Vision of Digitalisation in India and its impact on society and services

Dr. Nisha saini
Assistant Professor, Gargi College, Delhi University, Delhi, India

Abstract: Digitalisation in India laid the foundation of many new pathways in the field of education, healthcare, agriculture, banking and made them more accessible to the consumers. Telecom and IT sectors in collaboration with the government play a vital role in achieving the goals of digitalisation by providing internet facilities from urban to rural areas. It benefits every section of society and connects people to the entire world at a reasonable price. Nowadays everyone is highly dependent on digital technology for most work and it can be completed in a very less time with team work. Digital technology is still vulnerable to cyber attacks by various means and pose a threat to the government, consumers and service provider systems with a main aim of getting money from them. Although the government has taken many initiatives for cyber security, at the same time consumers should also be vigilant to prevent cyber frauds.

Keywords: Cyber attacks, Digitalisation, Initiatives, milestone

INTRODUCTION

Digital India is a flagship programme of the government of India launched in 2015 with the aim to provide all government services and connect the people of urban and rural areas together to make India a digitally empowered country. It is an umbrella programme in which digitalisation brought a drastic change in India and the number of internet users have increased to 1.2 billion in the past years. Internet connection in rural India is 41% as compared to 71% in urban areas which keeps on increasing. The main aim of digitalisation is to create digital infrastructure for digital services and digital empowerment of every citizen to improve the digital economy and reduce corruption. Central and state governments united together to bridge the gap between the urban and rural areas. The nine pillars of digital India are broadband highways, e-governance, e-kranti, electronics manufacturing, information for all, universal access to phones, public internet access programme, IT for jobs and early harvest programme which boosts the economy of India many fold.

Role of Telecom and Information Technology Sector in digitalisation

Telecommunication and Information Technology is the pathway for economic and social development of a country. Digitalisation is possible due to the collective efforts of the Government of India with the telecom and IT industries. It benefits both service providers and consumers to a great extent. With the increase in the number of users, hardware and software companies like Microsoft, Cisco, Google invest more in India. Companies like KPMG, E&G, PricewaterhouseCoopers, Accenture, shared their research techniques with the investors for digitalisation. Construction agencies like L&T and Reliance Infra provide infrastructure facilities such as nationwide fiber optic network and installation facilities.Both Telecom and IT sectors work together to provide connectivity to bridge the digital divide between the rural and urban areas.

IT industries design the software for all types of digital services like digital transactions, customer relationship management (CRM), enterprise resource planning (ERP) and many more with minimum error and make it available to numerous users at a time. Cloud computing allows users to keep the data on remote servers and that can be accessed as well as shared with others anywhere. Internet of things (IoT), Artificial intelligence, Augmented reality plays an important role in the various sectors from health to manufacturing processes. To reduce the cyber threats, the IT sector develops various security protocols, firewalls and encryption to protect the data from unauthorized attacks.

Telecom sector connects people worldwide with the digital infrastructure through telecom networks like broadband internet, mobile networks (3G, 4G, 5G), fiber optics, satellite communications and allows the data to transfer between different computers, devices and servers. 5G technology brings revolution by providing high speed internet to connect millions of devices simultaneously, making smart cities, smart homes, digital banking, e-Commerce, autonomous vehicles, e-healthcare to give the real time automation and monitoring of all the services. It helps in

expanding the businesses globally with digital tools on collaborative platforms like video conferencing, VoIP, cloud telephony and conducting virtual meetings. Apart from the above, the Telecom and IT sector helps in providing real time data collection and management of transport, energy, digital records, people engagement, digital learning platforms and public safety. Both the departments work together for the economic and social development of the country.

To provide digital services to every citizen, high speed internet connectivity is made available to even remote areas of the country. There are around 888 Mn broadband users in India as of September 2024 with 5, 90,020 Common Service Centres out of which 4,68773 are in rural areas.

