Cyber Crimes in India

June 30, 2023.

Cyber Crimes in India

Project Report

Jaswinderpal Singh, Hitika, Jasmeen Sharma,
Kartik Setia, Kanishka Jaggi, Kajol

M.Sc. Statistics, Semester - 4.

Under the guidance of: Prof. Narinder Kumar

Department of Statistics
Panjab University, Chandigarh - 160014 (India)

June 30, 2023.

Preface

Cyber Crimes

Cyber crimes are a new class of crimes rapidly increasing due to extensive use of Internet and I.T. enabled services. Any criminal activity with the use of computers, networks, or the internet for the exploitation of data and resources comes under cyber crimes. Examples include hacking, identity theft, phishing scams, and distributing malware etc. Women are commonly targeted for cyber stalking, cyber pornography, impersonation etc.

Objectives

• To analyze the year-wise trend and future prediction of the number of cyber-crimes registered in India using the data from 2002 - 2021.
• State and U.T. - wise comparisons for the cyber-crimes incidence.
• Application of Non-Parametric tests to check similarity of distributions and randomness of cases, keeping the population variation of the states under consideration.
• To identify major cyber-crime motives in India.
• Dividing States into clusters based on their fraud cyber crimes in the years 2017-2021.
• To analyze of Police Disposal of cyber crimes and dividing statistically similar crime-heads into clusters. • To analyze how court matters involving cyber crime are handled and disposal of persons arrested.
• To figure out major cyber crimes against women and children.

Keywords: Cyber Crimes, Phishing, Malware, Fraud, Statistics, Non-Parametric Inference, Statistical Cluster Analysis.

Major Cyber Crimes in India

Some major cyber crimes in India include:
1. *Hacking:* Unauthorized access to computer systems, networks, or websites to steal sensitive information or disrupt operations.
2. *Phishing:* Attempts to trick individuals into providing personal or financial information through fake emails or websites.
3. *Identity Theft:* Using someone else’s personal information to commit fraud or other crimes.
4. *Fraud:* Using the internet to scam people out of their money or personal information.
5. *Cyberstalking:* Harassment or bullying through electronic means.
6. *Child pornography:* Using the internet to distribute or view child pornography.
7. *Ransomware:* A type of malware that encrypts a victim’s files and demands payment to restore access.
8. *Crypto jacking:* Unauthorized use of someone’s computer or device to mine cryptocurrency.
9. *Distributed Denial of Service (DDoS) attacks:* Overwhelming a website or network with traffic to make it unavailable.
10. *Spamming:* Sending unsolicited messages through email or other means.

Various studies are done as far as cyber-crimes in India are concerned. M. Dasgupta (2009) has classified the cyber-crimes on different basis and grounds like computer as a target as well as victim. A. Bhangla and J. Tuli (2021) conducted the study on the legal framework of cyber-crimes in India. An increase of nearly 6 % from the year 2020 is noted in the yaer 2021 as far as the cyber crimes in India are concerned.

Contents

Chapter 1

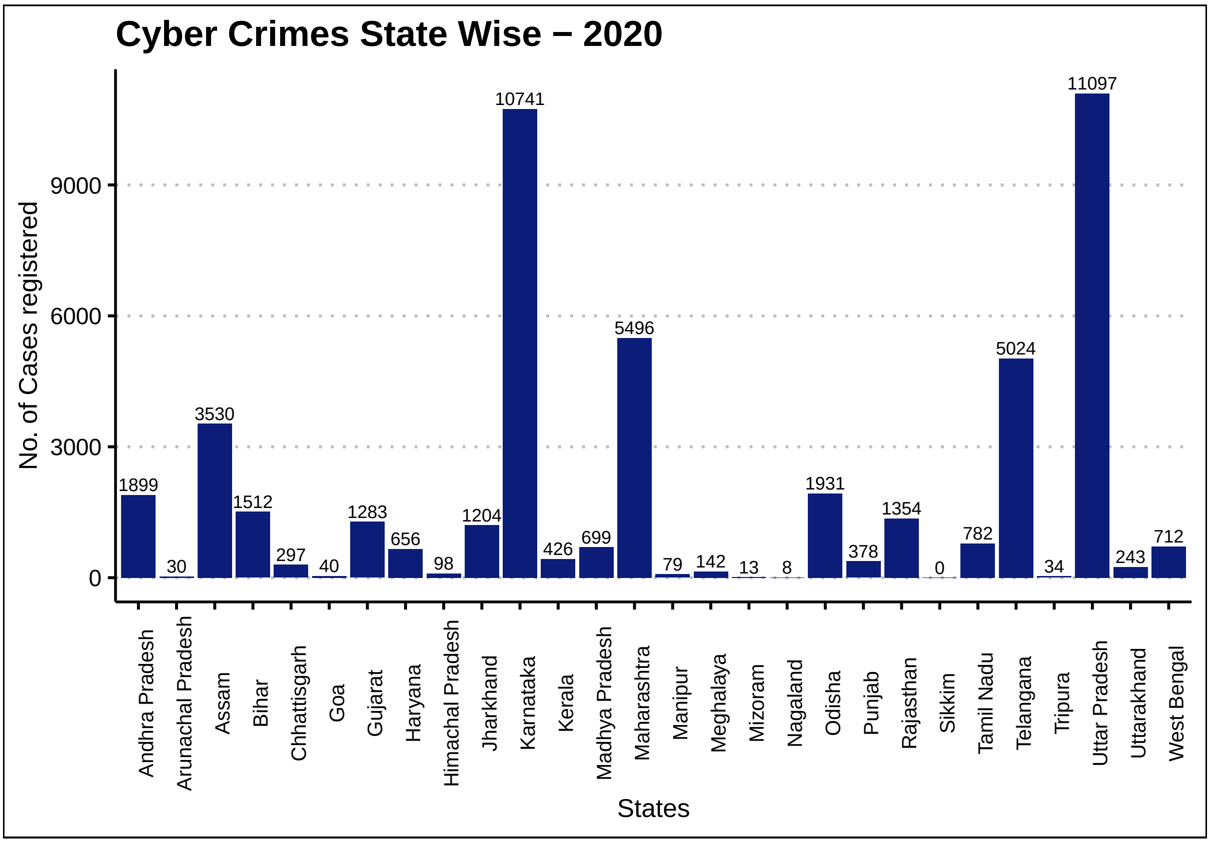
Cyber Crimes in India: Trend and Future Prediction

1.1 Introduction

Cyber Crimes are becoming serious threats to Digital India. As per the latest joint report published on May 3, 2023 by the *Internet and Mobile Association of India* (IAMAI) and data analytics firm 'Kantar', the active Internet users in India are more than 50% of the country's population. India reported **52,974** fresh incidents of cyber-crimes in 2021, as per Crime in India (2021) Statistics of the National Crime Records Bureau.
In this section, the main objective is to have a visualization of Cyber Crimes in India among states and U.T.s. and the trend analysis for the country over the years along with predictions for the coming years.

1.2 Cyber Crimes State-Wise:

Year 2020

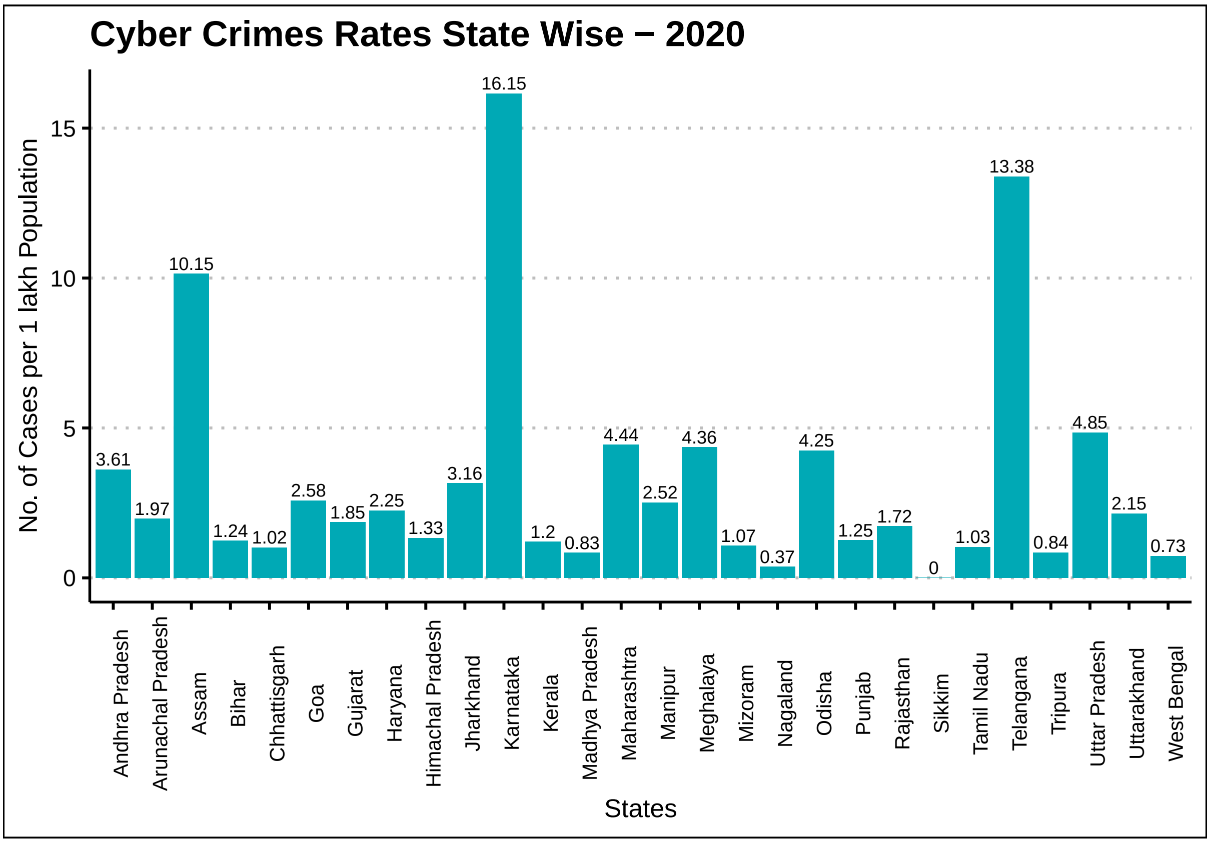


A total of **50,035** cyber crimes were registered in India with a rate of **3.7** cyber crimes per 1 lakh population as compared to 44,735 cyber crimes registered in 2019 with a rate of 3.34 cases per 1 lakh population, as per Crime in India (2020) Statistics of the National Crime Record Bureau.

The above figure shows the highest number of cases being registered in Uttar Pradesh in terms of numbers, followed by Karnataka, Maharashtra and Telangana. But one must note that the population in these states may vary. So, to get a better comparison, rates can be calculated, which gives the cyber-crime cases registered in the state per 1 lakh population. Mid-year projected population for each state for the year 2020 is available. Hence the Cyber Crime Rate can be calculated as

$$\text{Rate} = \frac{\text{No. of cases registered}}{\text{Mid year projected population (in lakhs)}}$$

Hence, keeping the population variation of the states into account, the better comparative picture here is given by the rates:



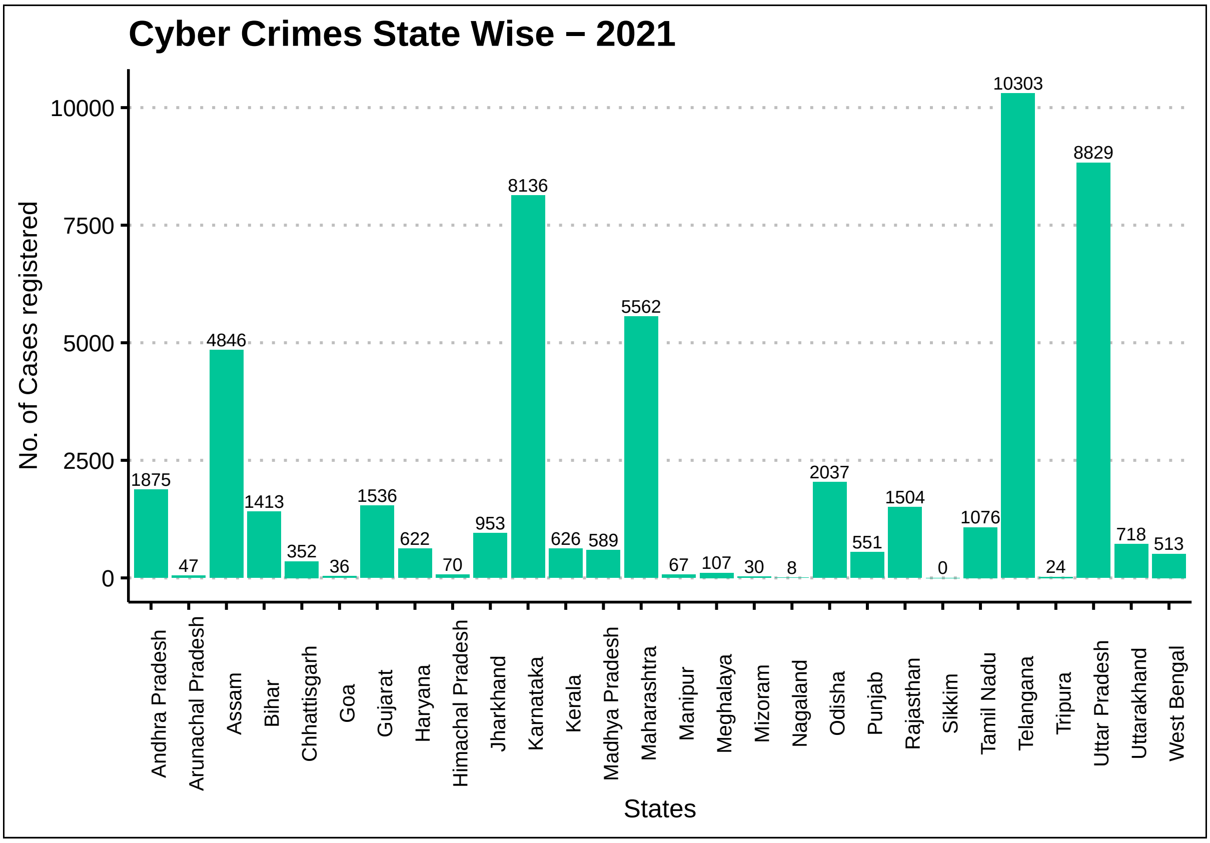
Interpretation:

- The maximum cyber crime rate can be seen in the state of Karnataka with **16.15** cyber crimes per 1 lakh population during the year 2020. However, in terms of numbers the state was at the second position after Uttar Pradesh with a total of 10,741 cyber crimes reported in 2020.
- The cyber crimes in the state of Telangana are extremely high as far as the Rates are concerned. Telangana registered **13.38** cyber crimes per 1 lakh population in 2020, which was the second highest rate in the country.
- In terms of numbers, Assam is far behind Maharashtra and Uttar Pradesh, but the rate in Assam is very high as compared to these populous states of the country. Assam registered cyber crimes with a rate of **10.15** in the year 2020.

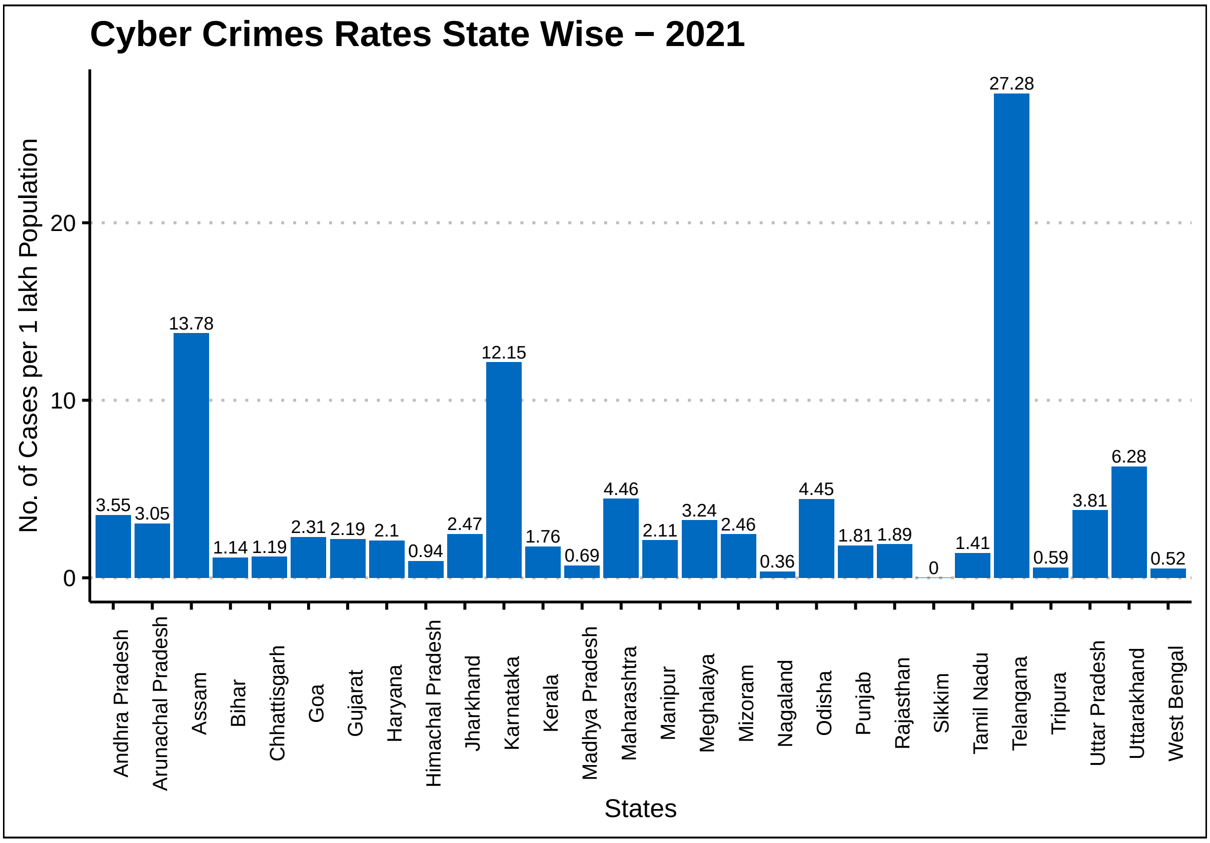
```
## [1] 0.7172579
```

The above value indicates that almost 71.72579 % of the total cyber crimes reported in the country India in 2021 came only from the five states: Telangana, Uttar Pradesh, Karnataka, Maharashtra and Assam. However, they contributed to almost 36% of the Indian Population.

Year 2021



From the above figure it looks like Telangana tops the Cyber Crimes tally followed by Uttar Pradesh and Karnataka in 2021. It can be noticed that the cyber crimes in the state of Telangana almost doubled in a year, which is a matter of huge concern.



But for better comparison, the Cyber Crime Rates, i.e. Cyber Crimes in a State per 1 lakh population, can be seen.

Interpretation:

- The state of Telangana emerged with the highest cyber crime rate of **27.28** cases per 1 lakh population. Telangana tops the tally in terms of number of cases also, during the year 2021, with **10,303** cyber crimes registered in the state during this year. The rate figures are far away from the other states of the country.
- Uttar Pradesh registered second highest number of cases in the country, but the population in the state is also highest in the country. Due to this fact, the cyber crime rate in U.P. is comparatively low as compared too other major states. The tally was **8,829** cyber crimes with a rate of **3.81** cyber crimes per 1 lakh population.
- Cyber Crimes in Assam are continuously taking pace. In terms of numbers, Assam registered **4,846** cyber crimes in 2021, which is the 5th highest in the country, but the cyber crime rate in this state is very high. The cyber crime rate in the state is **13.78** cyber crimes per 1 lakh population, which is the second highest rate in the country.

