MOL2NET, International Conference Series on Multidisciplinary Sciences
MOL2NET 2021, International Conference on Multidisciplinary Sciences, 7th edition

Cyber Security: Issues and Challenges in Covid - 19

Amrita Prakash
Assistant Professor, Department of Computer Science, Patna Women's College,
Patna, Bihar, India amrita.bca@patnawomenscollege.in

Ajit Singh
Department of Computer Science
Patna Women's College, Patna, Bihar, India

.

Abstract: A technology enhances a man's life in every aspect whether it is healthcare, transport, communication, education etc. During this Covid – 19 pandemic, the growths of technology usage have increased enormously. There are various issues and challenges which we face during the use of any technology. Security is the most important aspect, when we are using in any digital platform during Covid – 19. When we think about Cyber Security, the first thing that comes to our mind is "Cyber Crime" which is increasing immensely day by day. Cyber Security refers to the practice of ensuring the integrity, confidentiality and availability (ICA) of information. Basically Cyber security is the state or process of protecting and recovering networks, devices and programs from any type of Cyber Attack. It is comprised of an evolving set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access. Cyber-attacks in India have risen up to such an extent that our country ranks fourth out of the tenth targeted countries in the world. In this Covid – 19 pandemic Cyber-attacks are an evolving danger to many organizations, employees and consumers in different sectors. They may be designed to access or destroy sensitive data, change any kind of data or extort money. According to a Research, more than 50% of onliners are victim of some of cybercrime every year, which includes computer viruses, malware, credit card fraud, online scams, phishing, and identity theft and so on. These crimes will lead the country to lose millions of rupees or dollars, also time and expenses to put back the things in right directions. This paper mainly focuses on the different aspects of cyber security and the challenges faced in the implementation and by using latest technologies during Covid - 19. The paper also focuses on the India's legal framework for Cyber Security.

Keywords: Covid – 19, Cyber Crime, integrity, confidentiality and availability

Introduction

In this technological era, digital transmission of data is very common. This data can be of any form audio, video, e-mail, text etc. But when we transmit any data, the first thing comes into our mind is, How secure our data is? In 2009, compared to physical theft fraudulent money transfers has exceeded in bank branches of United States. Crimes have gone up by 60% every year, in 2012, 3500 cases and 2070 in 2011 reported in India. As Compared to other types of crimes, cyber crime is very common nowadays. It doesn’t require much investment and can be done in various locations simultaneously. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security.

Hence cyber security has become a latest issue as well as a challenge for all of us. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. We must enhance cyber security and protect our critical information infrastructures which are essential to each nation's security and economic wellbeing.

To fight against cyber crime we need a comprehensive and a safer approach. There are many technical measures alone which cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of critical information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

2. Cyber Security and Cyber Crime

The dictionary meaning says that Cyber Security is state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. There are various types of Cyber Security:

.

1. **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware. They prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
2. **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
3. **Information security** protects the integrity and privacy of data, both in storage and in transit. It avoids information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction
4. **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
5. **End-user education** involves educating end users with various information attacks and how to avoid them. For example, while registering password, tell end user what should be the length and characteristics of complex password.

.

2.1 Types of Cyber Threats

The threats countered by cyber-security are three-fold:

1. **Cyber-crime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyber-terrorism** is intended to undermine electronic systems to cause panic or fear.

2.2 Cyber Crime in Covid – 19 Pandemic period

There are 5 common trends which give chances to cyber crime:

1. More online transactions and digital data. Transaction and customer information, results of product launches, and other market information are easily available. Creating valuable intellectual property online is an attractive target.
2. Comparatively Corporations and companies are running their offices from home itself; therefore it is expected to be more transparent than before. Majority of people want to access to corporate networks through their mobile devices for day to day activities. Though smarter technology devices increases connectivity and but present latest types of security threats. Hackers can crack these securities and get an easy entry into corporate networks.
3. Malicious Software like viruses and spyware are strong enough to take the partial control of main applications.
4. In business, customer and vendors are joined to the networks to increase their business profits.
5. There is more technology advanced hackers, professional cyber crime organization. For example, hacker receives payment to infect end user device with malware. Today's Malwares are difficult to trace and they steal data for financial gain. Some people think that they get more money if they become hackers compared to securers.

