Research Article

A Visual Analytical Dashboard on Cyber Journalism: An Empirical Review

P SUDHANDRADEVI [a], Dr.V.BHUVANESWARI[b]

[a]Ph.D. Research Scholar, Department of Computer Applications, Bharathiar University, Coimbatore-46, TamilNadu, India.
[b]Associate Professor, Department of Computer Applications, Bharathiar University, Coimbatore-46, TamilNadu, India.
[a] psudhandradevi@gmail.com, [b]bhuvanes_v@yahoo.com

Abstract: Similar to humans, billions of stars who have made information visible and shareable surround us via digital platforms. Social media is a technology that debuted in 2000, sparking a digital revolution and transforming people's lives. Hundreds of millions of people use the internet to share their ideas, conduct bank transactions, make online purchases, and play online games. Technological innovation harms security and privacy. According to statistics, there were 27,000 crimes perpetrated in 2017, with one every ten minutes on average. A complex and multilayered cybercrime economy, like cybercrime itself, has signalled a fundamental shift. The term "web to profit" has been coined to describe cybercrime. The major aim of this work is to create an analytical dashboard that provides critical summaries of cyber vulnerability data from newspapers between 2012 and 2018. This dashboard provides significant insights into key parameters and allows users to make data-driven decisions on unstructured data. The dashboard displays a variety of insights from the cybercrime dataset, including demographic data, socioeconomic statistics, and quantitative information. The 'Rpubs' online publishing service was used to construct and publish the Cybercrime Analytical Dashboard on the web. The secondary objective of this work is to create an artificial intelligence (AI)-based chatbot that spans the cybercrime and cyber law domains specifically and what it is intended for. A chatbot represents the conversation between the user and an AI assistant. The limitation of the work is that a minimum amount of data has been collected in the dashboard, and it feeds a minimal number of intents to the machine to obtain a response from the chatbot. Future work will integrate this chatbot into the dashboard and not be restricted by crime laws.

Keywords: Artificial Intelligence, Chatbot, Cyber Crime, Cyber Journalism, Cyber Section, Flex-Dashboard, IT/IPC Act 2000, Visual Analytics.

1. Introduction

The news media has begun to devote a significant amount of coverage to the future arrival of information. The old journalistic professional culture is being challenged by the digitalization of news creation and the dissemination capabilities of the Internet. Online or cyber journalism is the next generation of internet journalism. Readers of newspapers and magazines were regularly bombarded with predictions of improved access to knowledge, education, healthcare, and entertainment as a result of the "500 channels" of information. The majority of online journalism has been webized versions of existing print and broadcast media. Because of the impact of new technology and globalization, cyber journalism has resulted in the merger of multiple traditional media, resulting in the expansion of media enterprises.Newspapers, magazines, radio stations, and television stations all over the world have created websites to provide news services and graphics in their headlines. The Indian Express, The Times of India, The Hindu, and NDTVare some of the media sites and news stations available on internet portals (DadgaranMand AzarR, 2012).

The rise of the world population in the 1990s tended to accelerate the rapid growth of digital communication and internet usage. The digital transformation revolution has increasedby number of internet users seeking information and connecting with peers and other digital entities. Although the Worldwide Web appears to be a massive phenomenon, its characteristics are startling in that they bring the world closer to its users. The two sides of cybercrime were like a technical sword, with the other end as sharp as a knife, inflicting harm on humanity. Data breaches have progressed into serious cybercrimes that endanger people in both trusted and untrustworthy environments. (Zuech et al., 2015)

Cyberspace is a limitless area of the internet that serves as a national environment for computer network communication. Cyberspace refers to the nonphysical landscape formed by electronics and electromagnetic signals manipulated through network connections and physical infrastructure. Cyberspace offends files, mail, text messages, graphics, and other modes of communication and delivery. Cybercrime refers to a group of organized crimes that target cyberspace and cybersecurity (Dashora& Patel, 2011)Click or tap here to enter text.. Cybercrime activities in India were explained by Tariq Banday M (2012). Piracy of software is a type of cybercrime that involves unauthorized access to personal or financial information. In this attack, the machine can be resolved by running a scan with the most recent anti-virus software. Cyberbullying includes unwanted communications, harassing behaviour, and sending abusive texts and emails. The majority of cyberbullying incidents take place on social media sites such as Twitter, Instagram, WhatsApp and Facebook.

Phishing is a type of cybercrime in which spam and junk emails, as well as SMS messages, are sent to individuals to obtain personal information's, passwords and debit/credit card details. Email spoofing is the practice of receiving emails from unknown sources (Gunjan V K and Kumar A, 2013). Internet fraud is committed by using internet services such as websites, forums, peer-to-peer networks, and sites that stream videos to fraud victims, which include depictions of adult sexual activity, illegal videos, and high-impact violence (Pahuja, 2018a). Online fraud is classified into three types: prize scams, unexpected money scams, and investment scams. To protect the cyber environment as well as an organization's and users' assets, follow cyber security tools, policies, safeguards, guidelines, assurance, procedures, and technology. Table 1 lists the various types of cybercrime as well as the relevant IT/IPC law sections (Kanika A, 2018; (Kapila, 2020)

Table.1. Cyber Crime: IPC/IT Acts

S. No	Cyber Crimes	Descriptions	IT/IPC Act 2000 - Sections
1.	Harassment via social media	A fake profile is created on social networking sites. This leads to harassment of the victim. (Karali et al., 2015)	**66A**:Send offensivemessages on electronic communication **67**, **67A**: sexual abuse via social media **420 IPC**: Bogus websites, Cyber Frauds **509 IPC**: Email abuse or online disparage
2.	Online Hate Community	It is made with the intention of motivating a religious group to act against a country or national figures (Sarmah et al., 2017)	**66A**:Send offensivemessagevia any electronic communication. **66F**- Cyber terrorism
3.	Email Account Hacking	Obscene emails are sent to persons in the victim's contact book once an email account is stolen. Unwitting victims would conduct online transactions on compromised machines (Pahuja, 2018)	**43**: Damages on Computer Hardware’s **66A**:Send offensive messagesvia any electronic communication **66C**: Theft of digital signature or password **67**, **67A**: sexual abuse via social media **67B**: Child phonography **499**, **500IPC**: Defamatory messages by e-mail or Email abuse **503IPC**: Threatening messages by e-mail.
4.	Credit Card Fraud	Victims are affected by while doing online transactions.(Institute of Electrical and Electronics Engineers., 2012)	**43**: Damages on Computer Hardware’s **66**: Hacking with computer system, data alteration **66D**- Cheating by characterization with the help of computer resources **420 IPC**: Bogus websites, Cyber Frauds
5.	Software Piracy	Viruses, worms, backdoors, Trojans, and bugs are malicious programmers that destroy or gain access to electronic data (UpadhyayaR and JainA,2016).	**43**: Damages on Computer Hardware’s **63**: Making copy of a computer programmer illicitly **66**: Hacking with computer system, data alteration **378**, **379IPC**: Thieving of computer hardware
6.	Email Spoofing and Phishing Scams	Receiving sensitive information by impersonating or untrusted institution. (Vijaya Kumar, 2016)	**463IPC** – Email spoofing and offences related with the Forgery **499**, **500IPC**: Defamatory messages by e-mail or Email abuse **503IPC**: Threatening messages by e-mail
7.	Online Trading Scams	Investors will be required to have a link to their online banking information Ramesh P andMaheshwari D, 2012).	**66C**- Identify theft **NDPSAct**: Online Drugs **ArmsAct**: Online sale of Arms

Table 1: The Information Technology Act of 2000 permits legal transactions to be carried out using an electronic communication device. To address the needs of cybercrime, the Indian Penal Code (IPC) will make changes to the various provisions of the IPC 1860 and the Indian Evidence Act 1872. (Government of India,

2000). A tabular view with all of the important cybercrime sections, as well as the types of illegality and offences cited, was proposed (Khanna & Khan, 2018).

The connections between data science and data crime laws have been investigated (Porcedda & Wall, 2018). BigData demonstrates how data play a role in crime and how people can help each other by discovering ethical and legal devices. The main goal is to use the data to help make sense of the BigData reality. BigData are investigated in three ways: theoretical and derives from a data source with data ethics; data crime markets based on the corpus to assist law enforcement organizations in deploying new challenges; and big data techniques to evaluate data crime, which assists investigators and assessors in locating criminals. Cybercrime has significant upstream criminal consequences as well as secondary downstream criminal consequences that span multiple jurisdictions. This effort cannot result in the omission of the information's heuristic relevance (JosephV and RayD, 2020)

Suvodeep Mazumdar talked about the challenges that corporations and governments face in regard to cyber defence. The readability of the data format is the most important issue in data analytics. In this context, the term "visual analytics" was coined to describe the process of transforming data into insights. The data in Endsley's situational awareness model are divided into three categories: perception, comprehension, and projection. Visual analytics is a technique for extracting information from complex and diverse data sets. According to the paper, visual analytics can project the 7th V of BigData. Visual analytics examines data, communicates them, interprets trends, and derives actionable insights from them. By presenting data in visual formats, data visualization connects to the data and displays patterns, trends, and statistical analysis. Flexdashboard is an HTML widget that lets create a dashboard by connecting graphical outputs, tabular data, value boxes, text annotations, HTML widgets, and static or dynamic orientations. Through static visualization, a single view of the data is provided. Dynamic visualization examines numerous insights from the same data by drilling deeper into it and extracting information (Mazumdar & Wang, 2018)

In 1955, artificial intelligence technology was introduced to allow machines to understand human conversation and, later, to "think." It can think like a human or observe real-world problems and use its intelligence to find solutions using AI. Today's AI is focused on three things: programming a computer in general language, measuring programme complexity, and learning to be self-impotent through learning. As a result, machines or computer program that use intelligence to learn to perform simple or complex tasks can be defined. Learning and reasoning on this knowledge to make decisions, problem solving, perception, and language comprehension have been the focus of AI research (AlayonD, 2018). Artificial intelligence (AI) A chatbot is a human–machine interaction that uses natural language processing. The user provides input, which is then passed through the interpreter, which converts it into a dictionary. The policy selects a response and sends it back to the user until the user decides to end the conversation (Lemaignan et al., 2017)

2. Related Methods

Many tools are available to visualize the data and analyse the impacts of cybercrime occurring worldwide. In literature review section, some kinds of cyber methods are described in BigData perspective, Visualization of Cybercrime, Spatial aspects of Cybercrime and AI-based Chatbots.

