IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Emerging India Witnessed A Substantial Rise In The Risks Posed By Cybercrime

Dr. Parag Garg, Associate Professor, School of Law Monad University, Hapur

Amit Sharma, Research Scholar, School of Law Monad University, Hapur

Abstracts: -

Due to its reliance on digital infrastructure for daily life, trade, and governance, India, like many other nations, is having to deal with an increase in cybercrime threats. These dangers are exacerbated by the economy's rapid expansion, rapid digitalization, and weak infrastructure. While there is a rapid growth in smartphone usage and internet penetration, there is also an expansion in the attack surface for hackers. Economic expansion has resulted in a rise in digital banking services, e-commerce, and online transactions, giving hackers new targets to attack: people, companies, and financial institutions. India still has weaknesses in its digital infrastructure, such as out-of-date systems, insufficient cybersecurity safeguards, and a shortage of qualified cybersecurity experts. The methods used by cybercriminals are evolving, and they are now using sophisticated strategies including malware assaults, phishing, ransomware, and social engineering. New security issues brought forth by emerging technologies like blockchain, internet of things (IoT), and AI leave them open to abuse by hackers. Cyberwarfare and cyberespionage are made more likely by geopolitical conflicts with neighbouring nations. Governmental organizations, defence installations, and vital infrastructure are possible targets for state-sponsored hackers looking to get information or interfere with operations. India's cybersecurity regulations are difficult to police and comply with, and to properly handle new threats, ongoing amendments to the current legislation are required. Stakeholders must cooperate to fortify cybersecurity infrastructure, improve public awareness and education, engage with foreign partners, impose strict rules, cultivate a workforce with the necessary skills, and promote to lessen these dangers.

Key Words: -Cybercrime, Cyber-Security, Blockchain

Introduction

Cybercrime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic wracking to denial-of-service attacks. It is a general term that covers crimes like phishing, Credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and or

distribution of viruses,spam and soon.

It also covers traditional crimes in which computers or networks are used to enable illicit activity. Cybercrime is increasing day by day, nowadays it has become a new fashion to earn money by fraud calls or to take revenge through hacking other accounts.

Cybercrime is criminal activity that either targets or uses a computer, a computer network, or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

The term "cybercrime" was introduced after the latest evolution in the computer industry and networks.
Cybercrimes are considered a major risk because they can have devastating effects like financial losses, breaches of sensitive data, failure of systems, and, it can affect an organization's reputation.
Cybercrime can be defined as “The illegal usage of any communication device to commit or facilitate in committing any illegal acts”.
Cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for the purpose of harm.
Cybercrimes are committed using computers and computer networks. They may target individuals, business groups, or even governments.
Investigators tend to use various ways to investigate devices suspected of being used or to be a target of a cybercrime.
Cybercrime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act. Cyber crime is the most prevalent crime playing a devastating role in Modern India. Not only the criminals are causing enormous losses to the society and the government but are also able to largely conceal their identity. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation it can be said that Cyber crime includes any illegal activity where computer or internet is either a tool or target or both. The term cyber crime may be judicially interpreted in some judgments passed by courts in India, however it is not defined in any act or statute passed by the Indian Legislature. Cyber crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark sides too.1 Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet.

Nature and Scope of Cyber Crime: Crime is a socially correlated phenomenon. No matter how much we try, we cannot experience a society cybercrime. In actual sense, when we are not yet able to control the crime rate to the desirable minimum in the real world, how would it be possible to curb the same in the