Milestone for Making Digital India

1. Nationwide connectivity- All states, districts and villages are connected with each other through State Wide Area Network (SWAN) and Community Service Centre (CSC) under the National e-governance plan. The main aim is to provide all government services at affordable cost by using information and technological advancement. Department of electronics and information technology (Deity) develops a National Information Infrastructure to provide high speed internet connectivity for technological, administrative and e-governance perspectives using cloud computing techniques.

2. Universal Access to Mobile phones- The vision of universal access to mobiles is to enable the people of rural areas to utilize their full potential for the development of the nation by virtue of mobile networks. Out of 6 lakh villages, around 60,000 villages have no mobile coverage from any of the mobile operators in India. Moreover there are still many villages where they have mobile connection but the voice quality is very poor with almost no mobile data services. It creates a digital divide followed by an economic divide in the population of India. Telecommunication networks in rural areas will have a huge impact on healthcare, education, agriculture and government services.

3. Rural Public Internet Access- India has the fastest mobile growing market but it lacks behind in digital literacy. More than 70% of the population lives in rural areas and out of this 40% people are illiterate which is quite a good count to affect the economy of India. Thus growth of the internet is restricted in rural areas due to awareness among people, education and connectivity. To achieve the target of delivery of all electronic government services, the government joined hands with the telecom industry for providing internet connectivity through National Optical Fibre Network (NOFN) in rural areas with content in local languages also. As population density per square kilometer is very less in rural areas, it will not be financially feasible for companies so in return the government gives lucrative offers to them. To bridge the gap in digital literacy the government set up Community Service Centers (CSCs) to enable the people of rural areas to access the digital government services for their development and empowerment. There are approximately 1 lakh CSCs for 6 lakh villages which are self funded from the revenue of filling services. People can avail government services like banking, education, bill payments, agriculture and healthcare as well as apply for identity documents like Aadhar card, ration card, birth certificate etc. Although CSCs centers are in urban areas also but more beneficial for rural citizens due to unaffordable and limited network connectivity.

4. Electronic Governance - It played an important role in the implementation of electronic services in various government departments at local, state and national level. The main aim is to spread the mission mode project into every corner of India with the help of support infrastructure like SWAN (State Wide Area Network), SDC (State Data centers), CSCs (Common Services Centres) (CSCs). To achieve the target of e-Governance government participate in different ways i.e. G2G (Government to Government), G2B (Government to Business), G2C (Government to Citizens) and G2E (Government to Employees).

Initiatives of Government under digital India programme

1. Digilocker- It is a digital wallet and cloud based application to save official documents like Aadhar card, PAN card, driving license, birth certificates. The uploaded documents can be accessed anytime and from anywhere. All these documents are legally valid, safe as per information technology act 2000 and are considered as par with the physical documents. It also provides a link to receive documents from the partners associated with digilocker and all these documents are issued by government departments. E-signature for self

attestation is a completely secure process to sign the electronic documents as Aadhar card and digital signature are both linked to each other. The digitalisation reduces the risk of fraud of false documents, allows easy online verification in less time and cuts down the administrative work for the verification of documents. The individual can avail free storage space of 10MB and maximum to 1GB. Verification agencies can directly verify the issued documents after taking user consent. Only Aadhar card users can use the facility of digilocker and NRIs can not make an account as their number is not registered in India.

2. Digital Identity - Earlier voter card, ID card, driving license, PAN card, passport and ration card is used as identity proof but the application and verification process is different for all these identity proofs. Government planned to give national identity proof of a unique biometric identification number for every citizen of India. It was launched by The Unique Identification Authority of India in 2008 and 12 digit numbers are given to all the citizens on the basis of biometric scanning which is unique for everyone. All the public and private services like banking, education, finance, healthcare etc, can be availed after giving aadhar card and it also becomes easier for the government to keep a complete record of all the citizens. But the UIDAI can not share the personal data to any service provider without the consent of the individual.