2.1 Cyber Crime: BigData Perspective

The critical reflections on Big Data security were elaborated by Matteo La Terro; the main focus of this paper is to identify the risks and challenges of data security, as well as the social-economic value of BigData. BigData's challenges include the loss of confidentiality, integrity, and availability. According to reviews, BigData mitigates these risks by improving human capital through know-how and innovations, relational capital through improved customer relations, and structural capital through changes in the management process. BigData addresses the hidden effects of redefinition in this work, focusing on technological aspects as well as sociological and ethical implications with moral judgement. (La Torre et al., 2018)

Kian Son Hon described machine learning approaches to apply BigData analytics in DDoS attacks. This paper, different types of simulations are compared in terms of performance based on the models. To handle heterogeneous data, WEKA and H2O were used. In that model, the training and test set is NSL-KDD. The model was evaluated according to the performance accuracy and optimization. That author concluded that supervised learning gives the best accuracy. Naive Bayes, gradient boosting and random forest algorithms are more suitable because of their accuracy and time consumption. The optimization algorithms gradient boosting machine and distributed random forest give more accuracy. Kian concluded that H2O is suitable for industry and more flexible than WEKA (HoonK S andYeoK C, 2018).

Cameron described the paper's main goal in terms of legal loopholes and enabling technologies in cybercrime. The author identifies systematic impediments to police investigations, actions, and digital forensics interrogation. The goal of this paper is to develop a practical approach based on extensive experience serving in police task forces, government agencies, and the private sector. The paper concludes that cyber war-gaming exercises and proactive defences against persistent adversaries are used to assess the agility and capability of the security operations centre. Brenner's assertion is revealed by the intricate mechanism(Brown, 2015).

Sung Hawn Kim explained how to protect data in the heterogeneous platform. The important element of big data security is finding the BigData key element for fetching the information, and the second element is focused on security for protecting the bigdata. They describe centralized storage as sensitive. Author outlined four BigData life cycle steps: infrastructure security, data privacy, data management, and reactive security. (KimSH, and KimNU, 2017).

2.2 Visualization of Cybercrime

Bayoumi, S(2018), focused on crime analysis and interactive visualization. In this paper, three aspects of crime have been discussed: crime against persons, property and society in the 2016 Marland State, USA. The Prime part of this work is geospatial data, which consist of 71,000 records. With the help of the tableau tool and MS Excel, visualization is progressed.Statewise crimes, crime days and kinds of insights have been provided. The extension of the study is to develop adaptive geoprimes to allow interactive geographical visualization of various data. Additionally, machine learning provides decision-makers for geographical and environmental conditions.

In Eastern European countries, crime addresses data analytics terms with criminology components to visualize crime maps. The temporal data distribution from 2012-2014 of Vilnius is distributed. The primary factors of the data are the spatial-temporal distribution of crime of violence, poverty, and distribution of drugs. For a decade, they worked on cartographic signs that are typical of 3D visualizations of the visual crime rate and juvenile crime numbers (2004-2014). This cartographic map is useful for representing urban crime at a scale of 1:1 L for the main map and 1:3 L for the complementary maps. According to the discussion, positive trends occur in mostly densely populated central areas, and violent crimes decrease to a lesser extent in the number of thefts.(Vasiliauskas&Beconytė, 2016)

The author developed a tool for cybercrime analysis with the support of a Geographical Information System (GIS) kit. This application receives inputs from various users in TamilNadu to analyse cybercrime and is plotted on a map for visualization.Google map Java Script API is used to display web pages, and Google map API supports the geo graphics features such as open layers, configuring, KML layers from Web Map Service (WMS) and Web Feature Service (WFS). Spatial data (latitude and longitude) will map every point of geo locations. The main objective of this work is to find the places that are reported as crime areas. From the analysis, a greater number of crimes occurred in the middle and north of the region. Future scope should be extended with semantic databases and queries and crime associated with geo location and visualized in a single frame(Subhashini & Milani, 2015).

2.3 Spatial Aspects of Cybercrime

Williams described the emerging criminology with BigData. The author estimates the patterns of the crime data from the social networks and associates them with the crime rate as per IPC. Day-to-day access to Twitter has increased in all parts of the world. These geolocation crime patterns are developed through the unsupervised method latent Dirichlet allocation (LDA). Classifying the tweets into predetermined tweets was implemented through the methodology “Broken Window”, which provides the criminal patterns of the textual context of social media. The hypotheses are tested for online crime data and offline crime data. The author concludes that the limitation of using social media data is the estimation of crime patterns based on geolocation (Williams et al., 2017).

Vineet Kandpal described the latest face of cybercrime and prevention in India. This paper focused on cybercrime, issues, trends and problems faced by methods to resolve the issues. Cybercrime includes cyber stalking, bot networks, transmitting virus, hacking, phishing, voice phishing, email spoofing, cybersquatting, cyber trafficking and so on. Surveys state that 57.1% of cybercrimes increased in 2012. According to the Indian Ministry of Communication and Information Technology, 78 government websites were hacked and 16035 security incidents related to scanning, span, malware, and denial of services. According to CERT-In, 78 government websites and 308371 websites were hacked during 2011-2013. Preventions to minimize cybercrime risks include updating computers, choosing strong passwords, shielding computers, social media savvy, and securing wireless networks. (Kandpal & Singh, 2013)

Tariq Banday explained the acts of cybercrime in India. Cybercrime is classified into two categories, namely, computer crimes such as hacking, viruses and traditional crimes. Computer crime is affected by unauthorized access, malicious codes, denial of service and theft. Traditional crimes are classified into obnoxious content, internet fraud and misconduct. The technological solution given in the paper is access control technologies, cryptoanalysis, monitoring, assurance tools, and the India Legal Approach, the primary goal of IPC to raise security awareness in India (MahmoodT andAfzalU, 2013).

2.4 AI Chatbots: A Helpline

Tobias Bauer discussed the recent viral trend on social media #MeToo. A chatbot is created to assist survivors of sexual harassment in Maastricht city. The purpose of this chatbot is to gather more data on harassment cases and institutes to help victims. To overcome this problem, data science and machine learning components are used to perform harassment classification, named entity recognition problems and slot-filling chatbots. They achieved more than 98% of the identification of harassment and 90% accuracy in finding spatial locations of harassment. Chatbots show great potential for further development and deployment for society as a whole (BauerT andDevrimE, 2020)

Kyoko Sugisaki described a chatbot-kit designed for web-based tools on text conversation to focus on computer-mediatedcommunication. The research study carries out real-time chat to generate structured messages with language performance data such as the speed of key-board handling, pause and mouse movements. To progress chat communication, two modes are developed: quasi-synchro and synchron modes and other typing indicators. This tool is embedded with Human-Computer Interaction and Natural Language Processing for the evaluation of chatbots (SugisakiK, 2019).

Ting-Hao K. Huang discussed with the help of chatbots that a text-based conversation is done by the user and AI assistant. Through smartphone apps such as Google Assistant or Amazon Echo, direct commands are sent to users. InstructableCrowd is created and allows users to input through conversation. In bot If -Then, rules are generated to connect all relevant sensors. The study conveys that those nonprogrammers can use this InstructableCrowd on their device to create IF-THEN rules with similar quality compared with rules created manually. Generally, it demonstrates how many users converse with their device not only triggering voice notes but also increasing the number of powerful and complicated devices (Huang et al., 2019).

In conclusion, all those studies were used to analyse visual aspects. Most of the work discussed crime and the spatial perspective. From this study, we aim to develop a dashboard to support dynamic charts and user interaction using crime geo-locations and chatbots to help the user for cyber law assistance.

3. System Development and Design

The objective of this work is to examine cybercrime instances that have been reported in e-news articles to visualize using a dashboard. In Dashboard, demographic data as well as the story of crime activity are visualized, allowing us to monitor many metrics at once and interact with different reports (Xie et al., 2021; (Chandrala& Therapeutics, 2021)**.** The secondary objective is to create an AI-based chatbot for IT/IPC Law Helpline. A text-based conversation with human and helpline for cyber laws. Figure 1 shows the methodology of visual analytics using cyber journalism data.