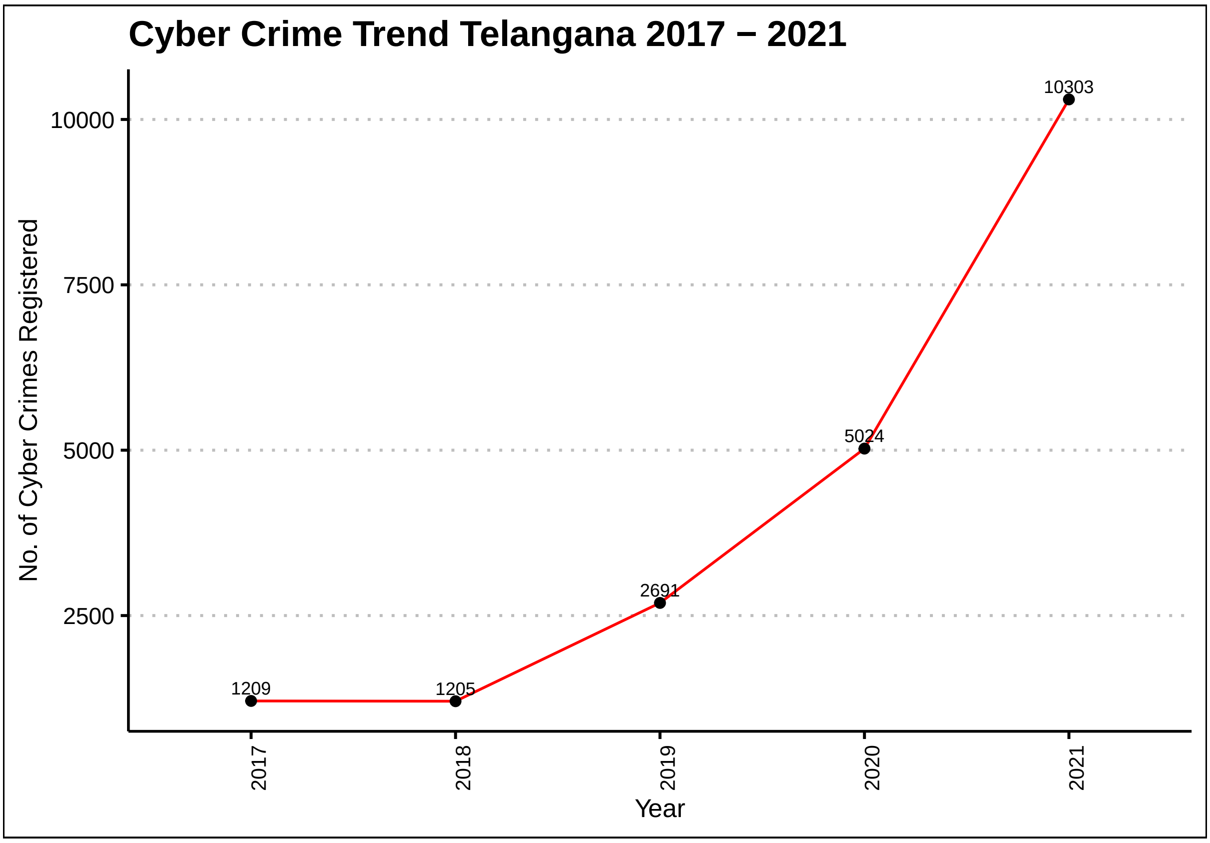
```
## [1] 0.7112168
```

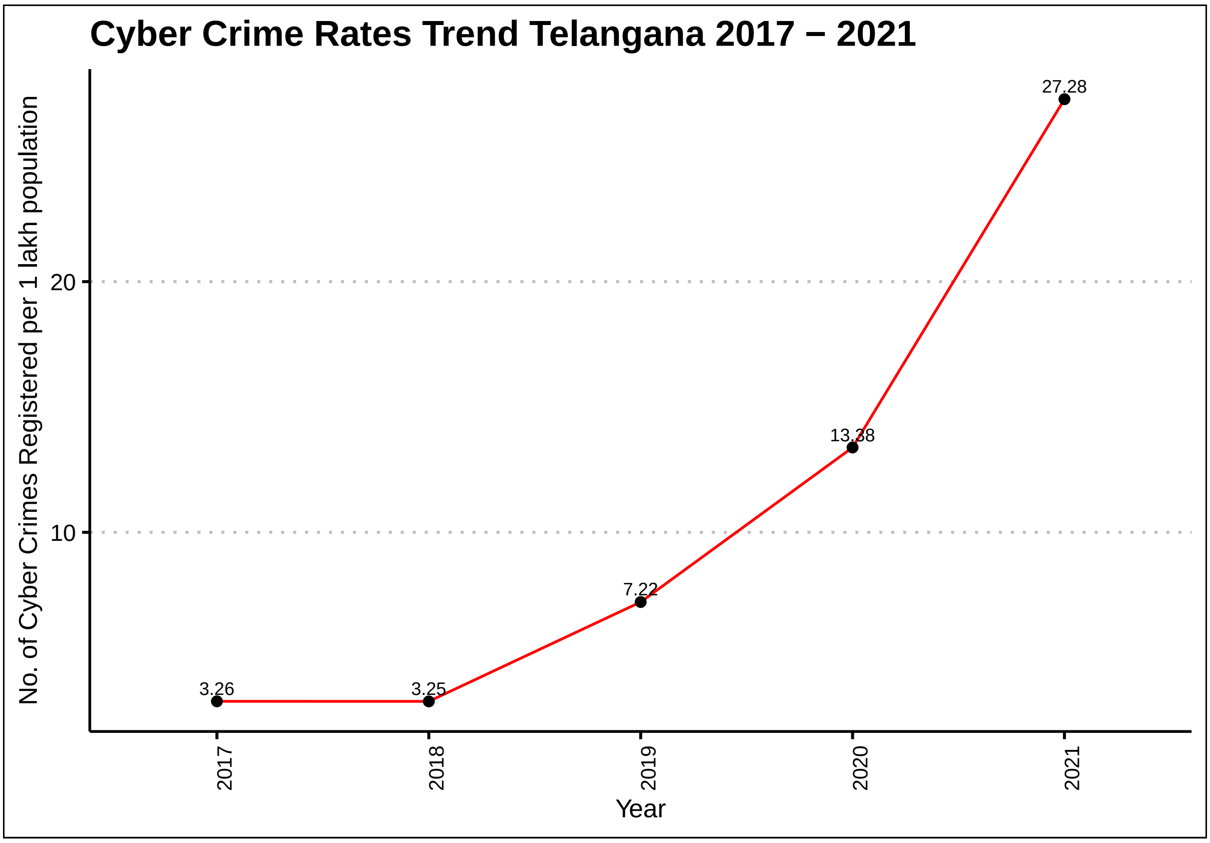
The above value indicates that almost 71.12168 % of the total cyber-crimes reported in the country India in 2021 came only from the five states: Telangana, Uttar Pradesh, Karnataka, Maharashtra and Assam. However, they together contributed almost 36% of the Indian Population.

1.2.1 Cyber Crimes Trend: Major States

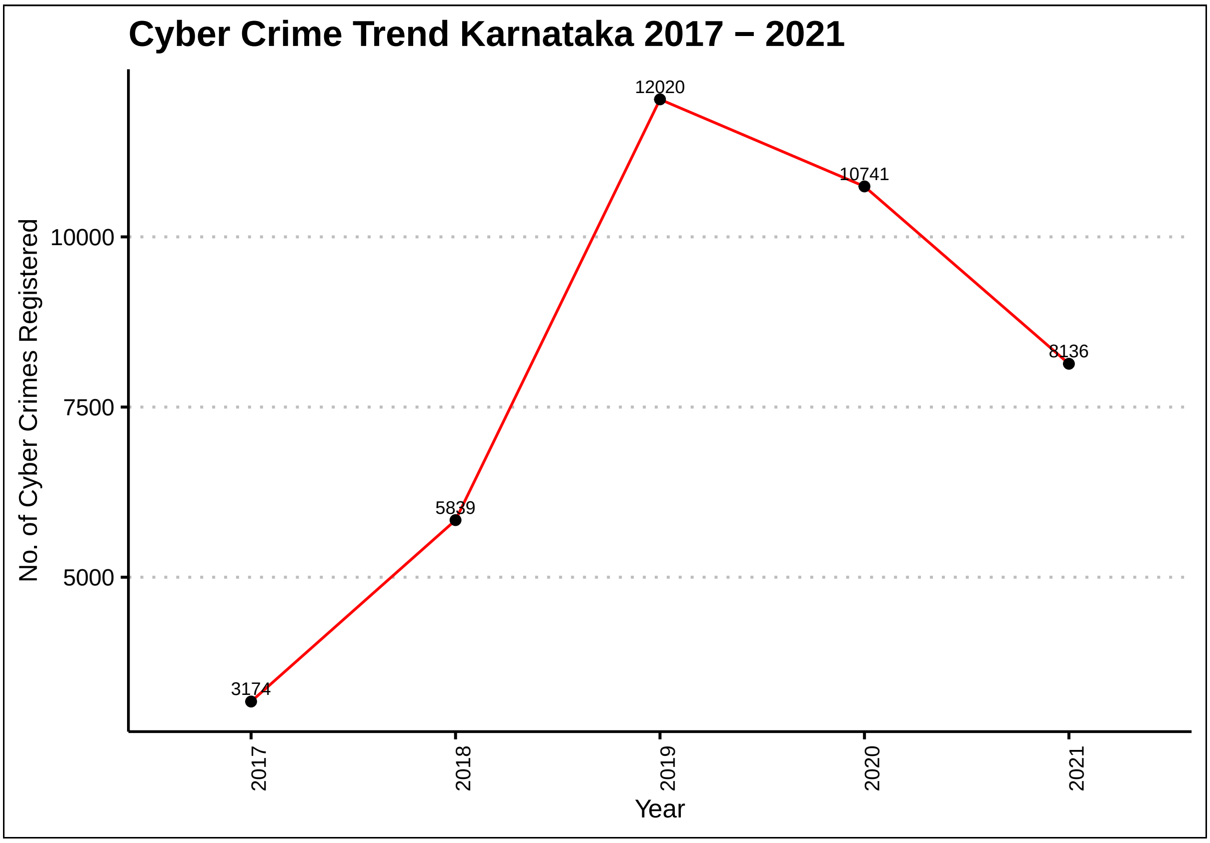
Now, for the past 5 years, the cyber crime trend in these 5 major states is to be viewed. The trend is shown for each state for the years 2017 - 2021. The data can be visualized both in terms of actual crime registered count as well as in terms of rates in these states.

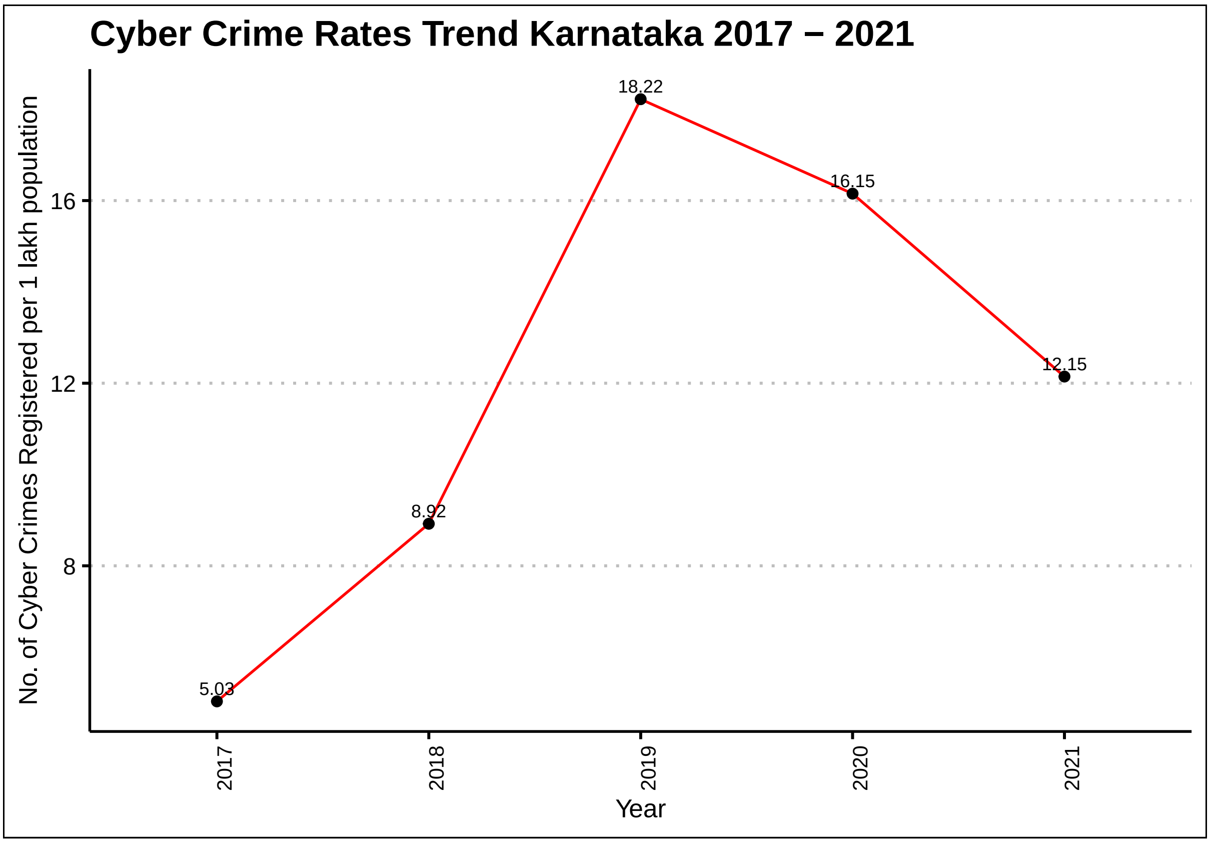
```
##
##  Telangana
```



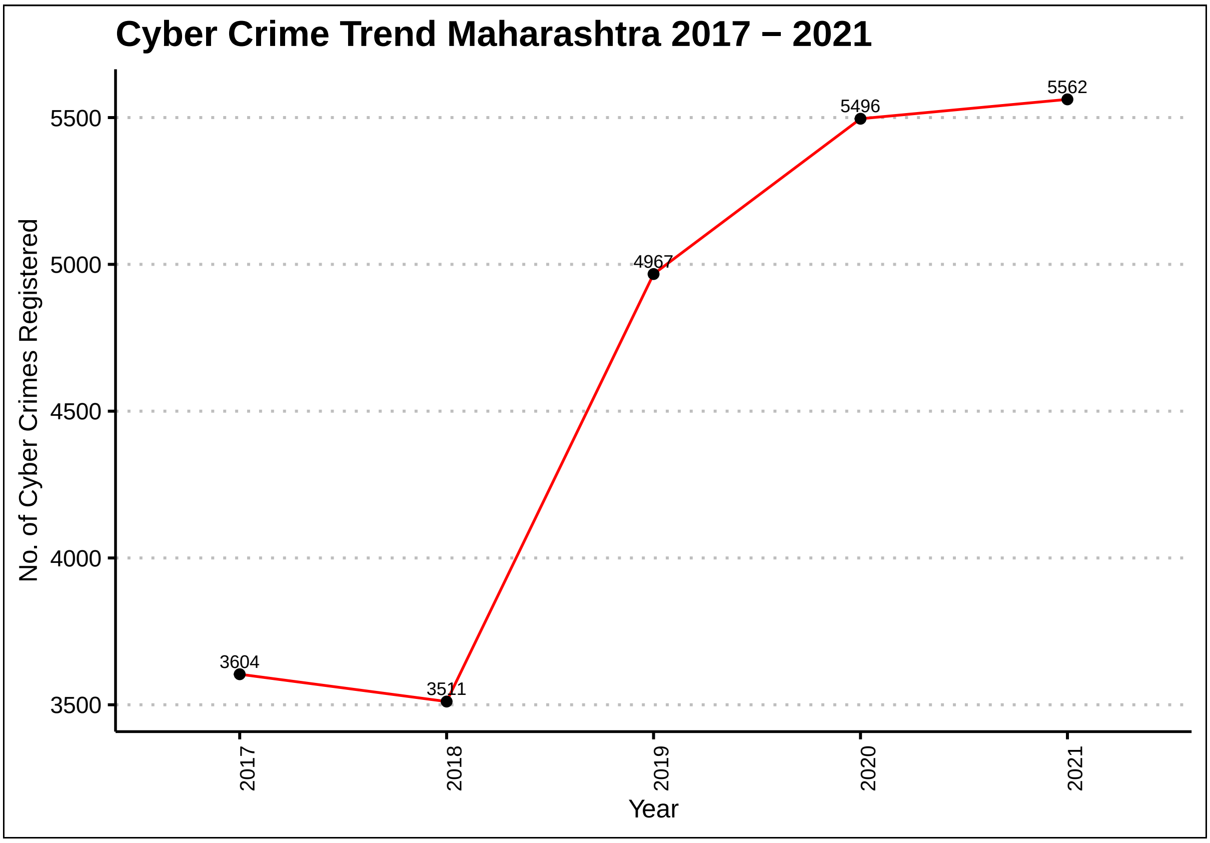

Cyber Crime Rates Trend Telangana 2017 − 2021
No. of Cyber Crimes Registered per 1 lakh population
20
10
3.26
3.25
7.22
13.38
27.28
2017
2018
2019
2020
2021
Year

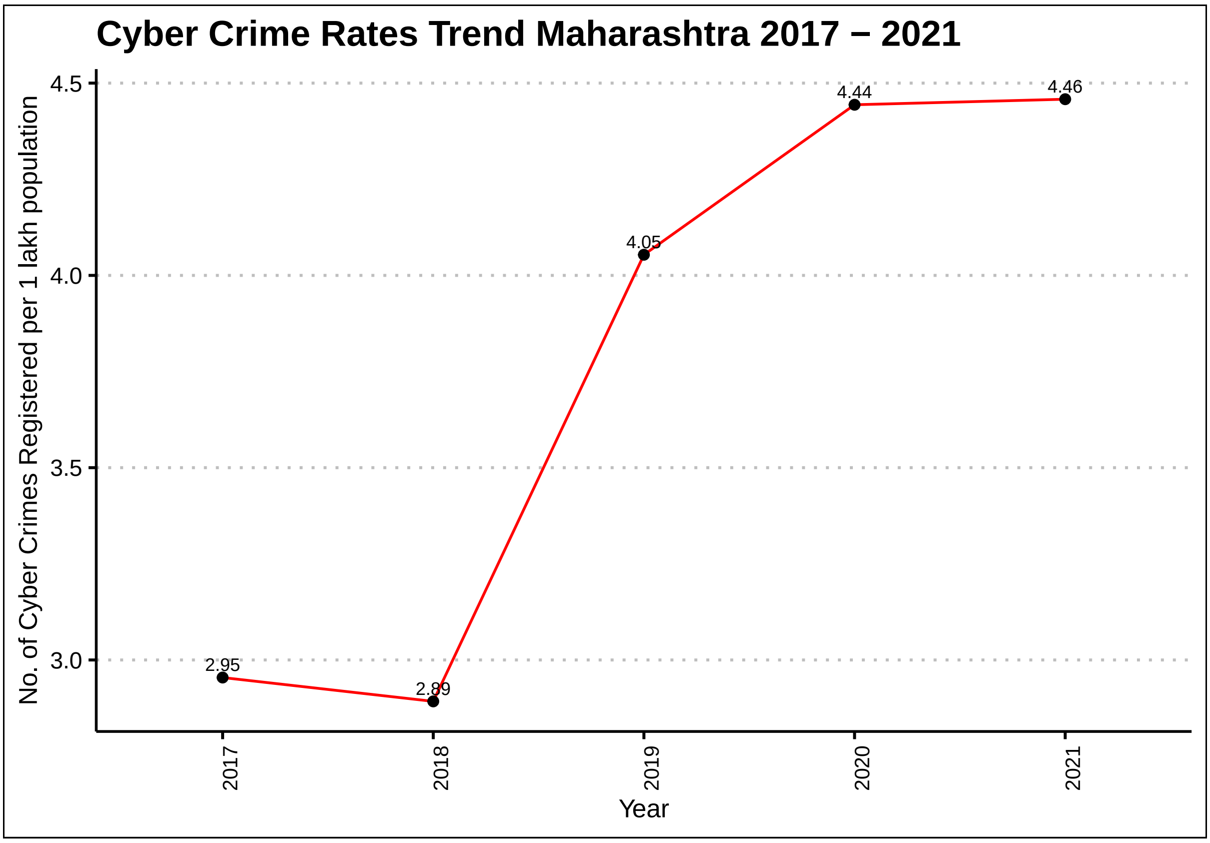
```
##
##
##  Karnataka
```


Cyber Crime Trend Karnataka 2017 − 2021
No. of Cyber Crimes Registered
10000
7500
5000
3174
5839
12020
10741
8136
2017
2018
2019
2020
2021
Year