3. e-Hospital- It is an online portal which works on an online registration system (ORS) where people can apply online in government hospitals with an Aadhar card across various states and union territories. Citizens can avail the facility of online appointment with a doctor of their choice, facility of blood, bed and availability of lab reports from the list of hospitals given on the portal. The patients from the rural areas benefit most from this program as they have to travel a long distance and many times have to face failure. Any Indian citizen with an Aadhar card can book an online appointment and the hospital will provide a Unique Health Identification Number from where the whole health record of the patient can be accessed. More than 500 hospitals have been enrolled in the list of e-Hospital in India and around 1 crore health cards are linked to make a seamless digital record of patients throughout the country. e-Health campaigns also make the people more aware about the diseases, vaccination and Ayushman Bharat Mission etc. during the covid-19 Aarogya Setu App and CO-WIN App helped all the people to fight with covid, what are the preventive measures, how many cases in their neighborhood, when and from where to get vaccinated for the deadly disease.

4. e-Pathshala- The main aim of this portal is to support the Samagra Shiksha Abhiyan, improve the quality and accessibility of education and it is initiated, developed and maintained jointly by MHRD, CIET and NCERT. To improve digital literacy, improving methodology all schools are connected with broadband and free wifi is provided in all primary and secondary schools. Learning material is available for students, teachers, parents and researchers in the form of NCERT books, audio video resources, periodicals and teacher training modules. The material can be downloaded for offline use with no limits on downloads. DIKSHA (Digital Infrastructure for Knowledge Sharing) is an initiative of NCERT under the Ministry of Education where educationists, experts, government and non-government organizations participate to provide learning material in the form of quizzes, question bank,content and QR code embedded textbooks which are useful for students of school level. The Ministry of Education also developed the SWAYAM portal which is an online learning platform for undergraduates and postgraduate students of various disciplines. The content is prepared by the teachers in the form of video, reading material, self assessment through quizzes, tests and online discussion forum for clearing doubts to enrich the learning experience.

5. e-Kranti- The mission of e-Kranti is to electronically deliver all government services to all the citizens in an integrated manner with transparency and efficiency at reasonable cost. This becomes possible with good connectivity and cloud technology for all government departments. Online services given to people are like e-healthcare, information to farmers, information for disaster related emergencies, e-Court, e-Police, , mobile banking etc. The other public utility portals include filing a RTI against government or government organization and filing of income tax forms become so easy that people will get the almost prefilled form from their employer. All government services can be accessed by people through mobile in Indian languages as well. The National GeoSpatial Information System is strengthened for all e-Governance services.

6. BHIM- On 8 November 2016. Government declared the demonetisation of 500 and 1000 Rs from

the market to stop the corruption and black marketing. To promote the digital transactions government launched BHIM App (Bharat Interface for Money) on 30 December 2016 which is a mobile payment application based on Unified Payment Interface for immediate payments directly through the bank unlike the Paytm, MobiKwik wallet which holds the money before transfer and supports all Indian languages. Now everyone from fruit sellers to businessmen accept the payments through UPI.

7. e-Marketplace (GeM)- This online platform provides 11.282 products and 329 services to connect buyer to seller by government departments and organizations to bring transparency. It was launched under the Ministry of Commerce on 9th August 2016. Products include handicrafts, handlooms, millets, personal care, groceries, printers, printing cartridges, laptops and medical equipment etc. Services include security, chauffeur, gardening, consulting and engineering etc. Government provides training to sellers throughout India by the central training team to sell the products as per rules and regulations of GeM and gives the list of the suspended sellers to avoid any dispute. It is similar to Amazon. Flipkart has similar features but is governed by the Indian government and made mandatory by the Ministry of Finance to make purchases by government users through the GeM portal only. It provides the options of e-bidding, reverse e-auction to facilitate the government users to get best value for money. It encourages MSMEs and startups to do business with the government. Government does not own the goods but the seller holds the responsibility of quality and timely delivery of products and buyer is responsible for timely payment of the purchase made. All e-bids and reverse auctions completed by the government through the GeM portal without any third party.