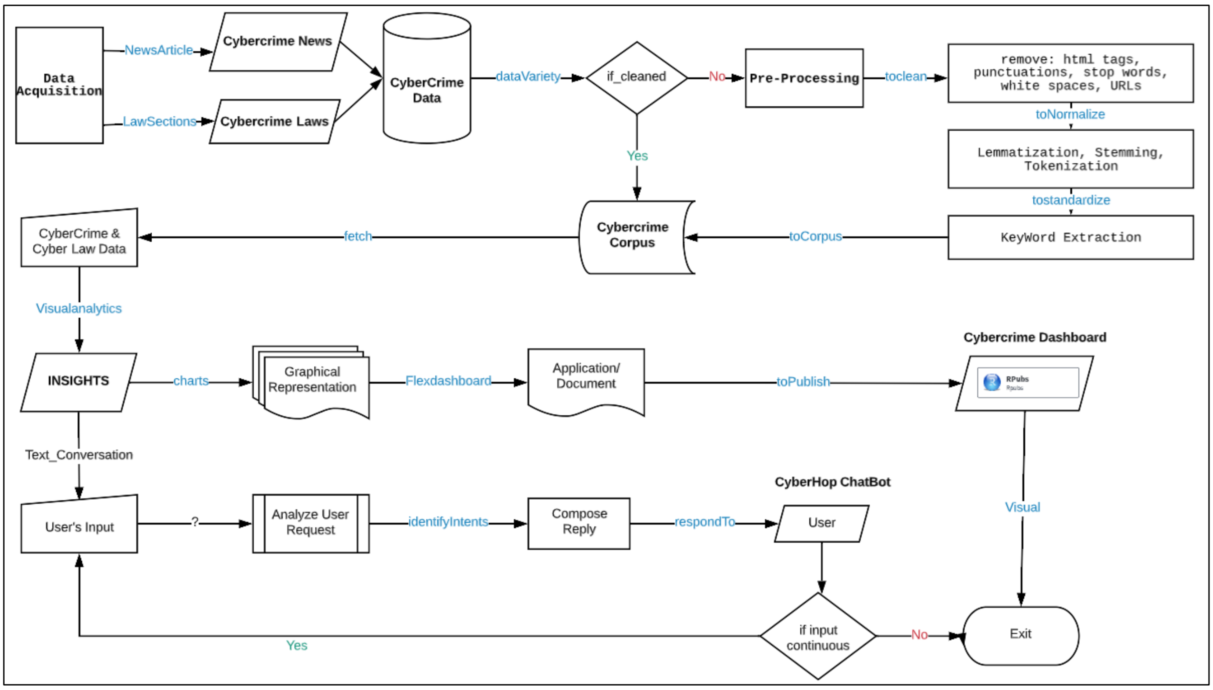


Figure 1. Visual Analytics framework for Cyber Journalism Data

3.1 Data Acquisition

The cybercrime-related data were collected from news articles from 2012 to 2018. The data consist of the crime label, article labels, geographic locations, year and content. Most of the cybercrime that occurred in the decade is phishing, email spoofing, pornography, bullying, scams, cyber stalking and web jacking. The relevant cybercrime is mapped with the IT/IPC Act 2000 using data from the government of India's Computer Emergency Readiness Team (CERT-In). As per guidelines of IT Act 2000, a cyber section with punishment is given here, **Section 43** (Computer Damage) – 3 years in prison and a fine of 5 lakhs. Section 63 (illegally making a copy of a computer programmer) – 6 months to 3 years in jail with a fine of Rs. 50,000 to Rs.1 lakh; **Section66** (Data Alteration) – three years in prison with a fine of Rs. 25,000 or both; **Section66A** (Sending offensive messages via communication services) – three years in prison with a fine; **Section66C** (Theft of one's digital signature) – three years in prison with a fine of Rs. 1 lakh; **Section 66D** (cheating by using computer resources) carries a three-year prison sentence and a one-lakh-rupee fine. **Section 66F** (Cyberterrorism) carries a life sentence. **Section 67** (Transmitting Obscene Materials in Electronic Form) carries a five-year prison sentence and a one-lakh-rupee fine; **Section 67A** (Transmitting of materials that contains sexually explicit contents) carries a one-lakh-rupee fine - 5 years in prison and a fine of Rs. 10 lakhs**. Section 67B** (Publishing of materials that depicts children in sexually explicit) - 5 years in prison and a fine of Rs. 10 lakh; **Sections 378 and 379** of the Indian Penal Code (computer hardware thievery) - Non-bailable and three years in prison with a fine, or both; **Section 420** of the Indian Penal Code (Bogus websites, Cyber Frauds) - Imprisonment for 7 years and a fine;**Section 463 IPC** (Offenses of Forgery) – Punishable for 2 years; **Section 499 IPC** (Sending defamatory messages) – Non bailable and imprisonment for 10 years and fine; **Section 500 IPC** (Email abuse) – Bailable and imprisonment for 2 years or fine or both; **Section 503 IPC** (Threatening messages by e-mail) – Bailable and imprisonment for 2 years or fine or both; **Section 509 IPC** (Online disparage) – Bailable and jail for 3 years and fine. NDPS Act (Onlin3e Drugs) – prison for year or fine of Rs. 10 thousand or both. Table 1 provides a detailed description of the law section. (Pandey A, 2017; Marg T, 2020)

3.2 Text Preprocessing

Data were collected from data sources and found to have unstructured format and noisy data. To avoid these noisy data, text preprocessing techniques are used. The first technique is to convert text into lowercases because the words ‘email’ and ‘Email’ have the same meaning, but machines will interpret different words. To avoid such cases, it should be converted into lower cases. The next technique is to remove the punctuation marks. In a sentence or paragraph, there will be a punctuation mark such as ~`! @#$%^&*()_-+={(})|\:’;”<,>?/. These punctuation marks in the sentence take more memory spaces by using regular expressions they will eliminate. Some words do not give any meaning or do not help in distinguishing between two words, which are known as stop words. Sometimes data contain some extra spaces or while performing processing techniques. More than one extra space between the words is to be removed. The next technique is stemming, which will reduce the prefix or suffix from words such as “ing, ed, s”. It directs the word to its root to avoid unwanted and repeated meaningful words; for example, the root word of ‘mapping’, ‘mapped’, is ‘map’. While stemming, we face some issues because of eliminating prefix or suffix letters. To have the systematic meaning lemma is used, it grabs the words from the language dictionary to match the stemmed word. The news content will be sentences or paragraphs. Sentences are a group of composed words. Tokenization is a technique that breaks the sentence or paragraph into words. Now, the text can be mined for extract feature analysis and for analytics (Anandarajan et al., 2019).

3.3Cybercrime Corpus

The cybercrime corpus is carried out using the MapReduce approach to measure the crime terminology in a news article with crime labels of IT/IPC sections. The pseudo code for the MapReduce task is given below (Philip Chen & Zhang, 2014); (Santhiya& Bhuvaneswari, 2018).

```
   Input
   Map function ()                      //map function
        {var key1=id, key2=id;
   var value1=p1, vaue2=p2;
   emit (key, value)}
   Reduce function (key, value)   //reduce function
   {commentfields= {}, id=’’;
   valueforeach (value {
    if (key in value) {
        result. collection2= ();}
        result. collection2.push (result. collection2, value.key2)}
   for (field in value)
        if (value (field) &&! (Field in commentfields)) {
       result(field)=value(field)}
           return (result)}
   //MapReduce
   db. collection. mapReduce (map function, reduce function)
   {out: collection;//Output
   query: document;//Query
   limit: number;//Limitation}
Output Result
```

Based on the MapReduce approach, a corpus has been built to categorize cybercrime terms with suitable Law sections. Mapping is performed on the top layer based on demographic categorization to link the four labels, which are listed below, (Zhang et al., 2018).

- Mapping of IPC Crime Label (IPCV CL) with Cyber Article Label (CAL).
- Mapping of Cyber Article Label (CAL) with IT/IPC Section (IPC_S).
- Mapping of IT/IPC Section (IPC_S) with IT/IPC Law (IPC_Law)
- Mapping of Cyber Article Label (CAL) with Crime Location (C_Loc)

3.4Cybercrime Analytical Dashboard

This work's primary goal is to create a dashboard that interacts with human inputs for better understanding. A dynamic and customized dashboard is built using RStudio. The layout is resized to a browser and adopted for mobile applications. The default dashboard is a standard HTML document and deployed on the web server using Rpubs. (ThompsonJ, 2018; RimalY, 2020)

Step 1: Data Preparation

Once the data are ready, they are put into the dashboard component. Based on the keyword search, anyone can retrieve the required data from the dashboard, and it will be presented over the screen. Making the file user-friendly, it can be downloaded in CSV or PDF file format or copied the selected content, and the printing option is also available.

Step 2: Built Static Dashboard

This dashboard component consists of HTML Widgets: interactive JavaScript; Graphs: a graphical representation; Tabular data: to sort, filter and download the data; Value boxes to highlight the important summary value; Gauges to specify the values on meter and story board to text annotations. A number of graphical representations will be discussed in the Results and Discussion sections.

Step 3: Making Static Dashboard into Dynamic Dashboard

The dashboard will be dynamic until the data changes. To create a dynamic dashboard, data should continue to change. So that it will be reflected in the dashboard unless developer reknit the document. After a refreshing document,the user can see the dynamics in the dashboard.

Step 4: Publishing the dashboard

Once all the components have been added, graphical parts are used to publish the dashboard. To publish the dashboard, either we go for commercial or free of cost. Here, 'Rpubs' is free of cost and sharing the document on the web. Cybercrime Analytical Dashboard is published and additionally linked with social media apps such as "Twitter", "Facebook", "Google +", "LinkedIn" and "Pinterest". (HeissA, 2020; MoragaP, 2019)

3.5CyberHop Chatbot

A chatbot is a computer program that conducts textual conversations or audio notes between computers and humans. These self-learning chatbots use machine learning and artificial intelligence techniques to obtain human input and respond appropriately. This chatbot helps users know about cybercrime law and punishments according to the Act IT/IPC 2000. Figure 2 shows the methodology of bot using crime law section and punishments.

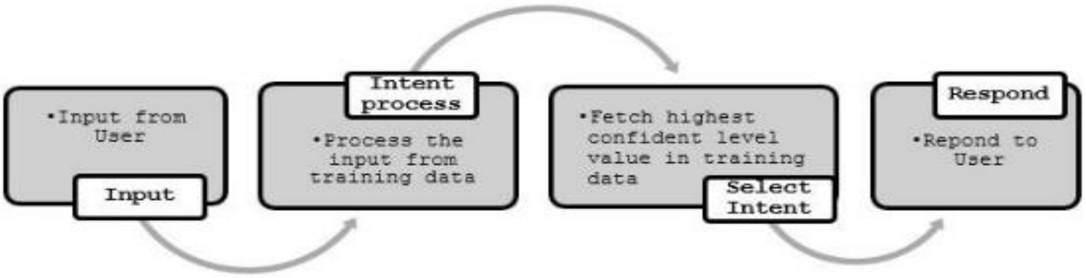

•Input from User
Input
Intent process
•Process the input from training data
•Fetch highest confident level value in training data
Select Intent
Respond
•Repond to User

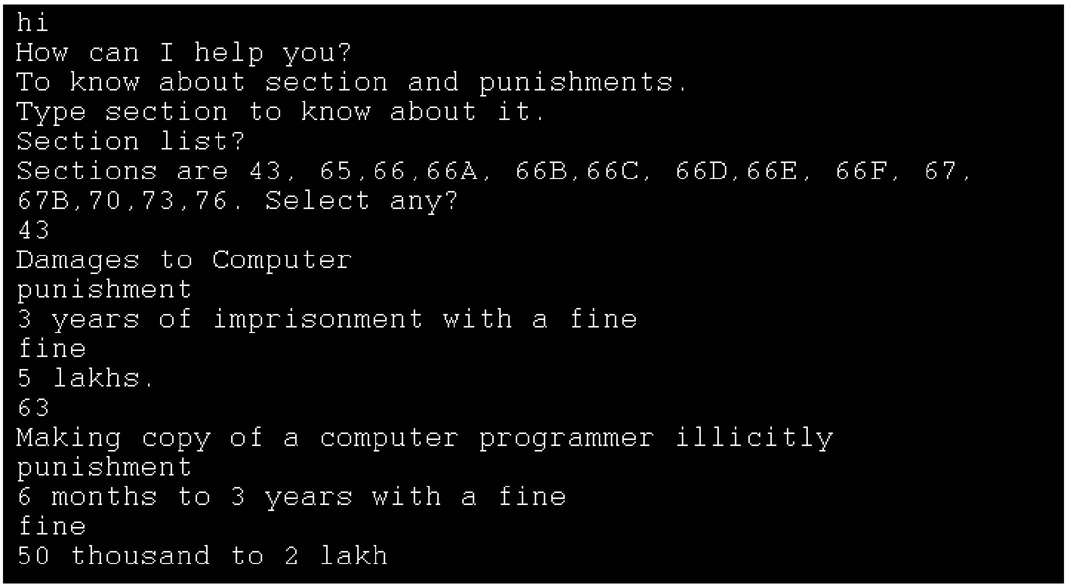
Figure 2. Working Methodology of Chatbot

Step 1: CyberHop Framework

CyberHop is designed using a flask framework, and data have been trained and integrated with web applications. To run web application, create a directory. Here, training data.CSS style sheet, template and SQLITE engine file will be part of this directory.