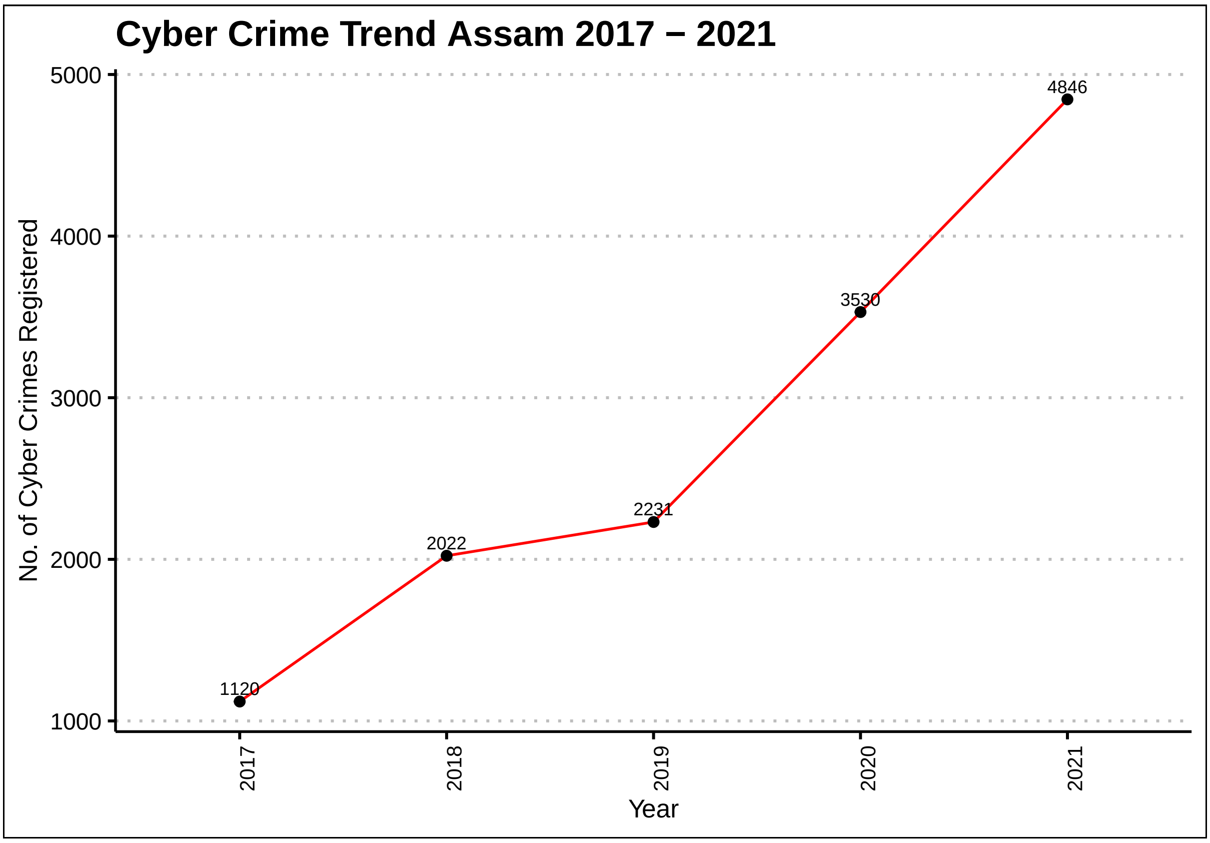


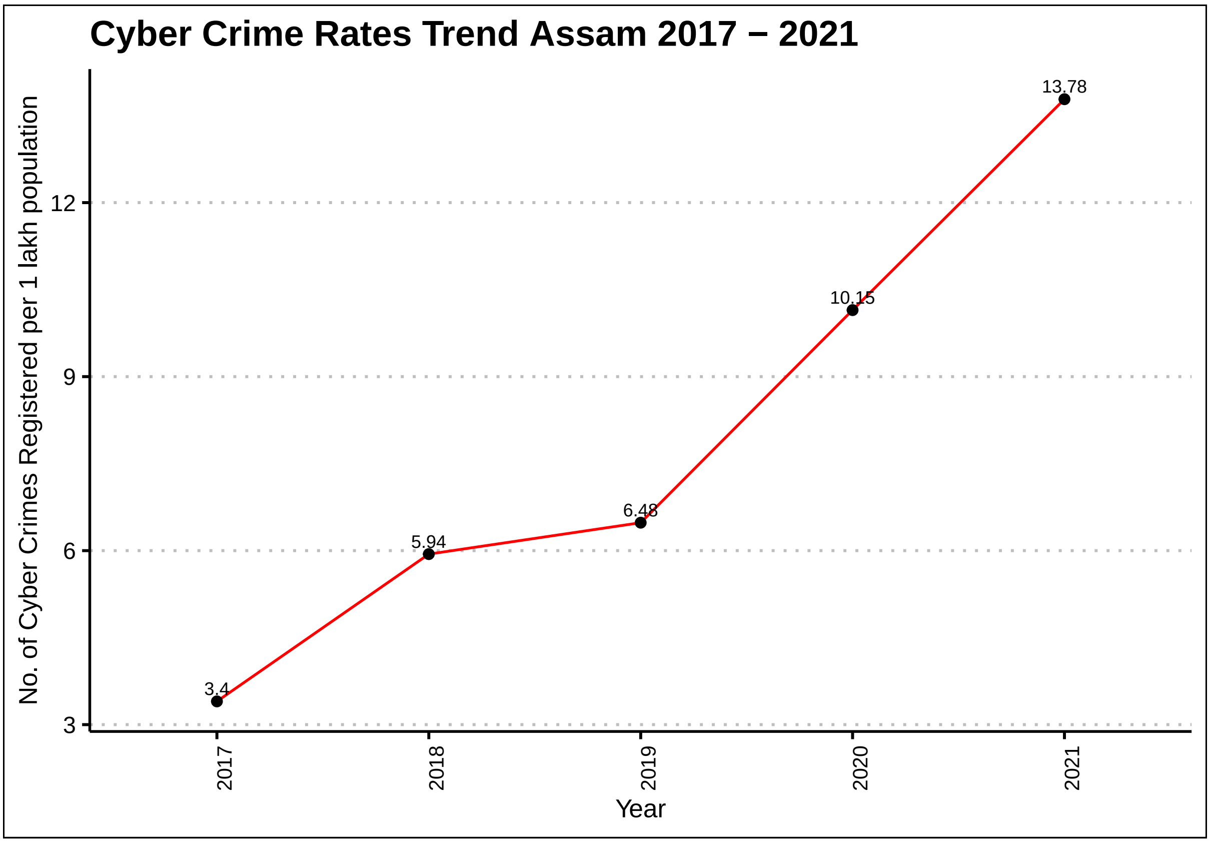
```
##
##
##  Maharashtra
```



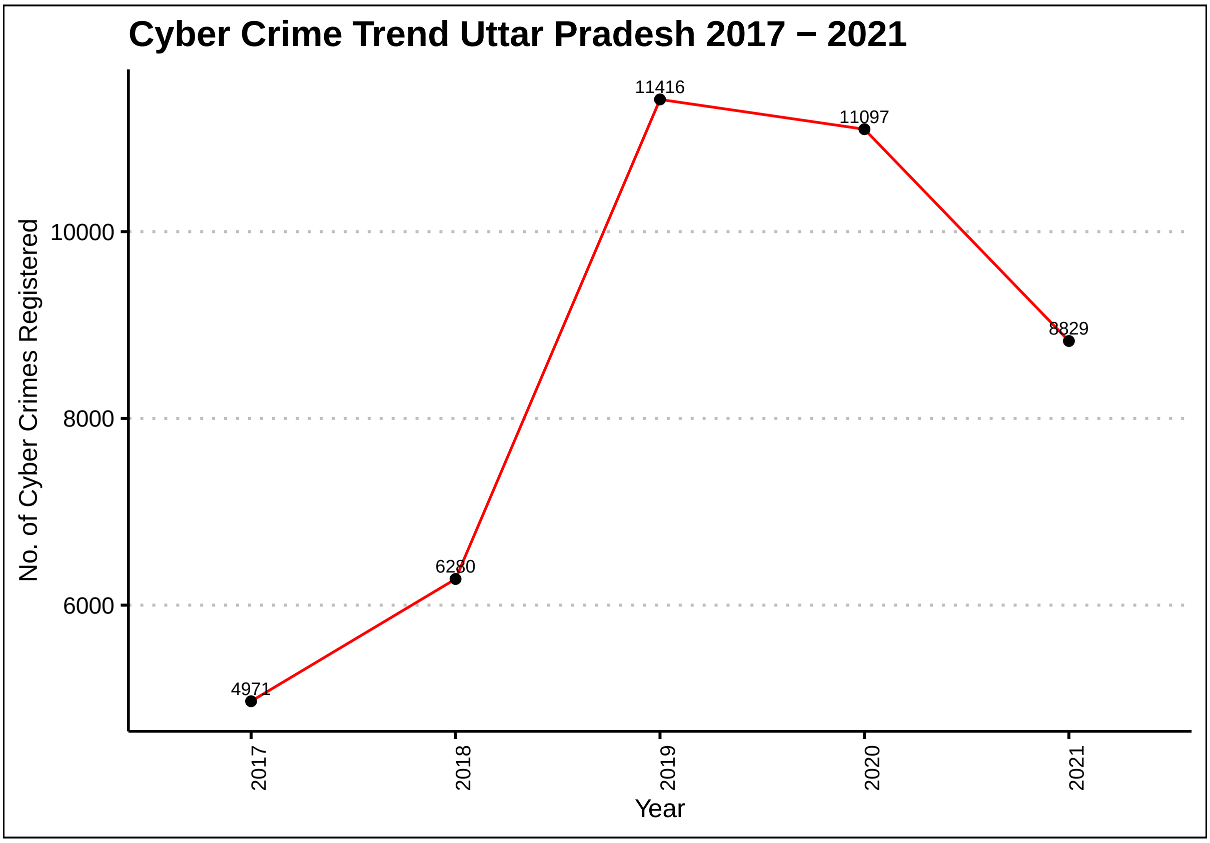

Cyber Crime Rates Trend Maharashtra 2017 − 2021
No. of Cyber Crimes Registered per 1 lakh population
4.5
4.0
3.5
3.0
2.95
2.89
4.05
4.44
4.46
2017
2018
2019
2020
2021
Year

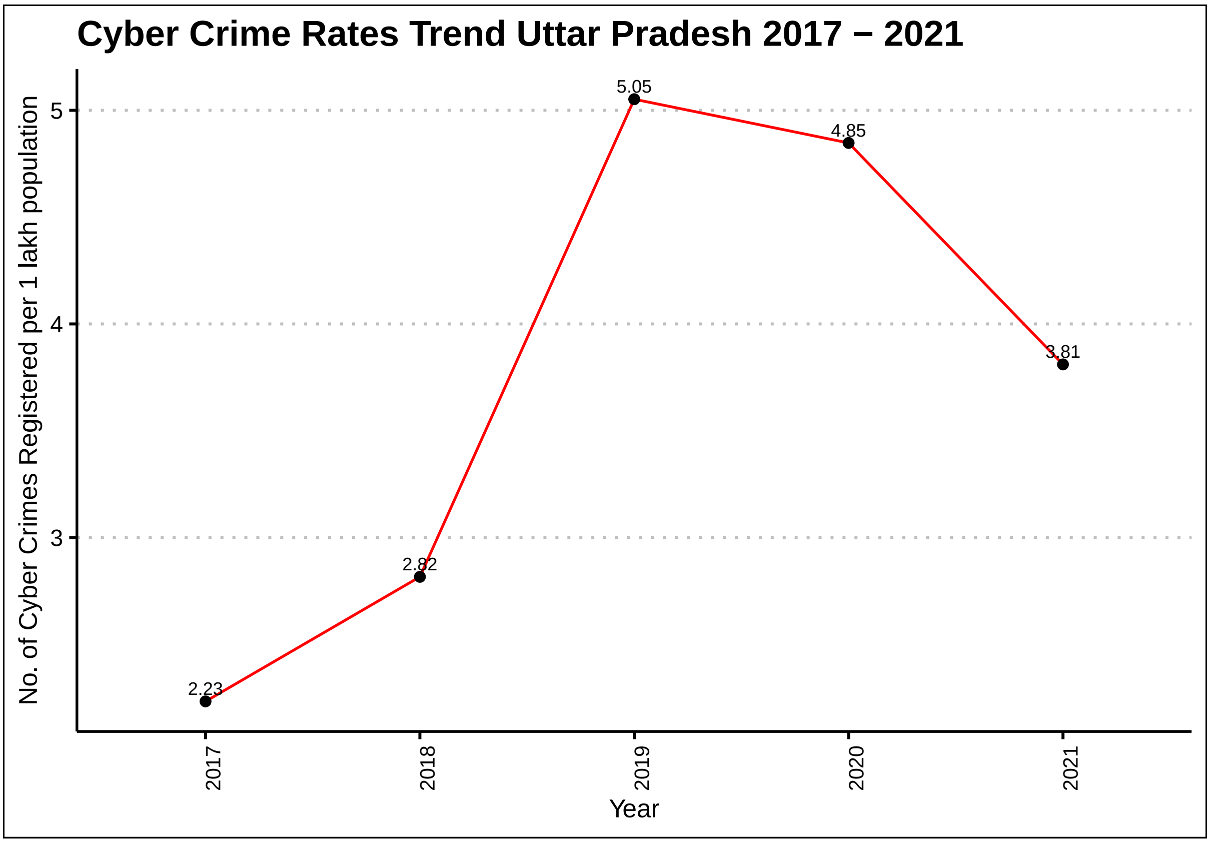
```
##
##
##  Assam
```


Cyber Crime Trend Assam 2017 − 2021
No. of Cyber Crimes Registered
5000
4000
3000
2000
1000
1120
2022
2231
3530
4846
2017
2018
2019
2020
2021
Year



```
##
##
##  Uttar Pradesh
```



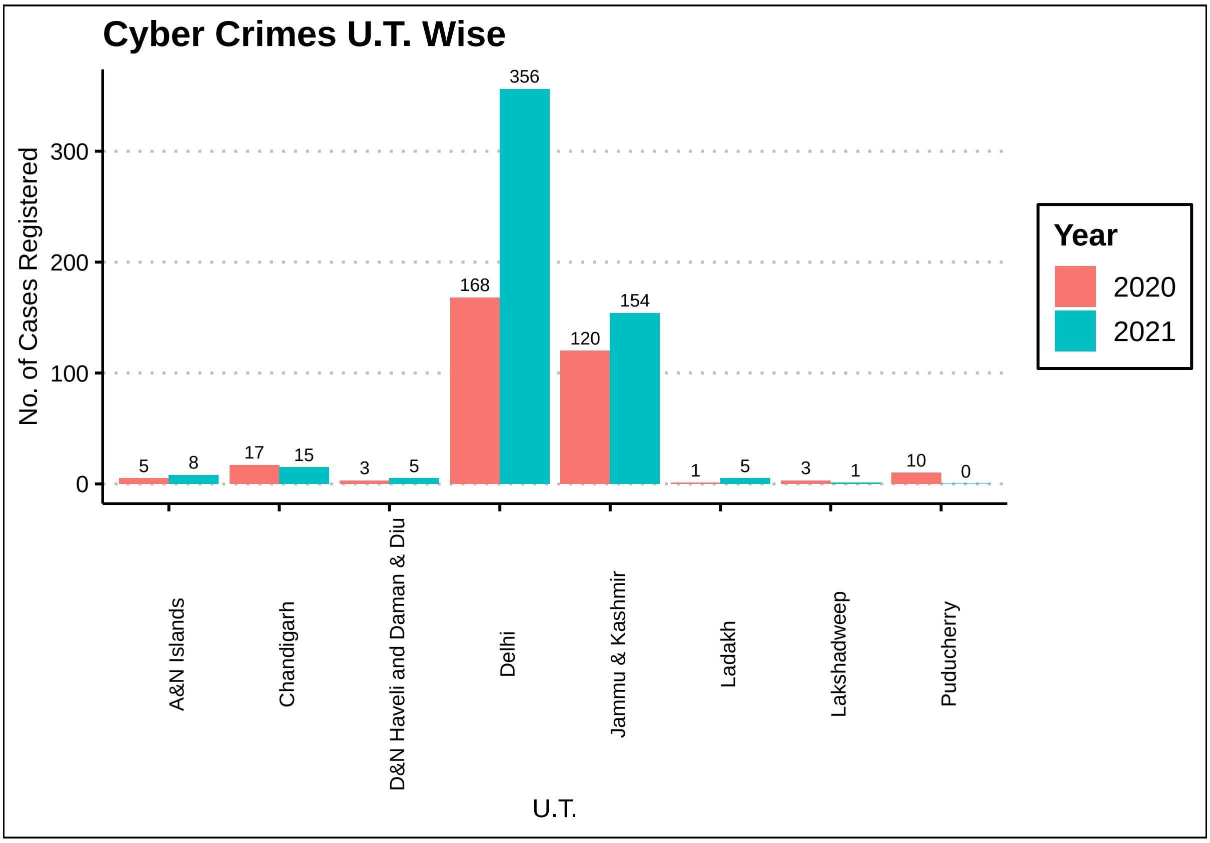


Major findings from Major States

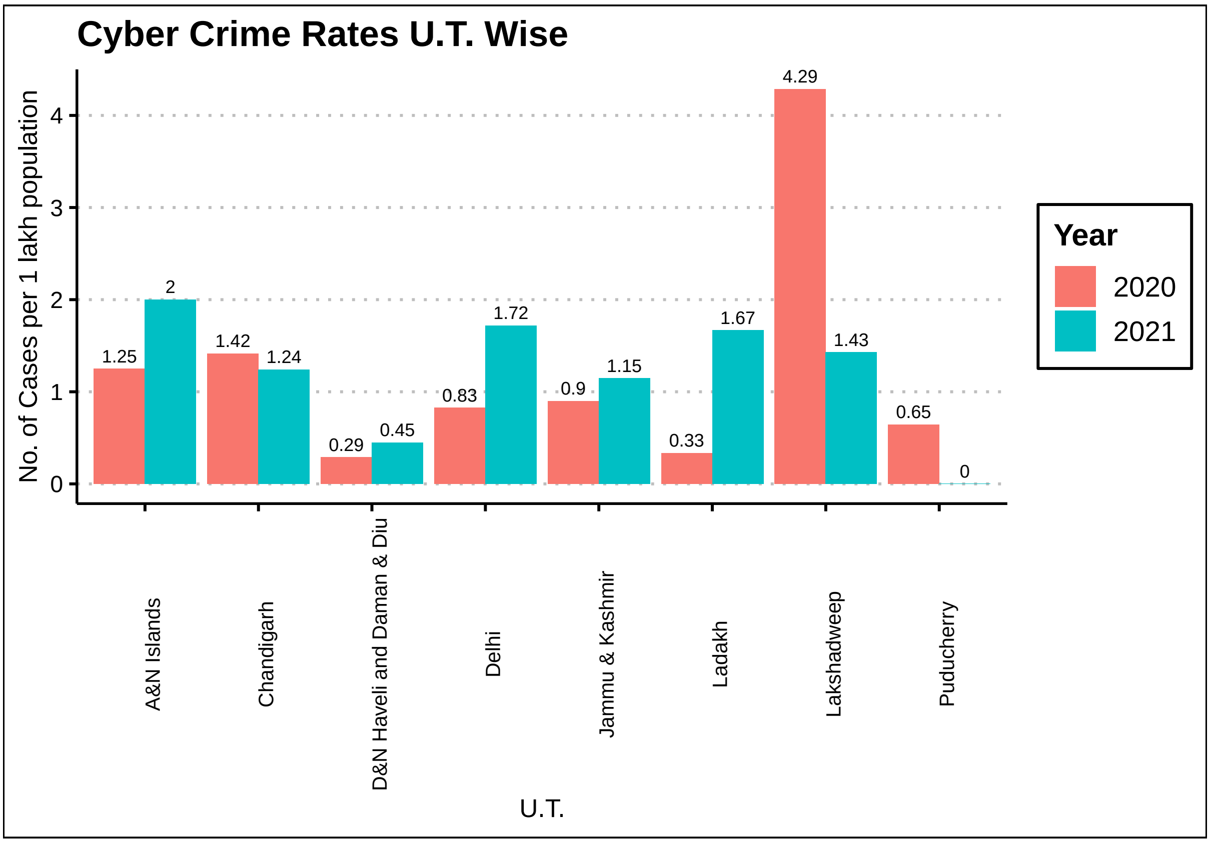
- ***Telangana:*** The cyber crimes are increasing very rapidly in the state of Telangana. It is getting doubled every year since 2018, which is a huge concern. Recently, Telangana got a high jump in number of cyber crimes registered. Telangana registered **10,303** cyber crimes in 2021 with a rate of **27.28** cyber crimes per 1 lakh population as compared to the **5,024** cyber crimes in 2020 with a rate of **13.38** cyber crimes per 1 lakh population.
- ***Karnataka:*** The state of Karnataka registered the maximum of **12,020** cyber crimes in the year 2019 with a rate of **18.22** cyber crimes per 1 lakh population, which were just above double of the 5,839 cases registered in 2018 with a rate of 8.92. However, after that cyber crimes have slightly declined in the state and the figures of 2021 are 8,136 cyber crimes registered with a rate of 12.15 cases per 1 lakh population.
- ***Maharashtra:*** Maharashtra, one of India's largest commercial and industrial centers of India is continuously having a high cyber crimes since 2018. The state seen a significant increase from 2018 to 2019 in which it registered 4,967 cyber crimes with a rate of 4.05 cyber crimes per 1 lakh population. Currently, the cyber crime rate in the state is stabilizing near **4.46** cyber crimes per 1 lakh population.
- ***Assam:*** The state with surprisingly rapidly increasing cyber crimes in the past few years is the state of Assam. The cyber crime rate in Assam is increasing by 3-4 % by every passing year since 2019. Currently, Assam is the second highest state as far as the cyber crime rates are concerned with a rate of **13.78** cyber crimes per 1 lakh population.
- ***Uttar Pradesh:*** Uttar Pradesh is not very far behind in terms of numbers as far as the cyber crimes are concerned, but the cyber crime rate in this state has declined in the past couple of years. Note that Uttar Pradesh is the most populous state in India as per the 2011 Census. In 2019, there were **11,416** cyber crimes registered in Uttar Pradesh with a high rate of **5.05** cyber crimes per 1 lakh population. However, in the recent year of 2021, the tally reduces to **8829** cyber crimes with a rate of **3.81** cyber crimes per 1 lakh population.

Now, it is evident from that the states of Assam and Telangana are showing rapid increasing trend in Cyber Crimes in last 5 years. However, U.P. and Karnataka are registering some lesser number of cases as compared to previous years.