8. My Gov - The main aim of this website "mygov.in" is to reduce the gap between government and Indian citizens for the formulation of policies and country development. It is also very popular like other social media platforms Facebook, Twitter. It allows the citizens to give their ideas to the government through discussions, talks, blogs, surveys, pledges, quizzes, competition, campaigns, vlogs, selfies. mann ki baat on this platform for the topics of public interest. Government can understand the people's opinion and take action accordingly.

9. Umang App (Unified Mobile Application for New-age Governance) - This is the digital India initiative of the government which is developed by the Ministry of electronics and Information technology along with National e-governance division to provide a single platform to Indian citizens to access central and state government services. 80 central and 127 state government departments provide around 2044 services to people related to travel, health and wellness, travel, social security, pensioners, birth certificates, e-District, passport, e-Panchayat, public grievances, agriculture, DBT scheme for scholarship, bill payments, education, youth skills and employment etc. Delhi Metro, AICTE, Indian railways, India meteorological department, ABHA, NHAI, Aadhar, PAN EPFO and many more are here. It is available in 23 Indian languages.

10. e-Sampark - It helps to connect the government directly to citizens by mail or messages for sharing national information about public services, policies and campaigns. Users can get the information in their regional languages as well.

11. e-Sign - It facilitates the users to sign the documents in online forms and documents and this application is based on OTP authentication.

12. Meri Pehchaan - National Single Sign -On (NSSO) is a user authentication service in which a single set of credentials are required to get access to multiple online services. It saves the user time, effort and they are also not required to prove the identity for every application.

13. RTI - It is the fundamental right of every Indian citizen to know the information about the government system and processes. Any person can file an RTI appeal to any central and state government department by filling an application form and submit the request with a minimal payment of 10 rs to the respective department. People who are below the poverty line and filing an rti appeal for the first time are exempted from the fees. Person should also state the reason for filing an RTI and attach the necessary documents if required. Application is first received by nodal officers of the concerned department and transferred to a specific central public information officer to furnish the required information within 30 days of appeal.

14. Income Tax Filing - It is an online platform developed by the Income Tax Department for taxpayers to file their income tax returns and eliminate the requirement of submission of hard copy. Process

becomes easier for the individuals working in government departments, PSUs and other organizations as they get pre pre-filled form from the employer. The income tax return form can be submitted as such if they do not have any other source of income and can also pay the extra tax by netbanking. It also allows the taxpayers to check the status of their return and refunds. Everyone can fill the income tax return form as it provides detailed instructions, guidance and even helpline desk for any difficulty. It is very important to keep the login credentials secure to prevent unauthorized access to the tax information.

Benefits of digitalisation

1. Collaborative Platforms- Collaborative platforms like Zoom, Google Meet, Microsoft Teams, Video Conferencing are the virtual online platforms where multiple users can work together on a document, spreadsheet and presentations for sharing ideas, giving suggestions, getting quick replies, updates on status of work, better communication and promote teamwork in a real time. These platforms are used in all the offices which helps them to save time, seamless teamwork, reduce paperwork and less expenditure on physical infrastructure as employees can work from home which enhance the creativity and productivity of the individual.
2. Industry- The Indian Government alone can not provide the service to such a large population, so it participates in private partnership. With the increase in the demand of internet users, India became the place of huge investment and employment in this sector which therefore provides more job opportunities for people. Improved internet connectivity benefits the telecom and Mobile companies due to increase in the demand of mobile phones as India's population is highest in the world.
3. Monetization- Any individual can express his experience, opinion, creativity in any field and even can do marketing of their products through Blogs and Vlogs in the online platform. Bloggers have good writing skills and Vloggers expert in making high quality videos but the content should be authentic. Vlogging platforms are like Youtube, Instagram, Facebook etc whereas Hubspot, Wix, WordPress, Bloggers are Blogging platforms. Bloggers and Vloggers can earn income from their followers, advertisements and sponsorships.
4. Reduce Paper work- Due to online filing of forms in all sectors, online transaction, online messages, digital board etc requirement of paperwork is reduced many folds which helps in making our environment more cleaner.
5. Digital empowerment of citizens - Every citizen irrespective of education becomes so mobile friendly to access all the digital services in a click.
6. Save Time - All digital services can be availed at the ease of home without going anywhere, thus saving a lot of time which can be put into useful purpose.
7. Digital Delivery of Services - It is not required to go to any office for filling any form or document and even not for shopping.

