SECURING DIGITAL SOVEREIGNTY IN THE CONTEXT OF PRESENT DAY CHALLENGES OF CYBER SPACE

ABHAY KUMAR

Roll No. 4517

(A dissertation submitted for the degree of Master of Philosophy in Social Sciences of the Panjab University, Chandigarh)

Under the guidance of

Guide: Dr. CHARRU MALHOTRA

45th Advanced Professional Programme in Public Administration

INDIAN INSTITUTE OF PUBLIC ADMINISTRATION, NEW DELHI
2019–20

CERTIFICATE

I have the pleasure to certify that **Mr Abhay Kumar** has pursued his research work and prepared his research work and prepared the present dissertation title "Securing Digital Sovereignty: In the context of Present Day Challenges of Cyber Space" under my guidance and supervision. The dissertation is the result of his own research and to the best of my knowledge , no part of it has earlier compromised any other monograph dissertation or book.

This is being submitted to Punjab University, Chandigarh, for the purpose of Master of Philosophy for social science in partial fulfilment of the requirement for the Advance Public Programme in Public Administration (APPPA) of the Indian Institute of Public Administration (IIPA),New Delhi.

I recommend the dissertation of **Mr Abhay Kumar** is worthy of consideration for the award of M. Phil degree of Punjab University , Chandigarh.

(Dr. Charru Malhotra)
Supervisor
Indian Institute of Public Administration (IIPA),
I.P.Estate ,Ring Road ,
New Delhi-110002

Acknowledgements

This study would not have been possible without the constant guidance and inspiration of my supervisor **Dr. Charru Malhotra**, Associate Professor, Indian Institute of Public Administration (IIPA), New Delhi. To her , owe patience , perseverance and training in meticulousness and organisation .The Love with which she guided me was a lesson in itself .

This study owes a huge debt to the officers of European Country ,USA , China , whose written work has helped me lot . I would also like to thanks different IT professionals working in developed country and India, whose written article has imparted indebt knowledge about the works of different aspects of Digital Sovereignty. And also to all 188 respondents who contributed lot in registering their responses. I also appreciate the help and co-operation extended by all staff of APPPA Office and other supportive staff of Library.

However , the greatest contributions to this work is undoubtedly goes to **Dr. Charru Malhotra**, **Mr. Neeraj Arora**; Advocate ,Dr. Mathur ,, Mr P K Singh, Mr. Surya Prakash, all my APPPA friends and many others.

Finally I dedicate this work to my children , Miss **Ashmita Rai and Mr Abhijeet Rai** without their emotional support it would have been difficult to complete this work.

Securing Digital Sovereignty

In the context of Present Day Challenges of Cyber Space

Table of Contents

Table of Figure

Table of Table

ABSTRACT

The entire world is witnessing a real confrontation between control and freedom, not only of the individual, but of entire populations and regions, enhanced by technologies and massive collection and analysis of data using AI and data Analytics from predicting and influencing behaviours, to the automation of public services and the ability to fully control and disrupt those services, even remotely. By breaching the security and gaining access to a global communications platform to losing the ability to protect the rights of those who are interconnected through those platforms. Are we witnessing a new form of digital colonialism? This article focuses on securing digital sovereignty in the scenario of complex architecture of cyber space with full of vulnerabilities and threats , thus challenging Protection and Security of Data . The regional, national, and community solutions to restore control and ownership on key information and communications infrastructures—the only possible first step to fix the current massive violation of privacy rights. It will later suggest some local measures to experiment with and advance alternatives at different levels of intervention and action, including proactive policy, capacity building, and new designs inspired in a set of values and principles different from those of the dominant actors in the market. Digital sovereignty is all about storage and protection of individuals personal data in digital form on cloud along with ensuring the right of privacy is secured.

Digitisation of data makes it easy to duplicate, easily portable, large data storage and innovative solutions. However most of the data is stored in the public cloud and the data storage centres are not located within the country from where the data is uploaded. It raises great concerns as security challenge for individuals, government and IT professionals. The concept of data sovereignty thus demands that the countries have their own data centres so that all the government related data from state and central departments, as well as individual's personal data stored in cloud storage networks, should be located in servers within the country and not in foreign countries. The proponents of Digital sovereignty within India call for it for not only projects such as Digital India and Make in India but also for security and well-being of the country. For example, the Digital India initiative seeks to provide delivery of public services related to health, education, banking etc. via e-governance mode to citizens from metros to gram panchayats. Towards this, there would be a need to upload huge

information in digital form on the cloud (such as beneficiary data, biometric information of beneficiaries and so on). Thus, if there is absence of strong data security, it can be a recipe for disaster. Similarly, there is a need to reap the digital dividend of faster growth, more jobs and better services by expanding affordable and safe Internet access to all. This can help India to be a breakout nation {a breakout nation is one that can grow faster than rivals in their income class, and expectations for that class}. But leveraging the information technology needs data security and thus importance of data sovereignty is underlined in efforts to eradicate poverty and misery also.

This apart, Data Sovereignty also has its importance for Make in India initiative. This initiative tries to promote the local production of goods by not only domestic but also the multinational. The MNCs demand a high IT standards and digital safety to start and run their business. So, low IT standards and undermining the digital data safety, may act as major barrier towards Make in India also. Towards infrastructure, there is a need to build and maintain strong data centres (SDCs). Towards policy measures, following can be suggested:-Use of legal and regulatory frameworks to cloud computing and data sovereignty. Restrictions on transfer of critical information related to health records, financial transactions and tax returns would to countries deemed unsafe or lacking in data protection laws. Government can use licence regime for the cloud providers on conditions that the foreign company if want to provide service in India, is required to open local data centres in India. India needs robust Cloud Policy and Secure element production . Personal Data Protection Law with Data localisation issue. Along with capacity building with cyber awareness and cyber safety for mass with research and innovation in technical institution.

1 INTRODUCTION

"It's the biggest, most complicated, and most interesting issue that we've ever faced, I think outside of blowing ourselves off of the face of the Earth. Climate change is the single most important issue economically, politically, socially, diplomatically – I mean it's got everything involved in it."

~ Timothy Wirth, Under Secretary of State for Global Affairs, US, 1993 – 97.

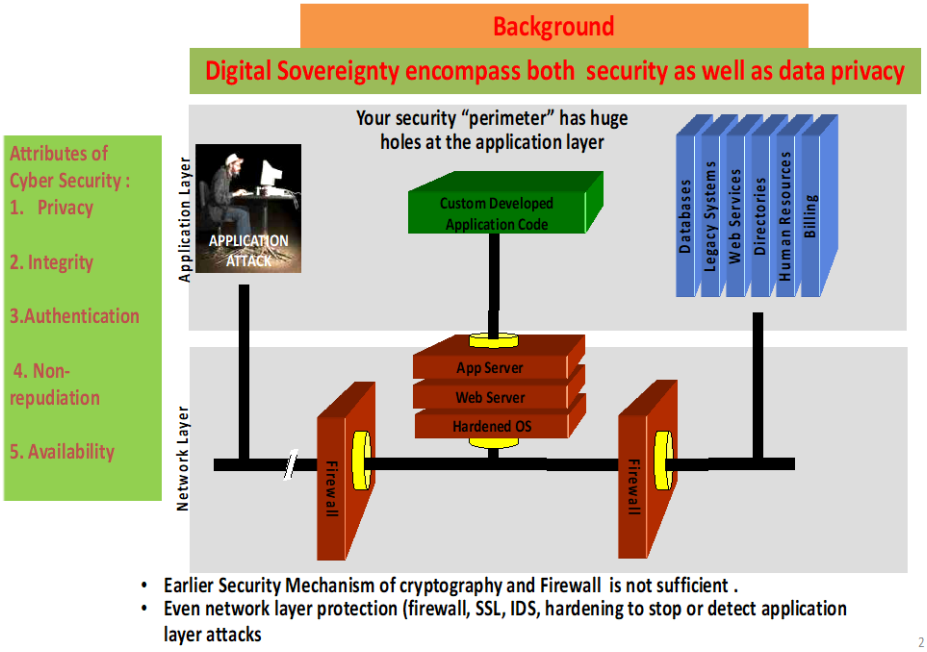


Figure 1-1 OSI layer with Vulnerability

I. Background Information

Present days cyber threats with respect to data theft - issue of SPYWARE/ RANSOMWARE, BOTNET , APT etc. With the impact of IOT devices (20 million devices will be connected on Cyberspace by 2020) and thus security cyber space is getting more challenging . IT ACT of MeitY and role of CERT-in is not able to address the issue of Cyber Attacks and secure cyber space , other than issuing the advisory on application layer Vulnerability and threats. NCSP -2013 of MeitY : lack completeness and directional approach . NDCP -2018 policy of DOT speaks of ensuring Digital Sovereignty . The data grows

@ 32% per annum and single individual generating huge data. Strong Data Protection Law missing in India scenario so far.