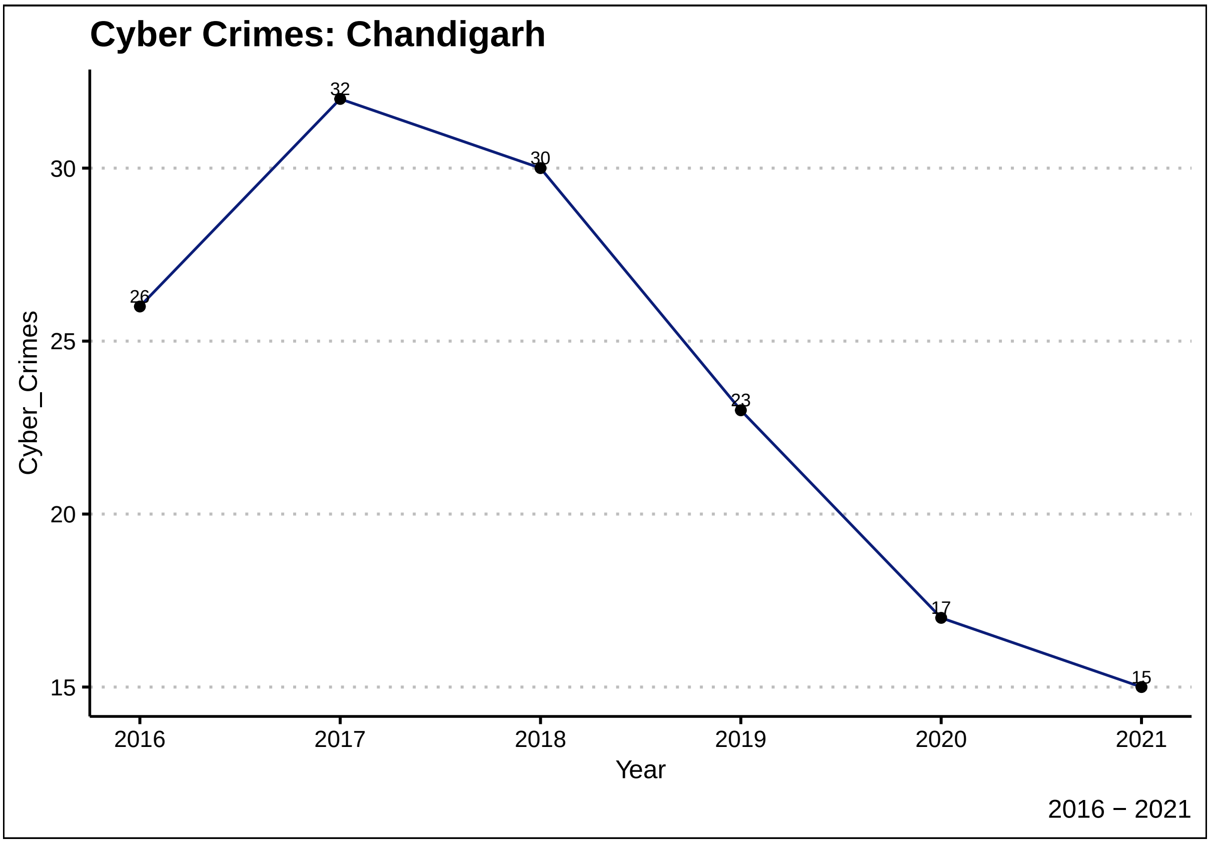
1.3 Cyber Crimes U.T. - wise

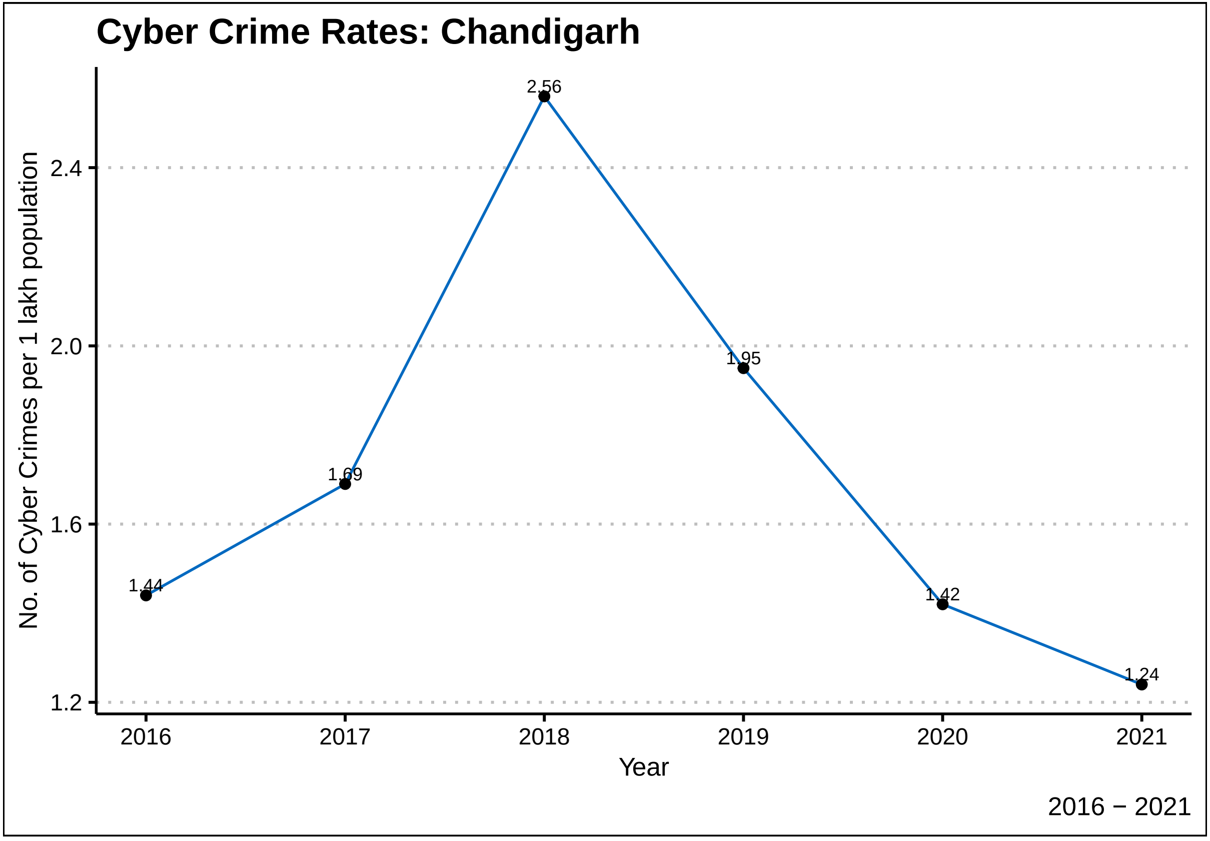


In terms of numbers, the Union Territory of Delhi registered the most 356 cyber crime cases in 2021. Also, **the cases in Delhi are more than double in 2021 from 2020.**



The Status of Chandigarh

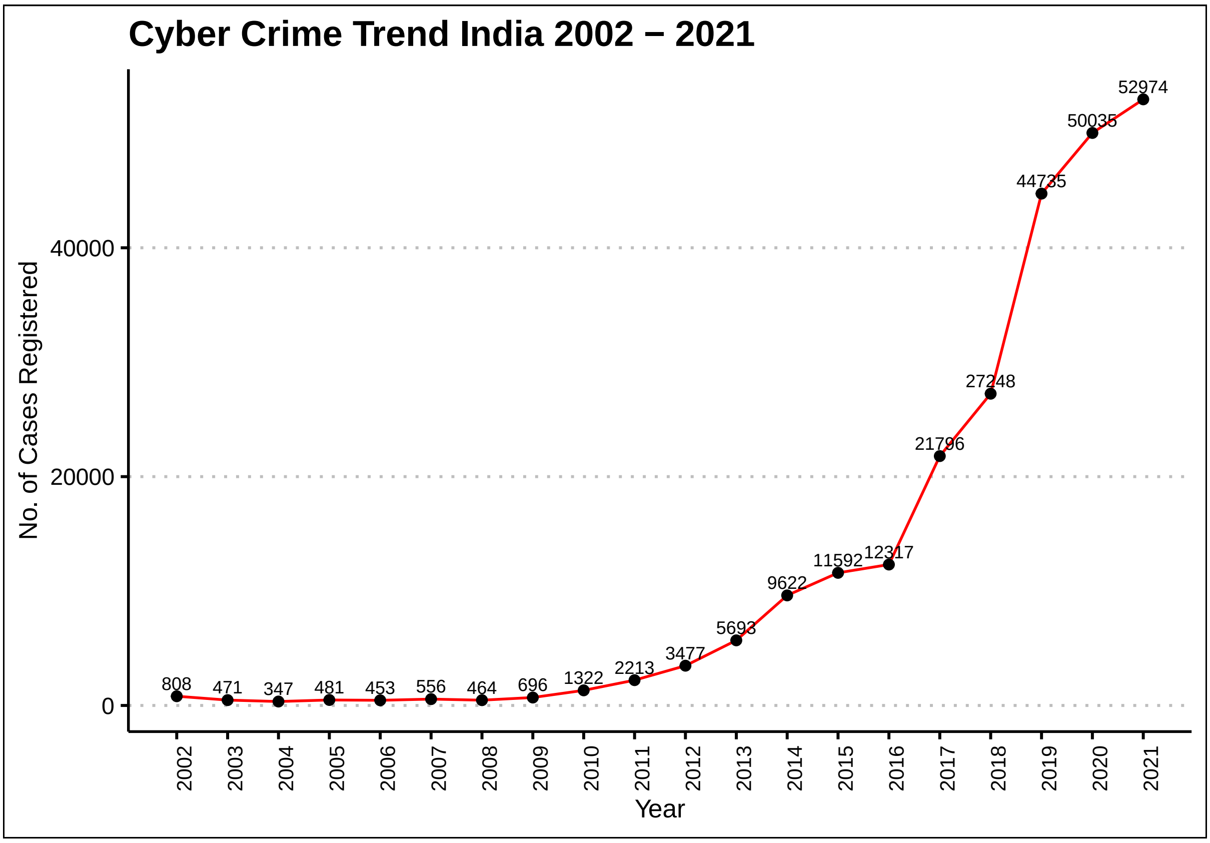




It seems that the Union Territory of Chandigarh has shown a good improvement as far as the cyber crimes in numbers are concerned. Also, the rate is declining in the past few years and in 2021 it was **1.24** cyber crimes per 1 lakh population. All time high was **2.56** cyber crimes per 1 lakh population in 2018.

1.4 Cyber Crime Trend and Forecast - India

The number of cyber crimes registered in India during the past 20 years are given by the following plot:



Now, the above plot shows the Trend for the number of Total Cyber Crimes registered in overall India from the year 2002 - 2021.

Now, it is evident from the plot, that India registered more than **4 times** cyber crimes in 2021 as compared to 2016.

Also, in a span of an year, India registered **1.5 times** more Cyber Crime cases in 2018 from 2017. And if we see 2018 from 2016, then the registration of the cases is **just above double**.

Also, one may note that initially, from the years 2002 - 2009, the cases registered were much much lower due to the fact that the internet was not that cheaply and easily accessible for the people of India.
But from the year 2016 to 2017, the cyber-crimes were **almost doubled** due to the fact that in this year the Telecom sector in India experienced drastic changes with the entry of Jio in the Telecom Market. To tackle with their business strategies, other telecom networks reduced the data charges to a huge extent, leading to a very large increase in the internet accessibility among the Indian Population.

Secular Trend

Secular Trend means the smooth, regular, long-term movement of the series, if observed long enough. Some series exhibit an upward or a downward trend or may remain more or less at a constant level. Sudden or frequent changes are incompatible with the idea of trend. It is a general systematic gradual change over time. It may be linear or non-linear. A Secular trend might change its direction from an increasing trend to a decreasing trend and vice-versa.
In order to measure the trend, we have to eliminate from the time series the other three components viz. seasonal, cyclical and irregular fluctuations. For example, if the period of seasonal fluctuation be a year, then the yearly totals or yearly averages will be free from the seasonal effect.
To eliminate the other two components viz. cyclical and irregular, one may consider the following methods:

- Method of freehand curve fitting
- Method of Semi Averages
- Method of Mathematical Curve fitting
- Moving Average Method
- Group Average Method.

Method of Mathematical Curve fitting for determination of Trend

This is perhaps the best and most objective method of determining trend. In this case, an appropriate type of trend equation is selected at first and then the constants involved in the equation are estimated on the basis of the data in hand. A Mathematical relationship is established between the response trend and the equi-spaced time points. Here, we have used the Method of Mathematical Curve fitting, which is more reliable and enable us to obtain trend values for all the given time periods.

Model Selection: In this study, by the visual inspection of the trend from the dataset, it seems that the trend follows some exponential type of pattern.

Estimating Parameters of the Model: Estimating the parameters of the model using different estimation methods, such as maximum likelihood estimation or least squares estimation. The estimated parameters are the values with the best fit, minimizing the discrepancy between the model predictions and the observed data. In this study, the least square method of estimation is being implemented in R.

Goodness of Fit of the Model: Assessing the goodness-of-fit is the process of determining how well the fitted model fits the data. Various methods to examine the goodness of fit of a model include computing Multiple R Squared and Adjusted R Squared, Residual Analysis, Visualizing Residual plots and normality characteristics of residuals etc. If the fit is good, the model has done a good job of capturing the patterns and variability in the data.

Model Validation: It is the process of determining whether the fitted model is valid by evaluating how well it performs on independent or holdout data. This procedure aids in determining whether the model's performance endures beyond the data used for fitting. Any given data set can be fitted with a wide variety of models, but the best one is the one that passes the goodness of fit test.

Forecasting: The main objective of a model is to control the present and predict the future. Forecasting is one of the major characteristic of any Model. Qualitative Techniques, Time series analysis and Projection are some of the basic types of forecasting. In this study, the forecasts are made for the Cyber Crimes and Cyber Crime Rates of India.
The exponential models, for which all the parameters and other helpful statistics are provided below, are the best fitted ones out of all the models that we tried to fit in "R" for the given data set.

Cyber Crimes Prediction

The cyber crime prediction for the coming years can be done using the following fitted model:

$$\log(Y_t) = 4.99265 + 0.29710\, t$$

or

$$Y_t = \exp(4.99265 + 0.29710\, t)$$

where:
t $\geq$ 1
Y_t : Predicted Cyber Crimes in India for the year $(2001 + t)$

Model Summary

```
##
## Call:
## lm(formula = log(data$creg) ~ t)
##
## Residuals:
##      Min       1Q   Median       3Q      Max
## -0.93246 -0.28671 -0.01779  0.21533  1.40482
##
## Coefficients:
##             Estimate Std. Error t value Pr(>|t|)
## (Intercept)  4.99265    0.24250   20.59 5.84e-14 ***
## t            0.29710    0.02024   14.68 1.86e-11 ***
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## Residual standard error: 0.522 on 18 degrees of freedom
## Multiple R-squared:  0.9229, Adjusted R-squared:  0.9186
## F-statistic: 215.4 on 1 and 18 DF,  p-value: 1.856e-11
```

Model Inferences

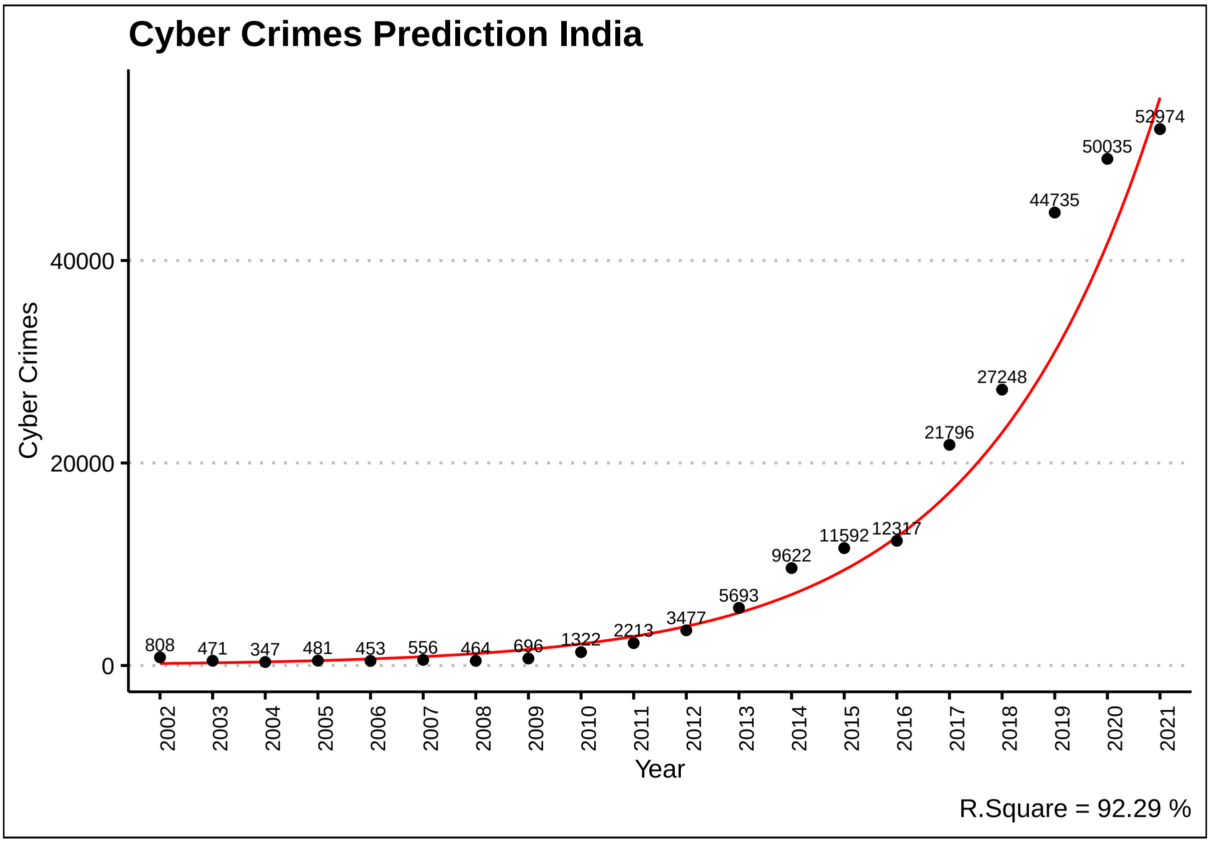
- ***P Value*** = 1.856×10^{-11}, much less than the level of significance, which means the coefficients of the model are highly significant.

- ***F-Statistic of ANOVA*** = 215.4, which is infact very high. It also indiactes the high significance of the model coefficients and can be compared with the critical values.

- ***Multiple R-Square*** = 0.9229 & ***Adjusted R Square*** = 0.9186, which are close to 1 and do not differ from each other. These values indicate a good fit of the model.
  Clearly, from the summary of the model, it is evident that the values of R^2 and Adjusted R^2 do not differ much. Here t denotes the time index. t = 1 corresponds to the year 2002, upto so on t = 20 for the year 2021. The parameter estimates are coming out to be highly significant.

Model Plot

In this plot the estimated curve along with the actual values is plotted against the time points. For the good fit of a model, the curve must pass closer to the actual values.
The plot of the fitted curve along with the actual values as dots is shown below:



Future Prediction

The Cyber Crimes predicted for the coming years using the above model are:

year	Predicted_Cyber_Crimes
2022	75488.5
2023	101603.7
2024	136753.4
2025	184063.2
2026	247739.7
2027	333445.0

2028	448800.1
2029	604062.2
2030	813037.1

These values indicate that the cyber crimes in India are expected to increase rapidly in the coming future and shall become almost double as compared to 2019-2021.

Testing Normality of Residuals

The residuals from this model are given by

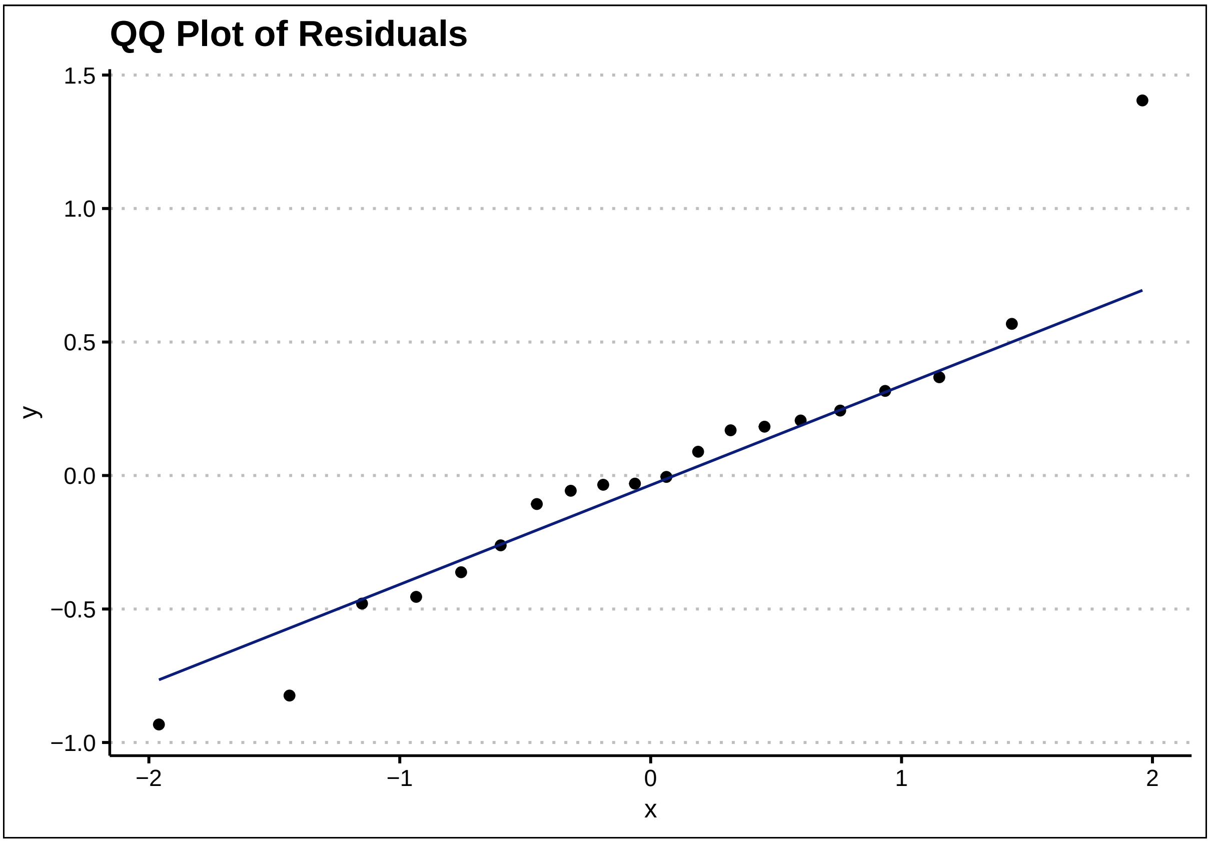
```
##            1            2            3            4            5            6 
##  1.404817423  0.568013911 -0.034618951 -0.005176008 -0.362250700 -0.454474079 
##            7            8            9           10           11           12 
## -0.932457368 -0.824091808 -0.479639995 -0.261536223 -0.106814978  0.089152971 
##           13           14           15           16           17           18 
##  0.316868217  0.206031731 -0.030402599  0.243243898  0.169398008  0.368074530 
##           19           20 
##  0.182941550 -0.057079531
```

In most of the Econometric and Time series models, it is assumed that the errors are iid and Normally distributed with zero mean and some constant variance , i.e. $N(0, \sigma^2 I)$. Residuals are considered to be the estimates of the errors. Therefore, it is good to test whether these estimates of the errors possess the desired characteristics of normality.

