Global Journal of Enterprise Information System

DOI: 10.18311/gjeis/2018/19960

Empirical Study of Cyber Crimes in India using Data Analytics

Disha Gupta[1] and Namrata Agrawal[2]*

[1]Gujarat Forensic Sciences University, Gandhinagar, Gujarat, India

[2]NIFM, Institution of Ministry of Finance, Government of India, nagrawal@nifm.ac.in

Abstract

The progression of technology has prepared man reliant on Internet for all his needs. Internet has given man trouble-free entrée to the whole thing while sitting at one position. Social networking, online shopping, storing data, gaming, online studying, online jobs, every promising thing that man can imagine of can be made through the means of internet. Internet is used in approximately every bubble. With the development of the internet and its associated payback also developed the thought of cyber crimes. Computer crime or cyber-crime in India has been embryonic hastily. Cyber crimes can be distinct as the prohibited acts where the computer is used moreover as an instrument or an idea or in assistance. The expression is a wide-ranging term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and many more that are addressed by the Information Technology Act, 2000.

Keywords: Analytics, Computers, Crime, Cyber, Data

Paper Code (DOI): 19960; **Originality Test Ratio:** 16%; **Submission Online:** 09-Feb-2018; **Manuscript Accepted:** 19-Feb-2018; **Originality Check:** 26-Feb-2018; **Peer Reviewers Comment:** 01-Mar-2018; **Double Blind Reviewers Comment:** 11-Mar-2018; **Author Revert:** 12-Mar-2018; **Camera-Ready-Copy:** 14-Mar-2018; **Editorial Board Excerpt:** 24-Mar-2018.

Editorial Board Excerpt: *At the Time of Submission (ToS) submitted manuscript had a 16% plagiarism which is an excellent evidence as far as originality report is concerned and falls under an established percentage for publication. The editorial board is of an examination that script had a subsequent close watch by the blind reviewer's which at a while had been set right and modified by an author (Disha and Namrata) in a diversity of phases as and when enforced to do as an outcome. The reviewer's had in a primary stages comment with minor revision with a following statement which at a short span rationalized by an author. The comments related to references, abstract and body text is noticeable both subject-wise and research wise by the reviewers during evaluation and further at blind review procedure too. All the comments had been shared at a variety of dates by the authors' in due course of time and same had been integrated by the author in accumulation. By and large all the editorial and reviewer's comments had been integrated in a paper at the end and further the paper had been earmarked and decided under* ***"Research Thought"*** *class as its things to see and underline the work in relation to Cyber Crimes in India using Data Analytics.*

1. Introduction

In modern life, cybercrime is an evil having its origin in the growing dependence on computers. In a day and age when everything from microwave ovens, refrigerators to nuclear power plants is being operated and controlled by mouse clicks, the crimes have started taking place even in the cyber space[4]. As there is a sharp increase in the number of mobile and internet user penetration in the country, the cybercrime is also rising proportionately. The exploitation and abuse of computers and IT platforms have given birth to this new age crimes which includes tampering of digital documents, damage or loss to computer resource/utility, obscene publication or transmission in electronic form, hacking, ignorance in compliances of orders of regulatory authorities, un-authorised access/attempt to access protected computer system/network, frauds related to Digital Signature Certificate, cybersquatting, phishing attack, email spoofing, cyber defamation including sending threatening e-mails[3].

During the year 2011 and 2015, more than 32,000 cases of crimes were reported in India and more than 24,000 cases were registered under the IT Act, various sections of Indian Penal Code (IPC) and State Level Legislations (SLL)[1].

There are multiple causes of cybercrime such as revenge, settling scores, greed, extortion, disrepute, including pranks. India being a large country with huge population and IT savvy citizens with high IT penetration rate. According to Mark Rutte, the annual cost of cybercrime to the global economy is more than $4 billion.

