International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 03 | Mar 2023 www.irjet.net p-ISSN: 2395-0072

CYBER CRIMES IN INDIA

Mr. Mohit Chauhan[1], Er. Poonam Chaudhary[2]

[1]Student, IV Semester M.Tech (Computer Science),
SIRDA Institute of Engineering and Technology NH-21 Sunder Nagar Distt. Mandi-175019(Himachal) (India)
[2]Associate Professor, Computer Science Engineering Department
SIRDA Institute of Engineering and Technology NH-21 Sunder Nagar Distt. Mandi-175019(Himachal) (India)

Abstract - *This research, titled "Cybercrime in India", focuses on digital security and considers the various aspects more explicitly through legal investigations to troubleshoot cybercrime. This exploration will help many people in India to become aware of cybercrime and solve these problems to some extent. Today, data is changing at such a rapid pace that it has become a key driver of business and economic development in every country. According to an IBM survey, human error is the primary driver of 95% of digital security breaches. Cybercriminals cannot effectively be considered a group as they engage in a variety of different criminal activities. The review is focused on digital awareness and addressing digital vulnerabilities.*

Key Words: Cyber Crime, NTRO, Criminals, Awareness, CERT-IN.

1. INTRODUCTION

Cybercrime is an illegal activity, global threat and it refers to the criminals who seek to exploit human or security vulnerabilities for his own means in order to steal information like passwords, data or money directly or indirectly. Cyber threat is a possibility identified with the adversary attempting to gain access to a system. In India cyber-attacks are rapidly increasing day by day.

- Associated Chambers of Commerce and Industry of India and PwC published a joint report in which the magnification of smartphone users in India is expected to ascend by 84% to 85.9 crore by 2022 from 46.8 crore in 2017.
- A global ICT statistics by International Telecommunication Union (ITU) estimates that at the end of 2019, 410 crore people that is 53.6 percent of the global population will utilize the internet.

1.1 Cyber Attack Reports

The data for the report is collected by State Crime Records Bureau (SCRB) from the District Crime Records Bureau (DCRB) and sent to National Crime Record Bureau (NCRB) at the end of every calendar year under the reference. Information from super urban areas (urban areas having populace of 10 lakh or more according to the most recent enumeration) is likewise gathered independently. Area shrewd information on some IPC heads is gathered and distributed independently. The primary release of 'Crime in India' relates to the year 1953 and the most recent version of the report relates to the year 2018.

1.2 Cyber Victim Reports

The NCIIPC under The National Research Organization (NTRO) has given standards that consolidate application whitelisting, blocking unused ports, slaughtering unused organizations. NTRO reports to the Prime Minister's Office (PMO) and the National Security Advisor (NSA).

- According to latest FBI Internet Crime Complaint Center (IC3) reports, India stands "Third" among top 20 cyber crime victims in the world in 2019.
- As per the most recent National Crime Records Bureau (NCRB) information, a sum of 27,248 instances of digital wrongdoing were enlisted in India in 2018. In Telangana, 1205 digital wrongdoing cases were enlisted around the same time. The National Cyber Crime Reporting Portal that was begun a year ago by the Central government got 33,152 grumblings till now, bringing about housing of 790 FIRs.

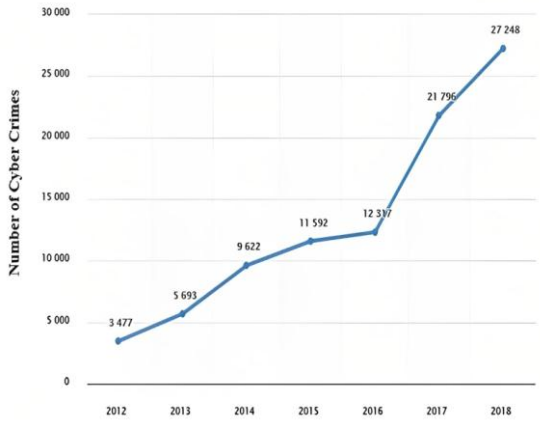

Fig -1: Cyber Crimes reported in India (2012-2018)