II. There has been modulation in nature and intention of cyberattacks

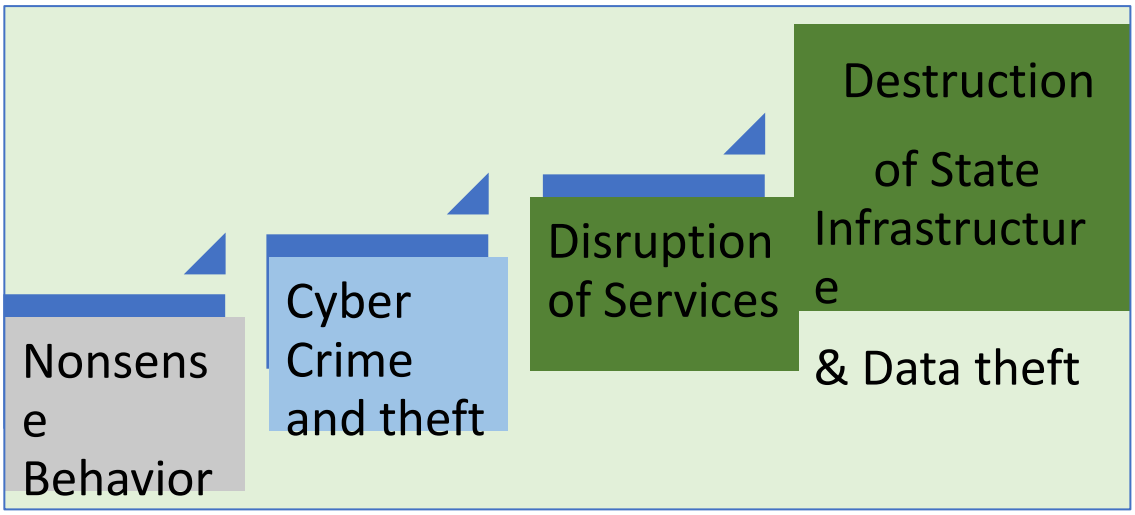


Figure 1-2 Cyber Attack Intention

III. And incident of data theft has increases to such extent that has financial implication $3trillion in comparison to natural disaster (flood, wire, earthquake, thunderstorm, etc.) has implication of $3.6 billion worldwide.

IV. With present requirement of 125Zbytes Storage Capacity and Data generation increases @32% per month. With the Technological advancement in ICT and Devices like IOT ; the security of each of Network element has to ensured in the condition when USA and China are dominating the market of IP based Devices and technology. With impact of Digital India and advent IOT devices , Data generation has increased manifold . It is estimated that 1.7Mbytes/second of Data ,every individual will be generating in cyber space with individual having 5000 data points So indeed requires the strong Data Protection Law. Digital sovereignty encompasses security and safety of Data.

1.1 Overview of Cyber Space And Emerging trends including IR4.0

Cyberspace comprises IT networks, computer resources, and all the fixed and mobile devices connected to the global Internet. A nation's cyberspace is part of the global cyberspace; it cannot be isolated to define its boundaries since cyberspace is borderless. This is what makes cyberspace unique. Unlike the physical world that is limited by geographical boundaries in space—land, sea, river waters, and air—cyberspace can and is continuing to expand. Increased Internet penetration is leading to growth of cyberspace, since its size is proportional to the activities that are carried through it.

Nations are investing heavily in their ICT infrastructures with a view to providing higher bandwidths, integrate national economies with the global marketplace, and to enable citizens or "netizens" to access more and more e-services.

Given the security problems, there is increased emphasis on, and investment in, the security of cyber infrastructure. Core Internet protocols are insecure, and an explosion of mobile devices continues to be based on the same insecure systems. This is adding up to increased usage of the Internet in more vulnerable cyberspace.

Protection of critical infrastructure operations has emerged as a major challenge. This is because trillions of dollars move through the networks every day involving a broad range of activities, including e-commerce, e-governance, travel, hospitality, health care, and general communications. Electricity distribution, water distribution, and several other utility services are based on ICT infrastructures. The defense sector relies heavily on electronic systems.

Ownership and Responsibility

Critical infrastructure is largely owned and operated by the private sector. But is security only the private sector's responsibility? Does this mean that government has a lesser role? These are some of the important cybersecurity issues that nations are grappling with. At an organizational level, too, cybersecurity is not merely a technology issue, but a management issue. This is grounded in enterprise risk management, which calls for an understanding of the human, process, legal, network, and ICT security aspects.

It is obvious that multiple agencies are involved in securing ICT infrastructure. These include private operators for their respective pieces of the infrastructure. Their efforts need to be firmly coordinated through an integrated command-and-control entity, which should serve as a unifying structure that is accountable for cybersecurity.

Roles and responsibilities of each of the parties need to be clearly defined. At the same time, governments need to establish the appropriate policy and legal structures. Nations, such as the United States, have advocated for a market-based, voluntary approach to industry cybersecurity as part of the National Strategy to Secure Cyberspace. But this has not worked entirely, because security investments made by industry, as per their corporate needs, are not found to be commensurate with the broader national interest. How will the additional private investments be generated? Is there a case for government incentives, as part of an incentive program to bridge the gap between those security investments already made and those additional ones that are needed to secure critical infrastructure?

Several security surveys point to this need. They reveal a lack of adequate knowledge among executives about security policy and incidents, the latest technological solutions, data leakage, financial loss, and the training that is needed for their employees.

Since cyberspace is relatively new, legal concepts for "standards of care" do not exist. Is there a case for governments to offer incentives to generate collective action? For example, they could provide reduced liability or tax incentives as a trade off for improved security, new regulatory requirements, and compliance mechanisms.12 Governments need to provide incentives for industry to invest in security at a level that is not justified by corporate business plans.

1.2 Threats and Vulnerability of Cyber S[pace

Cyber security is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of "cyber-threats" is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors. As commonly used, the term "cybersecurity" refers to three things:

- A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security;
- The degree of protection resulting from the application of these activities and measures;
- The associated field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality.

Cybersecurity is thus more than just information security or data security, but is nevertheless closely related to those two fields, because information security lies at the heart of the matter.

Cyber attacks are defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." Cyber exploitation or cyber espionage, on the other hand, refers to the penetration of adversary computers and networks to obtain information for intelligence purposes; this is espionage, not a destructive activity. Cyber attack weapons are easy to use and they can generate outcomes that range from the simple defacing of a web site to the stealing of data and intellectual property, espionage on target systems and even disruption of critical services.

Likewise, cyber attack as a mode of conflict raises many operational issues — for example, how will a country know whether it is the subject of a deliberate cyber attack launched by an enemy government? How will it prove this? Proving attribution in cyberspace is a great challenge. It is extremely difficult to attribute cyber attacks to a nation-state, since collecting irrefutable evidence has proved elusive in almost all cases of this nature in recent years. The very nature of botnets and zombies makes it difficult to do so. This has led many analysts to conclude that the Internet is the perfect platform for plausible deniability.