2. Research Objectives

The main objectives of the research are to analyse the cybercrimes in India with reference to the authentic data available. The data thus obtained has been standardised, studied and exhaustively analysed to study the following using analytical tools:

*Author for correspondence

i State-wise analysis and comparison of cybercrimes in India
ii Category wise analysis of various Cyber Crimes
iii State and Crime-wise Analysis
  a. Revenge/Settling Score
  b. Greed/Settling Score
  c. Extortion
  d. Prank
  e. Fraud/Illegal Gain
  f. Eve Teasing
iv Cybercrime for Monetary Gains
v Correlation between various types of Cyber Crimes

3. Methodology

The data has been sourced from Open Government Data Platform of India (data.gov.in) for the fulfilment of the above research objectives. The dataset comprises of state-wise listing of cybercrimes such as Revenge/Settling scores, Greed/Money, Extortion, Cause Disrepute, Prank/Satisfaction of Gaining Fraud/Illegal Gain, Eve teasing/Harassment, Others. Finally total of cybercrimes occurred and registered in particular states have been also calculated for the year 2013.

The data thus obtained has been standardised, analysed and the results have been displayed graphically.

4. Data Analytics and Observations

The observations and the results as obtained after exhaustive analysis of the data as obtained from the authentic source has been elaborated as follows[2]:

4.1 State-Wise Analysis and Comparison of Cybercrimes in India

It is evident from the above graph that the highest number (907) cases of cybercrimes have been registered in the state of Maharashtra[7].

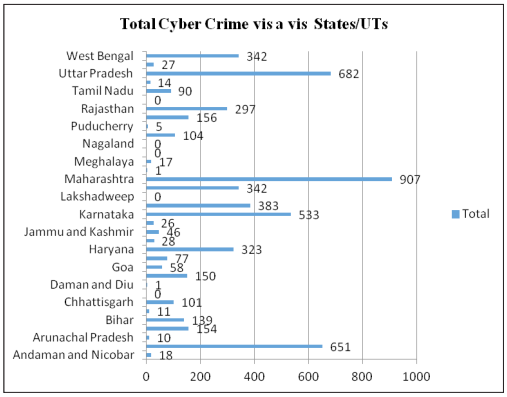


Figure 1. State-wise Total Cyber Crime.

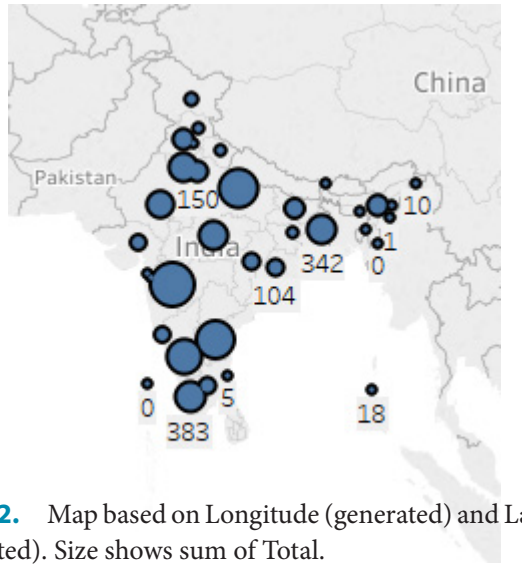


Figure 2. Map based on Longitude (generated) and Latitude (generated). Size shows sum of Total.

- Number of registered crimes in the state of Karnataka, Andhara Pradesh and Uttar Pradesh is more than 500.
- Rajasthan, Kerala, MP and Haryana have crime rate around 300.
- Punjab, Orissa, Delhi, Chattisgarh, Bihar and Assam have more than 100 cases.
- Lakswadeep, Dadar and Nagar Haveli and Sikkim have zero crimes. This may be attributed to limit IT infrastructure and related facilities available at these places.

4.2 Category Wise Analysis of Various Cyber Crimes

The analysis is based on various types/categories of cybercrimes such as Revenge/Settling scores, Greed/Money, Extortion, Cause Disrepute, Prank/Satisfaction of Gaining Fraud/Illegal Gain, Eve teasing/Harassment, Others[6].

