

## EMERGING TRENDS OF CYBER CRIME IN INDIA: A CONTEMPORARY REVIEW

Tanya Gupta\*

Faculty of Law, IIMT and School of Law, India\*

### Abstract

*The world has become more advanced in communication, especially after the invention of the internet. The 21st century has been characterized by massive technological innovations that have shaped the way people interact. The social, political, and economic dimensions of human life are facilitated by a digital age that has encompassed the whole world. Universally, there has been a rapid rise in the use of computers and electronic gadgets. These developments have led to significant growth in criminality, especially in cyberspace. Cybercrimes have grown progressively with perpetrators developing newer and sophisticated techniques every day. Despite the measures taken by the international community to combat the vice and mitigate its effects, cybercrimes have continued to rise alarmingly across the world. According to Cyber Security Breaches Survey of 2022, 39% of businesses worldwide have been a victim of cybercrime. In this paper, the author intends to give a brief account of historical background and evolution of cybercrime. This paper focuses that what are the types of cybercrime and provisions covered under Information and Technology Act, 2000 (IT Act). The author also tries to cover that how does number of cases related to cybercrime in India has been increasing day by day. This paper also focuses on the impact of cybercrime and what are the challenges faced during investigation and what will be the safety measures against cybercrime. In this paper, researcher intends to use the secondary data for illustrating the research paper to clarify certain cybercrimes and issues related to the Investigation and the impact of cybercrime.*

**Keywords:** internet, cybercrime, IT act, impact, challenges

### A. Background

In recent days, computers and internet are used in almost every field of human society either it is our home, school, colleges, factories or at business work. A computer is a small, powerful, helpful, and complete automated machine for humankind. And the internet, has surpassed all around the world unexpectedly. Although the computer today is a great convenience for many of us and brings many advantages, In the other hand, it brings not only benefits but also harms that people need to be aware of. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. Cyber Crimes, also known as e-crimes, are defined as computer related crime and they also considered as an offences or crime that takes place over electronic communications or information systems.<sup>1</sup> Sussman and Heuston first proposed the term "Cyber Crime" in the year 1995. Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conducts. These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both.

---

<sup>1</sup> Priya Rao, Abhay Kumar Tiwari. Laws Related to Cyber-crime in India. Research J. Engineering and Tech. 2020;11(2):41-44. doi: 10.5958/2321-581X.2020.00007.0

The first Cyber Crime was recorded within the year 1820. The primeval type of computer i.e. abacus, has been around since 3500 BC in Japan, China and India, but Charles Babbage’s analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard’s workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future, and referred to Cyber Security Breaches Survey of 2022, 39% of businesses worldwide have been a victim of cybercrime.<sup>2</sup>

In the 21<sup>st</sup> century, digitalization provides a platform to the consumer to pay online, and fraudsters are using innovative ways to dupe vulnerable consumers. Many of them are falling prey to these scams leading to disclosing their sensitive information. The Minister of Electronics and Information Technology has also quoted that the number of phishing incidents in India has more than doubled in 2021. In May 2022, the Government’s cybercrime department’s data stipulates that there were at least 61,100 complaints of digital payments fraud received by the government. With the advancement of technology, the cybercrime has been expanding its horizons.

Years	Types of Crime
1997	Cyber crimes and viruses initiated, that includes Morris Code and other.
2004	Malicious code, Torjan, Advanced worm etc.
2007	Identifying thief, Phishing etc.
2010	DNS Attack, Rise of Botnet Attack, SQL Attacks etc.
2013	Social Engineering, DOS Attack, Botnet Attack, Malicious E-mails, Ransomware attack etc.
Present Scenario	Banking, Malware, Key logger, Bitcoin wallet, Phone Hijacking, Android Hack, Cyber Warfare etc.

Information Technology Act 2000 was the first legislation in India on technology, computers and ecommerce, e-communications. Below is a list for some of the cybercrimes along with their indicative explanation such are: 1) **Child Pornography**: Child sexually abusive material (CSAM) refers to material containing sexual image in any form, of a child who is abused or sexually exploited. Section 67 (B) of IT Act states that “it is punishable for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.; 2) **Cyber Bullying**: A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc.; 3) **Cyber Stalking**: Cyber stalking is the use of electronic communication by a person to follow a person, or attempts to contact a person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; or monitors the internet; email or any other form of electronic communication commits the offence of stalking.; 4) **Cyber Grooming**: Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.; 5) **Online Job Fraud**: Online Job Fraud is an attempt to defraud