3. Methods of Attacks and avoidance

The most popular weapon in cyber attacks is the use of computer viruses and worms. That is why in some cases of cyber terrorism is also called 'computer terrorism'[1]. The attacks or methods on the computer infrastructure can be classified into three different categories.

(a) **Physical Attack**. The computer infrastructure is damaged by using conventional methods like bombs, fire etc.

(b) Syntactic Attack. The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack.

(c) Semantic Attack. This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the user's knowledge in order to induce errors.

3.1 Security Attack is an attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems is known as security attacks.

Following are the types of security attacks:

(a) Active attack. When an attacker tries to break in an application directly it is known as active attack. There are a variety of ways this could be done, from using a false identity to access sensitive data (masquerade attack) to flooding your server with massive amounts of traffic to make your application unresponsive (denial of service attack).

(b) Passive attack. When an attacker tries to learn or get information from an application without causing any damage to it, it is known as passive attack.

3.2 Types of Risks

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

- Viruses - This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.
- Worms - Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.
- Trojan horses - A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it

will speed up your computer may actually be sending confidential information to a remote intruder.

- Hacker, attacker, or intruder - people who exploit weaknesses in software and computer systems for their own gain. Though they do it for curiosity, their actions are typically in violation of the intended use of the systems. The results can range from creating a virus with no intentionally negative impact to stealing or altering information.
- Malicious code - This category includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics.
- E-Mail Related Crime- Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.
- Denial of Service -These attacks are aimed at denying authorized persons access to a computer or computer network.
- Cryptology-Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption.

4. Need for Cyber Security in India

9.4% houses in India have computer (any of Laptop or Desktop). Chandigarh (U/T), Goa and NCT of Delhi are top three stats/union territories with highest computer usage. According to 2011 Census, Only 3.1 percent of total houses have Internet access in India. The census covered 24,66,92,667 (246.7 million) houses in India and found only 76,47,473 (3.1%) of this houses use Internet. The Internet includes both broadband and low-speed connections. According to Internet World Stats on June 30 2012, there were 2.4 billion internet users (2,405,510,175) worldwide. China was the largest countries in terms of internet users with over 538 million users [10]. The following graph(figure 1) shows top 20 internet countries worldwide at mid-year 2012:

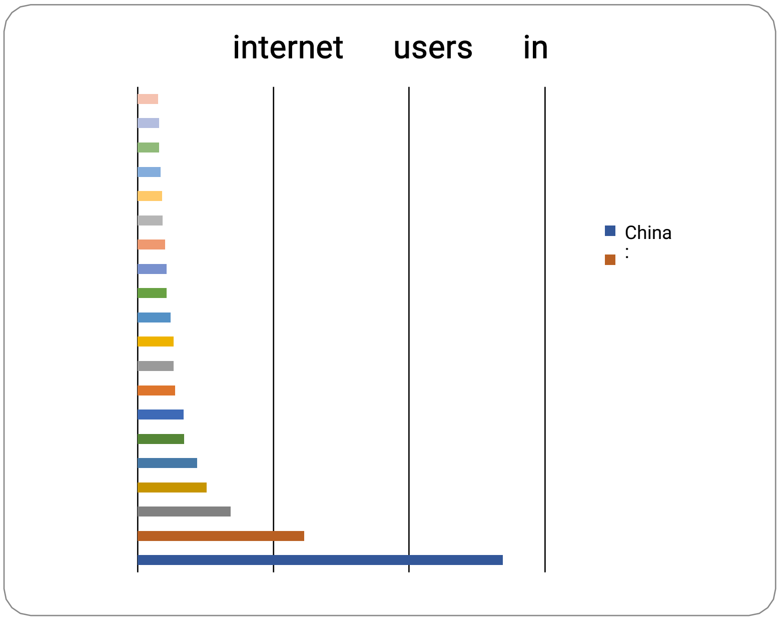


Figure 1: Internet usage in top countries world-wide at year 2012.

Following graph (figure 2) shows the growth of E-commerce in India; in 2011 it has reached 10000 million USD.