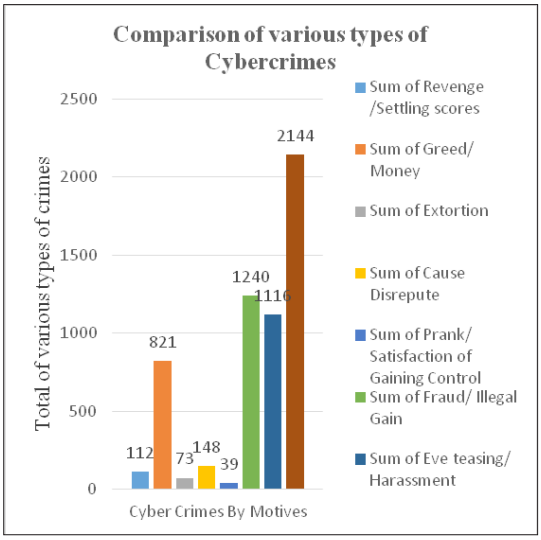


Figure 3. Comparison of various types of Cybercrimes.

- It is observed that the crimes included under 'Others' category have maximum number of occurrences.
- Crimes committed on account of Fraud and Illegal Gain is also significant followed by eve teasing and harassment.

4.3 State and Crime-Wise Analysis

4.3.1 Revenge/Settling Score

- It is observed that that the state of Kerala leads in this category as compared to any other state.
- Barring Maharashtra, Orissa, Uttar Pradesh and West Bengal, the Crime on account of revenge/settling score is negligible/zero in most of the states.

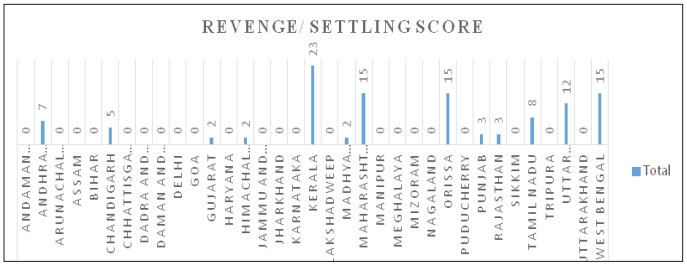


Figure 4. State-wise Analysis of Revenge/Settling Score.

4.3.2 Greed/Settling Score

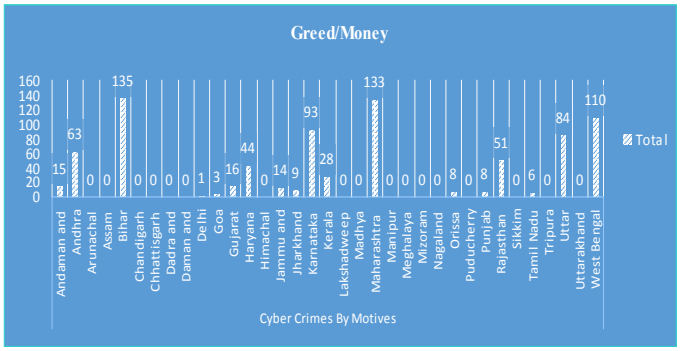


Figure 5. State-wise Analysis of Greed/Settling Score.

It is observed that the-

- Crimes on account of greed/settling scores are quite significant in the states of Bihar (135), Maharashtra (133) and West Bengal (110).
- Andhra Pradesh, Haryana, Rajasthan and Uttar Pradesh lie between 50 to 100 under this category.
- Other states have almost negligible crime under this category.

4.3.3 Extortion

It is observed that the

- Crimes on account of extortion are high in the states of West Bengal and Uttar Pradesh followed by Maharashtra.

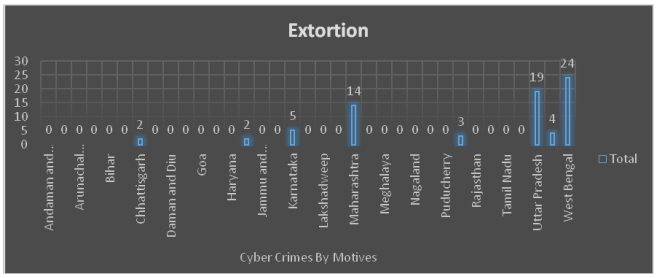


Figure 6. State-wise Analysis of Cybercrime Extortion.