Normality of residuals means that they are distributed symmetrically around zero, with no skewness or kurtosis. This assumption implies that the model captures the main patterns and sources of variation in the data, and that the errors are random and independent.

H_0: The residuals are normally distributed.
H_1: The residuals are not normally distributed.

QQ Plot



Clearly, it is evident from the above plot that the quantiles are nearly lying on the straight line, known as the QQ line, which indicates the presence of normality in the residuals. ***Shapiro-Wilk Normality Test***

```
##
##  Shapiro-Wilk normality test
##
## data:  ress$crimes
## W = 0.94005, p-value = 0.2403
```

Here, the p-value >> 0.01. It means we fail to reject the null hypothesis of Normality. Hence it can be concluded that the residuals are normally distributed, with 99 % confidence.

Kolmogorov Smirnov Goodness of fit Test

```
##
##  Exact one-sample Kolmogorov-Smirnov test
##
## data:  ress$crimes
## D = 0.25641, p-value = 0.1201
## alternative hypothesis: two-sided
```

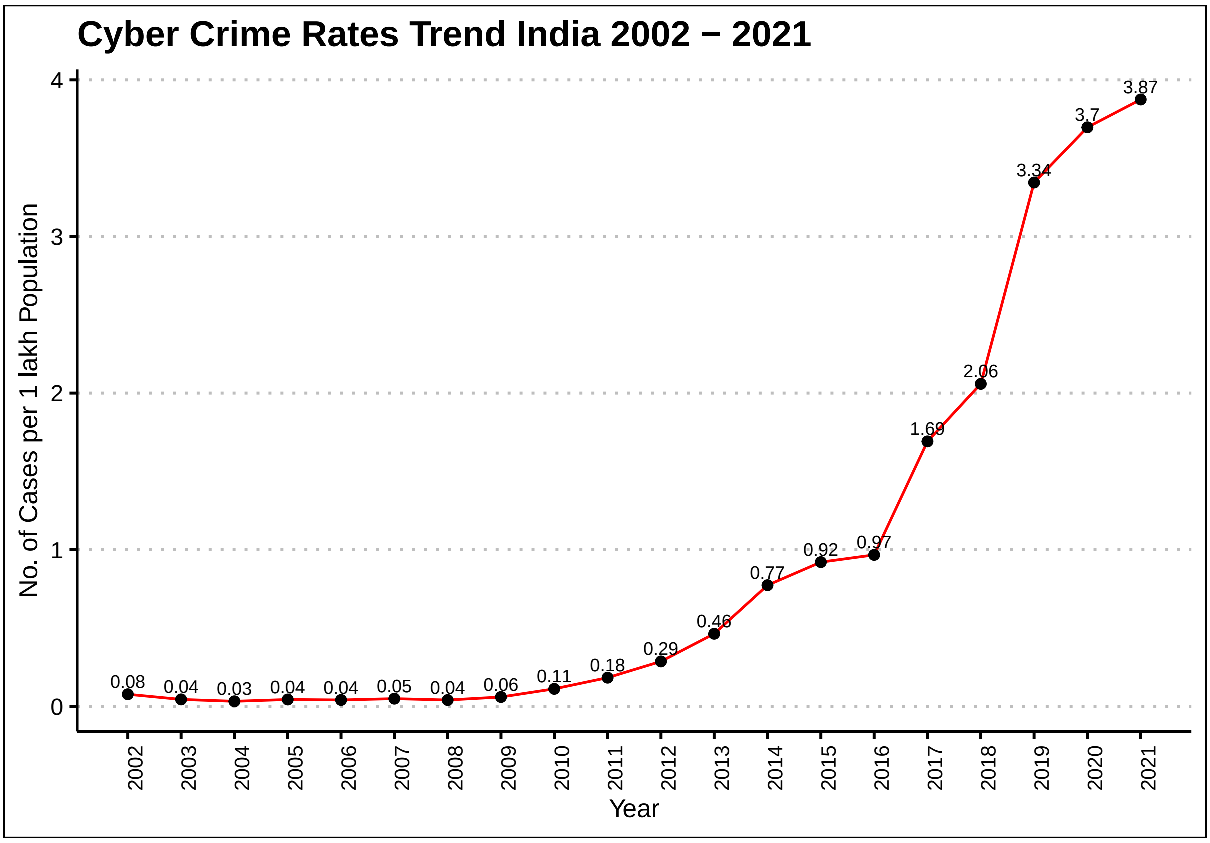
Again, from the Kolmogorov Smirnov Test as well, we conclude that the residuals are normality distributed.

Anderson Darling Test

```
##
##  Anderson-Darling normality test
##
## data:  ress$crimes
## A = 0.44091, p-value = 0.2613
```

Also, using Anderson Darling Test, the p-value is much greater than the level of significance. It indicates that the residuals are in fact normally distributed.

Cyber Crime Rate Prediction



So far we analyzed the cyber crimes trend in India. Further, it is of interest to do the same for the Cyber Crime Rates as well. It is a fact that the population of India also varied in these years. For that matter, we can observe the Cyber Crime Registration Rate of India from 2002 - 2021 as shown in the above figure.

The cyber crime rate prediction for the coming years can be done using the following fitted model:

$$\log(Y_t) = -4.26073 + 0.28345\, t$$

or

$$Y_t = \exp(-4.26073 + 0.28345\, t)$$

where:
$t \geq 1$
Y_t : Predicted Cyber Crime Rate in India for the year $(2001 + t)$

Model Summary

```
##
## Call:
## lm(formula = log(rate) ~ t)
##
## Residuals:
##      Min       1Q   Median       3Q      Max
## -0.93734 -0.29522 -0.01532  0.22008  1.41202
##
## Coefficients:
##             Estimate Std. Error t value Pr(>|t|)
## (Intercept) -4.26073    0.24395  -17.47 9.85e-13 ***
## t            0.28345    0.02036   13.92 4.47e-11 ***
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## Residual standard error: 0.5251 on 18 degrees of freedom
## Multiple R-squared:  0.915,  Adjusted R-squared:  0.9103
## F-statistic: 193.7 on 1 and 18 DF,  p-value: 4.475e-11
```

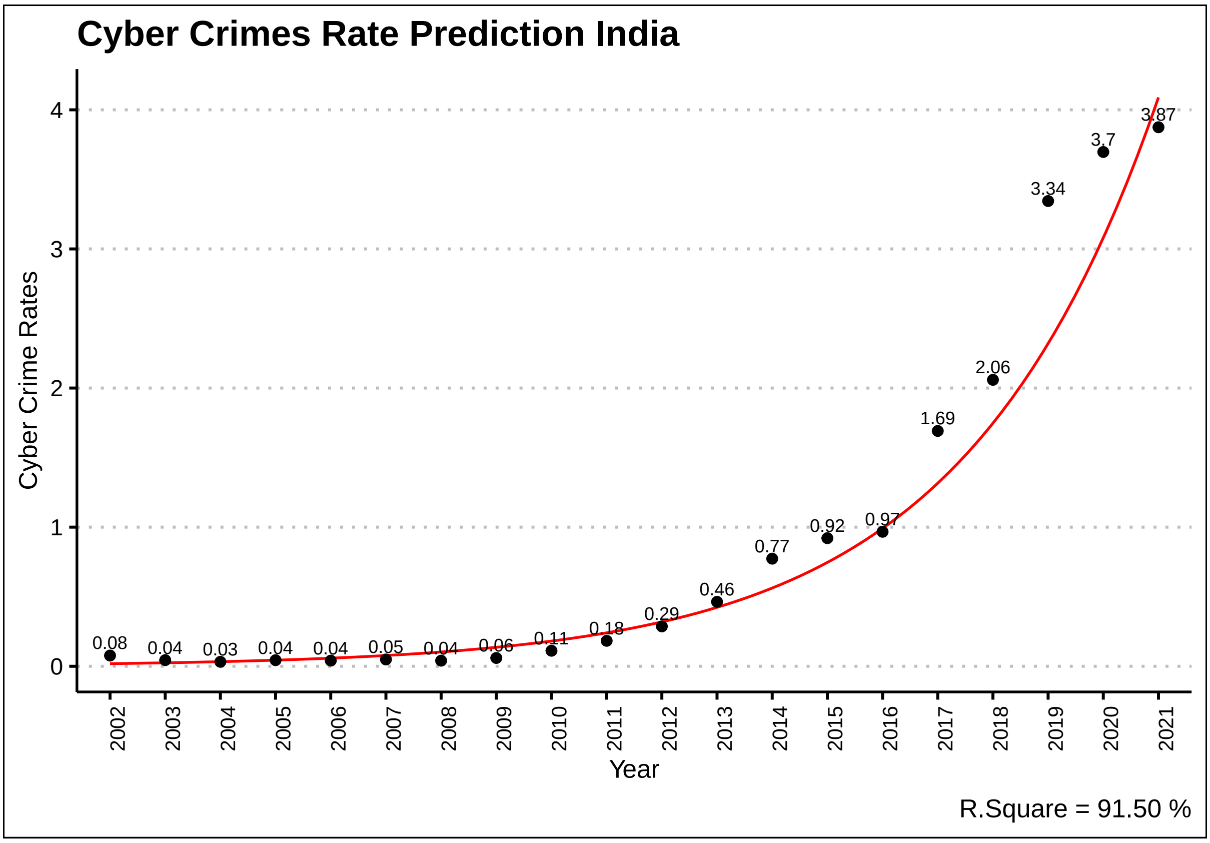
Model Inferences

- ***P Value*** = 4.475×10^{-11}, much less than the level of significance, which means the coefficients of the model are highly significant. The signif. codes "***" also indicate that the model coefficients are highly significant.
- ***F-Statistic of ANOVA*** = 193.7, which is infact very high. It also indicates the high significance of the model coefficients and can be compared with the critical values.
- ***Multiple R-Squared*** = 0.915 & ***Adjusted R Squared*** = 0.9103, which are close to 1 and do not differ from each other. These values indicate a good fit of the model.

Clearly, from the summary of the model, it is evident that the values of R^2 and Adjusted R^2 do not differ much. Here t denotes the time index. t = 1 corresponds to the year 2002, upto so on t = 20 for the year 2021. The parameter estimates are coming out to be highly significant.

Model Plot

- Years are taken along the horizontal axis and the Cyber Crime Rates are taken along the vertical axis.
- The estimated curve from the model is plotted for the Cyber Crime Rates and along with that the actual values of the rates during the corresponding years are also plotted and represented by dots in the following plot.



Future Prediction

The Cyber Crime Rates predicted for the coming years using the above model are:

year	Predicted_Rate
2022	5.429
2023	7.209
2024	9.571
2025	12.707
2026	16.871
2027	22.400
2028	29.741
2029	39.488
2030	52.428

Hence, from the predicted values from the model, the cyber crime rate in India is expected to increase rapidly and the forecast say that India will surpass almost above 50 cyber crimes per 1 lakh population.

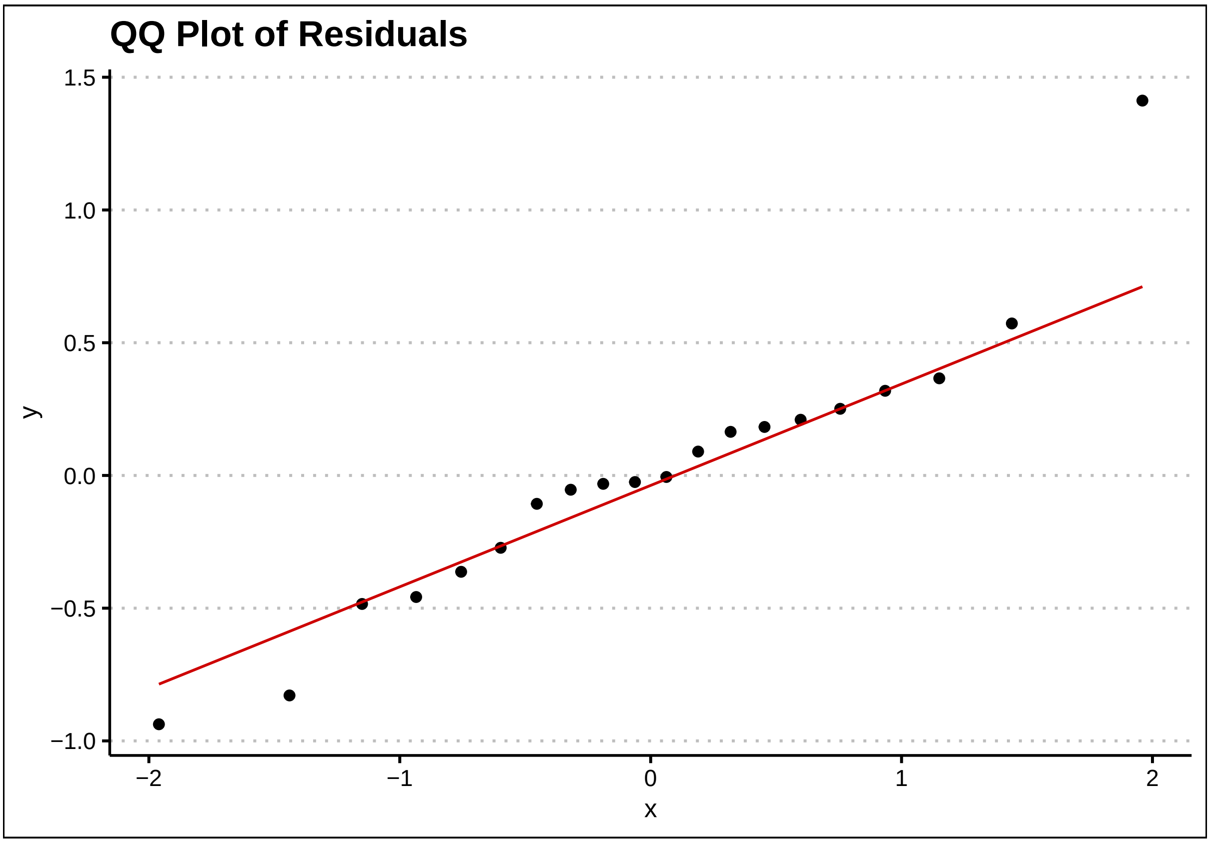
Testing Normality of Residuals

The residuals from this model are given by

```
##            1            2            3            4            5            6 
##  1.412023638  0.572523464 -0.031654495 -0.005787327 -0.362996583 -0.457975240 
##            7            8            9           10           11           12 
## -0.937339720 -0.828684483 -0.484090284 -0.272629399 -0.106935518  0.089897679 
##           13           14           15           16           17           18 
##  0.318865186  0.209748978 -0.024847703  0.251077557  0.164228196  0.365840994 
##           19           20 
##  0.182621289 -0.053886230
```

H_0: The residuals are normally distributed.
H_1: The residuals are not normally distributed.

QQ plot



Clearly, it is evident from the above plot that the quantiles are nearly lying on the qq line, which indicates the presence of normality in the residuals. But one can use some objective criteria to test the normality as follows:

Shapiro-Wilk Normality Test

```
##
##  Shapiro-Wilk normality test
##
## data:  ress$rate
## W = 0.94022, p-value = 0.2421
```

Here, the p-value >> 0.01. It means we fail to reject the null hypothesis of Normality. Hence it can be concluded that the residuals are normally distributed, with 99 % confidence.

Kolmogorov Smirnov Goodness of fit Test

```
##
##  Exact one-sample Kolmogorov-Smirnov test
##
## data:  ress$rate
## D = 0.25724, p-value = 0.1179
## alternative hypothesis: two-sided
```

Again, from the Kolmogorov Smirnov Test as well, we conclude that the residuals are normality distributed.

Anderson Darling Test

```
##
##  Anderson-Darling normality test
##
## data:  ress$rate
## A = 0.44009, p-value = 0.2625
```

Also, using Anderson Darling Test, the p-value is much greater than the level of significance. It indicates that the residuals are in fact normally distributed.

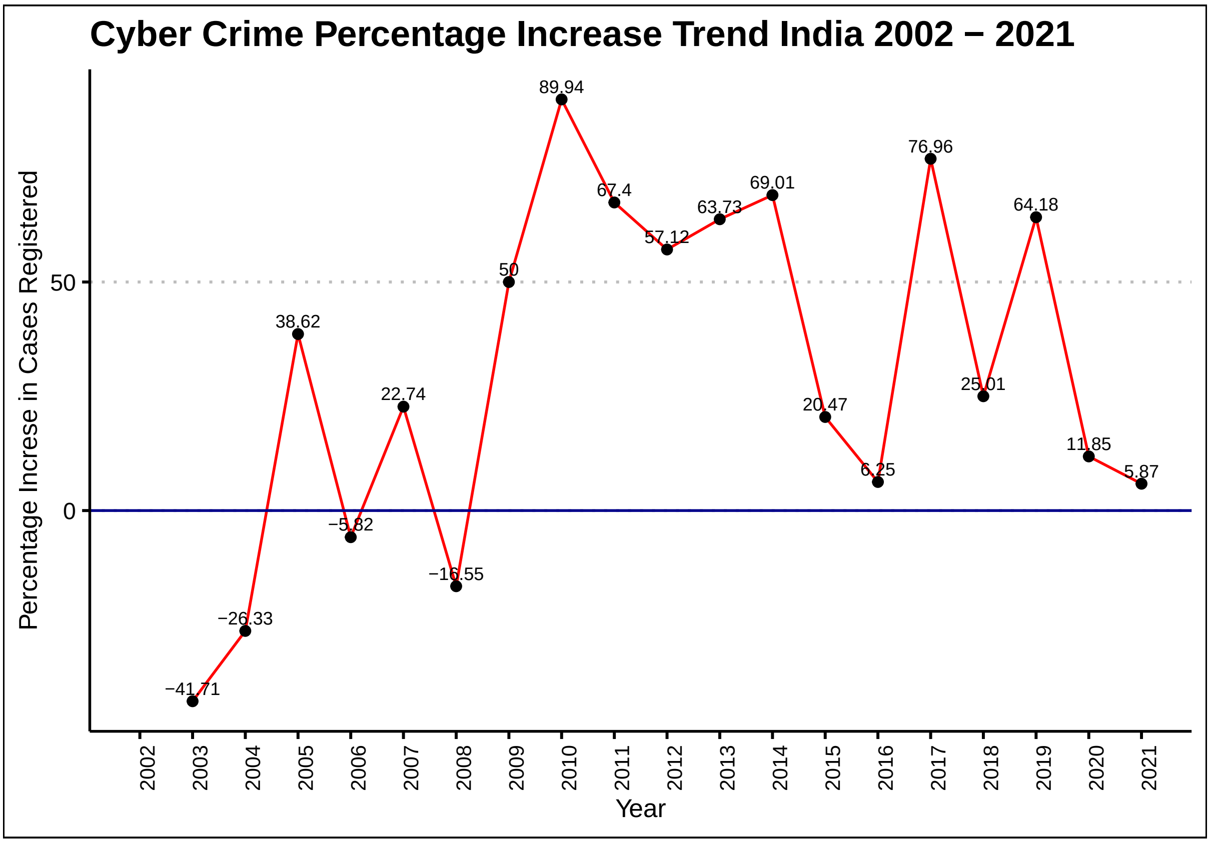
Percentage Increase Trend

To get a more clear idea about the previous year comparison, percentage increase in the cases can be calculated using the formula:

$$\text{Percentage Increase} = \frac{\text{Current Value - Previous Value}}{\text{Previous value}} * 100$$

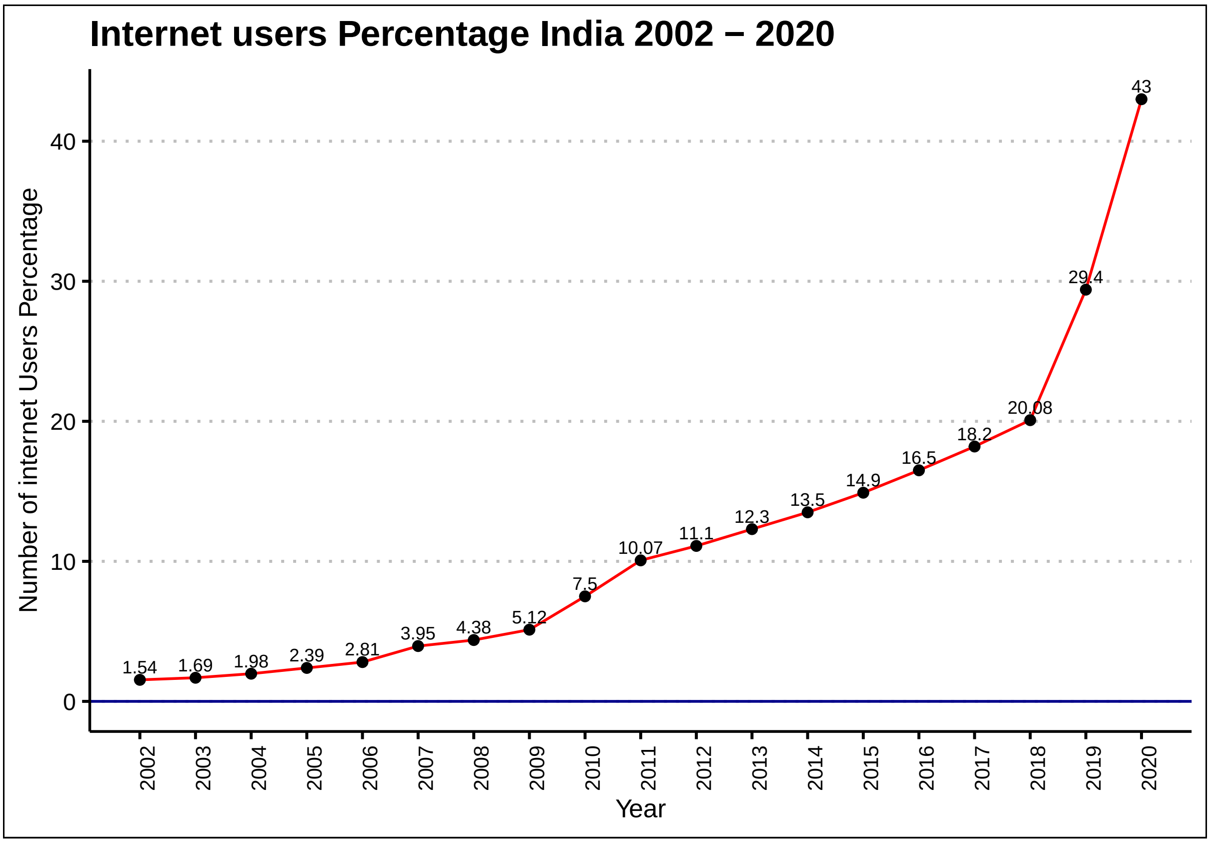
From the Percentage Increase plot, following facts can be noted:

- India registered 5.87% more cyber-crimes in 2020 as compared to 2021.
- It must be noted that the any dip in the graph does not mean decrease in the crimes, rather it means that there is less percentage increase in the cases as compared to previous year. However, any point below zero i.e., negative percentage increase indicates that there are lesser number of cases from the previous year.
- It can be noted that the negative values for the years 2003, 2004, 2006, 2008 indicate that the cyber-crimes have declined in these years as compared to the previous year.