<sup>2</sup> Department for Digital, Culture, Media & Sport, UK Government, Security Breaches Survey, 2022 <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022>

people who are in need of employment by giving them a false hope/ promise of better employment with higher wages.; 6) **Online Sextortion**: Online Sextortion occurs when someone threatens to distribute private and sensitive material using an electronic medium if he/ she doesn't provide images of a sexual nature, sexual favors, or money.; 7) **Vishing**: Vishing is an attempt where fraudsters try to seek personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.; 8) **Sexting**: Sexting is an act of sending sexually explicit digital images, videos, text messages, or emails, usually by cell phone.; 9) **Smishing**: Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.; 10) **SIM Swap Scam**: SIM Swap Scam occurs when fraudsters manage to get a new SIM card issued against a registered mobile number fraudulently through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through victim's bank account. Getting a new SIM card against a registered mobile number fraudulently is known as SIM Swap.; 11) **Debit/ Credit Card Fraud**: Credit card (or debit card) fraud involves an unauthorized use of another's credit or debit card information for the purpose of purchases or withdrawing funds from it.; 12) **Impersonation and Identity Theft**: Impersonation and identity theft is an act of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person.; 13) **Phishing**: Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source.; 14) **Spamming**: Spamming occurs when someone receives an unsolicited commercial messages sent via email, SMS, MMS and any other similar electronic messaging media. They may try to persuade recipient to buy a product or service, or visit a website where he can make purchases; or they may attempt to trick him/ her into divulging bank account or credit card details.; 15) **Ransomware**: It is a type of computer malware that encrypts the files, storage media on communication devices like desktops, Laptops, Mobile phones etc., holding data/information as a hostage. The victim is asked to pay the demanded ransom to get his device decrypts.; 16) **Virus, Worms and Trojans**: Computer Virus is a program written to enter to your computer and damage/alter your files/data and replicate them. Worms are malicious programs that make copies of themselves again and again on the local drive, network shares, etc. A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.; 17) **Data Breach**: A data breach is an incident in which information is accessed without authorization.; 18) **Denial of Services/ Distributed Denial of Services**: Denial of Services (DoS) attack is an attack intended for denying access to computer resource without permission of the owner or any other person who is in-charge of a computer, computer system or computer network. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.; 19) **Website Defacement**: It is an attack intended to change visual appearance of a website and/ or make it dysfunctional. The attacker may post indecent, hostile and obscene images, messages, videos, etc.; 20) **Cyber-Squatting**: It is an act of

registering, trafficking in, or using a domain name with an intent to profit from the goodwill of a trademark belonging to someone else.; 21) **Pharming**: It is cyber-attack aiming to redirect a website's traffic to another, bogus website.; 22) **Crypto Jacking**: It is an unauthorized use of computing resources to mine crypto-currencies.; 23) **Online Drug Trafficking**: It is a crime of selling, transporting, or illegally importing unlawful controlled substances, such as heroin, cocaine, marijuana, or other illegal drugs using electronic means.; 24) **Espionage**: It is the act or practice of obtaining data and information without the permission and knowledge of the owner.

This type of research has been done before in some, previous research regarding similar topic such are : Cybercrime in Asia: trends and challenges,<sup>3</sup> Cybercrime in India: Trends and Challenges,<sup>4</sup> and A Survey of Cyber Crime in India.<sup>5</sup> However, there is a novelty value in this research, which is the development of cybercrime after 5 years from the previous study and the shift in paradigm in cybercrime in India.

## B. Identified Problems

The Title of the paper is 'Emerging Trends of Cyber Crime in India: A Contemporary Review'. The Researcher has focused that how cyber crime is increasing day by day in India and on the various new challenges that has arisen in the investigation methods of cybercrime in India. This research also focuses on the impact of cyber crime. The main aim is to find out the efficiency of Indian cyber legislations to implementation of the investigation of cyber crimes.

## C. Research Methods

Researcher used the doctrinal approach for analyzing the research paper and used different statutes, texts, legal journals, magazines etc. and from these tries to collect all the relevant material on the topic and then with reasoning power, researcher tries to find out the problem and draws final conclusion. The research paper involves socio-legal research approach that what are the challenges faced by the society over the increasing cyber crime rate in India. In order to clarify certain cybercrimes and issues related to Investigation and impact of cyber crime researcher used secondary data based on the numbers and statistics inflicted by NCRB pertaining to the cyber crime rate.

## D. Research Findings and Discussions

### 1. How Cyber Crime is Increasing in India

The rate of cyber crime (incidents per lakh population) increased from 3.3% in 2019 to 3.7% in 2020 in the country, according to the National Crime Records Bureau (NCRB) data. In 2019, the country recorded 44,735 cases of cyber crime, while the figures stood at 27,248 in 2018, the data from corresponding years showed. India recorded 50,035 cases of cyber crime in 2020, with an 11.8% surge in such offences over the previous year, as 578 incidents of "fake news on social media" were also reported.