4.3.4 Prank

It is observed that the -

- Crimes on account of prank are high in the states of Maharashtra, Punjab and Uttar Pradesh.
- The remaining states have negligible or no crime.

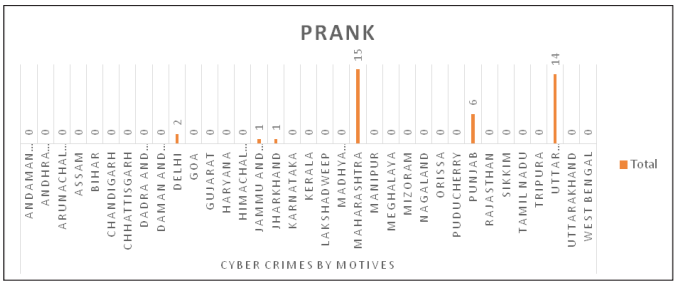


Figure 7. State-wise Analysis of Cybercrime Prank.

4.3.5 Fraud/Illegal Gain

It is observed that the-

- Crimes on account of Fraud/Illegal Gain are highest in the state of Uttar Pradesh.
- The states such as Andhra Pradesh, Maharashtra and Karnataka have significant crime under this category.
- The remaining states have negligible or no crime under this category.

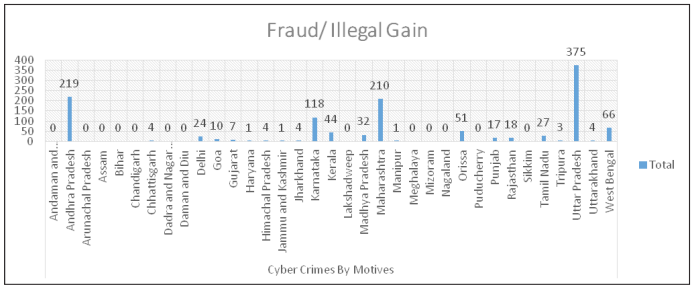


Figure 8. State-wise Analysis of Cybercrime Fraud/Illegal Gain.

4.3.6 Eve Teasing

It is observed that the-

- Crimes on account of eve teasing are highest in the state of Uttar Pradesh.

- Maharashtra and Andhra Pradesh have significantly high rate of such crime.
- Karnataka, Madhya Pradesh and Rajasthan account for moderate rate under this category.
- The remaining states have negligible or nil crime under this category.

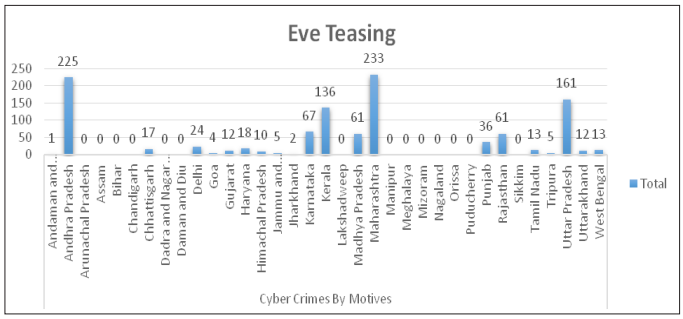


Figure 9. State-wise Analysis of Cybercrime Eve Teasing.

4.3.7 Others

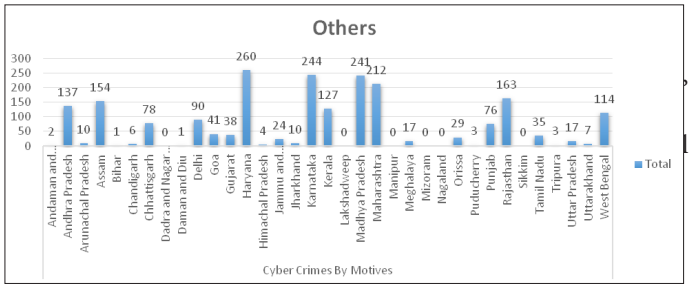


Figure 10. State-wise Analysis of Other Cybercrimes.