Internet user-base of India

Besides these cyber-crime incidents and trend analysis, one should also have a look on the active internet users in India over the years. Data of active internet users in the country is taken from the International Telecommunication Union Database (2021) and visualized as follows:



It can be seen that the percentage of internet users in the country has increased in the last few years. 43% population of India had access to the internet by the year 2020. According to a report by IAMAI and data analytics firm Kantar (2023), it was estimated that in 2025, number of active internet users would surpass 900 million in the country. In fact, India was ranked as the second largest online market worldwide in 2019, coming second only to China. The number of internet users was estimated to increase in both urban as well as rural regions, indicating a dynamic growth in access to internet.

Chapter 2

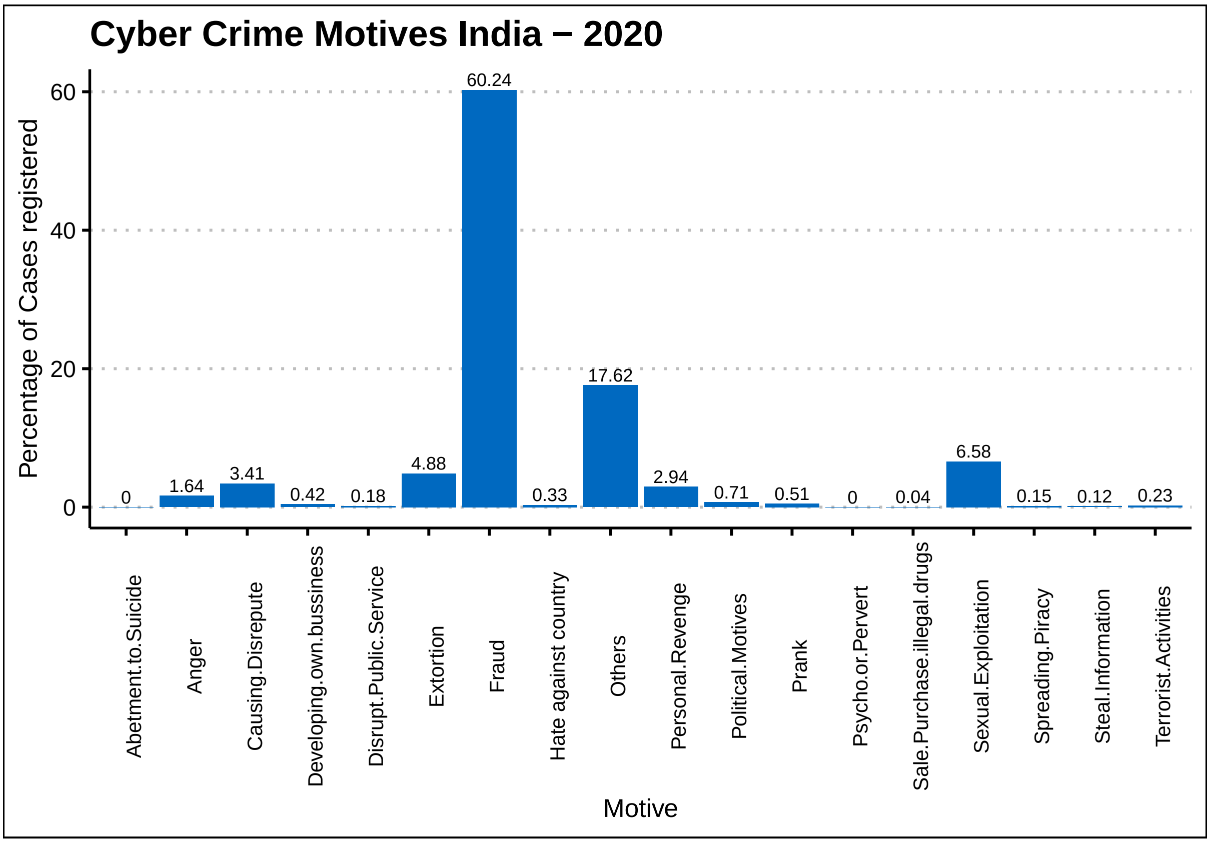
Cyber Crime Motives

2.1 Introduction

In this section, the motives behind the emerging cyber crime incidents in India are analyzed. Major motive is figured out and states are futher analyzed for that for the past few years. Cluster Analysis Technique is used to divide states into two groups (clusters) based on their crime incidence for the major motive keeping mid year projected population under consideration.

2.2 Cyber Crime Motives Year Wise

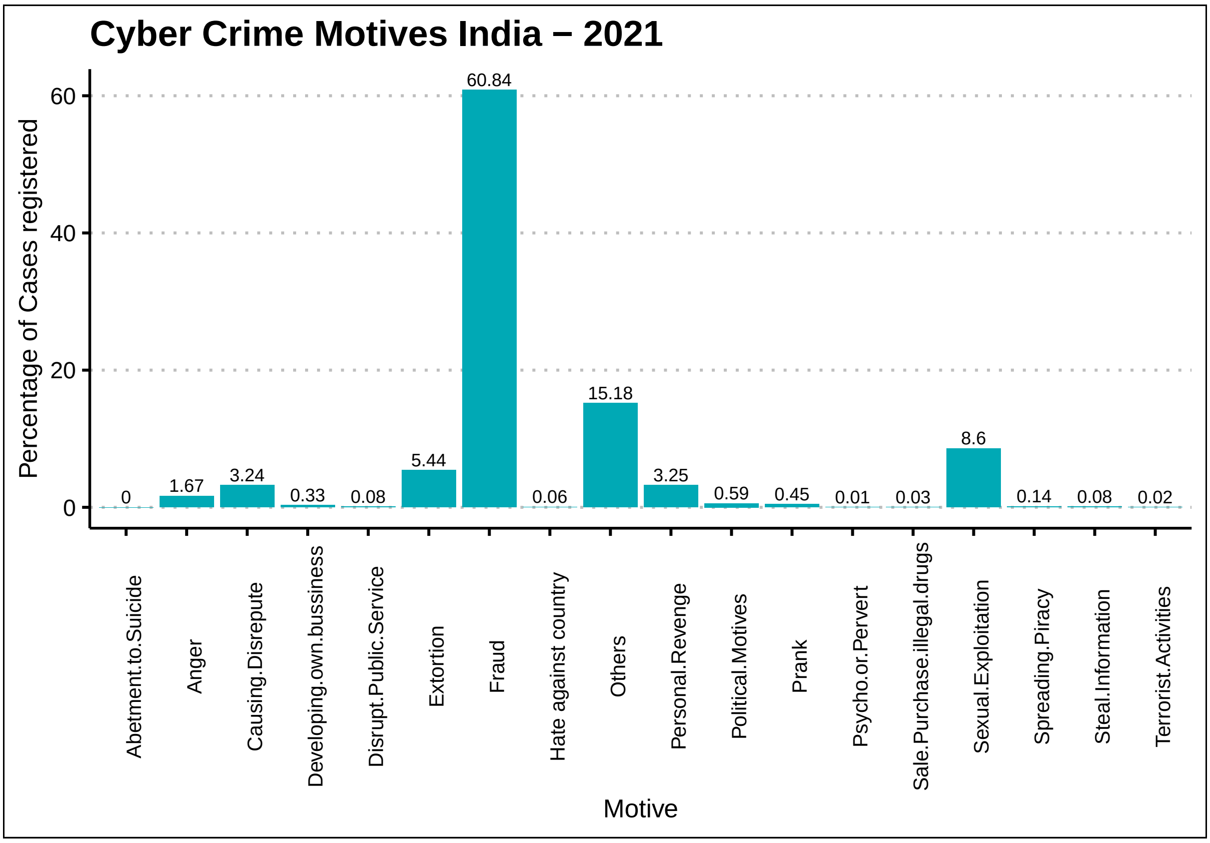
Year 2020



Major Motive

It is evident from the above figure that the **Fraud** as emerged as the major motive for cyber crimes in India during the year 2020. Note that **60.24 %** of cyber crimes registered in India were found to be with the motive of fraud.

Year 2021



Again in the next consecutive year 2021, the picture is almost similar. Again it can be seen that Fraud emerges as the major cyber crime motive in India during 2021 as well, contributing to **60.84 %** of the total cyber crimes in the country.

Key Points:

- As far as the motives behind cyber crimes in India are concerned, Fraud is the major motive. The country recorded more than 32 thousand cases of cyber crime motivated by fraudulent behavior that year.

- The other motive come second in the ranking, as labeled by the National Crime Records Bureau.

- Further, it may be noted that Sexual Exploitation, Extortion and Personal Revenge are the other prevalent motives behind cyber crimes in India.

2.3 Cluster Analysis

Cluster Analysis is an Exploratory Data Analysis Technique to group heterogeneous objects (multi-dimensional) into homogeneous groups.
The two well-known methods of Cluster Analysis are:
1. Hierarchical Cluster Analysis
2. Non-Hierarchical Cluster Analysis

Since, fraud is the major motive behind the cyber crimes in India. Hence, it is of interest to further analyze it among the states for the past few years.

For the fraud cases, different states of India are divided or grouped into clusters based on the fraction of fraud in the total cyber crimes in these states for the years 2017 to 2021.

States are divided into clusters using:
- K-Means Clustering (Non-Hierarchical)
- Agglomerative Cluster Analysis (Hierarchical)
- Divisive Cluster Analysis (Hierarchical)

2.3.1 Distance Matrix Calculations

Data has been scaled to centre 0, and unit variability of each year rate (Variables).

```
##                   Andhra Pradesh Arunachal Pradesh    Assam
## Andhra Pradesh          0.000000          3.937371 4.223798
## Arunachal Pradesh       3.937371          0.000000 3.029010
## Assam                   4.223798          3.029010 0.000000
```

This is some part of the 28x28 distance matrix of states.

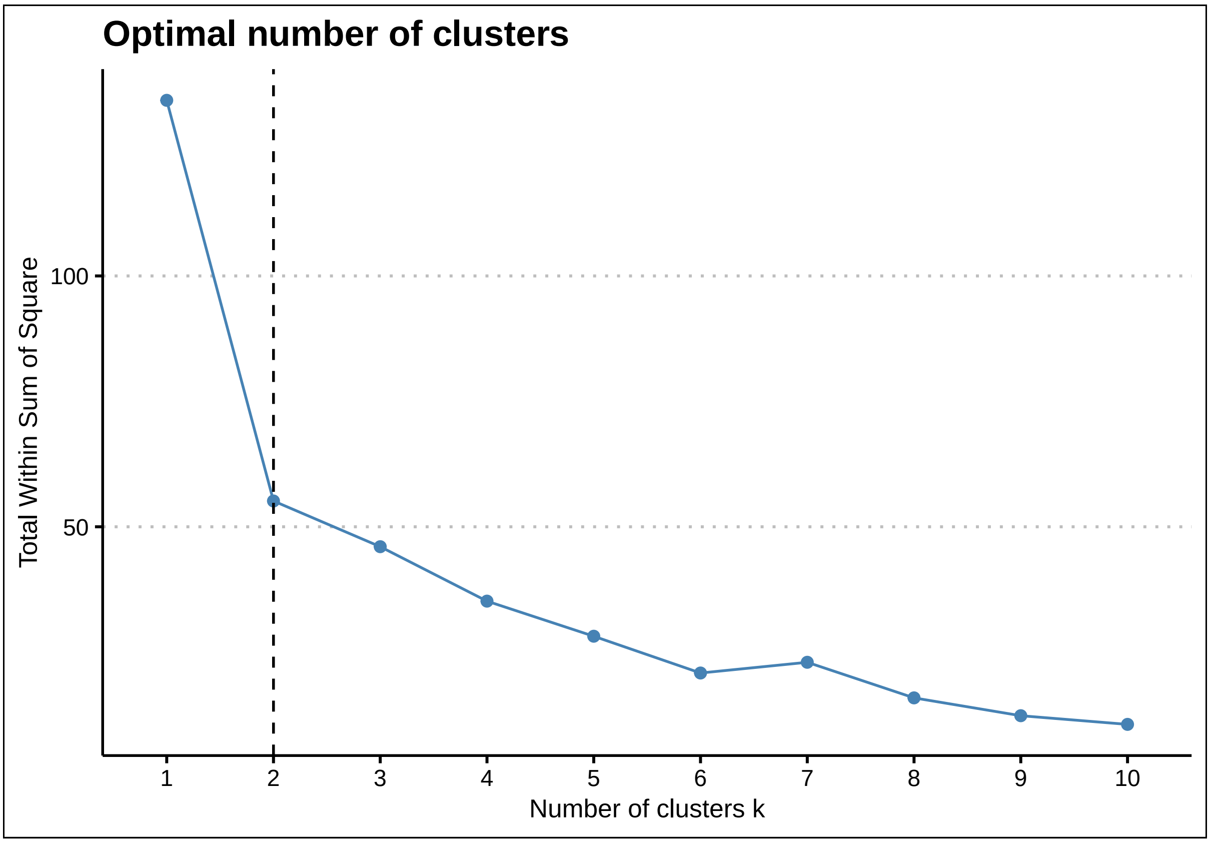
2.3.2 K-Means Clustering (Non-Hierarchical)

Optimal Number of Clusters:

- To determine the optimum number of clusters, consider the following plot of number of clusters v/s Total within sum of squares.

- Within Cluster Sum of Squares must be as minimum as possible. So accordingly the optimum number of clusters are to be chosen.

- From the following plot the optimum number of clusters is chosen as that value of k, where the value of Within Cluster Sum of Squares starts flattening down.



The Total within sum of squares starts flattening after **k = 2**, so We proceed with **K-Means clustering** with 2 clusters.

Cluster 1

```
##  [1] "Arunachal Pradesh" "Assam"             "Chhattisgarh"
##  [4] "Haryana"           "Himachal Pradesh"  "Kerala"
##  [7] "Madhya Pradesh"    "Manipur"           "Mizoram"
## [10] "Nagaland"          "Punjab"            "Rajasthan"
## [13] "Sikkim"            "Tamil Nadu"        "Tripura"
## [16] "Uttar Pradesh"     "Uttarakhand"       "West Bengal"
```

Mean Vector

```
##  rate2021  rate2020  rate2019  rate2018  rate2017
## 0.2908958 0.3307730 0.1836483 0.2436061 0.2606539
```

Cluster 2

```
##  [1] "Andhra Pradesh" "Bihar"          "Goa"            "Gujarat"
##  [5] "Jharkhand"      "Karnataka"      "Maharashtra"    "Meghalaya"
##  [9] "Odisha"         "Telangana"
```

Mean Vector

```
##  rate2021  rate2020  rate2019  rate2018  rate2017
## 0.7080721 0.7295737 0.7034289 0.6519850 0.6353667
```

This is the required clustering of 28 states into 2 clusters.

Define

$$Z_{ji} = 1, \qquad if\, \mathbf{X_i} \in \textbf{ jth cluster}$$

and

$$Z_{ji} = 0, \qquad if\, \mathbf{X_i} \notin \textbf{ jth cluster}$$

where $\mathbf{X_i}$ is the ith case vector. i = 1,2,… N.

Let $\mathbf{m_j}$ be the mean vector of jth cluster, and $\mathbf{m}$ be the grand mean.

Let n_j be the number of elements in the jth cluster.

The Within cluster sum of squares vector are given by:

$$WSSV = diag(S_W)$$

where

$$S_W = \frac{1}{N}\sum_{j=1}^{g}\sum_{i=1}^{N} Z_{ji}(\mathbf{X_i} - \mathbf{m_j})(\mathbf{X_i} - \mathbf{m_j})'$$

```
## [1] 40.44021 14.70286
```

The Total Within cluster sum of squares are given by:

$$WSS = trace(S_W)$$

where

$$S_W = \frac{1}{N}\sum_{j=1}^{g}\sum_{i=1}^{N} Z_{ji}(\mathbf{X_i} - \mathbf{m_j})(\mathbf{X_i} - \mathbf{m_j})'$$

```
## [1] 55.14307
```

and Between Cluster Sum of Squares are:

$$BSS = trace(B_W)$$

where

$$B_W = \frac{1}{N}\sum_{j=1}^{g} n_j(\mathbf{m_j} - \mathbf{m})(\mathbf{m_j} - \mathbf{m})'$$

```
## [1] 79.85693
```

The Total cluster sum of squares are given by:

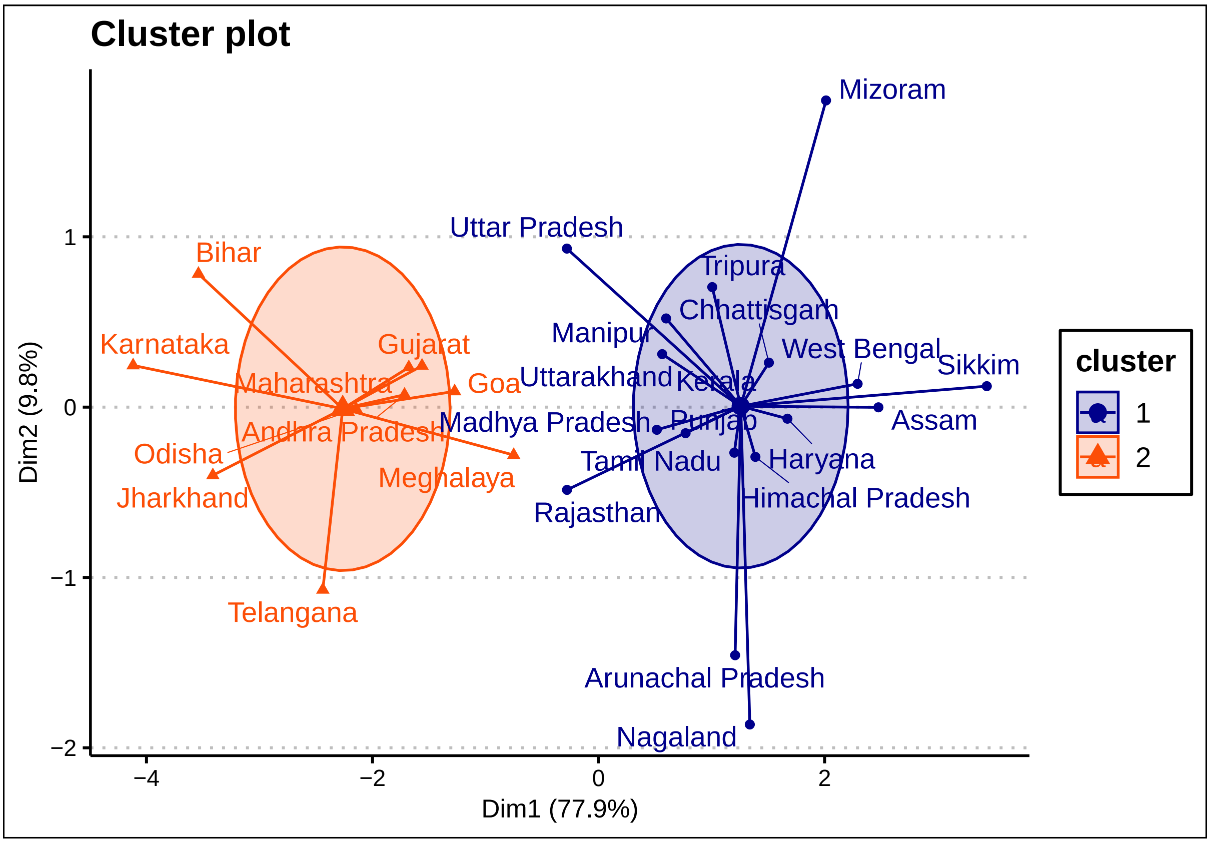
$$TSS = WSS + BSS$$

$\frac{WSS}{TSS}$ must be small.

```
## [1] 0.4084672
```

To have a better picture of the clusters, a look on the cluster plot will be helpful:

2.3.2.1 Cluster Plot



1. As it is evident from the above cluster plot that the states with fewer fraud Cyber Crimes : Arunachal Pradesh and Nagaland are in one cluster.
2. However the states with extensive fraud rates: Karnataka, Bihar,Telangana, Jharkhand,Uttar Pradesh, Maharashtra etc. are in other cluster.