SCRB	State Crime Records Bureau
DCRB	District Crime Records Bureau
IC3	Internet Crime Complaint Center
NSA	National Security Advisor
NTRO	The National Research Organization
PMO	the Prime Minister's Office
NCRB	National Crime Records Bureau

Table-1: Abbreviations

2. Analysis of Cyber Crimes

Risk analysis is systematic utilization of available information to determine how often designated events may occur and the intensity of their consequences. Risk is quantified in terms of impact and likelihood of the event. Risk is managed to identify vulnerably susceptible areas, implement efficacious controls and continually ameliorate processes. Risk analysis should occur on a recurring substructure and be updated to accommodate incipient potential threats. An analysis will be made on few cases of computer malefaction reported in India from sundry private and public sources to establish the pattern of abuse in various crime perpetration.

- Who are the victims?
- Who are the computer malefactors?
- Amount of loss, penalties and detection and edifications learnt from the reported cases.

The National Institute of Standards and Technology or NIST defines risk assessments as a way to identify, estimate, and prioritize risk to organizational operations, assets, individuals, and other organizations.

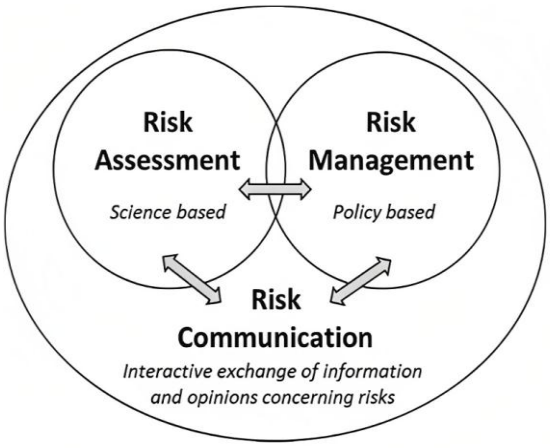

Fig -2: Risk Analysis

It is estimated that cybercrime around the world will cost businesses around 6 trillion dollars by 2021, and approximately 43% of cyber attacks target small businesses.

- Risk Assessment
- Risk Management
- Risk Communication

2.1 Risk Assessment

An all around done information review distinguishes what information your organization is putting away and what its worth may be. A good data audit highlights following parts:

- Data amassing
- Storing the data
- Data protection
- Time period for storing data

2.2 Risk Management

Following steps are taken for risk management:

Step 1: Identify the Risk.

Step 2: Analyze the risk.

Step 3: Evaluate the Risk.

Step 4: Treat the Risk.

Step 5: Monitoring the risk.

2.3 Risk Communication

Risk Communication is a significant tool for breaking data and comprehension about a hazard the executive's choice. People in general and compelling danger correspondence. At the point when the open need data about a hazard, they favor an unmistakable message with respect to dangers and related vulnerabilities, including the nature and degree of differences between various specialists.

3. CASE STUDIES

3.1 ATM System Hacked in Kolkata

In July 2018 fraudsters hacked into Canara bank ATM servers and wiped off virtually 20 lakh rupees from different bank accounts. There was more than 50 victims and it was believed that they were holding the account details of more than 300 ATM users across India. The hackers used skimming contrivances on ATMs to steal the information of debit cardholders and made a minimal transaction of INR 10,000 and the most of INR 40,000 per account.

3.2 SIM Swap Fraud

In August 2018, two men from Mumbai were apprehended for cybercrime. Both were involved in fraudulent activities concerning money transfers from the bank accounts of numerous individuals by getting their SIM card information through illicit intentions.

Fig -3: SIM Swap Fraud

3.3 Hacked Twitter Account of Indian Celebrity

In 2019, the actor Amitabh Bachchan's twitter handle was compromised and the culprits posted abhorrent messages putting everybody in shock. This can transpire to astronomically immense companies withal. However, if the news gets out this can be an immense blow to the credibility of any company.