Cyber attackers can support military operations. They can disrupt the target's command, control, and communications. They can support covert actions to influence governments, events, organizations, or persons, often disguising whoever is launching

those actions. Valuable information and state secrets can be obtained through cyber espionage.

1.2.1.1 Mechanism for Cyber Attacks

Cyber attacks can be carried out in a number of ways. Among them:

- Computer-network attacks
- Supply-chain attacks
- Social-networking-led attacks
- Attacks on radio networks for GPS and wireless networks
- Radio frequencies with sufficiently high power to disrupt all unprotected electronics in a given geographical area

Cyberattacks can be launched against the critical infrastructure of nations that includes telecommunications, energy, financial networks, transportation systems, and water distribution, among others. In many countries, such infrastructure is owned and operated by the private sector. Much of it depends on SCADA systems, which are computer-controlled in a networked environment. Taking advantage of vulnerabilities in these systems, attackers can disable them and disrupt essential services. An attack on the air traffic control system could not just wreak havoc with flight schedules but also, in the worst case, cause crashes. The effects are the same as if the infrastructure were bombed or attacked by some other physical measure, without the enemy coming in by air, sea, or land. Likewise, financial networks can be targeted to disrupt a nation's economy. Banks, stock exchanges, trading, online payment systems, and other transactions of all kinds can be brought to a grinding halt as if these were physically bombed. This is cyber war or information warfare. The effects are similar to what would be achieved by Weapons of Mass Destruction (WMD).

Cyber espionage is another area that can produce a high payoff for a relatively small investment. All someone needs are a few dedicated hackers who can crawl for information stored on the enemy's servers. Human beings are not exposed; nor do they have to travel to enemy's territory to gather or collect information. Terrorists, irrespective of their motives and location, launch cyber attacks on the

Internet even as they use the same medium to mobilize their resources. They have an unprecedented opportunity to access the global community to advance their aims. Cyber criminals began by committing petty crimes in different parts of the world. But with the expansion of cyberspace, financial payoffs have increased, which, in turn, have led to the emergence of organized gangs spread over different cities across countries. Crime syndicates, which sometimes include terrorists, are increasingly visible.

So are fundamentalists of different religious, social, and political groups, who are masquerading in cyberspace as protectors of their rights and the causes of allegedly aggrieved or wronged communities. They have already graduated from defacing websites to causing real damage to their "enemies," especially their critical infrastructure.

Cyber criminals have different motives, but they can command the resources to create attack vectors in order to achieve the results they want. They may commit fraud, identity theft, steal money, commit robbery against corporations, banks, nations, regions and even individuals. They may try to blackmail them, too.

1.3 Emerging Trends in Cyber Space Challenges : IoT and M2M communication

1.3.1 Machine-to-Machine Communication (M2M)

Introduction

Machine-to-Machine (M2M) communication is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication. M2M is also named as Machine Type Communication (MTC) in 3GPP. It is different from the current communication models in the ways that it involves:

- new or different market scenarios
- lower costs and effort
- a potentially very large number of communicating terminals - little traffic per terminal, in general

M2M communication could be carried over mobile networks (e.g. GSM-GPRS, CDMA EVDO networks). In the M2M communication, the role of mobile network is largely confined to serve as a transport network.

With a potential market of probably 50 million connected devices, M2M offers tremendous opportunities as well as unique challenges. These devices vary from highly-mobile vehicles communicating in real-time, to immobile meter-reading appliances that send small amounts of data sporadically.

Applications of M2M

The applications of M2M cover many areas and the areas in which M2M is currently used are given below:

1. Security : Surveillances, Alarm systems, Access control, Car/driver security
2. Tracking & Tracing : Fleet Management, Order Management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimization/steering

3. Payment: Pointofsales, Vending machines, Gamingmachines
4. Health : Monitoring vital signs, Supporting the aged or handicapped, Web

   Access Telemedicine points, Remote diagnostics

5. Remote Maintenance/Control : Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics
6. Metering : Power, Gas, Water, Heating, Grid control, Industrial metering
7. Manufacturing: Production chain monitoring and automation
8. Facility Management : Home / building / campus automation

1.3.1.1 Key features of M2M

Some of the key features of M2M communication system are given below:

1. Low Mobility : M2M Devices do not move, move infrequently, or move only within a certain region
2. Time Controlled : Send or receive data only at certain pre-defined periods
3. Time Tolerant : Data transfer can be delayed
4. Packet Switched : Network operator to provide packet switched service with or without an MSISDN
5. Online small Data Transmissions: MTC Devices frequently send or receive small amounts of data.
6. Monitoring: Not intend to prevent theft or vandalism but provide functionality to detect the events
7. Low Power Consumption : To improve the ability of the system to efficiently service M2M applications
8. Location Specific Trigger : Intending to trigger M2M device in a particular area e.g. wake up the device

1.3.1.2 Architecture and components of M2M

a simple architecture of M2M systems with its components. The various components and elements of an M2M system are briefly described below:

1. M2M Device: Device capable of replying to request for data contained within those devices or capable of transmitting data autonomously.

   Sensors and communication devices are the endpoints of M2M applications. Generally, devices can connect directly to an operator's network, or they will probably interconnect using WPAN technologies such as ZigBee or Bluetooth. Backhaul to an operator's network is than achieved via gateways that encapsulate and manage all devices. Consequently, addressing and identifying, e.g., routing, of the devices relies heavily on the gateways. Devices that connect via gateways are normally outside the operator's responsibility but belong to M2M applications that are provided by service or application providers.

   Sensors and devices that connect directly into an operator's network (via embedded SIM, TPM and radio stack or fixed line access) are endpoints of the network. Thus, the responsibility in terms of accountability, SLAs etc., lies within the network operator (or virtual network operator). This holds true especially with respect to TPM where it is necessary to ensure that the module is really that reliable and well protected.

2. M2M Area Network (Device Domain): Provide connectivity between M2M Devices and M2M Gateways, e.g. personal area network.
3. M2M Gateway: Equipment that uses M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network.

   Gateways and routers are the endpoints of the operator's network in scenarios where sensors and M2M devices do not connect directly to the network. Thus, the task of gateways and routers are twofold. Firstly, they have to ensure that the devices of the capillary network may be reached from outside and vice versa. These functions are addressed by the access enablers, such as identification, addressing, accounting etc., from the operator's platform and have to be supported at the gateway's side as well.

   Thus, platform and gateway form a distributed system, where generic and abstract capabilities are implemented on the gateway's side. Consequently,

there will be a control flow between gateway and operator's platform that has to be distinguished from the data channel that is to transfer M2M application data. Secondly, there may be the need to map bulky internet protocols to their lightweight counterpart in low-power sensor networks. However, the latter application might lose its relevance since there are implementations of IPv6 for sensor networks available, that allow an all-IP approach.

4. M2M Communication Networks (Network Domain): It covers the communications between the M2M Gateway(s) and M2M application(s), e.g. xDSL, LTE, WiMAX, and WLAN.