<sup>3</sup> Broadhurst, Roderic; Chang, Lennon YC. Cybercrime in Asia: trends and challenges. *Handbook of Asian criminology*, 2012, 49-63.

<sup>4</sup> Juneed Iqbal and Bilal Maqbool Beigh, "Cybercrime in India: Trends and Challenges," *International Journal of Innovations & Advancement in Computer Science* 6, no. 12 (2017): 187-96.

<sup>5</sup> Vinit Kumar Gunjan, Amit Kumar, and Sharda Avdhanam, "A Survey of Cyber Crime in India," in *15th International Conference on Advanced Computing Technologies (ICACT)* (Rajampet: IEEE, 2013), 1-6, <https://doi.org/https://doi.org/10.1109/ICACT.2013.6710503>.

According to the NCRB, the 2020 saw 4,047 cases of online banking fraud, 1,093 OTP frauds and 1,194 credit/debit card frauds, while 2,160 cases related to ATM were reported. There were also 578 cases of fake news on social media, 972 related to cyber stalking or bullying of women and children, 149 incidents of fake profile and 98 of data theft, it added. In terms of motive, the maximum 60.2% cyber crimes lodged in 2020 were done for fraud (30,142 out of 50,035 cases), the NCRB, which functions under the Ministry of Home Affairs, stated. It was followed by sexual exploitation with 6.6% (3,293 cases) and extortion 4.9% (2,440 cases), the data showed.

Among States, the maximum 11,097 cyber crime cases were reported in Uttar Pradesh followed by Karnataka (10,741), Maharashtra (5,496), Telangana (5,024) and Assam (3,530), it showed. However, the crime rate was highest in Karnataka with 16.2 % followed by Telangana (13.4%), Assam (10.1%), Uttar Pradesh (4.8%) and Maharashtra (4.4%), the data showed. National capital Delhi recorded 168 such cases during the year with a crime rate of 0.8%, according to the NCRB, which is responsible for collecting and analyzing crime data as defined by the Indian 'Penal Code and special and local laws in the country.

## 2. Challenges During Investigation of Cyber Crime

The Jurisdictional limits are becoming the hurdles in the implementation of cyber laws and conviction of the cyber criminals because concept of cyber space is like Universe and had no boundaries. The cyber crimes not mere physical offences but by and large they are the product of criminal psychology, criminal behavior and cannot be strict subject of local law of the land. With rapid evolution of IT space, keeping pace with the emanating threats and consequent legislative response in India lacks may vital links. Law enforcement investigators in India are not computer literate. It is needed to understand the basics of IP addressing in order to trace users of the Internet to a physical location. IP addresses provide a connection point through which communication can occur between two computers. Investigators must be familiar with how these various systems work and how one might be able to retrieve critical case information from stored communications or fragments of previous exchanges. Our criminal laws are still based on old policies, investigators must be aware of the different types of digital media that exist and be able to identify the media in the field. The variety, and more importantly the size, of media must be taken into consideration when applying for search warrants where digital evidence is suspected; the hiding places for this type of storage are countless.

The study pointed that the cybercrime handling requires an appropriate legal framework and technical infrastructure to analyze the cyber offences.<sup>6</sup> It also found that knowledge of cyber forensics tools for capturing evidence from the crime site and network which may vary in the cyberspace is a skillful task and demands special training for the investigators. It is also observed that for investigation of cybercrime and securing digital evidence, special software and tools are required for the effective cyber forensic. There is need for officers in handling and application of forensic tools and techniques. Wide publicity is needed on a sustained level, regarding modus operandi of cyber fraudsters, especially to alert

---

<sup>6</sup> Kethineni, Sessa. "Cybercrime in India: Laws, regulations, and enforcement mechanisms." *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020): 305-326.

them against dangers involved in responding to tempting e-mails or SMSs and preserving the electronic evidence in secured condition till the investigation ends.

### 3. **Impact of Cyber Crime**

Despite crimeless society is myth, crime is omnipresent phenomenon, and it is non-separable part of social existence, one may get irritate by the question, 'Why there is too much ado about crime? No one can deny that crime is a social phenomenon, it is omnipresent, and there is nothing new in crime as it is one of the characteristic features of the all societies existed so far, may it be civilized or uncivilized, and it is one of the basic instincts of all human behavior! However, it should bear in mind that the social concern for high crime rate is not because of its nature, but due to potential disturbance it causes to the society. In addition, some individuals are victims of crime in a more specific sense. The victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values, because they contribute to the satisfaction of many wishes.