virtual world, as the same is comparatively more unreal, everlasting, and legally less controllable. However with the time, nature and scope and definition of crime changes in a given society. Crimeless society is a myth and crime cannot be segregated from a society. Thus the nature of the crime depends upon the nature of a society. Complexity of the society determines the complexity of the crime that evolves' around it. To understand the crime in a society, it is essential and crucial to verify all the factors which influence and contribute to the crime. The socio- economic and political structure of the society needs to understand the crime and the recourse that may curb the same. The preventive and corrective measures adopted by the machinery to control the crime and delinquent behaviour in the society are also taken into consideration while studying the nature and scope of a crime. The state machinery is not equipped with enough sources and knowledge to handle the modern crime. Computers have transformed the modern society beyond expectations in last three to four decades. It has made life not only convenient but has also immensely helped different sections of the world come closer socially, economically and culturally. The Computer technology has made it possible to have access to all corners of the world while sitting in a room. Modern technology has put an end to the barriers of time and space. However, unlikely with the remarkable merits of having computers today, due to this the jurisdictional issue has been created in legal system. Jurisdiction is one aspect which is very difficult to determine in transnational transaction over the internet. There was unmanageable ambiguity when courts were subjected to questions pertaining to jurisdiction law and were unable to decide the proper forum to entertain cases involving cyber crime as the cyberspace or virtual world is borderless if we compare it with physical world and that is why it is very difficult to control cybercrime. Through the local machinery we are not able to tackle the problem related with cyber crime because our machinery is not without compatible to deal with transnational crimes. The law applicable to the territory is not advanced enough to regulate the cyber crime as their nature is far different from the existing crime. Thus, the global dimension of cyber crime is made it difficult to handle and dealt with. The evolution of internet technology has given us so many advantages to deal with future problems and grow at a rapid rate but also it has provided the scope for criminals to commit their crime with least chance of detection. The concept of cyber crime has gained speed and we are facing great threat of its impact on world society. The human society is become vulnerable to cyber crime due to more and more dependence on technology. Cyber crime becomes a global phenomenon and hence the nationwide generalization of crime cannot workable in present scenario. Our understanding and regulation of cyber crime cannot be national but has to be international. We have to enact new laws and prepare preventive and defensive mechanism globally, only then we can able to protect our society from this evil called 'Cyber Crime'. Therefore, the threat of cyber terrorism throws serious challenge to world and its agencies. The terrorist organizations using technology to spread hatred among people and using it to recruit militants and train them using teaching tools. They are also launching websites which show them how to use weapons make bombs etc. As far cyber crime goes it is very difficult to determine the mens rea in cybercrimes. In Cyber crimes, one should see what the state of mind of hacker was and that the hacker knew that the access was unauthorised. Thus, a "Particular Computer" needs not to be intended by the hacker. Cyber crimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in

internet and computers and internet to commit such a crime. The people who have committed cyber crime are well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to tackle the perpetrators of cyber crime.

Classification of Cyber Crime:

Cyber Terrorism –

1. Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens. In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.
2. **Cyber Extortion –** Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.
3. **Cyber Warfare –** Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

Why are Cybercrimes Increasing?

The world is constantly developing new technologies, so now, it has a big reliance on technology. Most smart devices are connected to the internet. There are benefits and there are also risks. One of the risks is the big rise in the number of cybercrimes committed, there are not enough security measures and operations to help protect these technologies. Computer networks allow people in cyberspace to reach any connected part of the world in seconds. Cybercrimes can have different laws and regulations from one country to another, mentioning also that covering tracks is much easier when committing a cybercrime rather than real crimes.

Analysis of Cybercrimes in India:

India is the second largest online market in the world with over 560 million internet users, Ranked only behind China. And it is estimated that by 2023, there would be over 650 million internet users in the country. According to the latest national crime records bureau NCRB data, a total of 27, 248 cases of cybercrime where registered in India in 2018.

In Telangana, 1205 cyber crime cases where registered in the same year. According to FBIs report, India stands third among top 20 cybercrime victim. The national cyber crime reporting portal (cybercrime.gov.in) which was started last year by the central government received 33,152 complaints till now resulting in lodging of 790 FIRs. In fact, according to a 2017 report, Indian consumers had lost over 18 billion US dollars due to cyber crimes. In 2018, there were over 27,000 cases of cyber crimes

recorded in the country, marking an increase of over 121% compared to the number of cases two years back.

Total number of cybercrimes reported in India from 2012-2018

Year	No. of Cases
2018	27,248
2017	21,796
2016	12,317
2015	11,592
2014	9,622
2013	5,693
2012	3,377

Table:1 Source National Crime Records Bureau (NCRB)

The above table clearly shows the increasing number of cybercrimes cases in India. The top 5 popular cybercrimes are-Phishing scams, identity theft scams, online harassment, cyber stalking, invasion of privacy.

Conclusion:

Victims of cyber fraud find themselves armed with an arsenal of avenues through which they can seek redress. From the expedient act of lodging complaints with specialized units like the Cyber Crime Investigation Cell to enlisting the formidable aid of pertinent law enforcement agencies, the avenues of recourse are both accessible and multifaceted. Simultaneously, stringent cyber security guidelines mandated by the Reserve Bank of India (RBI) work tirelessly behind the scenes, meticulously fortifying financial institutions against the twin threats of data breaches and the specter of financial fraud.

Personal Data Protection Act:

On the horizon, the imminent arrival of the Personal Data Protection Act serves as a testament to India's unwavering commitment towards securing data integrity and safeguarding the bulwarks of privacy. With a steadfast focus on empowering individuals with greater control over their personal data, this Act stands as a beacon, taking significant strides towards striking an elusive equilibrium between the preservation of privacy rights and the facilitation of legitimate data utilization.