Step 2: Training Data

The data required for the chatbot cybercrime section and punishment data. The crime law mentioned in Section 3.1 (Data Acquisition) is given as training data. Additionally, cybercrime-related keywords were added. With these data, the machine will train its own customized neural network and try to select a random response from the training data. Every intelligent machine needs data to interpret and respond. The input from the user may be irrelevant or not trained. At the time, the bot will answer randomly and not accurately. The sample of training data is given in Figure 3. (Zhou et al., 2019); Panchkula Police(Ed.), 2018).



```
hi
How can I help you?
To know about section and punishments.
Type section to know about it.
Section list?
Sections are 43, 65,66,66A, 66B,66C, 66D,66E, 66F, 67,
67B,70,73,76. Select any?
43
Damages to Computer
punishment
3 years of imprisonment with a fine
fine
5 lakhs.
63
Making copy of a computer programmer illicitly
punishment
6 months to 3 years with a fine
fine
50 thousand to 2 lakh
```

Figure 3. Sample of Training Data (image source: author)

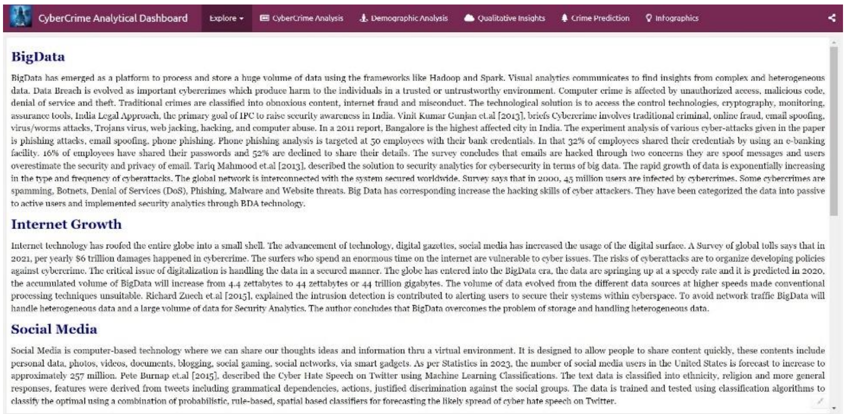
Step 3: Chatbot Process

The created chatbot is named ‘CyberHop’. This chatbot understands the crime semantics as they trained with the data in an earlier process, have a predefined flow and make sure that they solve the user requests regarding cybercrime and law perspectives. When the user gives their input, it is passed to the interpreter and responds to a random user request at any point of view. The problem while conversing is that the user’s input has different patterns, spellings, short forms, complex punctuations and local slangs (such as Thanglish). However, the process of training AI chatbots is similar to training a child to learn new language from scratch. Natural language processing (NLP) techniques help to create the best technology and machines that are more understandable to these language differences and nuances. In these two NLP techniques, that is, natural language understanding (NLU), which understands human languages and, for machine understanding, converts text into a structured format, and natural language generation (NLG), which reverses the process of NLU for human understandability. If the user gives input as ‘63’, the machine understands that 63 denotes the law section and responds to that act (Government of India,2000; AnjumS,2018).

4. Results and Discussion

The dashboard allows users to select aesthetics such as dynamic data visualizations and respond to results quickly. All Flexdashboard Components were used to develop this Cybercrime Analytical Dashboard. The dashboard is composed of the following insights.

- Cybercrime Analysis
- Demographic Analysis
- Qualitative Insights
- Infographics



BigData

BigData has emerged as a platform to process and store a huge volume of data using the frameworks like Hadoop and Spark. Visual analytics communicates to find insights from complex and heterogeneous data. Data Breach is evolved as important cybercrimes which produce harm to the individuals in a trusted or untrustworthy environment. Computer crime is affected by unauthorized access, malicious code, denial of service and theft. Traditional crimes are classified into obnoxious content, internet fraud and misconduct. The technological solution is to access the control technologies, cryptography, monitoring, assurance tools, India Legal Approach, the primary goal of IPC to raise security awareness in India. Vinit Kumar Gunjan et.al [2013], briefs Cybercrime involves traditional criminal, online fraud, email spoofing, virus/worms attacks, Trojans virus, web jacking, hacking, and computer abuse. In a 2011 report, Bangalore is the highest affected city in India. The experiment analysis of various cyber-attacks given in the paper is phishing attacks, email spoofing, phone phishing. Phone phishing analysis is targeted at 50 employees with their bank credentials. In that 32% of employees shared their credentials by using an e-banking facility. 16% of employees have shared their passwords and 52% are declined to share their details. The survey concludes that emails are hacked through two concerns they are spoof messages and users overestimate the security and privacy of email. Tariq Mahmood et.al [2013], described the solution to security analytics for cybersecurity in terms of big data. The rapid growth of data is exponentially increasing in the type and frequency of cyberattacks. The global network is interconnected with the system secured worldwide. Survey says that in 2000, 45 million users are infected by cybercrimes. Some cybercrimes are spamming, Botnets, Denial of Services (DoS), Phishing, Malware and Website threats. Big Data has corresponding increase the hacking skills of cyber attackers. They have been categorized the data into passive to active users and implemented security analytics through BDA technology.

Internet Growth

Internet technology has roofed the entire globe into a small shell. The advancement of technology, digital gazettes, social media has increased the usage of the digital surface. A Survey of global tolls says that in 2021, per yearly $6 trillion damages happened in cybercrime. The surfers who spend an enormous time on the internet are vulnerable to cyber issues. The risks of cyberattacks are to organize developing policies against cybercrime. The critical issue of digitalization is handling the data in a secured manner. The globe has entered into the BigData era, the data are springing up at a speedy rate and it is predicted in 2020, the accumulated volume of BigData will increase from 4.4 zettabytes to 44 zettabytes or 44 trillion gigabytes. The volume of data evolved from the different data sources at higher speeds made conventional processing techniques unsuitable. Richard Zuech et.al [2015], explained the intrusion detection is contributed to alerting users to secure their systems within cyberspace. To avoid network traffic BigData will handle heterogeneous data and a large volume of data for Security Analytics. The author concludes that BigData overcomes the problem of storage and handling heterogeneous data.

Social Media

Social Media is computer-based technology where we can share our thoughts ideas and information thru a virtual environment. It is designed to allow people to share content quickly, these contents include personal data, photos, videos, documents, blogging, social gaming, social networks, via smart gadgets. As per Statistics in 2023, the number of social media users in the United States is forecast to increase to approximately 257 million. Pete Burnap et.al [2015], described the Cyber Hate Speech on Twitter using Machine Learning Classifications. The text data is classified into ethnicity, religion and more general responses, features were derived from tweets including grammatical dependencies, actions, justified discrimination against the social groups. The data is trained and tested using classification algorithms to classify the optimal using a combination of probabilistic, rule-based, spatial based classifiers for forecasting the likely spread of cyber hate speech on Twitter.

Figure 4. Home Page: Cybercrime Analytical Dashboard

Figure 4 depicts the project and dataset details on the home page. On the dataset page, a description of the dataset is provided, and the dataset can be downloaded in a variety of formats, including CSV and PDF. The data table can also be searched using keywords or other parameters. It has different cybercrime images in the navigator part, as well as links to social media apps, including Facebook, Twitter, LinkedIn, GooglePlus, and Pinterest. The dashboard name, author name, and comments on dashboards are listed in the Toolbar dashboard, and the dashboard link has been shared on Twitter, Facebook, and GooglePlus.

4.1 Cybercrime Analysis

Domain Perspective on Cybercrime: The domain-specific vulnerability described in the news story is depicted in Figure 5. Cybercrime operations in India were classified in terms of cyber journalism from 2012 to 2018. According to the graph, email spoofing has been the most vulnerable crime in the United States for the previous seven years. In regard to monetary demand, mail appears to come from one source even though it was sent to another. By hacking their accounts to acquire personal information or by using cybercrime as a weapon and raising against their voices, attackers might use Twitter and Facebook as a weapon. Viruses that are similar to ransomware and data wiping viruses will alter the software and reroute links to undesirable websites.

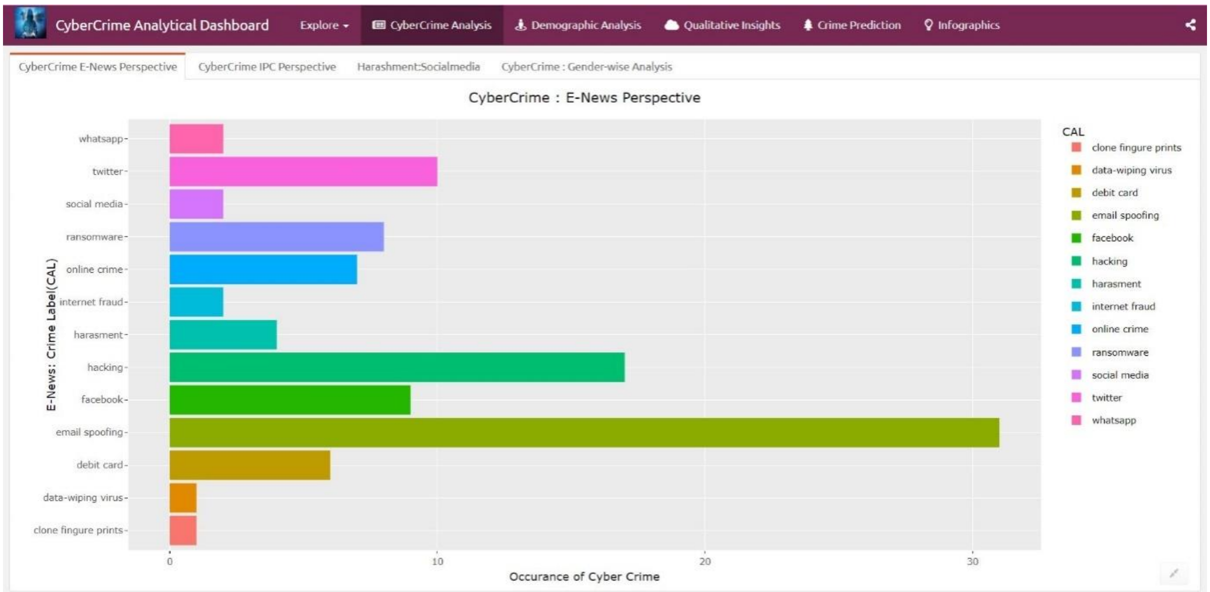


Figure 5. Cybercrime Domain Perspective (E-NEWS Article)

Crime Law Perspective on Cybercrime: Phishing sent spam, junk emails, or SMS messages to recipients without their consent, including personal details. The wrongdoing of Hacking and spoofing is becoming more common as people become more informed of how to use email. The majority of the victims are targeted via email employing brute-force attacks, which result in hacking and email spoofing for financial gain. According to the paper, exchanging debit card information has an impact on sectors such as banking, smuggling, shops, and government agencies. Cyberbullying is the second most common crime in India, with perpetrators using digital newspapers and social media to target society for their own gain. Individuals or groups of online jackers will target well-known websites, knowing that they will gain attention or be able to afford an opulent lifestyle. As per IPC aspects, the most prevalent cybercrime is given in Figure 6.