Fig -4: Sim Swap Fraud

3.3.1 Few More Incidents

- Even Congress President Rahul Gandhi (2017-2019) could not get away from its grasp as his Twitter account was hacked. After a day, the Congress' Twitter handle also was hacked and digital lawbreakers threatened to discharge mystery correspondence of the gathering.
- A parcel of wrongdoings are going on normal premise, "India needs more Cyber Security Experts" to handle these circumstances without hardly lifting a finger and a quicker way
- As per a most recent overview, 56% Indians were survivor of online tricks by tapping on malignant connections. Cyber security firm cautions Indians from turning into a casualty of web based shopping limits during the Christmas season. Watch to know more.
- 158 government sites hacked in most recent four years: IT Ministry in Rajya Sabha. According to the data answered to and followed by Indian Computer Emergency Response Team, an all out number of 110 and 48 sites of Central Ministries and Departments and State Governments were hacked during the year 2018 and 2019 separately.

4. CYBER CRIME AWARENESS

Cybercrime is an illegal crime committed over the Internet or by various types of computer engineering, such as using an online social network to intimidate someone or using a smartphone to send sexually explicit photos. But while cybercrime is a relatively new phenomenon, before the computer age, some of the same crimes that a machine or smartphone could be trusted with, including theft or child pornography, were committed in person. This subsection includes articles on cyberbullying and the different crimes that are commonly committed online or using computer web applications.

4.1) Role of Government in Cyber Awareness

Government has taken steps to spread awareness about cyber crimes has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (**I4C**) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

Government has taken several steps to prevent and mitigate cyber security incidents as following:

- Issue of alarms and warnings with respect to digital dangers and counter-measures by CERT-In.
- Issue of rules for Chief Information Security Officers (CISOs) with respect to their key jobs and obligations

regarding making sure about applications/framework and consistence.

- Provision for review of the administration sites and applications preceding their facilitating, and from that point at normal stretches.
- Empanelment of security inspecting associations to help and review usage of Information Security Best Practices.
- Formulation of Crisis Management Plan for countering digital assaults and digital psychological warfare.
- Conducting digital security mock bores and activities consistently to empower appraisal of digital security stance and readiness of associations in Government and basic areas.
- Conducting normal preparing programs for arrange/framework directors and Chief Information Security Officers (CISOs) of Government and basic part associations with respect to making sure about the IT foundation and moderating digital assaults.
- Education and Awareness Project (ISEA) - A venture to bring issues to light and to give exploration, instruction and preparing in the field of Information Security.
- Training of 1.14 Lakh people through 52 establishments under the Information Security.

4.2) Cyber Laws

According to Ministry of Electronic and Information Technology, Government of India, Digital Laws yields lawful acknowledgment to electronic archives and a structure to help e-recording and web based business exchanges and furthermore gives a legitimate structure to lessen, check cyber violations.

4.2.1) Importance of Cyber Law

- It covers all exchange over web.
- It keeps eyes on all exercises over web.
- It contacts each activity and each response in the internet.
- Laws related to Cyber Security in India:
- Information Technology Act, 2000
- The act manages utilization of PCs, PC frameworks, PC systems and furthermore information and data in electronic arrangement.
- The act records down in addition to other things, following as offenses:
- Tampering with PC source reports.
- Hacking with PC framework
- Act of digital psychological oppression for example getting to an ensured framework with the goal of undermining the solidarity, honesty, power or security of nation.
- Cheating utilizing PC asset and so forth.

4.2.2) Methodologies under National Cyber Policy

- Creating a safe digital biological system.
- Creating instruments for security dangers and reactions to the equivalent through national frameworks and procedures.
- National Computer Emergency Response Team (CERT-in) capacities as the nodal organization for coordination of all digital security endeavors, crisis reactions, and emergency the executives.
- Securing e-administration by actualizing worldwide accepted procedures, and more extensive utilization of Public Key Infrastructure.
- Protection and flexibility of basic data framework with the National Critical Information Infrastructure Protection Center (NCIIPC) working as the nodal organization.
- NCIIPC has been made under Information Technology Act, 2000 to make sure about India's basic data framework. It is situated in New Delhi.
- Promoting forefront innovative work of digital security innovation.
- Human Resource Development through instruction and preparing projects to construct limit.