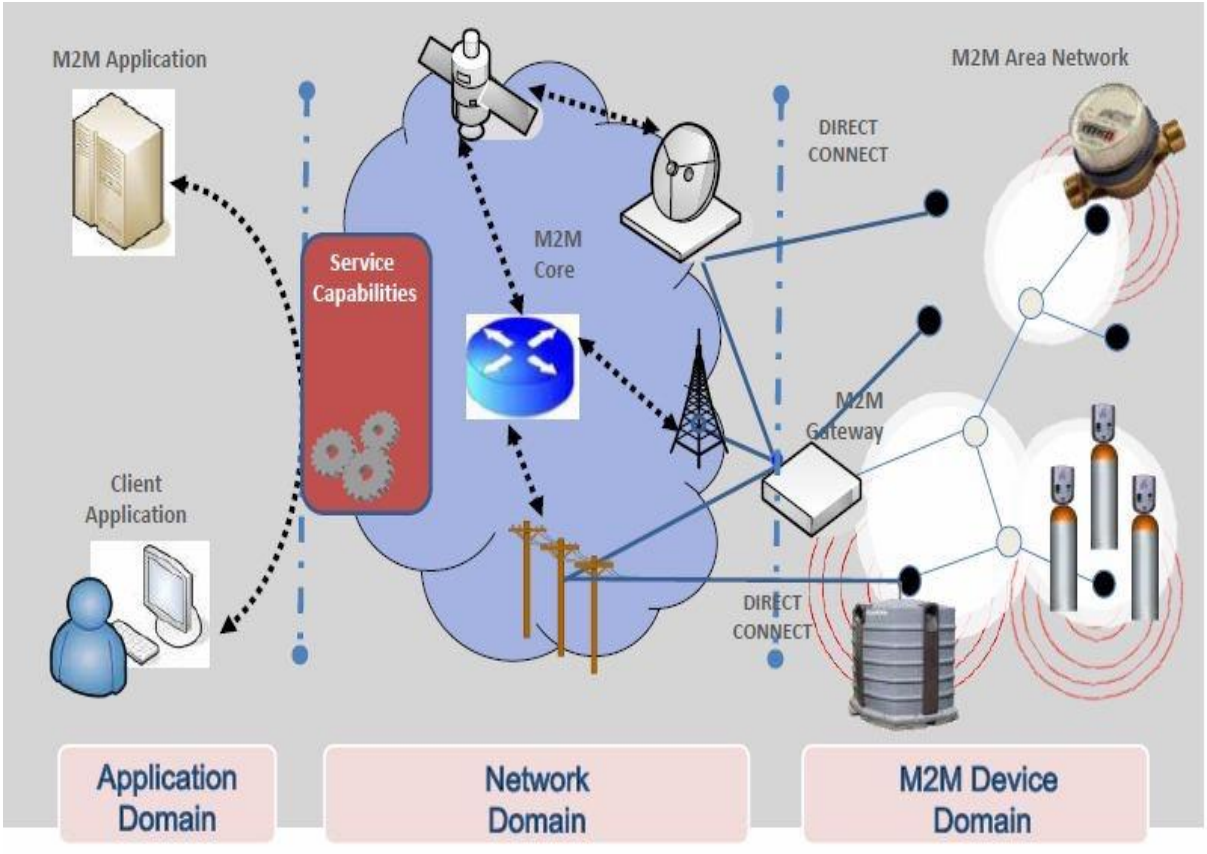


Figure 1-3 Architecture of M2M System

5. M2M Applications: It contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.

M2M applications will be based on the infrastructural assets (e.g., access enablers) that are provided by the operator. Applications may either target at end users, such as

user of a specific M2M solution, or at other application providers to offer more refined building blocks by which they can build more sophisticated M2M solutions and services. e.g. customer care functionality, elaborate billing functions, etc. Those services, or service enablers, may be designed and offered by an application provider, but they might be offered by the operator via the operator platform itself.

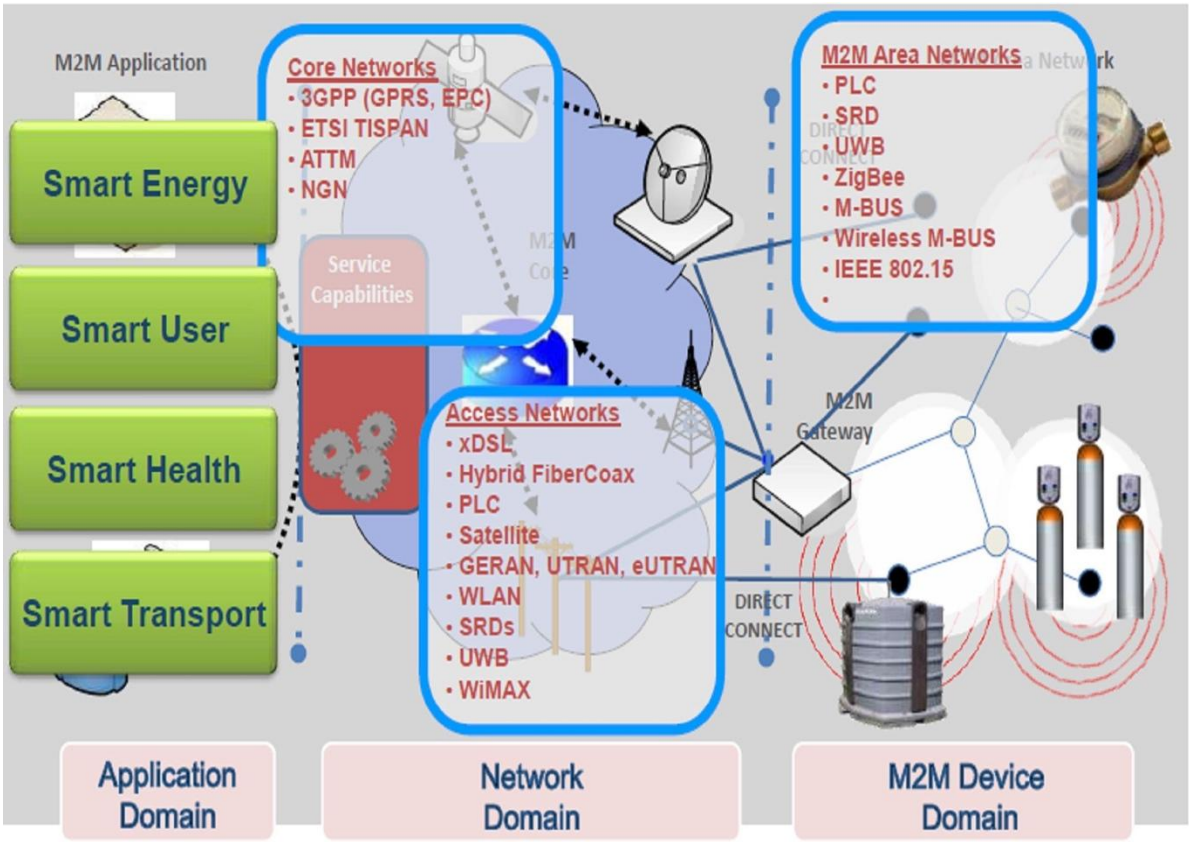


Figure 1-4 Components of M2M system

1.3.1.3 Requirements for M2M

Some of the general requirements for the M2M System, as specified by ETSI, are given below.

a. M2MApplicationcommunicationprinciples:TheM2Msystemshallbeableto allow communication between M2M Applications in the Network and Applications Domain, and the M2M Device or M2M Gateway, by using multiple communication means, e.g. SMS, GPRS and IP Access. Also a

Connected Object may be able to communicate in a peer-to-peer manner with any other Connected Object. The M2M System should abstract the underlying network structure including any network addressing mechanism used, e.g. in case of an IP based network the session establishment shall be possible when IP static or dynamic addressing is used.

b. Message Delivery for sleeping devices: The M2M System shall be able to manage communication towards a sleeping device.
c. Delivery modes : The M2M System shall support anycast, unicast, multicast and broadcast communication modes. Whenever possible a global broadcast should be replaced by a multicast or anycast in order to minimize the load on the communication network.
d. Message transmission scheduling: The M2M System shall be able to manage the scheduling of network access and of messaging. It shall be aware of the scheduling delay tolerance of the M2M Application.
e. Message communication path selection: The M2M System shall be able to optimize communication paths, based on policies such as network cost, delays or transmission failures when other communication paths exist.
f. Communication with devices behind a M2M gateway: The M2M System should be able to communicate with Devices behind a M2M gateway.
g. Communication failure notification: M2M Applications, requesting reliable delivery of a message, shall be notified of any failures to deliver the message.
h. Scalability: The M2M System shall be scalable in terms of number of Connected Objects.
i. Abstraction of technologies heterogeneity: The M2M Gateway may be capable of interfacing to various M2M Area Network technologies.
j. M2M Service Capabilities discovery and registration: The M2M System shall support mechanisms to allow M2M Applications to discover M2M Service Capabilities offered to them. Additionally the M2M Device and M2M Gateway shall support mechanisms to allow the registration of its M2M Service Capabilities to the M2M system.
k. M2M Trusted Application: The M2M Core may handle service request responses for trusted M2M Applications by allowing streamlined authentication procedures for these applications. The M2M system may

support trusted applications that are applications pre-validated by the M2M Core.