### 4. **Impact of Cyber Crime over Socio-Eco-Political Riders**

Conceptually, crime is a dynamic and relative phenomenon and subjected to the relative sociopolitical & economical changes occurring in existing system of society. Therefore, neither all-time suitable comprehensive definition encompassing all aspects of 'crime' is possible at any moment of time nor can a single definition be made applicable to different society. With its dynamicity, it is influenced by the changes occurring in the correlated phenomenon and value system generated by these changes. As evident in present scenario where money is more valuable than values, a definite hike in the corruption related offences are observed where social morality is low which influence the commission of crime attached less social stigma than ever before. Incidentally economic crime is on its peak. This clearly reflects that crime has its interdependency with other social phenomenon, economic systems and political machineries. Besides population, the other factors influencing the crime are such as situation at a particular place, rate of urbanization, migration of population from neighboring places, unemployment, income inequality, computer literacy in case of Cyber crime etc. At the same time, the economic structure of give society is also influence the economic crimes.

### 5. **Impact of Cyber Crime over Teenager**

These days a worst fear in teenager's eyes is Cyber Bullying. It is become common over past five years, generally from the age below eighteen are more susceptible and feared from Cyber Bullying as per inspection. It is becoming an alarming trend in our society. This is all done through core technologies described above mainly via online. Cyber Bulling can be done through chatting, instant messaging etc. Where website like Facebook, Orkut, Twitter user are more affected from Cyber Bullying. In my analysis generally feared person can reach a limit of depression, humiliation and threatens.

### 6. **Sexual Solicitation**

Sexual solicitation is a growing concern for youth who use forms of cyber communication. It may occur in chat rooms or on social networking sites. Sexual solicitation occurs when an adult or peer tries to engage in an online sexual relationship. A teen may be asked to disclose personal information, view pornography or discuss something sexual online. About 70 percent of teens who

are sexually solicited online are girls. Teens should be cautious in posting suggestive photos online and talking to strangers in chat rooms.

#### **7. Impact of Cyber Crime over Consumer Behavior**

The information revolution, coupled with the strategic leveraging of the Internet, has exposed a number of relatively open societies to the dangers of cybercriminal and cyber terrorist acts, especially in commercial business transactions. With the development of e-commerce, this commercial dark side has become known as cybercrime and has taken on many forms that affect the perceptions of the way we shop online. Corporations should realize that these threats to their online businesses have strategic implications to their business future and take proper measures to ensure that these threats are eliminated or significantly reduced so that consumer confidence in the Internet as an alternative means of shopping is maintained. These counter measures, coined as cyber security, have been developed to ensure the safety of consumer privacy and information and allow for a carefree shopping experience. There is need for the development of models that will allow corporations to study the effects of cybercrime on online consumer confidence and to counter through leveraging the benefits associated with the latest developments in cyber security. With these two facets of e-commerce impacting the online consumer, corporations must ensure that the security measures taken will ultimately prevail to assure that consumers will continue to use the Internet to satisfy their shopping needs.

#### **8. Impact of Cyber Crime over Business**

One of the worst consequences of a cyber attack is a sudden decrease in revenue as consumers seek refuge elsewhere to avoid cybercrime. Companies may also lose money due to extortion attempts by hackers, as well as confidence from investors who can withdraw interest, influence, and funds.

### **E. CONCLUSION**

Internet has become one of the integral parts of our daily life. It has transformed the way we communicate; make friends, share updates, play games, and shop. They are impacting most aspects of our day-to-day life. Cyberspace connects us virtually with crores of online users across the globe. With increasing use of cyberspace, cybercrimes especially against women and children such as cyber stalking, cyber bullying, cyber harassment, child pornography, rape content, etc. are also increasing rapidly. The victim can report it on National Cyber Crime Reporting Portal ([www.cybercrime.gov.in](http://www.cybercrime.gov.in)). To stay safe in the online world, it is important to follow some cyber safe practices which may help in making our online experience and productive such as: a) Talk to your children about the potential online threats such as grooming, bullying, and stalking, keep track of their online activities. Set clear guidelines for internet and online games usage; b) Never click on links or files received in e-mail, text message or social media from unknown person. This may be an attempt to infect computer with a malware.; c) Be mindful of your appearance on video chat & video calls.; d) Do not use Smartphone for taking sensitive personal photographs and videos.; e) Protect yourself from Cyber stalking.; f) Report if you find content related to of Child Pornography (CP)/Child Sexual Abuse Material (CSAM) or sexually explicit material.