Empowering Through Cybersecurity Awareness:

As a proactive shield against the relentless onslaught of cyber frauds, prevention emerges as a potent remedy. Collaborative endeavors between governmental bodies, private entities, and the collective might of civil society play an indispensable role in fostering public awareness about the myriad of cyber threats that lurk beneath the digital surface. The nurturing of cyber hygiene practices and the fostering of

responsible online behavior emerge as pivotal measures that can substantially bolster the resistance of individuals against the snares of cyber frauds.

Remedies Against Cyber Frauds in India:

1. **Cyber Crime Investigation Cells:** One of the primary remedies against cyber frauds is seeking the assistance of specialized law enforcement agencies like the Cyber Crime Investigation Cells. These units are equipped to handle digital crimes and are well-versed in the intricacies of cyber investigations. Victims can report incidents to these cells, which will initiate investigations and take necessary actions against the perpetrators.

2. **Filing Complaints with Law Enforcement:** Victims of cyber frauds can also approach their local police stations to file formal complaints. It's essential to provide all relevant information, such as details of the incident, communication, and any evidence collected. This helps initiate legal proceedings against the culprits and potentially recover losses.

3. **Data Privacy Regulations:** The Personal Data Protection act in India aims to empower individuals with more control over their personal data. This legislation will require organizations to adhere to strict data protection measures, reducing the risk of data breaches that often lead to cyber frauds. By ensuring compliance with these regulations, individuals and organizations can mitigate the risks associated with data theft and unauthorized access.

4. **Strengthening Cybersecurity Measures:** Businesses and individuals should invest in robust cybersecurity measures to prevent cyber frauds. This includes regularly updating software, using strong and unique passwords, and implementing encryption protocols. Cybersecurity awareness training for employees and individuals can go a long way in thwarting phishing and hacking attempts.

5. **Two-Factor Authentication (2FA):** Utilizing two-factor authentication adds an extra layer of security to online accounts. This method requires users to provide two forms of verification before accessing their accounts. Even if a password is compromised, the additional layer of security provided by 2FA can prevent unauthorized access.

6. **Vigilance Against Phishing Attacks:** Phishing attacks remain a prevalent form of cyber fraud. Individuals and organizations should be cautious while interacting with emails, messages, or links from unknown sources. Avoid clicking on suspicious links or sharing personal information without proper verification.

7. **Legal Remedies:** The Information Technology Act, 2000, serves as the legal backbone in addressing cyber crimes. It defines offenses and penalties related to cyber frauds. Individuals and organizations can seek legal remedies by filing complaints under this act, leading to investigations and potential prosecutions.

8. **Collaboration and Reporting:** Timely reporting of cyber fraud incidents to law enforcement agencies and relevant authorities is crucial. Additionally, collaboration among individuals, businesses, and the government can lead to a collective effort in combatting cyber frauds. Sharing information about new threats and fraud techniques can help others stay vigilant.

9. **Blockchain Technology:** Blockchain technology's inherent security features can be harnessed to prevent cyber frauds. Blockchain's decentralized and tamper-resistant nature makes it an effective tool for securing digital transactions and sensitive information.

   Blockchain technology is a decentralized, distributed ledger that stores the record of ownership of digital assets. Any data stored on blockchain is unable to be modified, making the technology a legitimate disruptor for industries like payments, cybersecurity and healthcare.

10. **Cyber Insurance:** Considering the rising threat of cyber frauds, individuals and businesses can explore cyber insurance options. These policies provide financial protection in case of data breaches, ransomware attacks, and other cyber-related incidents.

    In conclusion, the battle against cyber frauds requires a multi-pronged approach involving technology, legislation, awareness, and collaboration. By adopting preventive measures, staying informed about the legal framework, and working together, we can navigate the digital landscape with resilience and security.

11. **Paving the Path to a Secure Digital Future:** In the relentless pursuit of a secure digital future, a multi-pronged approach emerges as the guiding star. A robust legal framework, fortified by the innovations of technology and the indomitable spirit of proactive engagement, emerges as the unyielding bulwark against the inexorable rise of cyber frauds.

    By seamlessly interweaving these multifarious elements, India can navigate the intricate labyrinth of the digital era with audacity and assurance. In this delicate dance, India can simultaneously safeguard its cherished citizens and nurture its thriving businesses against the multifarious perils that arise from the ever.

References:

1. https://cybercrime.gov.in
2. https://indianexpress.com
3. https://builtin.com
4. https://www.kaspersky.com
5. Digital Personal Data Protection Act 2023
6. Information Technology Act 2000
7. https://www.fortinet.com/resources/cyberglossary/cyber-insurance