l. Mobility: If the underlying network supports seamless mobility and roaming, the M2M System shall be able to use such mechanisms.

m. Communications integrity: The M2M System shall be able to support mechanisms to assure communications integrity for M2M services.

n. Device/Gateway integrity check: The M2M System shall support M2M Device and M2M Gateway integrity check.

o. Continuous connectivity: The M2M System shall support continuous connectivity, for M2M applications requesting the same M2M service on a regular and continuous basis. This continuous connectivity may be de-activated upon request of the Application or by an internal mechanism in the M2M Core.

p. Confirm: The M2M System shall support mechanisms to confirm messages. A message may be unconfirmed, confirmed or transaction controlled.

q. Priority: The M2M System shall support the management of priority levels of the services and communications services. Ongoing communications may be interrupted in order to serve a flow with higher priority (i.e. pre-emption).

r. Logging: Messaging and transactions requiring non-repudiation shall be capable of being logged. Important events (e.g. received information from the M2M Device or M2M Gateway is faulty, unsuccessful installation attempt from the M2M Device or M2M Gateway, service not operating, etc.) may be logged together with diagnostic information. Logs shall be retrievable upon request.

s. Anonymity: The M2M System shall be able to support Anonymity. If anonymity is requested by an M2M Application from the M2M Device side and the request is accepted by the network, the network infrastructure will hide the identity and the location of the requestor, subject to regulatory requirements.

t. Time Stamp: The M2M System shall be able to support accurate and secure and trusted time stamping. M2M Devices and M2M Gateways may support accurate and secure and trusted time stamping.

u. Device/Gateway failure robustness: After a non-destructive failure, e.g. after a power supply outage, a M2M Device or Gateway should immediately return

in a full operating state autonomously, after performing the appropriate initialization e.g. integrity check if supported.

v. Radio transmission activity indication and control: The radio transmitting parts (e.g. GSM/GPRS) of the M2M Device/Gateway should be able to provide (if required by particular applications e.g. eHealth) a real-time indication of radio transmission activity to the application on the M2M Device/Gateway, and may be instructed real-time by the application on the M2M Device/Gateway to suspend/resume the radio transmission activity.

1.3.1.4 Issues /concerns in M2M

The key concerns in M2M are related to addressing and security. The M2M System should be flexible in supporting more than one naming scheme. Also it should support identification of connected objects or groups of connected objects by their names, temporary id, pseudonym (i.e. different names for the same entity), location or combination thereof (e.g. URIs or IMSI). It shall be possible to reuse names for certain classes of devices or for devices operating in certain (i.e. resource constrained) environments. The addressing schemes should include:

– IP address of connected objects.
– IP address of group of connected objects
(including multicast address).
– E.164 addresses of connected objects (e.g. MSISDN).

It is expected that M2M devices would typically operate unmanned and unguarded by humans and thus are subject to increased levels of security threats, such as physical tampering, hacking, unauthorized monitoring, etc. Terminal devices may also get geographically dispersed over time. Such M2M devices should therefore provide adequate security to detect and resist attacks. Devices may also need to support remote management including firmware updates to correct faults or recover from malicious attacks. Some M2M Equipments (M2Mes) are typically required to be

small, inexpensive, able to operate unattended by humans for extended periods of time, and to communicate over the wireless area network (WAN) or WLAN. M2Mes are typically deployed in the field for many years, and after deployment, tend to require remote management of their functionality. It is likely that M2Mes will be deployed in very large quantities, and many of them will also be mobile, making it unrealistic or impossible for operators or subscribers to send personnel to manage or service them. These requirements introduce a number of unique security vulnerabilities for the M2Mes and the wireless communication networks over which they communicate.

1.3.2 IoT Security

1.3.2.1 IoT Security-Introduction

I have always made it a point to go through the flaws of a technology first rather than focusing on its so called valuable benefits. Internet of things received a wide spread hype for its implementation scope. In the beginning of the year 2015 many experts claimed its going to be an existential year for IoT. We also made a statement on how this year is going to be the year for IoT Enterprise segment. However sluggish growth and poor development owing to IoT security has resulted in doubts.

Media for sure was adamant to prove the flaws and loop holes in connecting everything with internet. Media had their reason to be skeptic but they were not totally clueless. Kaspersky Lab went as far as stating IoT as Internet of Crappy Things openly criticizing the move to connect everything possible to internet. Internet of things security challenges are for real and they need to be addressed first.

1.3.2.2 How IoT Can Help To Prevent Electrical Fire

1.3.2.3 The State of Logging in IoT

But time and again it is proven that any emerging technology faces its fair share of challenges and criticism. IoT security issues are definitely a reality but it should not discourage you from developing your IoT applications.

1.3.2.4 IoT Security Issues

In the development of any IoT application security and testing frameworks play an important role. To help you create more secured and attack proof internet of things enabled devices and applications we have outlined top security concerns you should address.

IoT Security-Data Encryption

Internet of things applications collect tons of data. Data retrieval and processing is integral part of the whole IoT environment. Most of this data is personal and needs to be protected through encryption.

To address this IoT security issue you can use Secure Sockets Layer protocol or SSL wherever your data is present online. Websites already use SSL certification to encrypt and protect the user's data online. This is only half part of the equation other half is to protect the wireless protocol side. While data is being transferred wirelessly it needs encryption as well. Sensitive data like locations need to be available to be concerned user and no one else. Therefore make sure you use a wireless protocol with inbuilt encryption.

IoT Security- Data Authentication

After successful encryption of data chances of device itself being hacked still exist. If there is no way to establish the authenticity of the data being communicated to and from an IoT device, security is compromised.

For instance, say you built a temperature sensor for smart homes. Even though you encrypt the data it transfers is there is no way to authenticate the source of data then anyone can make up fake data and send it to your sensor instructing it to cool the room even when its freezing or vice versa. Authentication issues may not be upfront but they definitely pose a security risk.

IoT Security-Side-channel Attacks

Encryption and authentication both in place still leave scope for side channel attacks. Such attacks focus less on the information and more on how that information is being presented. For instance if someone can access data like timing information, power consumption or electromagnetic leak, all of this information can be used for side channel attacks.

1.3.3 IoT Security-Hardware Issues

From the very beginning the internet of things hardware has being the problem. With all the hype and sudden interest in IoT devices chipmakers like ARM and Intel are reinforcing their processors for more security with every new generation but the realistic scenario doesn't seem to ever close that security gap.

The problem is with modern architecture of the chips made specifically for the IoT devices, the prices will go up making them expensive. Also the complex design will require more battery power which is definitely a challenge for IoT applications.

Affordable wearable IoT devices won't use such chips meaning there is need for better approach.

1.3.4 IoT Security Solution-Testing Hardware

The best way to minimize the hardware security challenges of internet of things is to have stringent testing framework in place. Here are our top picks for secured testing of hardware.

Device Range

Coverage network of the IoT device is paramount. You need to be very specific about the range metrics for your application or device.

For instance if you are using Zigbee technology to empower your device's network you will have to calculate how many repeaters you will need within a establishment to provide communication range for your device. But you cannot blindly put any number of repeaters as with increasing number of repeaters the capacity of your system decreases. Therefore device range testing will enable you to find that sweet spot where you can maximize the range without reaching the breaking point.

Latency and Capacity

Capacity is the bps (bytes per second) handling speed of your network while latency denotes the total time taken for data transfer between the application endpoints.

Developers always look for ways to increase capacity and latency of their IoT applications to improve performance. Problem is both these factors are inversely proportionate, improving one degrades the other. Data intensive devices and applications should be thoroughly tested for latency and capacity balance.

