Dark Web and recent Cyber Crimes that happened in India in 2024

Abhishek Suresh Aahadi[1]
[1]*Sonopant Dandekar College, Palghar (W), Maharashtra, India;*

***Abstract*—Google, Instagram, Facebook these are normally used website which can be access by anyone easily. The internet is like easily available for everyone for every person, but the surface web is just 4% to 5% of the internet the remaining internet is non accessible easily which is Dark Web. The Dark Web is one of the reasons that is responsible for increasing crime rates in India. The Dark Web users or some Cyber criminals are harassing and cheating them with the fake allegation and scams. This paper looking for the recent cybercrimes such as house arrest, online financial frauds and other scams. By the current cyber rimes and other events, the paper aims to provide the recent activities and some countermeasures and analysis of the cybercrimes.**

***Index Terms*—Dark Web, Cybersecurity, Cybercrime, Digital Economy, Information Technology Act**

I. INTRODUCTION

The internet is changed because of some reason like how the people are communicating and do the work. The internet gave us so many benefits but also many more dangers and more dangers from the Dark Web is a part of the Deep Web. To access Deep Web the user can't use the normal web browser such as Chrome, Firefox or other, it is accessible only through specialize web browser like Tor Browser. Tor Browser help the user to hide the personal details such passwords, user id's etc. The Deep Web / Dark Web is known for the illegal activities. Tor Browser hides the user Identity and help the user to hide in shadows. The dark web works as an unseen world where substance is indexed and monitored, giving users anonymity. Whereas this anonymity is beneficial to certain privacy-related activities, it has additionally transformed into a haven for cybercrimes. In these past years, in India is became one of the largest economies, with many more and new internet users joins the ecosystem annually. The country is now an attractive goal for cybercriminals because of the rapid digital use, weak cybersecurity infrastructure, and its lack of understanding.

In 2024, the dark web has played a pivotal role in facilitating numerous cybercrimes in India, ranging from financial frauds and phishing scams to large-scale data breaches and ransomware attacks. In these it includes House Arrest, Financial frauds, Threatening People for money and so many. The "house arrest" scam is now recognized as one of the most worrying of these, taking use of victims' psychological weaknesses and technological shortcomings to extort them.

1.1 Background

The emergence of the internet has created revolution in communication, businesses and in entertainment sectors. However, it has also introduced new elements of threats that can affect the privacy, security, and trust of the people. The anonymity it provides, initially designed to safeguard privacy, has turned into a fertile ground for cybercrimes, which include data breaches, financial fraud, human trafficking, and ransomware attacks. As India positions itself as one of the rapidly growing digital economies, the nation is confronted with a dual challenge: to reap the advantages of digital advancements while also addressing the dangers posed by cyber threats.

1.2 Research Objective

This paper focuses to investigate the role of the dark web in aids the cybercrimes in India, in this paper focusing on incident or scams from 2024. It explores to identify the pattern in these cases or scams, asses their significance for individuals and organizations, and the actionable schemes to counter these threats and attacks.

II. RECENT CYBERCRIMES IN INDIA LINKED TO THE DARK WEB

The "house arrest" scam is one of the most popular cybercrimes in India in 2024. This fraudulent operation involves scammers posing as law enforcement officials or members of criminal syndicates. Scammers impersonating law enforcement officers or members of criminal syndicates are involved in this fraudulent scam. The phishing attacks are also increased in precious days, these attacks manly attacks on businesses. These attackers pretend to be an official person from an organization or company or they impersonate trusted officials to steal the confidential data suck as bank details, user logins and password. The stolen data is can be sold on the dark web in exchange of Bitcoins. It deals with the dark web of illegal businesses such as human trafficking, the sale of illicit drugs, the supply of illegal weapons. Indian law enforcement has recently intercepted several operations involving illicit drugs and counterfeit currency, further demonstrating the reach of these activities.

Another problem is there which is increasing attacks of Ransomware Attacks. These attackers are mostly target's the Educational Institutes, Hospitals, and corporate entities or businessmen. The Cyber Criminal use the dark web not only for to circulate the Ransomware but also collect large-scale ransom data in crypto currencies, complicating traceability and enforcement efforts.

III. MECHANISM OF CYBER CRIME ON THE DARK WEB

The obscurity offered by the dark web is crucial in enabling these crimes. Encrypted communication methods help ensure that offenders cannot be traced. Transactions using cryptocurrencies, particularly those that prioritize privacy such as Monero, serve as an ideal means for moving illicit profits. Additionally, progress in artificial intelligence and automated tools has made extensive social engineering efforts possible, thereby increasing the efficiency of cybercrime and making it more challenging to identify.

