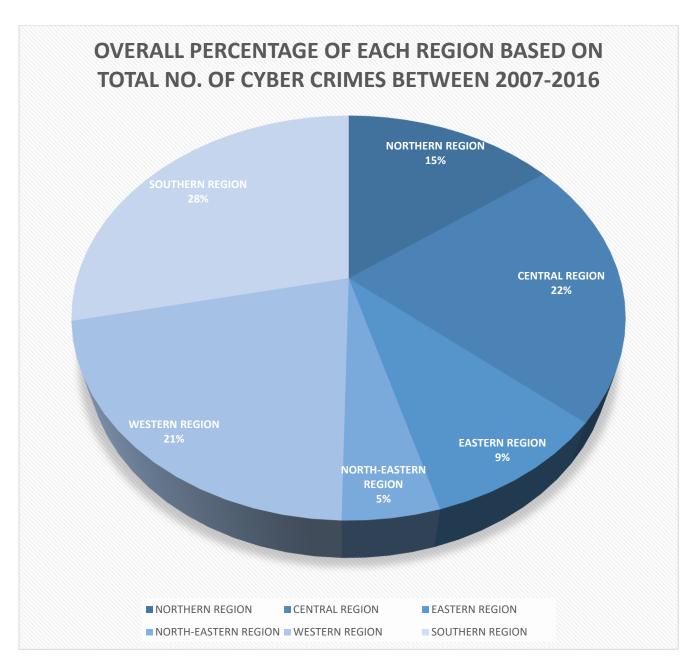
In this above graph it is shown that the cyber crime in western region of India been increased repeatedly from years 2007 to 2016.



In this above graph it is shown that the increasing of cyber crime is highest for year 2015 for southern region of India. Here we can see that the total no. of cyber crimes are increasing from year 2007-2015 in southern region but it is little bit decreased in the year 2016.



➤ In this above graph it is shown that the overall increase or decrease of cyber crime of all the six region of India between 2007 to 2016.



From this above graph it is shown that the southern region is the most cyber crime prone region among all regions in India and the north-eastern region is less cyber crime prone region among all regions in India from 2007 to 2016.

COMPUTATIONAL WORK

(TWO WAY ANOVA)

> read.csv(file="C:\\Users\\RanaDip\\Desktop\\RANADIP.csv",head=TRUE)

YEAR NORTHERN.REGION CENTRAL.REGION EASTERN.REGION NORTH.EASTERN.REGION WESTERN.REGION SOUTHERN.REGION

1 2007	41	17	2	0	53	104
2 2008	41	14	3	1	60	169
3 2009	70	41	15	4	81	209
4 2010	160	194	88	22	192	458
5 2011	309	199	83	56	378	766
6 2012	449	400	243	60	569	1155
7 2013	1011	1152	611	196	104	3 1680
8 2014	1430	2191	686	501	217	2 2642
9 2015	1660	2590	1206	573	3 245	3108
10 2016	1627	3049	1363	76	2 27	74 2742

> data<-read.csv(file="C:\\Users\\RanaDip\\Desktop\\RANADIP.csv",head=TRUE)

> yvar<-

c(data\$NORTHERN.REGION,data\$CENTRAL.REGION,data\$EASTERN.REGION,data\$NORTH.EASTERN.REGION,data\$NORTH.EASTERN.REGION,data\$NORTH.EASTERN.REGION,data\$NORTH.EASTERN.REGION,data\$NORTH.EASTERN.REGION,data\$NORTH.EASTERN.REGION,

> year<-

c(1,2,3,4,5,6,7,8,9,10,1,2,3,4,5,6,7,8,9,10,1,2,3,4,5,6,7,8,9,10,1,2,3,4,5,6,7,8,9,10,1,2,3,4,5,6,7,8,9,10,1,2,3,4,5,6,7,8,9,10)

> region<-

- > year<-factor(year)
- > region<-factor(region)
- > ANOVA<-aov(yvar~year+region)
- > summary(ANOVA)

```
Df Sum Sq Mean Sq F value Pr(>F)
year 9 35524347 3947150 34.8 < 2e-16 ***
region 9 10512387 1168043 10.3 4.31e-08 ***
Residuals 41 4650111 113417
---
Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 '' 1
```

CONCLUSION

Our null hypothesis is –

 H_{01} : the mean value of cyber crime for each year is equal $\mu_{Y_1} = \mu_{Y_2} = \dots = \mu_{Y_{10}} = c(\text{say})$ H_{02} : the mean value of cyber crime for each region is equal, β_i 's are all equal; i=1(1)6

From the test we have observed F> tabulated F for both for the year and region. i.e. the cyber crime significant for six regions in India.

Decision:

In our work we can see the overall cyber crimes prone regions of India from 2007 to 2016. The cyber crimes are increased day by day as the uses of internet is increased day by day. It can only be protected with the increase of consciousness among the people and the proper knowledge to handle the internet. Our work can be extended for other countries. We can also consider the developed countries for our work and compare their no. of crimes with that of our country. It has been consider further.

BIBLIOGRAPHY

***** Website:

- www.ncrb.nic.in
- www.cybercrime.gov.in
- www.cybercellmumbai.com
- www.britannica.com
- www.cyberlawsindia.net

Books:

- Cyber law and IT S.R. Myneni
- Law mantra International monthly journal
- Fundamentals of Statistics(v-1) − A. M. Gun, M. K. Gupta, B. Dasgupta
- Fundamentals of Statistics(v-2) − A. M. Gun, M. K. Gupta, B. Dasgupta
- Fundamentals of Mathematical statistics − S. C. Gupta, V. K. Kapoor
- Statistical Methods N. G. Das