Manufacturability Test

It is seldom that you will build you IoT device from scratch on your own. Most of the time, you will be using component and module manufactured by others in your application. Testing these modules on your own for proper functioning is very important.

Manufacturers always do the assembly line testing on their end but you should also verify the same. Also when you put all the modules together on a board testing is

required to make sure there are no errors introduced because of soldering and wiring. Manufacturability testing is necessary to make sure your application works as it is intended to.

1.3.5 How can we develop secured IoT Applications?

The security solutions listed above should be implemented strictly to ensure proper functioning with safety.IoT technologies are still immature to a large extent and being little paranoid about their security is indeed helpful. Before you start with development of any IoT application it is necessary that you do research and be informed as much as you can. There will always be trade offs like more security for poor UI but as mentioned before you need to find that sweet spot.

Also don't be in the rush to bring your product in the market without proper planning for long term support. IoT devices are cheap so chances are very high that manufacturers don't pay enough attention to provide security updates and patches. This is not a sustainable development model for internet of things.

As an IoT application developer always beware of threats. Security breaches are almost bound to happen and you should be ready for them. You should always be ready with an exit plan to secure maximum data in case of an attack.

Last and not least always take initiative to teach customers and employees on latest IoT security threats and solutions.

1.4 Challenges Data Centre and Cloud Security

Cloud is a boon to new generation technology. But if it fails to ensure proper security protection, cloud services could ultimately result in higher cost & potential loss of business thus eliminating all the potential benefits of cloud technology. So the aim of the cloud security & its researchers to help enterprise information technology and decision makers to analyze the security implications of cloud computing in their business. When a customer moves toward cloud computing, they have a clear understanding of potential security & risk associated with cloud computing.

1.4.1 Defining Cloud Security

It is a set of control-based technologies & policies adapted to stick to regulatory compliances, rules & protect data application and cloud technology infrastructure. Because of cloud's nature of sharing resources, cloud security gives particular concern to identity management, privacy & access control. So the data in the cloud should have to be stored in an encrypted form. With the increase in the number of organizations using cloud technology for a data operation, proper security and other potentially vulnerable areas became a priority for organizations contracting with cloud providers. Cloud computing security processes the security control in cloud & provides customer data security, privacy & compliance with necessary regulations.

1.4.2 Security Planning for Cloud

Before using cloud technology, users should need to analyze several aspects.

These are:

i. Analyse the sensitivity to risks of user's resources.

ii. The cloud service models require the customer to be responsible for security at various levels of service.

iii. Understand the data storage and transfer mechanism provided by the cloud service provider.

iv. Consider proper cloud type to be used.

1.4.3 Cloud Security Controls

Cloud security becomes effective only if the defensive implementation remains strong.

There are many types of control for cloud security architecture; the categories are listed below:

1. Detective Control: are meant to detect and react instantly & appropriately to any incident.
2. Preventive Control: strengthen the system against any incident or attack by actually eliminating the vulnerabilities.

3. Deterrent Control is meant to reduce attack on cloud system; it reduces the threat level by giving a warning sign.
4. Corrective Control reduces the consequences of an incident by controlling/limiting the damage. Restoring system backup is an example of such type.

1.5 Understanding The Data Security

As we all know the data is transferred via the internet, so one of the major concerns is data security. The major points that one should adopt to secure cloud data are:

1. Access Control
2. Auditing
3. Authentication
4. Authorization

1.5.1 CSA (Cloud Security Alliance) MODEL

This stack model defines the boundaries of each service model & shows with how much variation the functional units relate to each other. It is responsible for creating the boundary between the service provider & the customer.

CSA Model's Key Points:

- IaaS is the most basic level among all services.
- Each of the services inherits the capabilities and security concerns of the model beneath.
- The infrastructure, platform for development & software operating environment are provided by IaaS, PaaS & SaaS respectively.
- The security mechanism below the security boundary must be built into the system that is required to be maintained by the customer.

1.5.2 Encrypt Cloud Data:

Encryption protects data from being compromised. It helps in protecting data that is being transferred & stored in the cloud. Encryption helps both protect unauthorized access along with the prevention of data loss.

1.5.3 Challenges of Cloud Computing

This emergent cloud technology is facing many technological challenges in different aspects of data & information handling & storage.

Some of the challenges are as follows:

- Availability & reliability
- Security & Privacy
- Interoperability
- Performance
- Portability

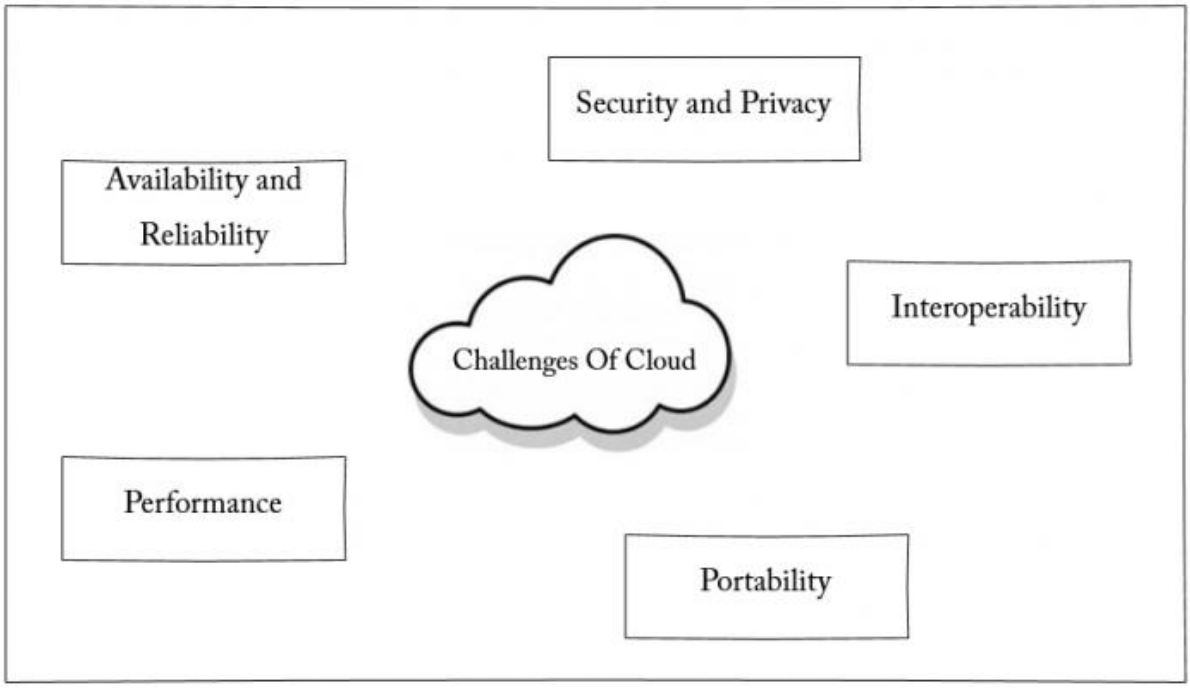


Figure 1-5 challenges of cloud

The challenges as mentioned above are the most important and concerned points that should be processed for the betterment.

1.6 Digital Sovereignty

Digital Sovereignty or Cyber Sovereignty is the degree of control an individual, organization or government has over the data they generate and work with at local or online platforms.

"It will take time to create a coherent framework to make 'digital sovereignty' work in a fair and transparent manner." Digital sovereignty encompasses both data security and data protection. Digital sovereignty encompasses the idea that users, being citizens or companies, have control over their data.

"Digital sovereignty can be approached in various ways, but one should not expect European technologies to replace U.S. or Chinese products, services and platforms everywhere," Renda told CNBC via email.

The European Union has taken steps on the regulation side of technology. It introduced in May of last year the General Data Protection regulation (GDPR) which gives users some protection over how their data is processed.