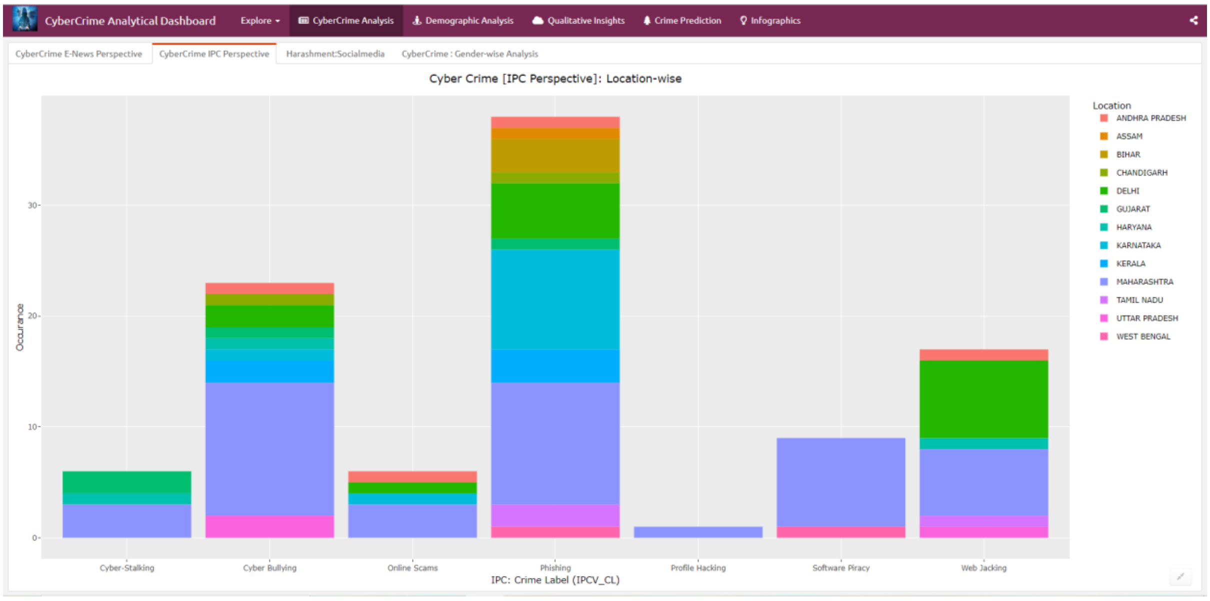


Figure 6. Analysis of Cyber Crime in India (IPC Perspective: Locationwise)

Cyber Vulnerable Crime in India (Gender-based): Figure 7 depicts a gender-based examination of cybercrime. According to the findings, phishing has been the most vulnerable crime in India for the previous seven years, and men are particularly vulnerable. Men appear to be particularly prone to phishing and cyber bullying assaults, according to the majority of crimes reported. Women are more vulnerable to cybercrime. Hackers might use the footprints left by social media sites to track down their intended victims.

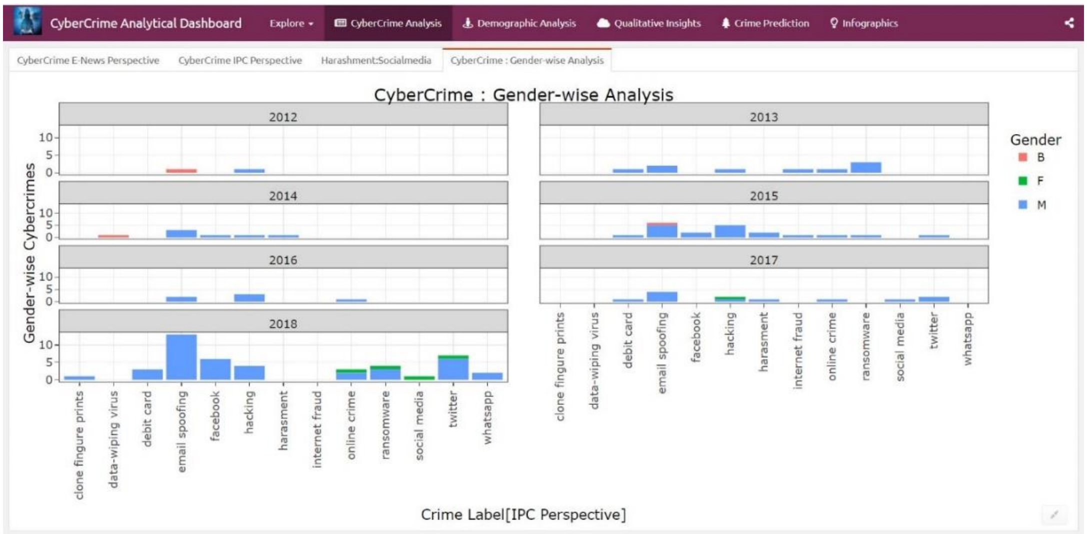


Figure 7. Gender wise Analysis of Cyber Crime in India

4.2 Demographic Analysis

State-by-State Crime Prediction in India (2012-2018): In India, state-by-state cyber activities are examined. According to data collected between 2012 and 2018, Maharashtra has the highest number of documented offences. Maharashtra's population is predicted to be 12.24 crores, and there is a risk of crime as a result. When compared to Maharashtra, Uttar Pradesh had a higher population of approximately 19.91 million people but a lower rate of crime. The reason for this is that Maharashtra's literacy rate is approximately 82.34 percent, which means that people are wellversed in utilizing gazettes and are technologically savvy. Because the literacy rate in Uttar Pradesh is 67.68 percent, many people are unaware of technology and smart gazettes. Delhi and Karnataka are India's second and third most crime-prone states, respectively. Assam was the state with the fewest crimes. Figure 8 depicts cybercrime in India by state.

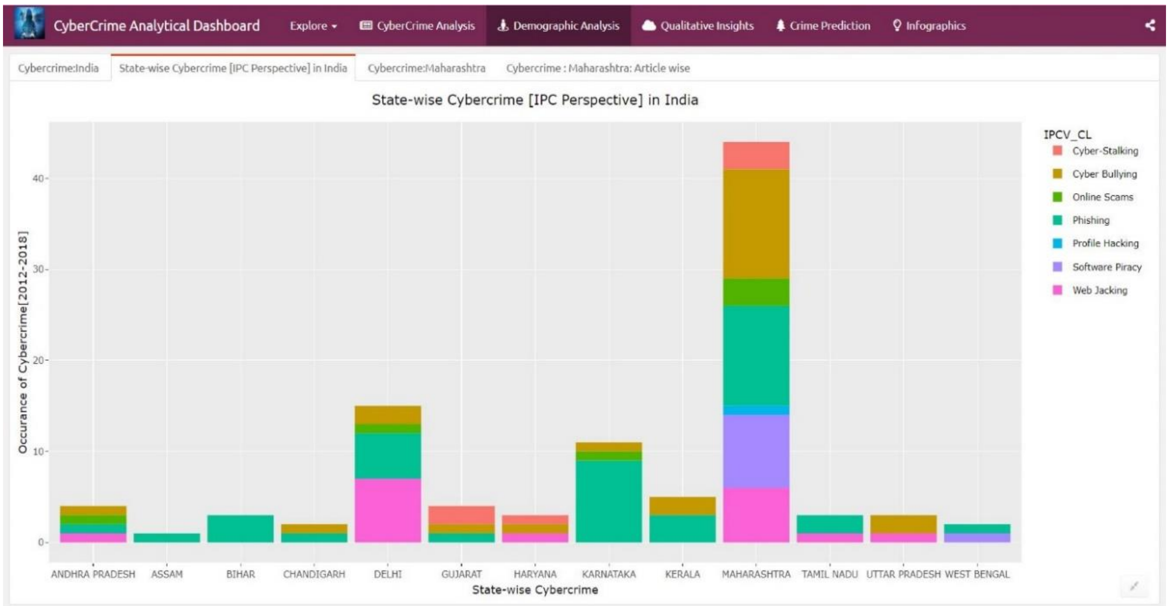


Figure 8. Visual Analytics of Statewise Crime Prediction in India (2012-2018)

Crimecrime in Maharashtra (Articlewise): The scenario behind the greater number of offences in Maharashtra is the population and literacy rate. The number of instances has been steadily growing in recent years. In comparison to the previous year, social networking applications are becoming increasingly popular among consumers, posing a threat to hackers. When a user is subjected to cyberbullying, they are subjected to harassment, hate speech, rumours, sexual remarks, and threats. All these threats make the user feel unsafe. Criminals will engage with victims through chat rooms or email inboxes and sexually assault them. Cyberbullying, phishing, and software piracy have all increased in frequency in recent years (2015-2018). Figure 9 shows how sophisticated criminals exploit weaknesses in computers or other devices using Facebook and Twitter as important venues for crime occurrence and ransomware.