4.4 Cybercrime for Monetary Gains

The chart below gives the total number of cybercrimes carried out for monetary gains. Uttar Pradesh is the state with maximum crimes whereas Arunachal Pradesh, Assam, Chandigarh Daman & Diu, Lakshadweep, Manipur, Meghalaya, Mizoram, Nagaland, Puducherry and Tripura has negligible crime on account of monetary gains.

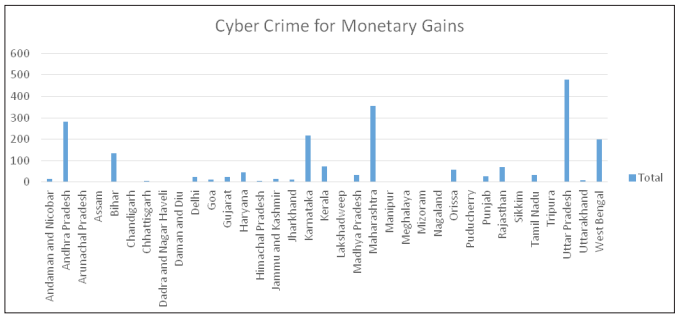


Figure 11. State-wise Analysis of Cybercrime for Monetary Gains.

4.5 Correlation between Various Types of Cyber Crimes

It is observed that the correlation between Fraud/Illegal Gain and Eve teasing/Harassment is highest (0.83) followed by Fraud/Illegal Gain and Prank/Satisfaction (0.76).

5. Conclusion

It is clear from the above study and analysis that with the advancement in technology the instances of cybercrime is also increasing. The highest number cases of cybercrimes have been registered in the state of Maharashtra, followed by Karnataka, Andhra Pradesh and Uttar Pradesh with more than 500 cases of cyber crimes. Rajasthan, Kerala, MP and Haryana have crime rate around 300 whereas Punjab, Orissa, Delhi, Chhattisgarh, Bihar and Assam have more than 100 cases of reported cyber crimes[5].

Table 1. Correlation between various types of cybercrimes

	Revenge / Settling scores	Greed/ Money	Extortion	Cause Disrepute	Prank/ Satisfaction of Gaining Control	Fraud/ Illegal Gain	Eve teasing/ Harassment	Others
Revenge/Settling scores	1.00							
Greed/Money	0.44	1.00						
Extortion	0.53	0.65	1.00					
Cause Disrepute	0.50	0.46	0.33	1.00				
Prank/Satisfaction of Gaining Control	0.41	0.49	0.63	0.65	1.00			
Fraud/Illegal Gain	0.53	0.60	0.65	0.37	0.76	1.00		
Eve teasing/Harassment	0.60	0.58	0.42	0.64	0.65	0.83	1.00	
Others	0.26	0.44	0.21	0.40	0.18	0.30	0.51	1.00