4.2.3) Areas of Cyber Law

Digital laws contain various sorts of purposes. A few laws make rules for how people and organizations may utilize PCs and the web while a few laws shield individuals from turning into the casualties of wrongdoing through deceitful exercises on the web. The significant territories of digital law include:

a) Extortion

Shoppers rely upon digital laws to shield them from online extortion. Laws are made to forestall data fraud, charge card robbery and other monetary wrongdoings that happen on the web. An individual who carries out data fraud may confront confederate or state criminal allegations. They may

likewise experience a common activity brought by a casualty. Digital attorneys work to both safeguard and indict against claims of misrepresentation utilizing the web.

b) Copyright

The web has made copyright infringement simpler. In beginning of online correspondence, copyright infringement was excessively simple. The two organizations and people need legal advisors to carry activities to force copyright assurances. Copyright infringement is a territory of digital law that ensures the privileges of people and organizations to benefit from their own imaginative works.

c) Criticism

A few faculty utilize the web to express their genuine thoughts. At the point when individuals utilize the web to make statements that are false, it can go too far into maligning. Criticism laws are respectful laws that spare people from counterfeit open articulations that can hurt a business or somebody's very own notoriety. At the point when individuals utilize the web to offer expressions that disregard common laws called Defamation law.

d) Badgering and Stalking

Some of the time online proclamations can abuse criminal laws that deny badgering and following. At the point when an individual offers undermining expressions over and over about another person on the web, there is infringement of both common and criminal laws. Digital legal counselors both arraign and safeguard individuals when following happens utilizing the web and different types of electronic correspondence.

e) Freedom of Speech

The right to speak freely of discourse is a significant region of digital law. Despite the fact that digital laws preclude certain practices on the web, the right to speak freely of discourse laws additionally permit individuals to express their genuine thoughts. Digital legal advisors must instruct their customers on the cutoff points regarding free discourse including laws that restrict foulness. Digital legal advisors may likewise protect their customers when there is a discussion about whether their activities comprise of admissible free discourse.

f) Trade Secrets

Organizations doing organizations online frequently rely upon digital laws to secure their proprietary innovations. For instance, Google and other online web indexes invest bunches of energy building up the calculations that produce query items. They additionally invest a lot of energy creating different highlights like guides, insightful help and flight search administrations to give some examples. Digital laws help these organizations to make legitimate move as fundamental so as to secure their proprietary innovations.

g) Agreements and Employment Law

Each time you click a catch that says you consent to the terms and states of utilizing a site, you have utilized digital law. There are terms and conditions for each site that are by one way or another identified with protection concerns.

5. PROTECTION AGAINST CYBER CRIME

Following is the hierarchy of **cyber space** in India:

a) PM Office/Cabinet Secretariat

- National Security Council
- National Technical Research Organization
- National Critical Information Infrastructure

b) Protection Centre

- Joint Intelligence Committee
- National Crisis Management Committee
- Research and Analysis Wing
- Multi-Agency Centre
- National Information Board

c) Ministry of Home Affairs

- National Cyber Coordination Centre
- Directorate of Forensic Science
- National Disaster Management Authority
- Central Forensic Science Laboratories
- Intelligence Bureau

d) Ministry of External Affairs

- Ministers and Ambassadors
- Defense Attaches
- Joint Secretary (IT)

e) Ministry of Defense

- Tri-Service Cyber Command
- Army/Navy/Air Force Intelligence
- Defense Information Assurance & Research Agency
- Defense Research and Development Authority

f) Ministry of Communications and IT

- Department of Information Technology
- Department of Telecom
- Indian Computer Emergency Response Team
- Educational Research Network
- National Informatics Centre
- Centre for Development of Advanced Computing
- Standardization Testing and Quality Certification

g) Non-Governmental Organizations

- Cyber Security and Anti-Hacking Organization
- Cyber Society of India
- Centre of Excellence for Cyber Security Research and Development in India
- National Cyber Security of India

5.1 Government Initiatives against Cyber Crimes

Indian Government is trying it's best for the mitigation of cyber crimes. Few of the initiatives are as following:

5.1.1 National Cyber Crime Reporting Portal

A cyber portal **https://cybercrime.gov.in** is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This gateway obliges grumblings relating to digital wrongdoings just with exceptional spotlight on digital violations against ladies and kids.