2.3.3 Hierarchical Clustering

2.3.3.1 Agglomerative Clustering

Also, under the Hierarchical Clustering, using **Agglomerative Custering** with *Ward D2 Linkage*, the states are more likely to be divided into 2 clusters.

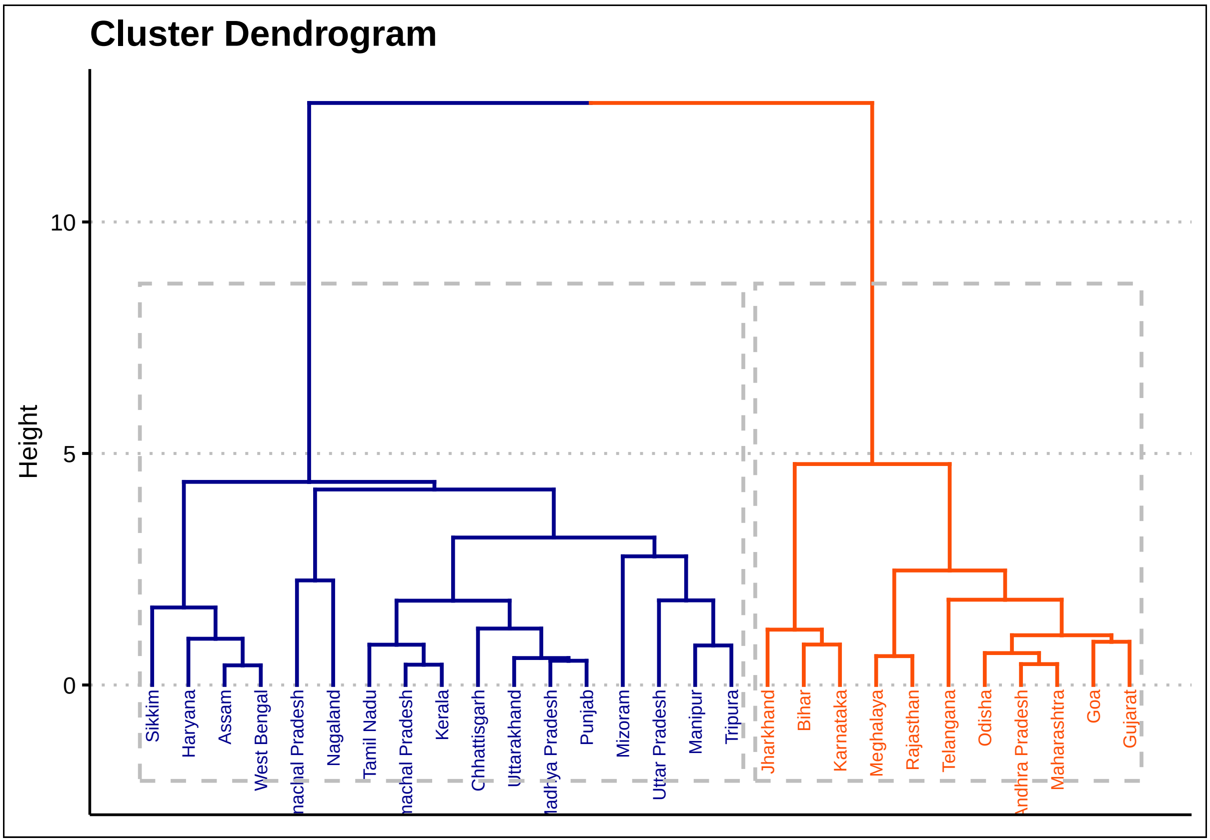
The states with major fraction of the Fraud cases are in one cluster: Telangana, Jharkhand, Bihar etc.

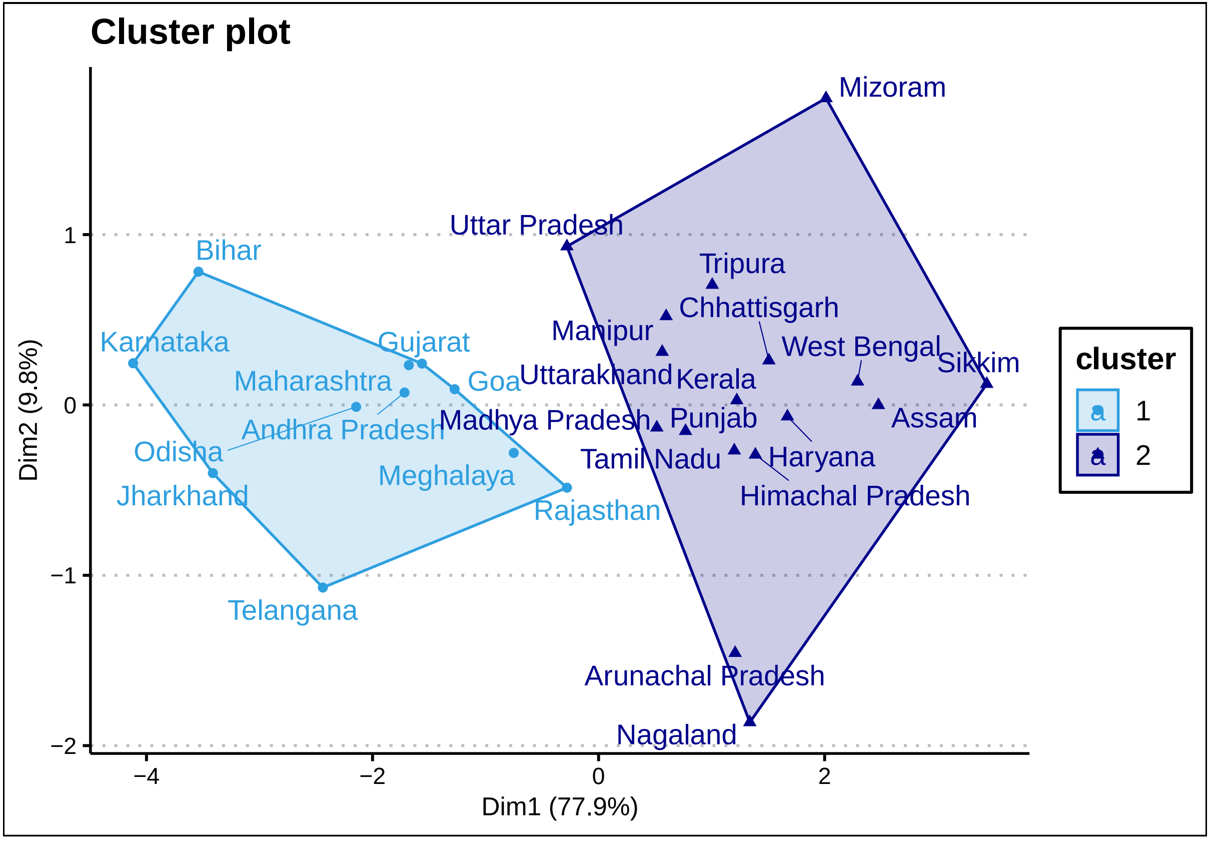
However, the states with comparatively lesser number of frauds are in the other cluster.

The cluster means are given by

```
##  rate2021  rate2020  rate2019  rate2018  rate2017
## 0.5713483 0.6334256 0.5143662 0.4825693 0.4667825
```

```
##  rate2021  rate2020  rate2019  rate2018  rate2017
## 0.2367204 0.2255833 0.1450668 0.2455529 0.2827396
```





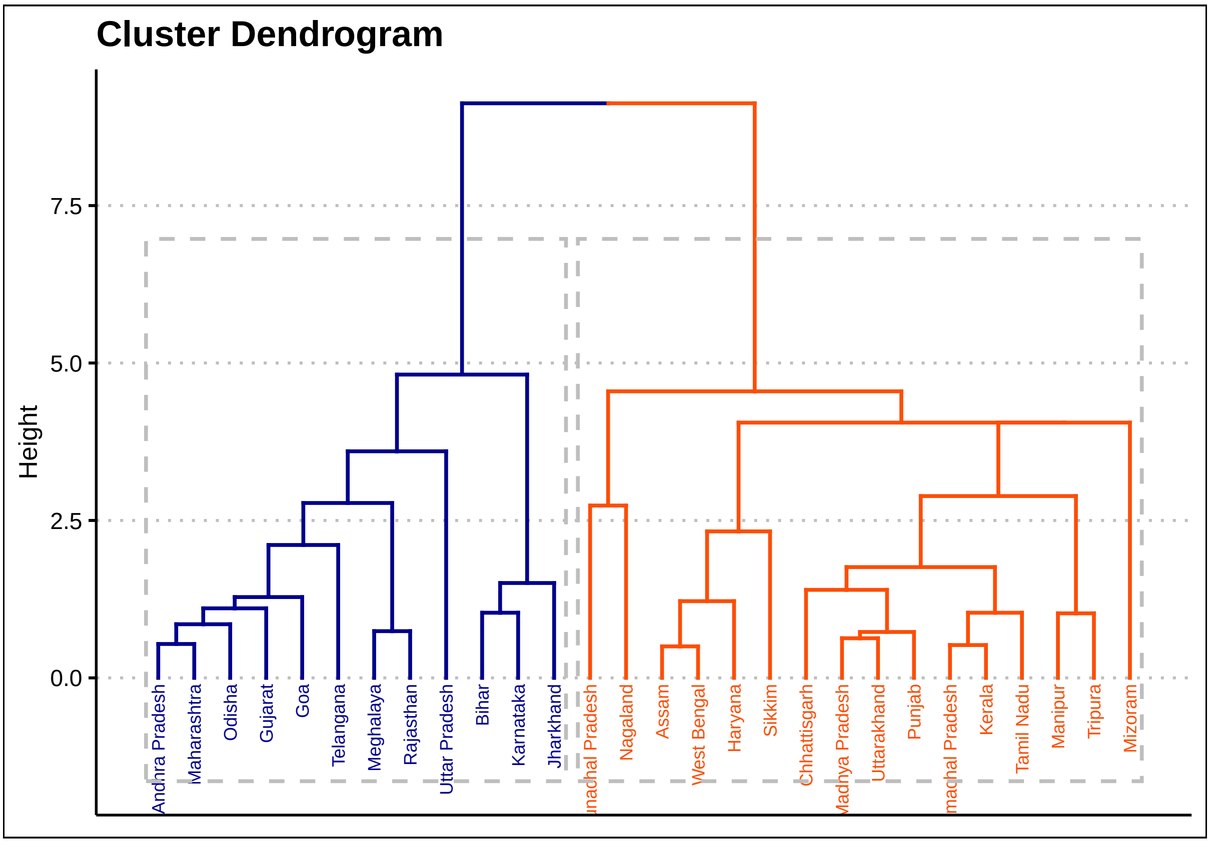
Previously, for better demarcation, we applied K-Means clustering for 4 clusters. However, under the Hierarchical Clustering, using **Agglomerative Clustering** with *Ward D2 Linkage*, the states are more likely to be divided into 2 clusters.

2.3.3.2 Divisive Clustering

Divisive method operates by successive splitting of groups. The steps involved are as follows:

- Algorithm initially starts with a single group (cluster) with all the cases.
- This cluster is then divided into two clusters such that the objects in one subgroup are as far as possible from the objects in the other subgroup.
- This process continues till there are N groups, each with a single object.

If **Divisive Clustering** is applied, the two main clusters so formed are given as follows:



Summary

Using all the three techniques, the number of clusters formed = 2. The cluster assignments by Agglomerative and Divisive techniques are almost the same as that of K-Means Clustering except the following:

- The state of Rajasthan goes to the Cluster 2 using Agglomerative and Divisive techniques.
- The state of Uttar Pradesh goes to the Cluster 2 using Divisive technique.

Chapter 3

Analysis of Cyber crimes under IT Act and IPC Act

3.1 Introduction

3.1.1 Information Technology ACT, 2000

The IT Act was introduced in 17 October 2000. It is the primary law in India dealing with cyber crime and electronic commerce. The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law. The sections of IT Act included in the analysis are:
- Tampering Computer Source Documents (Section 65)
- Computer Related Offenses (Sec 66 & Sec 66 B to E)(Total)
- Cyber Terrorism (Section 66F)
- Publication/ transmission of obscene / sexually explicit act in electronic form

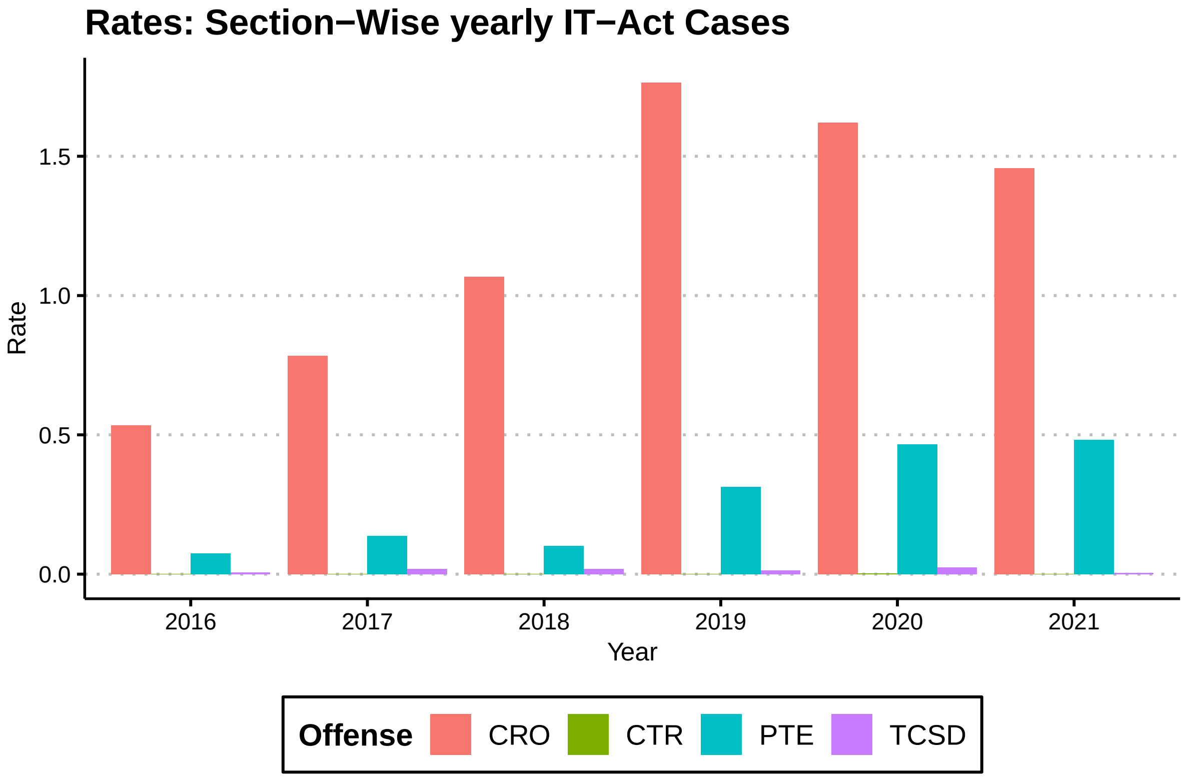


Figure: 3.1

Abbreviations Used :

TCSD: Tampering Computer Source Documents (Section 65)
CRO: Computer Related Offenses (Sec 66 & Sec 66 B to E)(TOTAL)
CTR: Cyber Terrorism (Section 66F)
PTE: Publication/ transmission of obscene / sexually explicit act in electronic form

3.1.1.1 Computer Related Offenses (Sec 66 & Sec 66 B to E)

This includes punishment regarding sending offensive messages through communication service,punishment for dishonestly receiving stolen computer resource or communication, punishment for identity theft, punishment for cheating by personation by using computer resource, Punishment for violation of privacy, penalty and compensation for damage to computer, computer system, etc.

3.1.2 Indian Penal Code , 1862

The Indian Penal Code (IPC) is the official criminal code of India. It is a comprehensive code intended to cover all substantive aspects of criminal law. It came into force in India during the British rule in 1862.

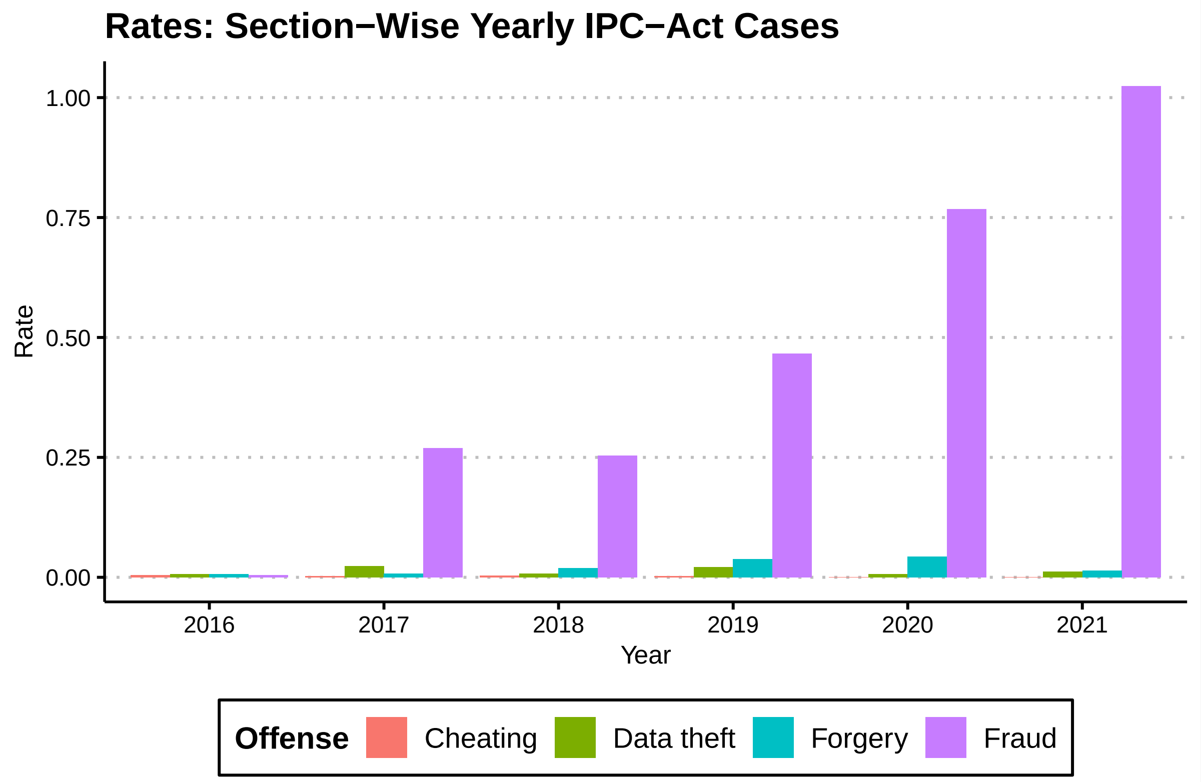


Figure: 3.2

Sections of the Offenses under IPC included in this analysis:

Data theft (Sec.379 to 381)
Fraud (Sec.420 r/w Sec.465,468-471 IPC)
Cheating (Sec.420)
Forgery (Sec.465, 468 & 471)

The figure 3.2 shows the rate of cases of Indian Penal Code (here only those sections are included which include punishments to cyber-crimes) being registered in India per 1 lakh population in years 2016-21. One must note that the Fraud cases are reported mostly.

3.1.2.1 Fraud (Sec.420 r/w Sec.465,468-471 IPC)

This include that whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment and shall also be liable to fine.

3.2 Percentage share of major crimes under IT Act and IPC

Year	CRO	Total	Percentage_Share
2016	0.5351648	0.9667975	55.3544
2017	0.7844598	1.6915400	46.3755
2018	1.0685517	2.0589702	51.8974
2019	1.7652248	3.3300190	53.0095
2020	1.6198963	3.6969307	43.8173
2021	1.4566373	3.8746626	37.5939

Year	Fraud	Total	Percentage_Share
2016	0.004395604	0.9667975	0.4547
2017	0.268988693	1.6915400	15.9020
2018	0.253366380	2.0589702	12.3055
2019	0.465976884	3.3300190	13.9932
2020	0.768054263	3.6969307	20.7755
2021	1.024510127	3.8746626	26.4413

The above data table shows that Computer Related Offenses (Sec 66 & Sec 66 B to E) ,(here , Computer Related Offenses (Sec 66 & Sec 66 B to E) is named CRO) , has been contributing about 48% and Fraud contribute about 15% of the total cyber crimes each year as per the NCRB data for cyber crimes from year 2016 - 2021. Hence Computer Related Offenses (Sec 66 & Sec 66 B to E) is the major contributor to the cyber crimes in India.

3.3 Randomness and Association

3.3.1 1-sample Run test for randomness

1-sample run test is used to test whether the observations are random

3.3.1.1 Computer related offenses (Sec 66 & Sec 66 B to E)

```
##
##  Runs Test for Randomness
##
## data:  cro_c
## runs = 2, m = 3, n = 3, p-value = 0.2
## alternative hypothesis: true number of runs is not equal the expected number
## sample estimates:
## median(x)
##     17028
```

This shows that year wise incidence of cases of Computer related offenses are random .