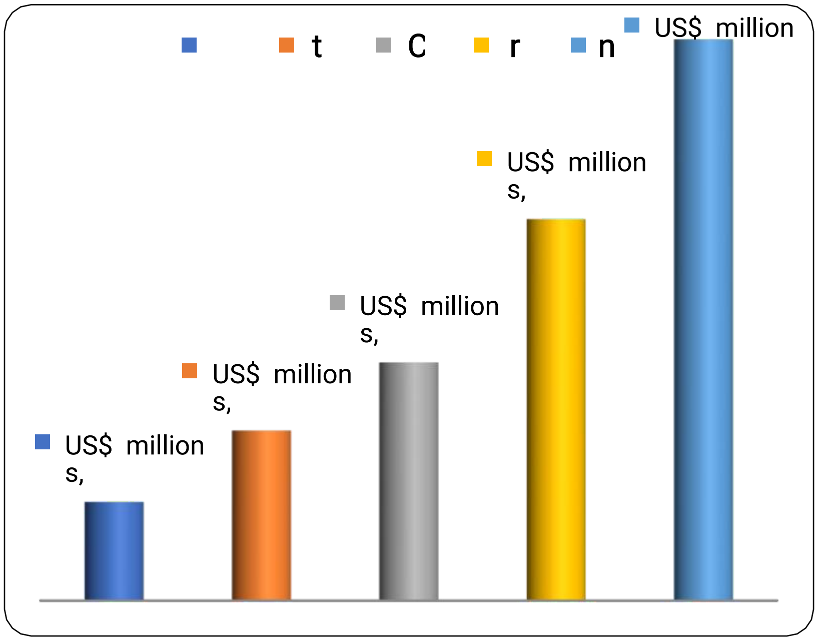
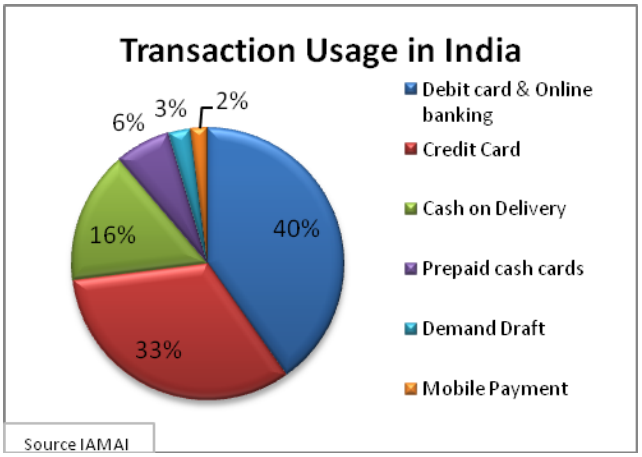


Figure 2: Increasing usage of E-commerce in India

Most of today's transactions are online. The following graph (figure 3) shows Indian payment type in the year 2012 according to which is online transactions is more [8].


Transaction Usage in India

Source IAMAI

Figure 3: Percentage of usage of different online payment methods in India

With all these statistics ensures that India as a fast growing country especially in the field of information technologies and E-commerce has a high alert for Security for its online channels to monitor over frauds and financial losses.[9]

5. Cyber security initiatives in India

ISO 27001 (ISO27001) is the international Cyber security Standard that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

According to Ministry of Electronic and Information Technology, Government of India : Cyber Laws yields legal recognition to electronic documents and a structure to support e- filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

5.1 Importance of Cyber Law:

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

5.2 Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. Fraud

   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

2. Copyright

   The internet has made copyright violations easier. In early days of online communication, a copyright violation was too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

3. Defamation:

   Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

4. Harassment and Stalking

Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

5. Freedom of Speech

Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

6. Trade Secrets

Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

7. Contracts and Employment Law

Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

5.3 India’s legal framework for Cyber Security.

1. Indian IT Act, 2000

   Section 65 - Tampering with computer source code, Section 66 - Hacking & computer offences, Section 43 – Tampering of electronic records

2. Indian Copyright Act

   States any person who knowingly makes use of an illegal copy of computer program shall be punishable. Computer programs have copy right protection, but no patent protection.

3. Indian Penal Code

   Section 406 - Punishment for criminal breach of trust and Section 420 - Cheating and dishonestly inducing delivery of property[4].

4. Indian Contract Act, 1872

   Offers following remedies in case of breach of contract, Damages and Specific performance of the contract

5.4 Other Indian Government Initiatives

Indian government released National Cyber Security Policy on July 2, 2013. This policy addressing the growth of information technology, increasing number of cyber crimes, plans for social transformation [4]. It has 14 objectives which includes enhancing the protection of India’s Critical infrastructure to investigation and prosecution of cyber crime, developing 50,000 skilled cyber security professionals in next five years.