Cyber Attacks

Digital system is easily penetrable not to the individual but at the national and international level also, as it affects the critical infrastructure like communication network, financial system, transportation, health services and power systems etc. and increasing cases of cyber attack support the need to take necessary steps and formulate guidelines to prevent hacking. The rapid digitalisation in the world when every data is available on cloud, social media platforms and shared with customer service providers makes the personal details like name, phone number, aadhar card number, address etc so vulnerable that it can be very easily misused by cyber criminals . In India the number of internet users is expected to go beyond 1000 million by the year 2026 which further increases the chance of cyber frauds many folds. It is not an individual problem but all the service providers are also vulnerable to cyber attacks. The virus attacks the system to disable the security software to get access to it and steal the important data. These cyber attacks are also called ransomware attacks as the attackers demand a heavy amount, threaten the organization to leak the data and for reputation the company has to pay the amount in terms of money or bitcoins. Worldwide there are many cases of cyber attacks:

1. Gundermmingen which is the highest output nuclear power plant of germany got infected with a computer virus W32 called Ramnit which has the potential to shut down the plant.
2. In August 2018 cyber attack on Cosmos Cooperative Bank Pune led to unauthorized transactions which caused a significant financial loss to the bank.
3. In 2018 numerous cases of data breach linked to Aadhar card came into notice like name, contact number, address which poses a serious threat to the people of India.

4. In 2017 cyberattack called WannaCry ransomware attack affected around two lac computer systems which are outdated and highly vulnerable to attack of government agencies, banks and healthcare facilities. After this attack everyone understood the necessity to update the computer system regularly.
5. In 2023 health services came to halt in AIIMS hospital Delhi as patient data was hacked which caused the server shutdown.
6. Malicious virus attacked the broadband systems of BSNL and made 60 thousand broadband modems malfunctional.
7. Power systems of Telangana, Andhra Pradesh and Uttar Haryana Bijli Vitran Nigam were hacked by the attackers and they demanded a ransom from the government.
8. In 2013 around 1 billion Yahoo and in 2019 500 million Facebook accounts were exposed and made the user's data public and these are the largest hack in the history of the internet.