1.6.1 Digital Sovereignty & Strategic risks

Digital Sovereignty:
At the core of Digital Sovereignty are the makes an attempt to let the tip customers maintain authority over their private knowledge. That is what the European Union says. Digital Sovereignty might be roughly outlined as follows:

Digital sovereignty is the query of proudly owning the private knowledge of customers, collected by completely different firm web sites on the Internet with or without the consent of the customers.

Strategic risks :

Loss of control over data represents a strategic risk for our society. individuals, businesses and governments are surveilled and their data is monetized by foreign corporations. Most data from citizens and businesses is at a small number of large, for-profit corporations. Most of these are headquartered in and thus under political control of the US and China. Everyone else, including hundreds of millions of users in India, Indonesia, Brazil or the entire continent of Africa are deeply dependent on services these companies provide.

1.6.2 Ideal Data Sovereignty

According to digital sovereignty activists, the private knowledge of customers must be collected with their consent solely or no less than the customers must be knowledgeable of what all knowledge is being collected. They additional state that the private knowledge of a person must be saved in a knowledge heart that is current within the nation the place the person is residing or utilizing the Internet. This is not sensible nevertheless because it is the age of cloud computing and nearly all main web sites or corporations have their datacentres unfold over a spread of nations with various legal guidelines about IT and cloud.

1.6.3 Concept of Digital Sovereignty

A spectre of digital sovereignty is haunting not only Europe but other developing country like India. The said fact has correlation to Incidence of the 2013 revelation of massive U.S.-driven data surveillance, both European policy-makers and stakeholders from EU member states have urged action to strengthen data security and data protection with a view to improving European or even national self-determination as it refers to the digital sphere.

As this process has been ongoing, the word digital sovereignty has spread in both the political and economic spheres, and has occasionally achieved some prominence. Several governments and companies have not hesitated to call for a re-nationalisation of the digital.

In 2014, a paper published by the Global Public Policy Institute (GPPi) together with the Open Technology Institute and the New America Foundation – remarkably funded "with the assistance of the European Union" – assessed a significant number of measures aiming at safeguarding Europe's digital sovereignty. Asking whether Europe is missing the point when striving for "technological sovereignty", the authors eventually concluded that the proposals, ranging from localised routing to IT security brands, mostly would not meet their aims and even would threaten the open internet. The situation back then was prompted by massive pressure on EU officials caused by public disillusion and outrage. Realising the fact that Europeans were obviously exposed to the digital supremacy of foreign powers forced European decision-makers into a corner where they had to affirm Europe's capacity to act in a self-determined way; Europe was in a state where technology faced a political rationale. And even after the dust settled, the term digital sovereignty still stimulated the discourse. But it had changed. The discourse has shown that there is more to digital sovereignty than localised routing, national e-mailing or restrictions for public tenders. The term has evolved and broadened its scope. (TIM MAURER, November 2014)

Sovereignty = Protectionism :

Reviewing past developments, globalisation, Europeanisation and digitalisation have blurred the lines between states as well as national and supranational institutions. In the process, they have changed the way we think about physical borders. Europeanisation has called the term sovereignty into question, while nation states have questioned the process of Europeanisation. Digitalisation in these matters is the embodiment of blurring lines per se: on- and off-line merge, the internet is objectified, industry and society are translated into bits.

Digitalisation certainly increases the pressure on European economies whose incumbents are world leaders in traditional, analogue industries: automotive, manufacturing, engineering, pharmacy. The challenge to keep up with global competition accelerates as market entrants from the IT sector set trends by establishing new digital business models that demand digital transformation. Data processing, as a skill to develop new business models and societal

solutions, has to be integrated in our thinking. Therefore, Europe's economy and society has to be aware of the characteristics of this new resource. However, the fear that results from this development – reaching beyond the fear from being a victim of surveillance – has given birth to a phrase that is likewise haunting European debates: Europe must not become a workbench for U.S. or Asian innovators But, digital protectionism cannot be an answer to these fears either. Rejecting the challenge of moving to the new would waste the potential digital sovereignty is able to unleash. Protecting the status quo while thereby promoting outdated business models instead of promoting innovation will do little to foster sustainable economic growth in Europe. What should a legitimate concept of digital sovereignty look like then?

1.6.4 Privacy :

Where is our data today?

Democratic oversight is minimal and access to these platforms can easily be weaponized. Just like economic sanctions harms financial services, digital sanctions could shatter the means of communication in a country and isolate it from international trade and information access.

Challenges of Privacy :-

In digital age, Privacy faces challenges from three key actors :-

- Hackers
- Private Firms
- The Govt

There is possibility of serious data breach and misuse of personal information.
Vast silos of data may be used to profile people and to discriminate against vulnerable groups. There is a chilling effect on free speech and disclosure of information

The constitution of India protects right to personal freedom , human dignity and liberty . Today every individual is viewed in terabytes of information of information and every individual is viewed as a collection of data represented by activities on internet on internet like shopping preferences , social media patterns , geographical location and personal biometric information . This defines two new horizon :-
The data aggregations , is collection of unconnected data to map the identity of individual . This has potential of to seriously threat the right of individuals to keep the keep their personal and sensitive information private and how their information is used .
Artificial intelligence , which comprehends machine learning analysis of political beliefs, religious affiliation , race , ethnicity , health status, gender and sexual orientation.

Our individual data is aggregated and disaggregated to sort ,score , classify , evaluate and rank people.

1.6.5 Need for ICT Devices and Equipment Security and Compliances.

The effect of the liberalization of the Telecom Sector and subsequent dawn of the NGN era, TEC had to transform itself into an independent technical organization to draw up standards and specifications for seamless inter-working of a multi-operator convergent network supporting multimedia services. Thus TEC was required to redefine its role to benefit the entire telecom industry rather than limiting it to a single incumbent as was traditionally the case before liberalization. Convergence of technologies in the Telecom, IT, Broadcasting, and Entertainment sectors, resulted into horizontal and vertical integration of market segments, and this further prompted the need for change. It is now imperative to ensure seamless working in a converged network capable of carrying multimedia communications and applications. The need to specify Network-Network Interfaces (NNI) and User- Network Interfaces (UNI) in such a network by an independent standards organization is of paramount importance

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DoT), Government of India. Its activities include:

i. Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR) and Standards for Telecom Products and Services
ii. Field evaluation of products and Systems
iii. National Fundamental Plans
iv. Support to DoT on technology issues
v. Testing & Certification of Telecom products

Role of TEC is to bring together the Telecom Industry to decide the standards that network elements and services would have to conform to in order to make Indian Telecom Network deliver acceptable service in a multioperation environment at par with global standards. TEC, therefore, has created a more

interactive mechanism, which includes all stakeholders, for formulation of Generic Requirements (GR) for network elements, Interface Requirements (IR) for interfaces between different network elements, Service Requirements (SR) for networks and services and Test Schedule and Test Procedures (TSTP) thereof.

Generic Requirements (GR) for a telecom network element or a set of network elements, are its requirements to work seamlessly in Indian Telecom Network. Requirements are classified in two parts – minimum "mandatory" requirements and "desirable" requirements. These requirements refer to the following

i. Interconnectivity and interoperability requirements
ii. Quality requirements
iii. EMI/EMC requirements
iv. Safety requirements
v. Security requirements
vi. Any other equipment specific requirements that are considered mandatory
vii. Desirable requirements, if any

With the notification of Indian Telegraph (Amendment) Rules 2017 enabling mandatory testing and certification of telecom equipment (MTCTE), TEC has been designated as the Telegraph Authority for the purpose of administration of MTCTE procedure and Surveillance Procedure, and for formulation of Essential Requirements under MTCT The final detailed procedure for Mandatory Testing and Certification of Telecom Equipment's (MTCTE) under these rules has been notified separately. The testing is to be carried out for conformance to Essential Requirement for the equipment, by Indian Accredited Labs designated by TEC and based upon their test reports, certificate shall be issued by TEC.