3.3.1.2 Fraud

```
##
##  Runs Test for Randomness
##
## data:  fr_c
## runs = 2, m = 3, n = 3, p-value = 0.2
## alternative hypothesis: true number of runs is not equal the expected number
## sample estimates:
## median(x)
##    4849.5
```

This shows that year wise incidence of cases of Fraud are random .

3.3.2 Kolmogorov Smirnov test

This test is used for testing whether both the samples come from same distribution

Test statistics,

$$D_{n,m} = \sup_x |F_{1,n}(x) - F_{2,m}(x)|$$

where $F_{1,n}$ and $F_{2,m}$ are the empirical distribution functions of the first and the second sample respectively, and *sup* is the supremum function.

```
##
##  Exact two-sample Kolmogorov-Smirnov test
##
## data:  y2016 and y2021
## D = 0.14286, p-value = 0.9333
## alternative hypothesis: two-sided
```

```
##
##  Exact two-sample Kolmogorov-Smirnov test
##
## data:  y2017 and y2021
## D = 0.14286, p-value = 0.9366
## alternative hypothesis: two-sided
```

```
##
##  Exact two-sample Kolmogorov-Smirnov test
##
## data:  y2018 and y2021
## D = 0.10714, p-value = 0.9956
## alternative hypothesis: two-sided
```

```
##
##  Exact two-sample Kolmogorov-Smirnov test
##
## data:  y2019 and y2021
## D = 0.14286, p-value = 0.9301
## alternative hypothesis: two-sided
```

```
##
##  Exact two-sample Kolmogorov-Smirnov test
##
## data:  y2020 and y2021
## D = 0.14286, p-value = 0.9361
## alternative hypothesis: two-sided
```

This shows that the distribution of computer related offenses throughout the states remains the same in the years 2016 - 2021 i.e. cases are concentrated in specific states and are distributed similarly each year.

3.3.3 Kendall Tau Measure of Association

It is a non-parametric measure based on ranks of the data.

H_0: There is no significant association between the variables. H_1: There is significant association between the variables.

Test Statistic

$$\tau = \frac{C - D}{C + D}$$

where C = number of concordant pairs.
and D = number of discordant pairs.

```
##
##  Kendall's rank correlation tau
##
## data:  cro_c and fr_c
## T = 11, p-value = 0.2722
## alternative hypothesis: true tau is not equal to 0
## sample estimates:
##       tau
## 0.4666667
```

This shows that there is no association between cyber crimes under Computer Related Offenses (Sec 66 & Sec 66 B to E) and Fraud.

3.4 Testing variability and location

Now, checking for variability w.r.t location and scale for Computer Related Offenses (Sec 66 & Sec 66 B to E) in years 2016-21 using Levene's Test for variability and Kruskal Wallis Test for location.

3.4.1 Levene Test for the equality of variances.

Let σ_i^2 denote the variance of the ith population, i = 1,2, … , k.
H_0: $\sigma_1^2 = \sigma_2^2 = \; ... \; = \sigma_k^2$
H_1: Atleast one pair of σ^2's differ.

Test Statistic

$$W = \frac{(N-k)}{(k-1)} . \frac{\sum_{i=1}^{k} N_i(\bar{Z}_{i.} - \bar{Z}_{..})^2}{\sum_{i=1}^{k}\sum_{j=1}^{N_i}(Z_{ij} - \bar{Z}_{i.})^2}$$

where, k: number of different groups to which the sampled cases belong.
N_i: Number of elements in different groups.
N: total number of cases in all groups

Here, Z_{ij} can have one of the following three definitions:

1. $Z_{ij} = |Y_{ij} - \bar{Y_{i.}}|$, where $\bar{Y_i}.$ is the mean of the i-th subgroup.
2. $Z_{ij} = |Y_{ij} - \tilde{Y_i}.|$ where $\tilde{Y_{i.}}$ is the median of the i-th subgroup.
3. $Z_{ij} = |Y_{ij} - \tilde{Y_i}.^{'}|$ where $\tilde{Y_{i.}'}$ is the trimmed mean of the i-th subgroup.

$\bar{Z_{i.}}$ are the group means of the Z_{ij} and $\bar{Z}..$ is the overall mean of the Z_{ij}.

and, Y_{ij} denote the value of jth case and ith group.

Test is to reject null hypothesis for larger values of W.

```
## Levene's Test for Homogeneity of Variance (center = median)
##        Df F value Pr(>F)
## group   5  0.6081 0.6938
##       162
```

Since p-value > 0.05 , for Levene's test, we fail to reject null hypothesis. Therefore there is no significant variability in the data through 2016-21.

3.4.2 Kruskal Wallis Test

Now testing for equality in location using Kruskal Wallis Test:

Let θ_i denote the location of the ith population, i = 1,2,3, … , k.

H_0: $\theta_1 = \theta_2 = \ \dots \ = \theta_k$
H_1: At least one pair of θ' s differ.

Test Statistic

$$H = \frac{12}{N(N+1)} \sum_{i=1}^{k} \frac{R_i^2}{n_i} - 3(N+1)$$

where R_i = Sum of Ranks of the ith sample.
n_i = size of the ith sample.

$N = \sum_{i=1}^{k} n_i$

Test is to reject H_0 for large values of H.

```
##
##  Kruskal-Wallis rank sum test
##
## data:  cases by as.factor(year)
## Kruskal-Wallis chi-squared = 1.0211, df = 5, p-value = 0.9608
```

Since p-value > 0.05 , for Kruskal Wallis test, we fail to reject H_0. There is no significant change in the sense of location of the Computer Related Offenses (Sec 66 & Sec 66 B to E) throughout the years 2016-21.

3.5 Computer Related Offenses (Sec 66 & Sec 66 B to E): State - Wise

3.5.1 Cyber Crimes in Numbers: State Wise

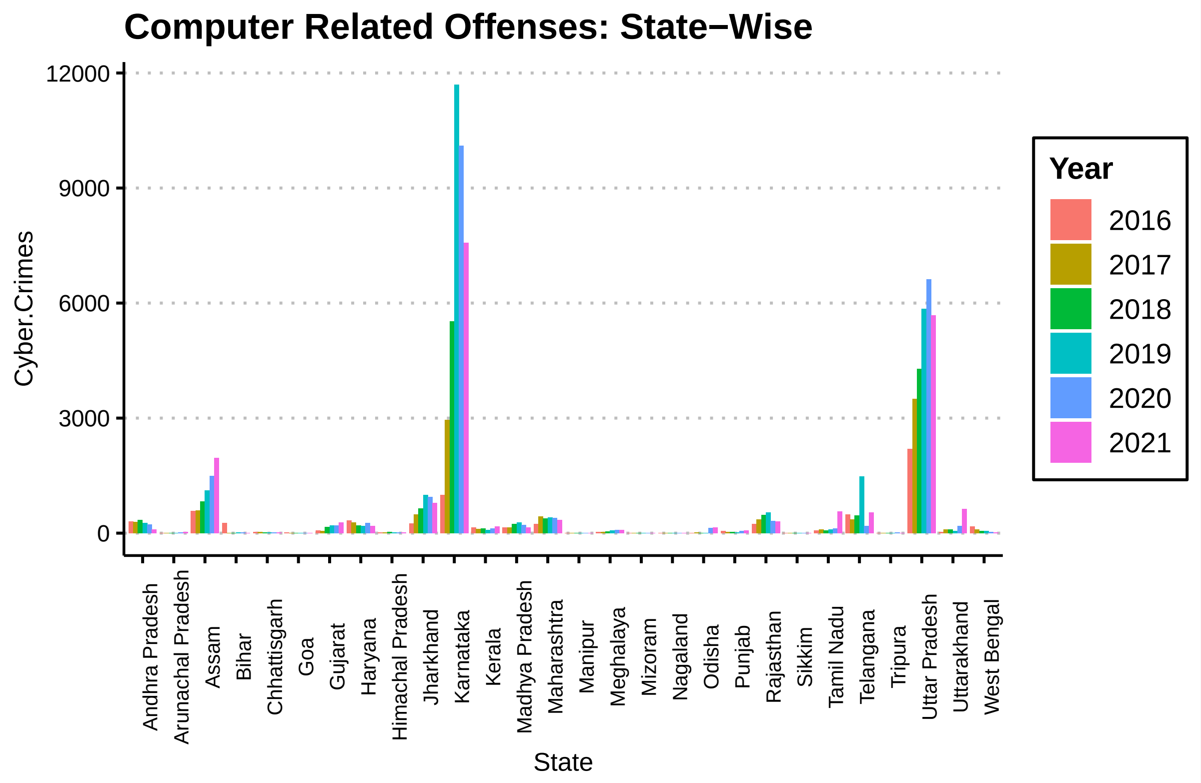


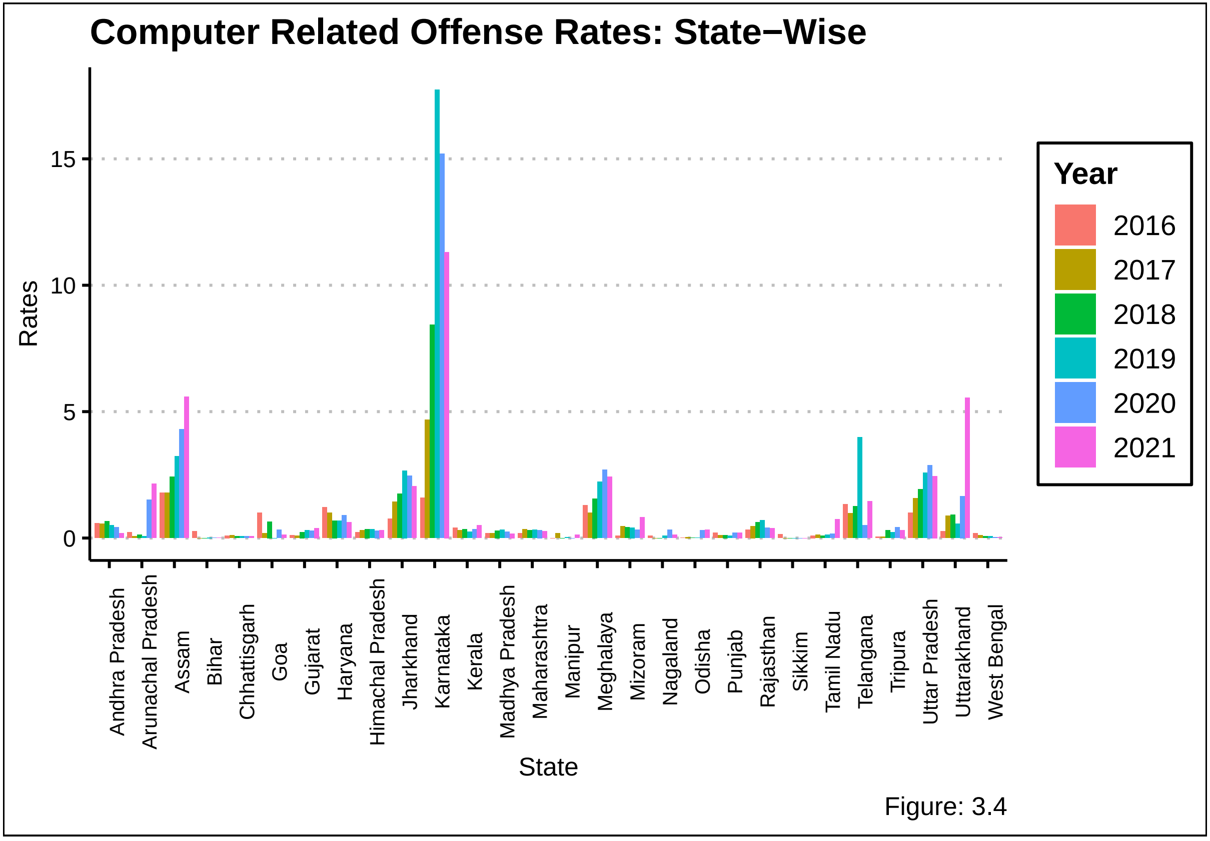
Figure: 3.3

The figure 3.3 shows the highest number of cases being registered in Karnataka, followed by Uttar Pradesh and Assam. But one must note that the population in these states may vary. So to get a better comparison, rates can be calculated, which gives the cyber-crime cases registered in the state per 1 lakh population. Mid-year projected population for each state for the year 2016 - 2021 is available. Hence the Crime Rate can be calculated.

$$\text{Rate} = \frac{\text{No.of cases registered}}{\text{Mid year projected population (in lakhs)}}$$

3.5.2 Crime Rate in each state: Computer Related Offenses

Apart from the actual count of the Computer Related Offenses in each state, one can also have a look at the number of computer related offenses per 1 lakh population in these states. For that matter, the following plot, Figure 3.4 of Crime Rates is given:



Interpretation

- The state of Karnataka emerged with the highest crime rates of Computer Related Offenses (CRO) in the past few years. The Crime Rate of CRO in Karnataka is **continuously above 10** in the past few years, and it has passed **the mark of 15** during 2019.
- The states of Assam, Uttarakhand, Meghalaya, Jharkhand and Telangana are having the CRO rate in the bracket of 3 - 5 cases per 1 lakh population.
- One must note that the Uttarakhand had observed a peak in year 2021, where the rate suddenly surpass 5 in this year, which is a matter of concern.

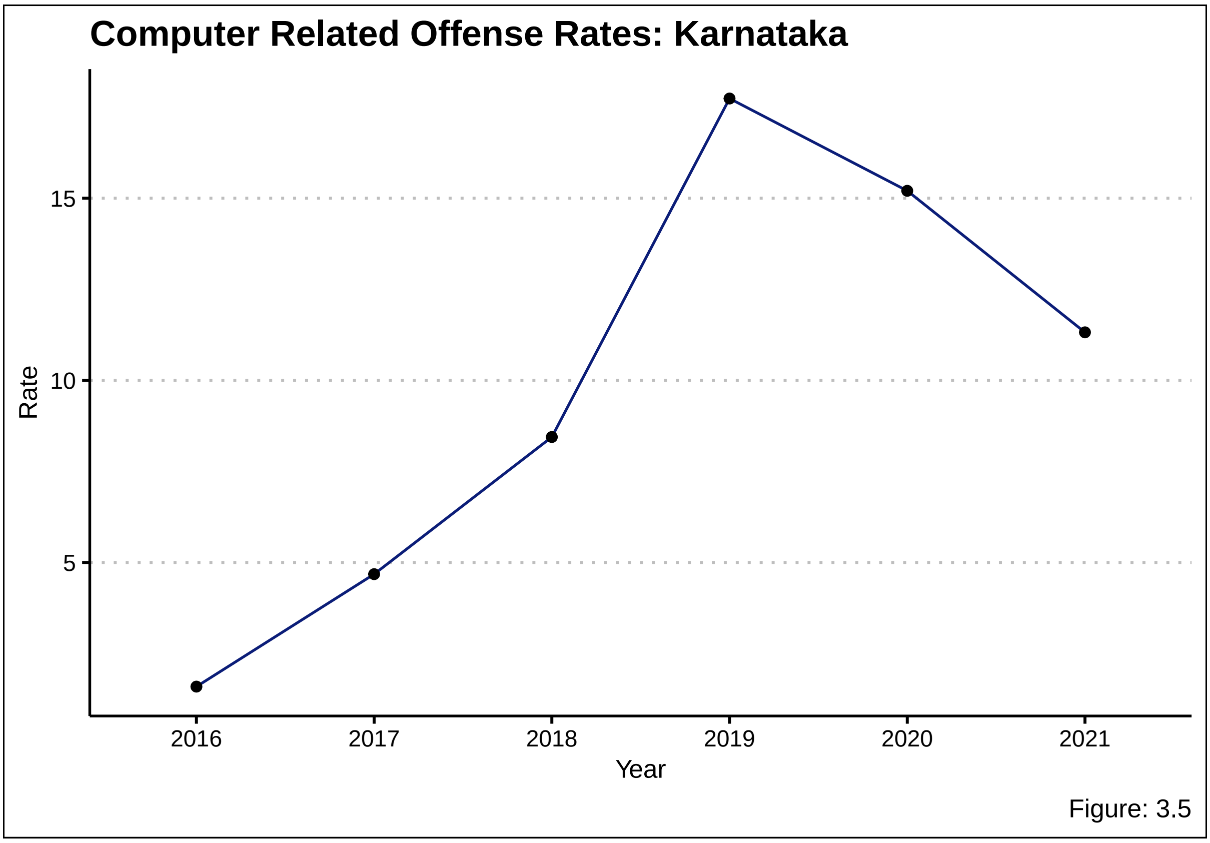


Figure: 3.5

The pattern of crime per 1 Lakh population in respective year in Karnataka can be seen in figure 3.5.The crime rate as well as counts of cyber crimes in Karnataka is surprisingly high.

3.5.3 Year wise increment of Computer Related Offenses (Sec 66 & Sec 66 B to E)

Year	CRO	Percentage_Increase
2016	0.5351648	NA
2017	0.7844598	46.5828
2018	1.0685517	36.2150
2019	1.7652248	65.1979
2020	1.6198963	-8.2329
2021	1.4566373	-10.0784

The above data table shows the Computer Related Offenses got a peak in year 2019 when they increased by **65 %** as compared to previous year 2018. However a slight % decrease can be seen after that .

Chapter 4

Police Disposal of Cyber Crimes in India

4.1 Introduction

kkk

ll

4.2 Statistics and Data Visualization

4.2.1 Total Cases Investigated

dd

4.2.2 Total Cases Disposed

ddd

xxx

4.2.3 Total Cases Pending

xxx

xx

xxx

xxx

xx

xx x

4.3 Testing location (Crime Head-wise)

dds

sdd

4.3.1 Testing variability and location (state-wise)

dsd

ds

dse

4.3.2 Paired Wilcoxon Signed-Rank test

ddf

dfd

4.4 Hierarchical Cluster Analysis

dsf

dds

sdd

swd

Chapter 5

Court Disposal of Cyber Crime Cases

5.1 Introduction

fff

5.2 Analysis of Court Disposal of Cyber Crime Cases (State/UT-wise)

ghh

5.2.1 Total No. Cases in The Court

dff

fffd

dfrd

dffgr

dsd

fdd

5.2.2 Cases in Which Trial Were Completed

fef

dssd

dsd

5.2.3 Conviction Rate

ddd

dwd

ded

5.2.4 Cases Pending Trial at End of the Year

dsde

edd

eded

5.2.5 Pendency Rate

dfe

ded

deefd

5.3 Analysis of Court Disposal of Cyber Crime Cases (Crime Head-wise)

ssd

wesw

5.3.1 Pie-charts

dwd

ed3

5.3.2 Analysis for Offences Under I.T. Act

33

33213

1swd

eewe

ewewe

5.3.3 Analysis for Offences Under IPC

wdw

wswd

wswd

wded

wde

5.3.4 Analysis for Offenses Under SLL

wdw

wswd

wswd

wded

wde

5.3.5 Predicted Offences for 2022: Percentage Contribution and Comparison

5.4 Gist of The Analysis

sdewd

sds

5.5 Remedies

qwqs

wsws

5.6 Conclusion

sws

Chapter 6

Disposal of Persons Arrested Under Cyber Crime

6.1 Disposal of Persons Arrested under Cyber Crimes (State Wise)

as

a

6.2 Analysis of Disposal of Cyber Crime (State-wise)

6.2.1 Persons Arrested

dd

dwd

ww

dwd

sd

6.2.2 Persons Charge sheeted

ww

dwd

sd

6.2.3 Persons Arrested Year-Wise In India

dwd

ww

dwd

sd

6.2.4 Persons Charge sheeted Year-wise In India

ww

dwd

sd

6.2.5 Analysis for Relationship Between No. Of Persons Arrested and Charge sheeted

ww

dwd

sd

6.2.6 Some Statistical Results Based on Persons Convicted, Discharged and Acquitted

dwd

sd

6.3 Disposal of Persons Arrested Under Cyber Crimes (Crime Head-wise)

6.4 Total Offences Under I.T. Act

6.4.1 Persons Arrested

dwd

ww

dwd

sd

6.4.2 Persons Charge sheeted

ww

dwd

sd

6.4.3 Comparison Between People Arrested and People Charge sheeted

dwd

ww

dwd

sd

6.4.4 Persons Convicted Year-wise

sw

de

6.4.5 Persons Discharged Year-wise

sw

de

6.4.6 Persons Acquitted Year-wise

sw

de

6.5 Total Offences Under IPC

sw

de

6.5.1 Persons Arrested

sw

de

sw

de

6.5.2 Persons Charge sheeted

sw

de

sw

de

6.5.3 Comparison Between People Arrested and People Charge sheeted

sw

de

sw

de

sw

de

6.5.4 Persons Convicted Year-wise

sw

de

6.5.5 Persons Discharged Year-wise

a

6.5.6 Persons Acquitted Year-wise

sw

de

6.6 Total Offences Under SLL

qa

6.6.1 Persons Arrested

sw

de

sw

de

6.6.2 Persons Charge sheeted

sw

de

sw

de

6.6.3 Comparison Between People Arrested and People Charge sheeted

sw

de

sw

de

sw

de

6.6.4 Persons Convicted Year-wise

sa

6.6.5 Persons Discharged Year-wise

sw

de

6.6.6 Persons Acquitted Year-wise

sw

de

6.7 Statistical Analysis of Total Number of Cases Obtained

sw

de sw

de

Chapter 7

Cyber Crimes against Women and Children

7.1 Introduction

7.2 Cyber Crimes against Children

wdw

sws

7.2.1 Runs Test for randomness

7.2.2 Kolmogorov-Smirnov Test

wdw

swswdw

swswdw

swswdw

sws

7.3 Cyber Crimes against Women

7.3.1 Kolmogorov-Smirnov Test

swswdw

sws

7.3.2 Runs Test for randomness

swswdw

sws swswdw

sws swswdw

sws swswdw

sss

Chapter 8

Conclusion