6. Recommendations

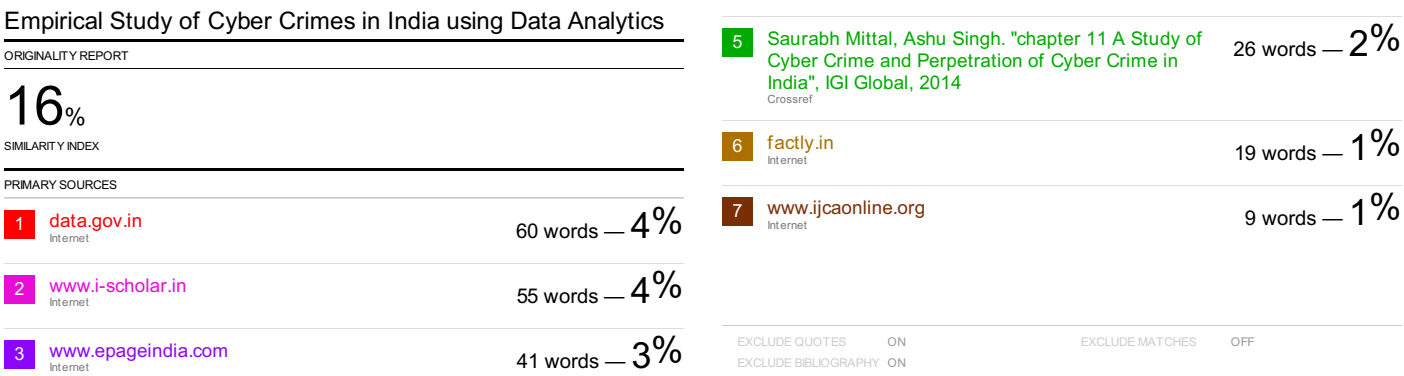
Generally, the literate class happens to commit cybercrime, hence it is essential to spread awareness among the people about implications related to this crime. The Cyber law may be revisited time to time so that it acts as deterrent to commit such crimes. Further, the law should be able to find a perfect balance between cybercrime protection and infringement of people's rights.

State level stringent monitoring of such crimes may be introduced in addition to the present infrastructure/efforts that exist with the Centre. The states like Uttar Pradesh, Andhra Pradesh, Maharashtra, Karnataka, Bihar and West Bengal account for higher crime with respect to monetary gains, corrective actions may be taken towards this area. AP, Maharashtra, Kerala and UP have high cybercrimes against women and hence need policing and corrective action[4].

7. References

1. 2012 Trends Report: Application Security Risks. Cenzic, Inc; 2012 Mar 11.
2. James RE. Business analytics: Methods, models and decisions; Pearson.
3. Fonseca J, Vieira M, Madeira H. Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on. IEEE, 2007
4. Lopez J, Oppliger R, Pernul G. Authentication and authorization infrastructures (AAIs): A comparative survey. Computers and Security. 2004; 23(7):578–90. https://doi.org/10.1016/j.cose.2004.06.013.
5. Meier JD, et al. Improving web application security: threats and countermeasures. Microsoft Corporation; 2003.
6. Teodoro N, Serrão C. Web application security: Improving critical web-based applications quality through in-depth security analysis. Society (i-Society), 2011 International Conference on. IEEE; 2011
7. Winston WL. Microsoft excel data analysis and business modelling. Prentice Hall of India.

Annexure-I



Empirical Study of Cyber Crimes in India using Data Analytics

ORIGINALITY REPORT

16%

SIMILARITY INDEX

PRIMARY SOURCES

1	data.gov.in Internet	60 words — 4%
2	www.i-scholar.in Internet	55 words — 4%
3	www.epageindia.com Internet	41 words — 3%
4	www.studymode.com Internet	32 words — 2%
5	Saurabh Mittal, Ashu Singh. "chapter 11 A Study of Cyber Crime and Perpetration of Cyber Crime in India", IGI Global, 2014 Crossref	26 words — 2%
6	factly.in Internet	19 words — 1%
7	www.ijcaonline.org Internet	9 words — 1%

EXCLUDE QUOTES ON EXCLUDE MATCHES OFF
EXCLUDE BIBLIOGRAPHY ON

Source: http://www.ithenticate.com/

Prevent Plagiarism in Publication

The Editorial Board had used the ithenticate plagiarism [http://www.ithenticate.com] tool to check the originality and further affixed the similarity index which is 16% in this case *(See Annexure-I)*. Thus the reviewers and editors are of view to discover it suitable to publish in this *Volume-10, Issue-1, January-March, 2018.*

Citation:
Disha Gupta and Namrata Agrawal
"Empirical Study of Cyber Crimes in India using Data Analytics",
Global Journal of Enterprise Information System. Volume-10, Issue-1, January-March, 2018. (http://informaticsjournals.com/index.php/gjeis)
DOI: 10.18311/gjeis/2018/19960
Conflict of Interest:
Author of a Paper had no conflict neither financially nor academically.