Types of cyber attacks

1. Phishing Mails - In this attack the attacker sends the virus through email in the form of a link which seems to come from a legitimate source. When a victim clicks on the link, it downloads the virus on the system and steals the sensitive information. Messages will be received like this in the mail. "My package wasn't delivered".Is this actually FedEx? Attackers will attach the link to reschedule the visit on your mail. This link will take the customer to a different URL which can create a big problem. Copy and paste the Tracking Id into the FedEx system and also check the return address, if it is not recognised then it is fake. Do not click on anything that looks suspicious and check the "Reply Path" whether it goes to the same mail id or different.
2. Whale Phishing Attack- The virus attacks the system through mail in the form of a link but the target is the big shot of an organization who keeps all the crucial information about business.
3. Spear Phishing Attack- Normal phishing targets the masses of people whereas attack in spear phishing is on a selected one. The attacker made a research on the interest of a specific target related to their personal and professional life, sent the relevant messages which seems to be from legitimate sources and can be trusted very easily. It can be through email, text messages, whats app or phone calls and the attacker already got the information about the target name, bank details, hobbies, family friends etc.
4. Denial of Service (DoS) attack- This attack is designed to overwhelm/shutdown or disrupt the website to an extent that it is unable to reply to legitimate requests. If a website can accept 100 requests per minute or 100 people can access it in a minute then DoS sends the 100 illegitimate requests in a minute so the legitimate requests will not be entertained by the website. Thus the victim site is unable to provide the services to the actual user as it is overloaded with fake users which results in complete shutdown of the site. These attacks can be stopped by using firewall or cloud based DDoS protection services, as they can detect whether the request is fake or real.
5. Man in the Middle (MITM) - It is called 'Man in the Middle' attack because the middleman modifies the data communicated between two people and they feel like they are communicating with each other. Middlemen can act as an official from the bank to fetch the required information from the target and also send irrelevant messages to malign someone's image. It is also an example of an eavesdropping attack.
6. Hash Attack- Hash algorithms are used to verify the authenticity of messages by converting the input into a fixed output. For example for cyber security the password on any platform is saved in terms of hash value which is fixed for a particular input. If the password matches with that hash value then only that web page will be opened. Even a slight change in input can change the hash value. But if the hacker is able to create a similar hash value then the hacker can access that application. It is always advised to use a strong password which will make the hash value longer that can not be easily hacked.
7. Brute Force Attack- The attacker makes a number of uneven attempts to fetch the login details of a victim and it is a time consuming process to access the secure data. It can be prevented by freezing the account with the "Lock Out" policy where the account will not be allowed to sign in after a few attempts.
8. Ransomware- The attacker sends the malware to the computer system of a single or multiple target and target can be individual, multinational company or government organizations. It is given a special name "ransomware" as the attacker demands for money in lieu of it.
9. URL Interpretation- In this attack hacker may get access to the desired site by URL interpretation and do required changes to the site and also steal information about the users. If the URL is very easy to target like StayHappy.com then the attacker can get entry to the admin login page by typing

http://StayHappy.com/admin. Access to the admin password can be obtained by brute method or through someone else. To prevent this attack, use multifactor authentication for the site.

10. Domain Name System Attack- Attack can easily be done on the vulnerable sites, hacker alter DNS system and direct it to send the data put in by user to fake site which seems to be legitimate to the user to steal their information and ruin the name of the company. To avoid this attack DNS servers should be updated regularly.

11. Session Hijacking- It is quite similar to the man in the middle attack but the attacker uses its IP address. If the meeting is going on between two parties like customer and company then the attacker substitutes its IP address for the customer computer and the meeting is now continued between attacker and company. If the attacker inserts its IP address between the session then the breach will not be noticed because the server is already engaged in the trusted connection.

12. Web Attacks- Web attacks occur when the web application is vulnerable to any changes. Whenever we are using any such application, some information is to be entered to perform any activity like using UPI, filling forms, paying challans/ electricity or water bill etc. The attacker changes the script to get access to login credentials for using that web application like a legitimate user. Some common web attacks are- SQL Injection, XSS, CSRF.

13. Trojan Horses- In this attack malware is hidden inside the legitimate software and when the user executes the program, the malware inside the trojan makes an alternate way for the attacker to do the desired changes on the system. To prevent it one should verify the source before installing anything on the computer.

How to prevent cyber attacks

Our lives have changed in many more ways than it was 20 years back. We are too much dependent on the internet for everyday chores but at the same time we should be very much careful while using the internet and its services to prevent cyber attacks.

1. A secure website URL always begins with ‘https:// rather than http:// where ‘s’ stands for secure. HTTP transfers data in plain text whereas HTTPS in encrypted text.
2. Timely keep the software updated on your system.
3. Install a firewall in the system which prevents it from network attacks.
4. Always scan others USB before using it on the computer as it may contain infected files.
5. Keep the wifi network always secure with encrypted password and virtual private network (VPN). VPN encrypts all the data and hackers will not be able to make any conclusion from it. It is advisable to use VPN while accessing public wifi.
6. Never store password on browser.
7. In an organization employees get a common pattern of mail Id and password, it should be changed regularly in every month.
8. Use a strong password of more than 10 characters with special characters.
9. Do not open email from an unknown email address.
10. When not required disable bluetooth and automatic connection to networks.
11. Do not let Apps and Websites remember your name.
12. Use different passwords for different accounts.
13. If a person suspects that he was caught up in a cyber fraud then immediately file a FIR at the police station.
14. Always keep a backup of data.