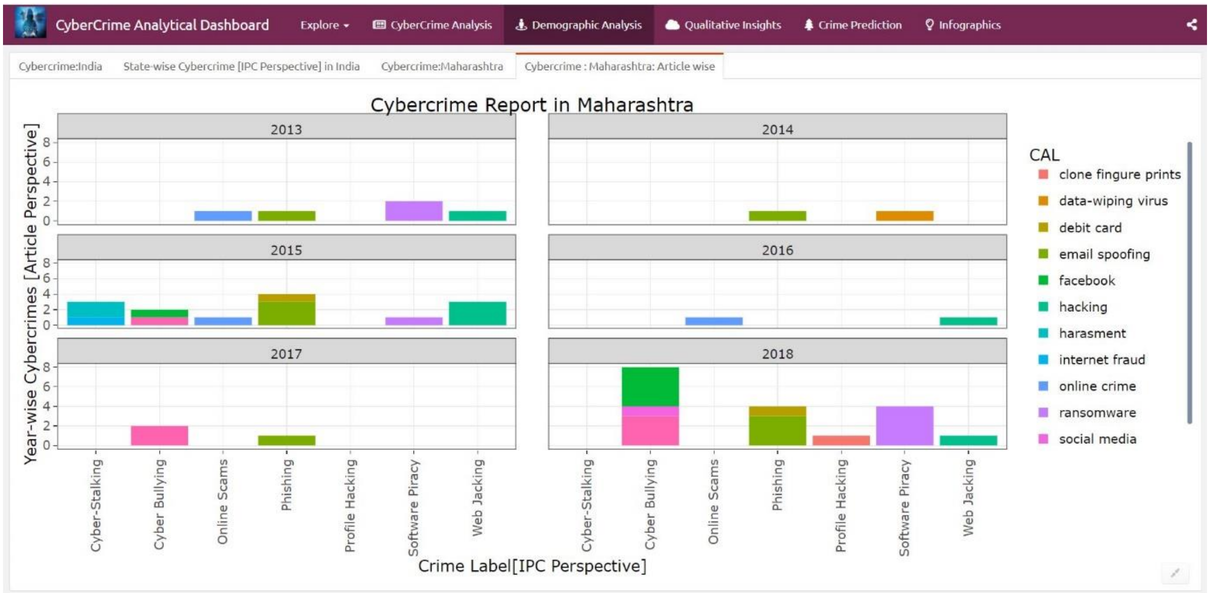


Figure 9. Cybercrime in Maharashtra (Article wise)

4.3 Qualitative Insights

Comparison of Crime Classes: The crime data were divided into binary labels such as “Techno Centric” and “People Centric.” Techno Centric news includes Cyber Bullying, Phishing, Software Piracy, and Web Jacking, while People Centric news includes Cyber-Stalking, Online Scams, and Profile Hacking. Figure 10 shows a document-by-document comparison based on binary labels.

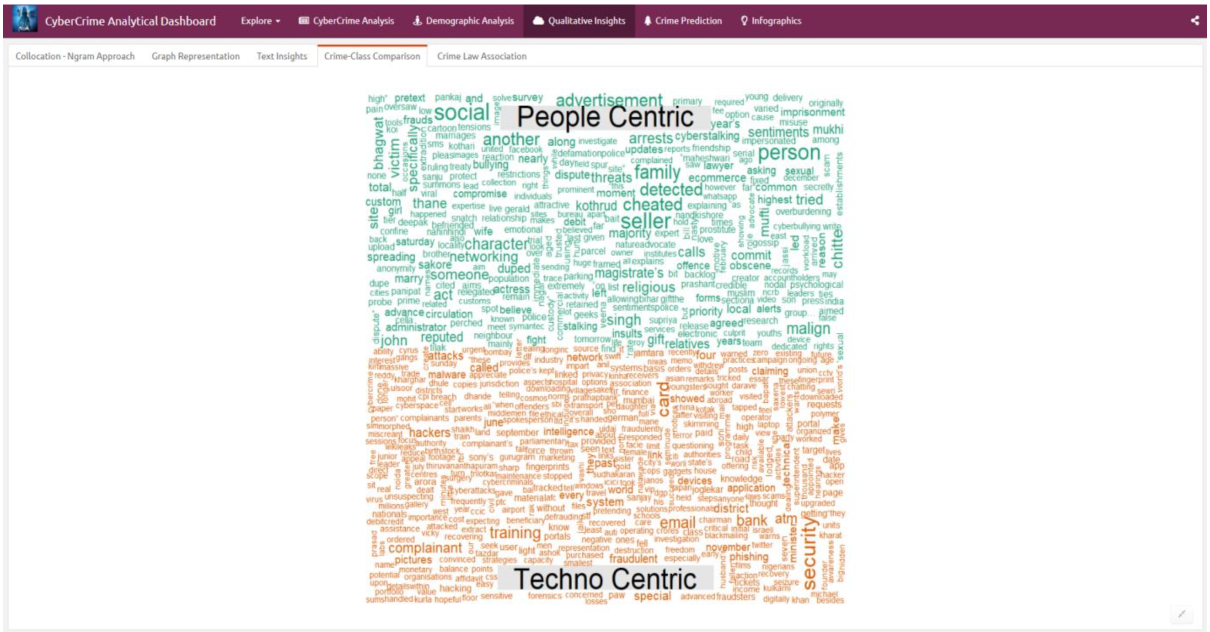


Figure 10. Crime-Class Comparison: Binary Labels

Crime Law Association (IPC Section and Punishments): According to the Indian government, the term “cybercrime” is related to the IPC and IT Act of 2000. Figure 11 depicts the IPC sections and punishments, with cyber bullying falling under Section 67, which carries a five-year jail and a fine of up to ten lakhs. Phishing is a crime that falls under Section 70 and carries a ten-year prison sentence as well as a fine.

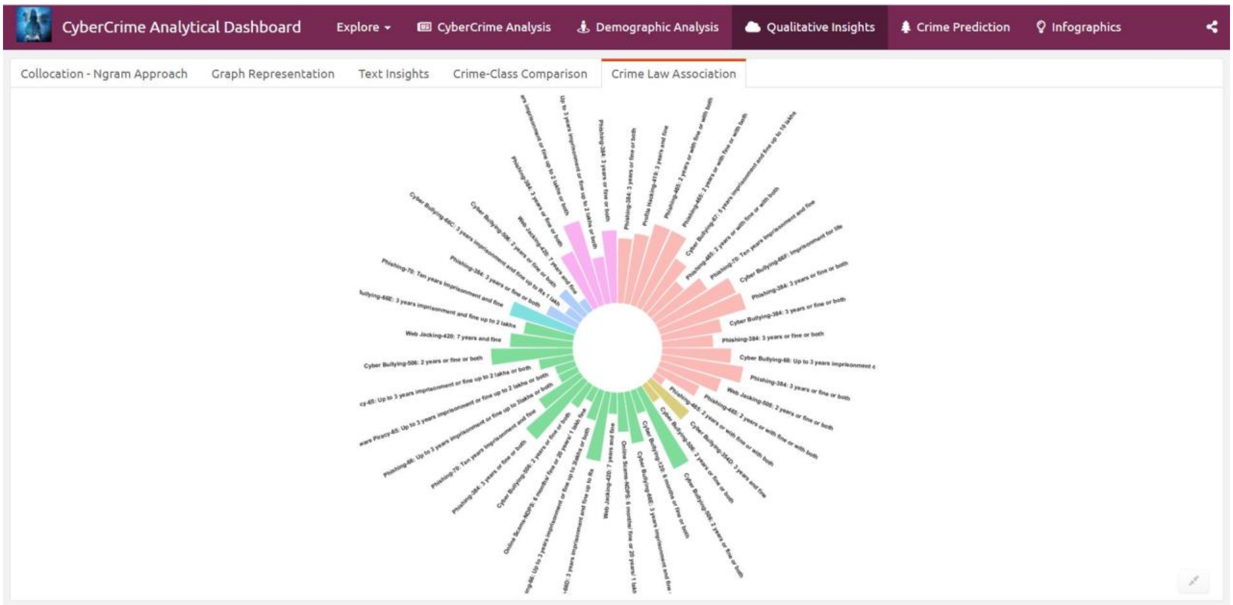
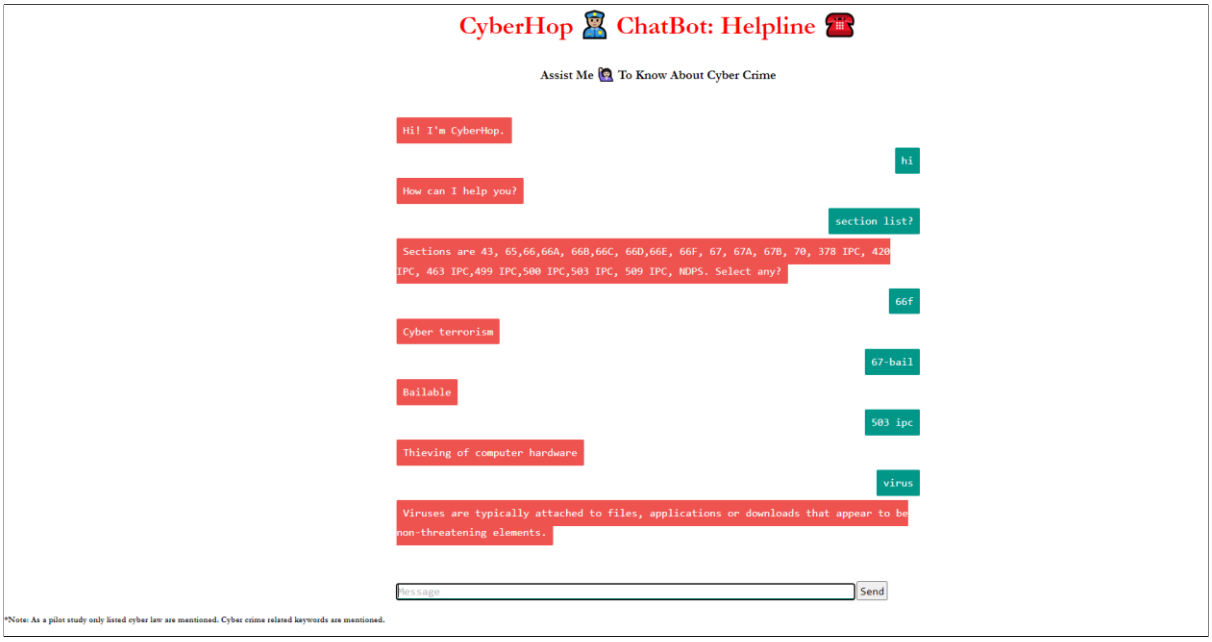