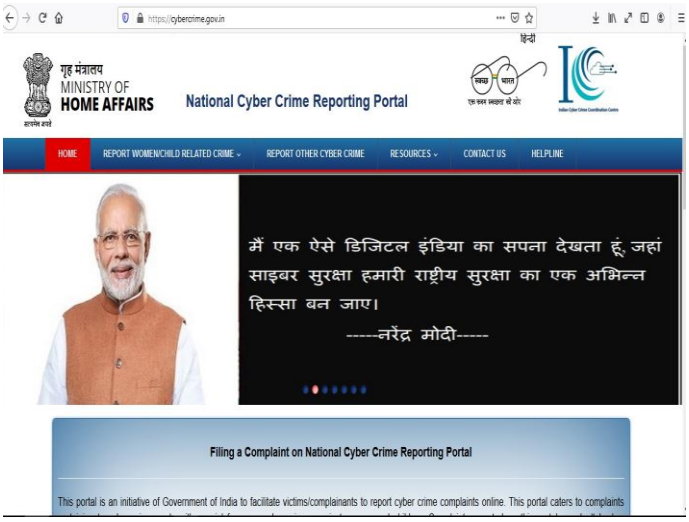

Fig -5: National Cyber Crime Reporting Portal

5.1.2 Indian Computer Emergency Response Team

It is a functional organization of Ministry of Electronics and Information Technology, CERT-In portal https://www.cert-in.org.in/ is established for securing cyber space and it mainly provides incident prevention and response services as well as security quality management services.

5.1.3 National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC portal https://nciipc.gov.in/ is set up for protection of basic data framework in the nation from unauthorized access, change, use, revelation, interruption, crippling or interruption through intelligent coordination, collaboration and raising data security awareness among people.

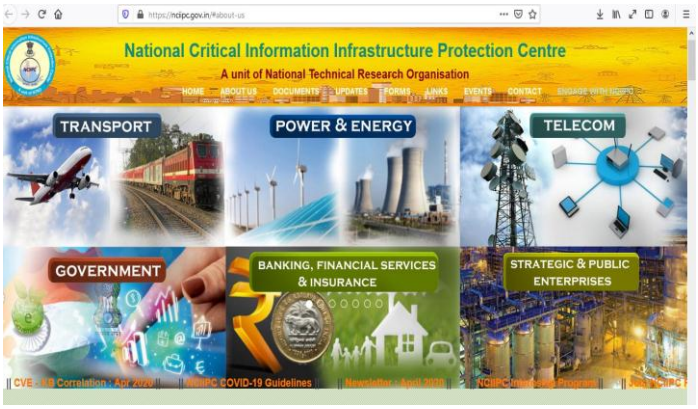

Fig -6: NCIIPC

5.1.4 Cyber Swachhta Kendra

Botnet cleaning and malware analysis centre has been launched for providing detection of malicious programs and free tools to remove such programs. It provides information and tools to users to secure their systems/devices. This inside is being worked by the Indian Computer Emergency Response Team (CERT-In) under arrangements of Section 70B of the Information Technology Act, 2000. The portal can be accessed at https://www.cyberswachhtakendra.gov.in/

Fig -7: Cyber Swachhta Kendra

5.1.5 Cyber Surakshit Bharat Initiative

It was propelled in 2018 with a plan to spread awareness about cybercrime and building limit with respect to wellbeing measures for Chief Information Security Officers (CISOs) frontline IT staff across all government departments.

Notations:

NCRB	National Crime Record Bureau
I4C	Indian Cyber Crime Coordination Centre
CERT-IN	Indian Computer Emergency Response Team
NCIIPC	National Critical Information Infrastructure Protection Centre
CISO	Chief Information Security Officers

Table -2: Abbreviations

6. OUR INITIATIVES AGAINST CYBER CRIMES

The enormous development being used of web-based social networking stages has given a rich ground to cyber criminals to engage in illegal activities.