Government steps to prevent cyber fraud

Government has taken many initiatives for the cyber security:

1. The Indian Computer Emergency Response Team (CERT-In): The CERT-In plays an important role in protection against cyber attack by providing guidelines and conducting online public awareness campaigns. It also helps in resolving cases of cyber attacks like data breaches and denial of service attacks.

2. Cyber Surakshit Bharat: The Cyber Surakshit Bharat was launched by the Ministry of Electronics and Information Technology (MeitY) with National Electronic Governance Division (NeGD) to make government and industry representatives more aware about the latest cybercrimes, cybersecurity challenges and the ways to protect the digital system from cyber attacks.

3. Cyber Swachhta Kendra: The Cyber Swachhta Kendra focuses on detecting and removing malicious botnet programs from computers and devices. It works in collaboration with internet service providers and antivirus companies and provides free tools to users to secure their systems from malware attacks.

4. National Cybersecurity Policy: The National Cyber Security Policy is an initiative of the

government to reduce cyber threats to build the trust of users on the digital services, particularly transactions through a strong regulatory framework. It also helps to protect other critical infrastructure like Power & Energy, Banking, Health services, Financial Services & Insurance, Telecom, Transport. The Indian Government has made guidelines for chief Information security Officers (CISOs) of all government organizations for protecting apps and infrastructure. They also find security measures to be taken with every new technical innovation.

5. National Critical Information Infrastructure Protection Center- It has been established to protect the critical sectors like banking, energy, telecom and health services from the cyber attack. If all these services get disrupted it can adversely impact the security and economy of the country.

6. Digital Personal Data Protection Bill 2023- India has a framework for the personal data protection which include age, gender, name, address and identification documents like aadhar card, official id, driving license. Data can not be processed without consent of an individual and should be erased after the expiry of consent except when it is required for legal purposes.

7. Vishvasya-Blockchain Technology Stack - The government of India is using the blockchain technology for national security in the sectors of insurance, finance, e-governance, e-Sign, digilocker, Aadhar, e-pramaan and many more services. It helps to protect the data of government sectors, individuals, businesses from cyber attacks and build the trust of users on the digital services. It has a decentralized digital ledger that stores data in blocks which are linked together in a chain and data can not be modified or deleted without the consensus of the network. It has an in-built system to prevent unauthorized entries. It is highly resistant to cyber attacks and eliminates the single point of failure as hackers have to gain control of the entire system which is never ever possible.

However all the above policies are not that efficient due to the lack of manpower, trained officials, cyber forensic facilities, cyber security standards and coordination among various organizations. India needs to invest more for cyber security by involving private partnership and collaboration with international organizations like the United Nation, International Telecommunication Union and Interpol.

Ethical Issues in Cyberspace

Technology should be for the benefit of the society without any of its consequences but now the people become more prone to online threats in different ways. Some of the ethical issues in technology are given as-

1. Breach of personal data- With the rapid digital transformation, everyone is dependent on the online mode of working for all the activities like filing of online forms, paying household bills, shopping online. When browsing online shopping sites, social media platforms and many others, it always asks for more information like mail id, password, access to photos from the mobile, accept the cookies etc. Companies want to know more about their customer choices and area of interest to provide more refined research with more options. Sometimes the people are in a hurry or unaware of the consequences or believe so much on the site, then problems arise regarding the security of their account. Actually to maintain one particular site, in certain cases third parties are involved which increases the chances of breaching of Personal data.