CyberCrime Analytical Dashboard
Explore
CyberCrime Analysis
Demographic Analysis
Qualitative Insights
Crime Prediction
Infographics
Collocation - Ngram Approach
Graph Representation
Text Insights
Crime-Class Comparison
Crime Law Association
Phishing-384: 3 years or fine or both
Phishing-384: 3 years or fine or both
Profile Hacking-419: 3 years and fine
Phishing-465: 2 years or with fine or with both
Phishing-465: 2 years or with fine or with both
Cyber Bullying-67: 5 years imprisonment and fine up to 10 lakhs
Phishing-465: 2 years or with fine or with both
Phishing-70: Ten years imprisonment and fine
Cyber Bullying-66F: Imprisonment for life
Phishing-384: 3 years or fine or both
Cyber Bullying-384: 3 years or fine or both
Phishing-384: 3 years or fine or both
Cyber Bullying-66: Up to 3 years imprisonment c
Phishing-384: 3 years or fine or both
Web Jacking-506: 2 years or fine or both
Phishing-465: 2 years or with fine or with both
Phishing-465: 2 years or with fine or with both
Cyber Bullying-354D: 3 years and fine
Cyber Bullying-506: 2 years or fine or both
Cyber Bullying-506: 2 years or fine or both
Cyber Bullying-120: 6 months or fine or both
Cyber Bullying-66E: 3 years imprisonment and fine
Online Scams-NDPS: 6 months/ fine or 20 years/ 1 lakh
Web Jacking-420: 7 years and fine
-66D: 3 years imprisonment and fine up to Rs
ng-66: Up to 3 years imprisonment or fine up to 3lakhs or both
Online Scams-NDPS: 6 months/ fine or 20 years/ 1 lakh fine
Cyber Bullying-506: 2 years or fine or both
Phishing-384: 3 years or fine or both
Phishing-70: Ten years imprisonment and fine
Phishing-66: Up to 3 years imprisonment or fine up to 3lakhs or both
ware Piracy-65: Up to 3 years imprisonment or fine up to 2 lakhs or both
cy-65: Up to 3 years imprisonment or fine up to 2 lakhs or both
Cyber Bullying-506: 2 years or fine or both
Web Jacking-420: 7 years and fine
Bullying-66E: 3 years imprisonment and fine up to 2 lakhs
Phishing-70: Ten years imprisonment and fine
Phishing-384: 3 years or fine or both
Cyber Bullying-66C: 3 years imprisonment and fine up to Rs 1 lakh
Cyber Bullying-506: 2 years or fine or both
Web Jacking-420: 7 years and fine
Phishing-384: 3 years or fine or both
ars imprisonment or fine up to 2 lakhs or both
Up to 3 years imprisonment or fine up to 2 lakhs or both

Figure 11. Cyber Law Association (IPC Section and Punishments)

4.4 CyberHop ChatBot – A Helpline

In this section,the chatbot is designed and named "CyberHop" to help users become aware of cybercrime law and punishments. These data are trained based on IT/IPC Act 2000 to generate many responses. While chating, it gets the input from the users and delivers appropriate answers. Machine learning algorithms learn from the input and improve its performance. This is possible when the user gives the input the bot saves the inputs with its responses for future study. It makes the bot self-learn from the data to generate automated responses each time while getting inputs from the user. Based on the best-fit bot, select the most relevant response. By giving an increasing number of inputs, the accuracy of the responses will be accurate.



CyberHop 👮 ChatBot: Helpline ☎

Assist Me 🙋 To Know About Cyber Crime

Hi! I'm CyberHop.

hi

How can I help you?

section list?

Sections are 43, 65,66,66A, 66B,66C, 66D,66E, 66F, 67, 67A, 67B, 70, 378 IPC, 420 IPC, 463 IPC,499 IPC,500 IPC,503 IPC, 509 IPC, NDPS. Select any?

66f

Cyber terrorism

67-bail

Bailable

503 ipc

Thieving of computer hardware

virus

Viruses are typically attached to files, applications or downloads that appear to be non-threatening elements.

*Note: As a pilot study only listed cyber law are mentioned. Cyber crime related keywords are mentioned.

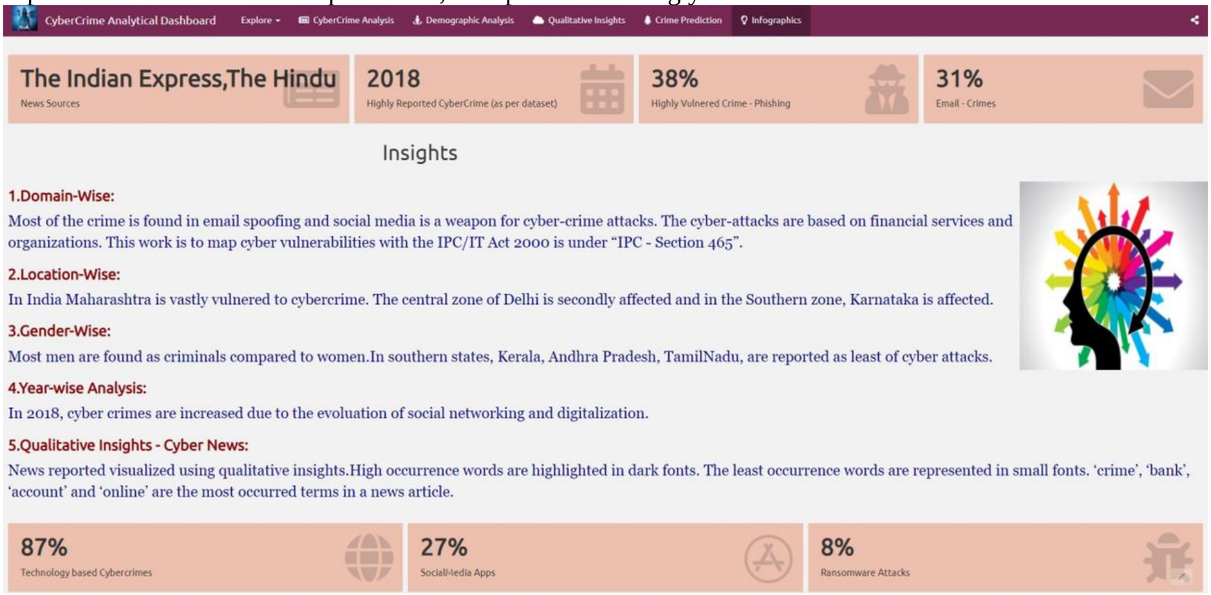
Figure 12. Outcome of CyberHop – Chatbo

TheNatural Language ToolKit is implemented in Chatbot using the Natural Language Processing application. The bot is created to assess cyber crime law and cyber crime-related information. Based on the user input, it responds randomly. The intent should be trained with all possibilities. Therefore, it responds to the user with expected outcomes. For one intent, there may be one or more patters or tags. Figure 13 shows the conversation between the user and AI assistant. This CyberHop chatbot gives replies for all related cyber crime terms with short definitions. Figure 12 gives the definition for law section '66F', cyber term 'virus' and punishment details for the '503 IPC' section.

5. Insights

In this paper, an empirical examination of cybercrime reported in news items is conducted. The following are present in a multilayer framework that is proposed. According to an overall review, the use of mobile and smartphones is growing cybercrime. Technology is responsible for 87 percent of all crimes. The majority of the crimes are classified as “Phishing,” followed by “Cyber Bullying,” “Profile Hacking” and “Online Scams.” Men are said to be more vulnerable than women. It has sparked a lot of interest in Maharashtra and New Delhi. Southern states with the lowest reported incidences include Andhra Pradesh, Tamil Nadu, and Kerala. Figure 13 shows the infographic specifics of this investigation.

Because social media applications account for 27% of all crimes, awareness of the secure usage of sources such as email, social media, and the internet must be established. Due to a lack of understanding of what constitutes cybercrime, it was discovered that crimes committed on social media are not recorded. It is necessary to raise public awareness about cyber law so that laymen will be aware of the many types of cybercrime and the penalties associated with them. As a result, the following cybercrimes term discussion and trained with chatbots to help the user. Based on user requirements, it responds accordingly.



The Indian Express,The Hindu
News Sources

2018
Highly Reported CyberCrime (as per dataset)

38%
Highly Vulnered Crime - Phishing

31%
Email - Crimes

Insights

1.Domain-Wise:

Most of the crime is found in email spoofing and social media is a weapon for cyber-crime attacks. The cyber-attacks are based on financial services and organizations. This work is to map cyber vulnerabilities with the IPC/IT Act 2000 is under “IPC - Section 465”.

2.Location-Wise:

In India Maharashtra is vastly vulnered to cybercrime. The central zone of Delhi is secondly affected and in the Southern zone, Karnataka is affected.

3.Gender-Wise:

Most men are found as criminals compared to women.In southern states, Kerala, Andhra Pradesh, TamilNadu, are reported as least of cyber attacks.

4.Year-wise Analysis:

In 2018, cyber crimes are increased due to the evolution of social networking and digitalization.

5.Qualitative Insights - Cyber News:

News reported visualized using qualitative insights.High occurrence words are highlighted in dark fonts. The least occurrence words are represented in small fonts. ‘crime’, ‘bank’, ‘account’ and ‘online’ are the most occurred terms in a news article.

87%
Technology based Cybercrimes

27%
SocialMedia Apps

8%
Ransomware Attacks

Figure 13. Infographics of Cybercrime Analysis

6. Recommendation

- When people receive emails from selected lottery prize awards, they are unaware that they are being targeted as vulnerabilities.
- Unawareness refers to the inability to recognize that the email sources are spoofing or email-spoofing certain unknown users with the same name.
- Hacking is a widespread crime in which people leave digital trails without sufficient singing mechanisms, resulting in a hack.
- Data breaches are frequently reported in social media chats due to a lack of understanding about disclosing private information and insecure sources.
- Ignorance of the causes of cybercrime has resulted in an upsurge in cybercrime.

7. Conclusion

In this research, a multi-layered approach is used to extract cyber vulnerabilities stated in news items for analysis and study. According to data research, more financial-related crimes are reported. Men’s crime is not publicised, although it is increasing at an alarming rate. It is necessary to raise awareness about the dangers of accessing online as well as the penalties and rules governing cyberspace under the IPC IT Act 2000. It is recommended that users be educated on the following topics: i) cybercrime vulnerability causes, (ii) cybercrime penalties and punishments, (iii) cybercrime IPC acts, and (iv) Do’s and Don’ts in digital space to avoid becoming victims of cybercrime. People should be made aware of the significance of secure access to online sites and media in order to preserve human life. In the future, automatic crawlers will be associated with dashboards to crawl cyber news to visualize insights. These insights will be emphasis with human emotions. Looking forward that to contribute on relationship between emotions and crime victims to detect consequences of emotions of the victim.