Here are some of important steps you should take to protect yourself and your information while using social media platforms:

- Do not acknowledge friend requests from outsiders on long range interpersonal communication locales.
- Do not trust online clients except if you know and can confide in them, in actuality.
- Do not share your OTP, own data, for example, address, telephone number, date of birth and so forth via web-based networking media.
- Do not share your touchy individual photos and recordings via web-based networking media.
- Share your photographs and recordings just with your confided in companions by choosing right protection settings via web-based networking media.
- Immediately advise the online networking specialist co-op, on the off chance that you notice that a phony record has been made by utilizing your own data.
- Always utilize a solid secret word by utilizing letter sets in capitalized and lower case, numbers and extraordinary characters for your online life accounts.
- Do not share your get-aways, itinerary items and so on via web-based networking media.
- Always keep area administrations turned off on your gadgets except if essential.
- Do not permit long range interpersonal communication locales to filter your email record to search for your companions and send spam sends to them without your assent or information.

7. CONCLUSIONS

The research shows that a lot of users are not aware about cybercrime. The exploration shows that a great deal of clients don't know about cybercrime. There are quantities of devices and assets accessible to sort such issues of concerns. Receiving not many preventive measures and best practices, we can unquestionably keep cybercrime under control. To execute increasingly powerful counteraction systems, it is obligatory that instructors, guardians, law authorization, and officials comprehend the main driver of the event of such cybercrimes. Schools and universities ought to normally instruct the two understudies and guardians on safe surfing, through workshops and courses.

ACKNOWLEDGEMENT

I express my sincere appreciation and thanks to all those who have guided me directly or indirectly in my research. Also much needed moral support and encouragement was provided on numerous occasions by whole division. Finally, I thank my parents for their immense support.

REFERENCES

[1] https://meity.gov.in/content/cyber-laws

[2] https://www.assocham.org/newsdetail.php?id=7099

[3] https://censusindia.gov.in/

[4] https://cybercrime.gov.in/Webform/FAQ.aspx

[5] https://www.newindianexpress.com/cities/thiruvananthapuram/2020/apr/26/cyber-attacks-on-the-rise-during-lockdown-period-2135338.html

[6] https://geekflare.com/cyberattack-simulation-tools/

[7] https://telecom.economictimes.indiatimes.com/news/smartphone-users-in-india-to-double-60-population-to-be-internet-users-by-2022-cisco-report/66918448

[8] https://www.testbytes.net/blog/cyber-attacks-on-india/

[9] https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226

[10] https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[11] https://www.tribuneindia.com/news/features/cyber-crime-net-widens-21638

[12] https://timesofindia.indiatimes.com/topic/Cyber-crime

[13] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[14] https://www.cyberralegalservices.com/detail-casestudies.php

[15] https://www.dnaindia.com/india/video-increasing-number-of-indians-falling-prey-to-online-scams-2805342

[16] https://www.geeksforgeeks.org/cyber-law-it-law-in-india/

[17] https://ncrb.gov.in/crime-in-india-table-addtional-table-and-chapter-contents?page=24

[18] http://data.conferenceworld.in/IIMT_NHSEMH/16.pdf

[19] https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

[20] https://www.projectmanager.com/training/how-to-analyze-risks-project

[21] https://economictimes.indiatimes.com/news/politics-and-nation/cyber-attack-fears-high-due-to-work-from-home-ntro/articleshow/75440471.cms

[22] https://www.researchgate.net/publication/338526977_Analysis_of_Cyber_Security_Threat_Environment_and_Information_Security_System_of_Financial_Industry_Under_New_Situation/link/5e196be7299bf10bc3a35355

[23] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific &Engineering Research, Volume 3, Issue 6, June-2012, ISSN 2229-5518.

[24] Bagyavati (2009) 'social engineering' in lech j.janczewski and andrew m.colarik cyber warefare and cyber terrorism.

[25] Sudit, M., A. Stotz, and M. Holender. 2005. Situational awareness of coordinated cyber attack. In Proceedings of the International Society for Optical Engineering Conference, Orlando,FL

[26] Norton "cybercrime definition". Retrieved 24th October 2015, http://us.norton.com/cybercrime-definition.

[27] International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No1, February 2014

BIOGRAPHIES

Mohit Chauhan

Student, IV Semester M.Tech (Computer Science),SIRDA Institute of Engineering and Technology NH-21 Sunder Nagar Distt. Mandi-175019(Himachal Pradesh(India)