2. Misinformation- In today's world when anyone can spread information or misinformation in one click, everyone should be more attentive. Information spread through the internet does not undergo any check, so there are higher chances of its distortion. Technology like artificial intelligence allows manipulation with digital images and videos which can twist the person saying, we believe in it without checking facts. If it is related to a political agenda, then it has the potential to create havoc in the society.

3. Lack of accountability- When business involves third parties for data governance, then there are high chances of mismanagement of data for which no one will take the responsibility.

Ethical practices to be followed by Industry

1. In this competitive era, every company wants to excel in the field of technology but before implementing technology, they should inspect all the potential risks associated and work on its ways of mitigation. It helps in building trust in the companies which can further increase the customer base for their business. For extension of business, collaboration should be with the vendors who have a good name in following ethical principles and guidelines.

2. Companies should value their employees and take care of their rights because they are the direct point of contact of customers. Protection of employees helps in the protection of customer data.

3. Organizations should maintain some ethical standards and Guidelines for data privacy and transparency. A single piece of information, even if it

is not very important, should never be revealed to anyone. They have to organize sessions on the ethical culture and its impact on business for their employees in a regular period.

4. It is important to take feedback from the customers, conduct audits and review the technology to keep a track on it.

5. Companies should never give false information about their products or services.

Ethical practices to be followed by Individual

It is very important to have etiquette in the world of the internet, as it is not between a few people but the entire world, so everyone has to be mindful of browsing social media platforms. Good etiquette gives respect and fame in the digital world but at the same time everyone should follow a few practices .

1. It is good if individuals want to share information that has potential to help others but there should not be hidden tricks. If it is not completely true and others are following it as such, it can have serious consequences.

2. Avoid personal attacks and do not try to defame others while using social media platforms. Once the truth is revealed, it will be very difficult to build an image again.

3. People usually go for a free App or software and install it without checking its authenticity and advise the same to others. It can steal or corrupt the data on your device, so always check the legal requirements of such an App.

4. We should not blindly follow the shared information and make comments on it, it has to be verified from other sources. Even if a person deletes the content, it can be stored by others and shared further in future to malign your image.

5. Always read the content before forwarding it to others.

REFERENCES

[1] Priyadarsini, K. and Vijayaratnam, N. “Digitalisation of India : Smart Villages towards Smart India” International Journal of Innovative Research in Information Security, Vol. 9(3), pp 33-37, 2016.

[2] Gulati, M. “Digital India : Challenges and Opportunities,” International Journal of Management, Information, vol. 10(4), pp 1-4, 2016

[3] Gupta, N and Arora, K. “Digital India : A Roadmap for the development of Rural India,” International Journal of Business Management, vol. 2(2), pp 1333-1342, 2015

[4] Kumar, S. “Digital Empowerment : Need and Challenges in 2023,” IOSR Journal of Business and Management, vol. 25, pp 44-49, 2023

[5] Sharma, J. “Digital India and its impact on society,” International Journal of Research in Humanities and Social Sciences, vol 4(4), pp 64-70, 2016

[6] Saeed, S., Altamini, S., Alkayyal, N., Alshehri, E. and Alabbad, D., “Digital Transformation and Cybersecurity Challenges for Businesses Resilience : Issues and Recommendations”, Vol 23(15), 2023

[7] Uddin M.H., Ali, M. H., Hassan, “Cybersecurity Hazards and Financial system vulnerability : A synthesis of Literature”, Risk Management, Vol 22, pp 239-309, 2020

[8] Belkhamza, Z., “Cybersecurity in Digital Transformation applications : Analysis of past research and future directions,” International conference on cyber warfare and security, vol 18(1), pp 19-24, 2023

[9] Baig, A. Z., “Future Challenges for smart cities : cyber security and digital forensics,” Digital Investigation, vol. 22, pp 3-13, 2017

[10] Li, Y. and Liu, Q., “A Comprehensive review study of cyber attacks and cyber security ; Emerging trends and recent developments,” Energy Reports, vol. 7, pp 8176-8186, 2021