References

Dadgaran, M., &Azar, R.(2012).An inquiry into challenges of cyber journalism.Culture of Communication, 2(7), 69–89.
Zuech, R., Khoshgoftaar, T. M., &Wald, R.(2015).Intrusion detection and bigheterogeneousdata: Asurvey. Journal of Big Data, 2(1). https://doi.org/10.1186/s40537-015-0013-4
Dashora, K.(2011).Cyber crime in the society: Problems and preventions.Journal of Alternative Perspectives in the Social Sciences, 3(1), 240–259.
Tariq Banday, M., &Mir, F. A.(2012).A study of Indian approachtowardscybersecurity, International Conference on Emerging Technology Trends in Electronics, Communication and Networking. https://doi.org/10.1109/ET2ECN.2012.6470114
Gunjan, V. K., &Kumar, A.(2013).A survey of cybercrime in India15th International Conference on Advanced Computing Technologies (ICACT), 1–6. IEEE Publications.
Pahuja, R.(2018).Impact of socialnetworking on cybercrimes: Astudy.Epitome: International Journal of Multidisciplinary Research, 4(4), 09–14.
Kanika, A.(2018).'An Improved Security Threat Model for Big Data Life Cycle',Asianjournal of computer science and technology.Research Publications, 7(1), 33–39.
Kapila, P., "Cyber Crimes and Cyber Laws in India: An Overview", Contemporary Issues and Challenges in the Society.(2020)Edition, New Era International Imprint, 2020, 36–48.
Karali, Y., &Panda, S.(2015).Cyber crime: Ananalyticalstudy of cybercrimecases at the mostvulnerable states and cities in India.International Journal of Engineering and Management Research,5(2), 43–48.
Sarmah, A., &Sarmah, R.(2017).A briefstudy on cybercrime and cyberlaws of India.International Research Journal of Engineering and Technology (IRJET), 4(6), 1633–1641.
Upadhyaya, R., &Jain, A.(2016).Cyber ethics and cybercrime: AdeepDwelvedstudy into legality, Ransomware, undergroundweb and Bitcoin walletInternational Conference on Computing, Communication and Automation (ICCCA), 143–148, 2016. https://doi.org/10.1109/CCAA.2016.7813706
Vijaya Kumar, P. N.(2016).Growing cybercrimes in India: AsurveyInternational Conference on Data Mining and Advanced Computing, 2016,246–251, https://doi.org/10.1109/SAPIENCE.2016.7684146
Ramesh, P., &Maheshwari, D.(2012).Survey of cybercrimeactivities and preventivemeasures. Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, 301–305. https://doi.org/10.1145/2393216.2393267.
Khanna, A., &Khan, Sami.(2018).Information Technologyact, 2000: Internationalperspective with special reference to Bitcoin.National Journal of Cyber Security Law, 1(1), 15–21.
Porcedda, M. G., &Wall, D. S.(2018).'Data Science, Data Crime and the Law',researchhandbook on data science and the law in V. In E. TjongTjin Tai&A. Berlee(Eds.), M-ak: Elgar, E. (2018). https://ssrn.com/abstract=3152946. SSRN Publication(pp. 214–244).
Mazumdar, S., &Wang, J.(2018).'Big Data and Cyber Security: A Visual Analytics Perspective: An Artificial Intelligence Approach',computercommunications and networksguide to vulnerabilityanalysis for computernetworks and systems, springerinternationalpublishing. Computer Communications and Networks, 367–381. https://doi.org/10.1007/978-3-319-92624-7_16
Lemaignan, S., Warnier, M., Sisbot, E. A., Clodic, A., &Alami, R.(2017).Artificial cognition for social human–robotinteraction: Animplementation.Artificial Intelligence, 247, 45–69. https://doi.org/10.1016/j.ar tint.2016.07.002
La Torre, M., &Dumay, J. C.(2018).Breaching intellectualcapital: Criticalreflections on bigdatasecurity. Meditari Accountancy Research. https://doi.org/10.1108/MEDAR-06-2017-0154
Hoon, K. S., &Yeo, K. C.(2018).Critical review of machinelearningapproaches to applybigdataanalytics in DDoSforensicsInternational Conference on Computer Communication and Informatics (ICCCI), 2018. https://doi.org/10.1109/ICCCI.2018.8441286
Brown, C. S. D.(2015).Investigating and prosecutingcybercrime: Forensicdependencies and barriers to justice.International Journal of Cyber Criminology, 55–119. https://doi.org/10.5281/zenodo.22387
Kim, S.-H., &Kim, N.-U.(2017).Attribute relationshipevaluationmethodology for bigdatasecurity International Conference on IT Convergence and Security, https://doi.org/10.1109/ICITCS.2 01 3.6717808
Bayoumi, S., &AlDakhil, S.(2018).A review of crimeanalysis and visualization. Case study: Maryland State, USA21st Saudi Computer Society National Computer Conference (NCC), 1–6, 2018. https://doi.org/10.1109/NCG.2018.8592982
Vasiliauskas, D., &Beconyte, G.(2015).Cartography of crime: Portrait of metropolitanVilnius.Journal of Maps, 1–6. https://doi.org/10.1080/17445647.2015.1101404
Subhashini, R., &Milani, V.(2015).Implementing geographicalinformationsystem to provideevidentsupport for crimeanalysis.Procedia Computer Science, 48, 537–540. https://doi.org/10.1016/j.procs.2015.04.132
Williams, M. L., Burnap, P., &Sloan, L.(2016).Crime sensing with bigdata: Theaffordances and limitations

of usingopen-source communications to estimatecrimepatterns.British Journal of Criminology, 57(2), 320–340. https://doi.org/10.1093/bjc/azw031

Kandpal, V.(2013).Latest face of cybercrime and its prevention in India.International Journal of Sciences: Basic and Applied Research (IJSBAR), 2(4), 150–156.

Mahmood, T., &Afzal, U.(2013).Security analytics: Bigdataanalytics for cybersecurity: A review of trends, techniques and tools2nd National Conference on Information Assurance (NCIA), 2013. https://doi.org/10.1109/NCIA.2013.6725337

Bauer, T., Devrim, E., Glazunov, M., Jaramillo, W. L., Mohan, B., &Spanakis, G.(2020).#MeTooMaastricht: Building a Chatbot to assistsurvivors of sexualharassment.Communications in Computer and Information Science, 1167, 503–521. https://doi.org/10.1007/978-3-030-43823-4_41

Sugisaki, K.(2019).Chat-Bot-Kit: Aweb-based tool to simulatetext-based interactionsbetweenhumans and withcomputers. In Proceedings of the ACM Conference, ArxivPreprintArxiv:1911.00665.

Huang, T. K., Azaria, A., Romero, O. J., &Bigham, J. P.(2019).InstructableCrowd: CreatingIF-THENrules for smartphonesviaconversations with the crowd. Human Computation. Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, 6, 113–146. https://doi.org/10.15346/hc.v6i1.7

Chandrala, S., &Allogene Therapeutics. (2021).Interactive clinicaldashboardsusingRStudio.Pharmacia. Proceedings, EphicacyConsulting Group Inc SURGEON2021 Conference.

Xie, Y., Allaire, J. J., &Grolemund, G. (2021).R markdown: Thedefinitiveguide.Research Series.Chapman & Hall/CRC Press.https://bookdown.org/yihui/rmarkdown/.

Anandarajan, M., Hill, C., &Nolan, T.(2019).Text pre-processing: Practicaltextanalytics.Advances in Analytics and Data Science, 2, 45–59. https://doi.org/10.1007/978-3-319-95663-3_4

Philip Chen, C.L., &Zhang, C.-Y. (2014).Data-intensive applications, challenges, techniques and technologies: Asurvey on bigdata.Information Sciences, 275, 314–347. https://doi.org/10.1016/j.ins.2014.01.015

Santhiya, K., &Bhuvaneshwari, V.(2018).An automated MapReduce framework for crimeclassification of news articlesusing MongoDB.International Journal of Applied Engineering Research, 13(1), 131–136.

Zhang, B., Wang, X., &Zheng, Z.(2018).The optimization for recurringqueries in bigdataanalysissystem with MapReduce.Future Generation Computer Systems, 87, 549–556. https://doi.org/10.1016/j.future.2017.09.063

Rimal, Y.(2020).'Reproducible Academic Writing and Interactive Data Visualization Using R Markdown (R Programming Flex-Dashboard: Flex_Dashboard Packages)'.Advances in Intelligent Systems and Computing,1187, 603–615. https://doi.org/10.1007/978- 981-15-6014-9_73

Zhou, K., &Zhang, K.(2019).Unsupervised contextrewriting for opendomainconversation. Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing(pp. 1834–1844), arXiv preprint arXiv:1910.08282. https://doi.org/10.18653/v1/D19-1192.

Joseph, V., &Ray, D. (February2020).Cyber crimesunder the IPC and ITact—Anuneasyco-existence, National Seminar on Cyber Crime and Cyber Warfare at Symbiosis Law School.Argus Partners.

Alayon, D.(2018).Understanding artificialintelligence. Medium blog. https://medium.com/future-today/understanding-artificial-intelligence-f800b51c767f. RetrievedNovember2021

Pandey, A.(2017).List of bailableandnon-bailableoffencesunder Indian penal code. Ipleadersblog. https://blog.ipleaders.in/bailable-non-bailable-offence/. RetrievedApril2021

Marg, T.(2020).'Indian Penal Code (IPC) Section 503. Criminal Intimidation',IPC. Criminal intimidation. https://tilakmarg.com/acts/indian-penal-code-ipc-section-503-criminal-intimidation/. RetrievedAugust2021.

Thompson, J.(2018).Using Flexdashboard to monitorclinicalresearch.Using Flexdashboard to Monitor Clinical Research.https://jenthompson.me/2018/02/09/flexdashboards-monitoring/.

Heiss, A.(2020).Create a dynamicdashboard with R, Flexdashboard and shiny. https://www.andrewheiss.com/blog/2020/01/01/flexdashboard-dynamic-data/. (Accessed on: October)

Moraga, P.Chapter 14: Interactivedashboards with Flexdashboard and shiny. Geospatial healthdata: Modeling and visualization with R-INLA and shiny, chapmanandhall/CRCbiostatisticsseries.CRC Press.(2019).

Panchkula Police(Ed.).(2018).Panchkula police: Crime: Cybercrime: ITact2000. https://panchkula.haryanapolice.gov.in/it-act-2000_htm. RetrievedDecember2021

Government of India. (2000).https://www.indiacode.nic.in/bitstream/123456789/13116/1/itact2000updated.pdf Access ed on December 2021.Ministry of Electronics and Information Technology.

Anjum, S.(2018).List of 14 cybercrime scenarios in Indiaalong with penalties.Youth KIAwaaz. https://www.youthkiawaaz.com/2018/06/common-cyber-crime-scenarios-and-applicability-of-legal-sections/, RetrievedNovember2021.