IV. ROOT CAUSE OF CYBERCRIMES IN INDIA

The increase of cybercrime in India linked to the dark web can be apply to several factors. These factors are weak cybersecurity infrastructure, insufficient public awareness, economical challenges, and Other some social issues

4.1. Weak Cybersecurity Infrastructure

India's cybersecurity infrastructure is in under development phase. Many organizations and multiple institution's lack advance security tools, that leaves their systems exposed and that inspire the cybercriminals. Weak internet protocol and old system contributes fundamentally to the increasing number of data breaches and cyber-attacks.

4.2. Rapid Adaptation of Digitalization

In every year theirs is growth in internet users, many people are not completely prepared to handle the risk of digitalization and digital platforms. The lack of digital knowledge inflames the various issues, that increase sensitivity to privacy and security.

4.3. Insufficient Legal Enforcement

India has law to address cybercrimes, as suck IT act 2000. It's a legal framework for activities in digital spaces, but due to lack of resources, technical knowledge, and jurisdictional challenges these challenges weakened the law enforcement. The weak law's leaves the gaps for the cyber criminals to attack on people.

V. IMPLICATION OF CYBER CRIMES

The economic impact of cybercrimes in India is immense, resulting in annual losses up to billions due to fraud and ransomware. Above the financial losses, people are suffering from psychological trauma, particularly in the "House Arrest" scam cases because of the intimate behaviour of the scammer and their tactics. These crimes destroy the trust of a person from digital platforms and it affects financial institutions, potentially hindering India's digital economy. Furthermore, these cybercrimes cause threat to national security, with some highly sensitive and important information and it can harm the vital infrastructure.

VI. THE COUNTERMEASURES AND RECOMMENDATION

As a society to keep the data safe and to avoid financial harm, Government and all of us need to make some concrete decisions that can stop these cyberattacks or reduce it to some extent. We need to take some decision and do some countermeasures. As follows

6.1. Strengthening Cybersecurity Infrastructure

Organization and institutions must advance the cybersecurity tool, including endpoint protection, intrusion detection or security breaches detection and encryptions data storage solutions.

6.2. Public Awareness and Education

It launches campaign to educate people about online safety, that can help people to recognize the phishing attempts, and the importance of strong and unique password for better security of google accounts, Devices like mobile phones, laptops, personal computers, databases etc.

6.3. International Cooperation

Cyber criminals can attack from the other countries that can make international collaboration can play a crucial role to catch the cyber criminals. India should participate in global agreements to share and share details related to the cybercrimes and cyber criminals, that can help to combat with the cyber threats.

6.4. Encourage Ethical Hacking

Promote ethical hacking drives and bug bounty programs & drives to find and fix the problems in the system. This not only counter the breaches but also provides a certain outlet for skill programmers or ethical hackers.

6.5. Cyber Security Insurance

Cyber Security Insurance cheers businesses to support cybersecurity insurance to reduce financial losses from cyberattacks. This can work as a safety net and advance aggressive risk management.

6.6. Secure Crypto currency Transactions

Securing crypto currency transactions works on frameworks to check crypto currency transactions without any privacy compromission. Association with block chain analytic firms can help to find prohibited activities connected to cryptocurrencies.

6.7. International Partnerships

It initiates a campaign aimed at informing the public about online safety, which can assist individuals in identifying phishing attempts and understanding the significance of having strong and unique passwords for enhanced security of Google accounts, mobile devices, laptops, personal computers, databases, and more.

VII. CONCLUSION

The involvement of the dark web in facilitating cybercrimes in India throughout 2024 highlights the pressing necessity for collaborative initiatives to address these dangers. By tackling fundamental issues, improving technological defences, and enhancing public awareness, India can establish a strong digital environment. Confronting cybercrime demands not only a solid infrastructure but also a united dedication to ensuring a safe and reliable digital future.

REFERENCE

[1] Journal of Information Security Studies. Kumar, S., & Gupta, P. (2024). Trends in Cybersecurity in India.
[2] National Cyber Crime Bureau Report, 2024. Government of India.
[3] Indian Journal of Technology and Law.
[4] Singh, R. (2024). The Role of Cryptocurrency in Cyber Crime.