The author also suggests that there should be the provision by the government such as: a) Trap and Trace order: The new IT Act should make such legislation that it is easier



for cyber investigators to obtain “tap and trace” orders. Trap and Trace devices are used to capture incoming IP packets to identify the packet’s origins. Due to the ease with which the hackers are able to spoof their true origin, the most effective way to reconstruct the path of a virus, DoS or hacking assault is to follow a chain of trapping devices that logged the original malicious packets as they arrived at each individual router or server. In a case of single telephone company, it has been relatively easy for investigators to obtain trap and trace orders but today one communication is being carried by several different {ISPs}, by one or more telephone company or one or more cell company and very soon by one or more satellite company. Once the segment of the route goes beyond the Court jurisdiction, investigators must then go the next jurisdiction and file a request for a trap and trace order for the next segment. The new legislation would authorize the issuance of a single order to completely trace on-line communication from start to finish.;

b) We proposed new legislation such that makes young perpetrators fifteen years of age and older eligible for offences in serious computer crime.;

c) The Cyber Cafes, Computer Training Centre, and other Institute where computer is the mode of training should be incorporated under some act.;

d) Cyber Crime must become a part of a curriculum in the schools, so that students must be aware about the same.



## REFERENCES

- Arshi Khan, "The First Recorded Cyber Crime Took Place In The Year 1820", <https://www.scribd.com/doc/71120466/The-First-Recorded-Cyber-Crime-Took-Place-in-the-Year-1820>
- Dr. Priya Rao, Abhay Kumar Tiwari, "Laws Related to Cyber-crime in India", Research Journal of Engineering and Technology, [https://ijersonline.org/HTML\\_Papers/Research%20Journal%20of%20Engineering%20and%20Technology\\_PID\\_2020-11-2-3.html](https://ijersonline.org/HTML_Papers/Research%20Journal%20of%20Engineering%20and%20Technology_PID_2020-11-2-3.html)
- Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer Crime Laws, Santa Clara University, Vol 16, Number 2. "India reported 11.8% rise in cyber crime in 2020; 578 incidents of 'fake news on social media': Data" The Hindu, September 15, 2021, <https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece>
- National Cyber Crime Reporting Portal, "Learn About Cyber Crime", accessed on May 28, 2022, <https://cybercrime.gov.in/Webform/CrimeCatDes.aspx>
- Neelesh Jain and Vibhash Shrivastava, "Cyber Crime Changing Everything – An Empirical Study", International Journal of Computer Application, Issue 4 Volume 1,(PDF) "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY" (researchgate.net)
- Nyman Gibson Miralis, "The 5 key challenges for law enforcement in fighting cybercrime", Last Modified on August 3, 2020, accessed on May 29, 2022 <https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4>
- Prachi Mishra, "Explained: What is Cyber Crime, its Types and Laws in India" News 18 , May 14 2021 ,<https://www.news18.com/news/india/explained-what-is-cyber-crime-its-types-and-laws-in-india-3735560.html> "Rise of growing threat of cyber frauds due to digital payment" Times of India, July 19,2022, <https://timesofindia.indiatimes.com/gadgets-news/rise-of-the-growing-threat-of-cyber-frauds-due-to-digital-payments/articleshow/92968264.cms>
- Showkat Ahmad Dar Dr.Naseer Ahmad Lone, "Cyber Crime in India", Sambodhi (UGC Care Journal) Vol-43 No.-04 The Information Technology Act, 2000 UNDOC, "THE CHALLENGES FACING SPECIALIST POLICE CYBER-CRIME UNITS: AN EMPIRICAL ANALYSIS", accessed on May 29, 2022
- UNI, "Cyber crime a new challenge for CBI", March 12, 2003, [www.rediff.com](http://www.rediff.com)
- Vishwa, " All about classifications of cybercrimes", Last Modified on September 4, 2022,<https://blog.ipleaders.in/all-about-classifications-of-cyber-crimes/>
- Kethineni, Sessa. "Cybercrime in India: Laws, regulations, and enforcement mechanisms." *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020): 305-326.
- Iqbal, Juneed, and Bilal Maqbool Beigh. "Cybercrime in India: Trends and Challenges." *International Journal of Innovations & Advancement in Computer Science* 6, no. 12 (2017): 187–96.
- Gunjan, Vinit Kumar, Amit Kumar, and Sharda Avdhanam. "A Survey of Cyber Crime in India." In *15th International Conference on Advanced Computing Technologies (ICACT)*, 1–6. Rajampet: IEEE, 2013. <https://doi.org/https://doi.org/10.1109/ICACT.2013.6710503>.