- Cyber Security Research And Development Centre Of India (CSRDCI) - This concentrates on Techno Legal Cyber Security Issues of India and World Wide [3]. This Platform and Website is managed by Perry4Law, Perry4Law Techno Legal Base (PTLB) and Perry4Law Techno Legal ICT Training Centre (PTLITC)[8]. the Cyber Security Initiatives and Projects of PTLB at a single place.
- Cyber Crimes Investigation Centre Of India - The Cyber Crime Investigation Centre of India (CCICI) is the exclusive Techno Legal Cyber and Hi-Tech Crimes Investigation and Training Centre (CHCIT) of India[5]. The objective of CCICI is to

spread Cyber Law

Awareness and Cyber Security Awareness in India and abroad. Further, CCICI also intends to develop Cyber Crimes Investigation Capabilities and Expertise in India and abroad.

- **National Intelligence Grid (NATGRID)** - This Project of India is one of the most ambitious Intelligence Gathering Project of India. It has been launched at a time when the Intelligence Infrastructure of India is in a bad shape [7]. It is an essential requirement for robust and effective Intelligence Agencies and Law Enforcement functions in India.
- **National Critical Information Infrastructure Protection Centre (NCIPC) Of India** - intends to ensure critical infrastructure protection and critical ICT infrastructure protection in India.
- **National Cyber Security Database of India (NCSDI)** - This Database would work in the direction of fighting against Cyber Threats and Cyber Attacks including Cyber Terrorism Against India, Cyber Warfare Against India, Cyber Espionage Against India, Critical Infrastructure Protection in India, Managing India's Cyber Security Problems, Issues and Challenges, etc.

6. Challenges in Cyber Security

Cyber security has been considered as one of the most urgent national security problems. A report says, in a speech during his presidential campaign, President Obama promised to "make cyber security the top priority that it should be in the 21st century . . . and appoint a National Cyber Advisor who will report directly" to the President.

Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize a network in unpredictable ways.

The defense of cyberspace necessarily involves the forging of effective partnerships between the public organizations charged with ensuring the security of cyberspace and those who manage the use of this space by myriad users like government departments, banks, infrastructure, manufacturing and service enterprises and individual citizens. The defense of cyberspace has a special feature. The national territory or space that is being defended by the

land, sea and air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest.

7. Cyber safety tips - protect yourself against cyber-attacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1. **Update your software and operating system:** This means you benefit from the latest security patches.
2. **Use anti-virus software:** Security solutions like Kaspersky Total Security, Norton, Quick Heal will detect and removes threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:** Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:** These could be infected with malware.
5. **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
6. **Avoid using unsecure WiFi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.[11]

Conclusions

As there is a drastic growth in the digital transmission of data in this pandemic period, especially in e-commerce, internet or cyber security is a major issue in the growing countries like India. According to recent survey , which announced in TOI that India will require twenty lakh cyber security professionals by 2025 to support its fast growing internet economy as per an estimate by the Union ministry of information technology. The financial sector alone is expected to hire over 2 lakh people while telecoms, utility sectors, power, oil & gas, airlines, government (law & order and e-governance) will hire the rest. Employment news says - Based on academic background and work experience, ethical hackers can don the roles of network security administrators, network defense analysts, web security administrators, application security testers, security analysts, forensic analysts, penetration testers and security auditors. the job role would be to develop and test IT products and services of organizations and ensure that they are as secure as possible. Secure programming, authorized hacking and network security surveillance are specializations in this domain.

References

The following are the comprehensive list of resources-

[1] Col SS Raghav: " cyber security in india's counter terrorism strategy"

[2] http://www.cybersecuritycareers.com/

[3] CSRDCI: http://perry4law.co.in/cs.html

[4] Nandkumar Saravade, Director, Cyber Security and Compliance NASSCOM : Cyber Security Initiatives in India

[5] CECSRDI: http://perry4law.org/cecsrdi/?p=123

[6] http://techinasia.com

[7] en.wikipedia.org/wiki/NATGRID

[8] perry4law.org/cecsrdi/?p=735

[9] www.indiastats.com

[10] techcircle.vccircle.com › *Feature*

[11] https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security