1.6.6 Need for cyber Security and Cyber hygiene

Cyber defence is a computer network defence mechanism which focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. All responsible nation states have their strategic plan to provide priorities for cyber security R&D in alignment with their national framework for Improving Critical Infrastructure. The four strategic defensive elements of the strategic plan consist of Deter, Protect, Detect and Adapt, as defined below[12]:-

- Deter. The ability to efficiently discourage malicious cyber activities by: measuring and increasing costs to adversaries carrying out such activities; diminishing the spoils; and increasing risks and uncertainty for potential adversaries.
- Protect. The ability of components, systems, users and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability and accountability.
- Detect. The ability to efficiently detect and even anticipate adversary decisions and activities, given that perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.
- Adapt. The ability of defenders, defences and infrastructure to dynamically adapt to malicious cyber activities by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration and adjusting to thwart similar future activity.

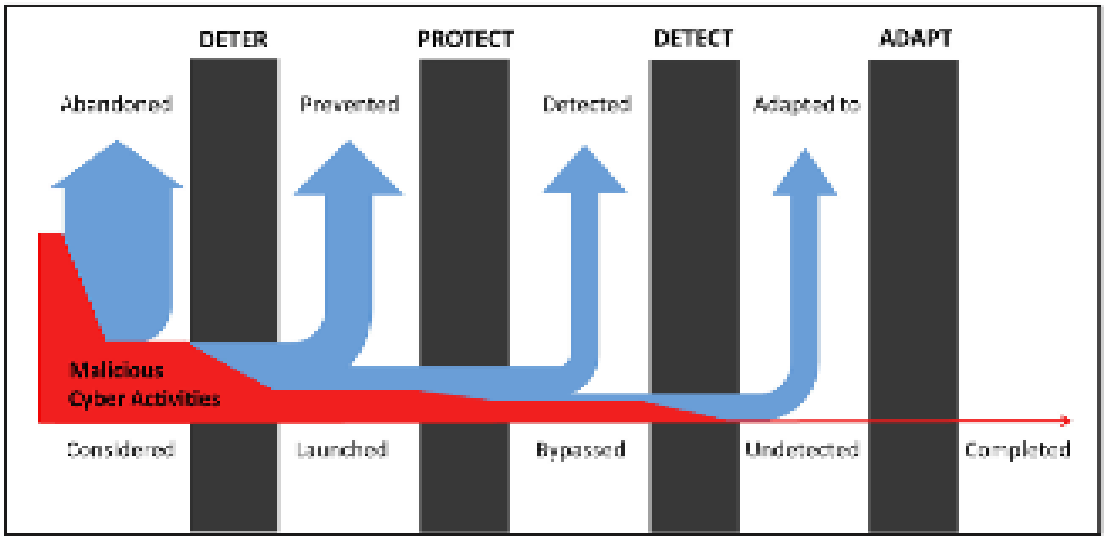


Figure 1-6 Strategic Defence System

As shown in figure four defensive elements thwart malicious cyber activities and the value of continuous outcome-driven improvements in efficacy and efficiency.

2. Literature Review

2.1 Rationale for Study

- Securing digital sovereignty implies to ensure digital security and sovereignty; thus enables community to thrive (develop and prosperity) . Viz.

  "Digital Sovereignty will mean not merely that the individual are owners of own data but also they have effective autonomy ,control, choice , integrity, security in context present day state of Cyber space. as there are four guiding principles in connection with digital sovereignty: freedom of choice, self-determination, self-control and security. "

2.2 Literature Review

Several studies in the context of Data Security and Cyber security i.e. Digital Sovereignty is explored, a brief has been presented a ready reference :-

J. Adams Md. Alba Kajal in his paper title "A New threat to the the sovereignty of state" (Malcic, 2015) (Neil Robinson) (lewis, 2010) (Gueham) (Ayers) (Arnd Weber, March 2018) (shen, 2016) (Dar, 2019) (Srikrishna) (Jackson Adams, Nov-Dec,2016) (Kolton, 2017) (Pinto, 2018) (Lowe, 2019) (Placeholder1)has referred that that The internet has always been recognized as a global decentralized computer network system or a network of networks (Chaffey & Ellis-Chadwick, 2012). Therefore, activities conducted over this network may acquire a cross-border dimension, where people of different countries could be affected by these activities; and hence, different laws, regulations, and policies may apply in cases of legal disputes. The virtual nature of the cyberspace implies de-materialization (everything is paperless), de-temporalization (instant communication), and de-territorialisation (breaking the geographical boundaries and distances) of online activities and interactions. The combined effect created by such virtualization process leads to the notion of

ubiquity (Schultz, 2004). Hence, the impact of cyberspace on sovereignty can be recognized through the temporal and spatial dimensions

The legal challenge associated with cyberspace activities is caused by the fact that cyberspace is a decentralized network, with the ease of accessibility by masses of people and the ability to allow making three types of communication configurations (which no-other media can combine simultaneously): one-to-one, one-to-many, and many-to-many (Biegel, 2001). Again, communications made the internet networks happen independently without considering any territorial account—an independent state of cyberspace (Kucklich, 2009).

The cyberspace with its characteristics (de-materialization, de-temporalization, and de-territorialisation) can cross borders and the territory of the state despite all the precautions taken by the state to protect its sovereignty. These characteristics make national laws unable to keep up to date with technological developments. states should look for new means to regulate the cyberspace, such as soft law. Therefore, legislators and regulators must be more flexible by giving an important role to the civil actors in regulating the cyberspace and the e-commerce issues. In this way, the state can reserve the framework powers or constitutional prerogatives.

The formation of the state, sovereignty is considered as an essential component of the state. Thus, the state has endeavoured to maintain its sovereignty over its territories and has sought to protect its geographical boundaries by all possible means to prove its identity. However, technological revolution, including the telecommunication advancements, imposed new challenges to the state's sovereignty in maintaining its cyber space. the research shows that cyberspace with its characteristics (de-materialization, de-temporalization, and de-territorialisation) can cross borders and the territory of the state despite all the precautions taken by the state to protect its sovereignty. These characteristics make national laws unable to keep up to date with technological Consequently, states should look for new means to regulate the cyberspace, such as soft law. Therefore, legislators and regulators must be more flexible by giving an important role to the civil actors in regulating the cyberspace and the e-commerce issues. In

this way, the state can reserve the framework powers or constitutional prerogatives.

However this paper has research gap Cyberspace with its characteristic of (dematerialisation, de-temporalization and reterritorialization) can cross borders and the territory of state despite of all precautions to protect its sovereignty. And the paper could not reveal about the technological. Complexity of cyber space , with regard hacking and data theft. Also this paper doses not illustrate the complexity problem of Data Centre.

Renato Avila Pinto , in his article titled " Digital Sovereignty or Digital Colonialism" (Pinto, 2018)reiterated that leaving apart from issues of privacy and security of data of individual, the present world acknowledging a real confrontation between control and freedom, not only of the individual, but of entire populations and regions, enhanced by technologies and massive collection and analysis of data by AI – thus predicting and influencing behaviours, managing the automation of public services and the ability to fully control and disrupt those services, even remotely. From gaining access to a global communications platform to losing the ability to protect the rights of individuals, who are interconnected through those platforms. Thus highlighting the new issue of digital colonialism i.e. indirectly . Rapid digitisation programmes linked with e-governance initiative are relying heavily on mobile technologies to plug new users into the increasingly commercialised Web.

They increase the risk of surveillance and profiling of disadvantaged populations, because mobile phones in several countries are linked to a registered SIM card.[8] The monitoring and monetisation of all users' activities online is the main motivation for the quasi-philanthropic efforts to connect the next billion, and therefore get hold of their data. User data is the basic raw material for machine learning and artificial intelligence, when combined with sophisticated algorithms and computational power of the concentrated tech conglomerates.

The mentioned " Digital Sovereignty or Digital Colonialism" by Renato Avila Pinto (Pinto, 2018)recommends for development of State Funded long term strategy for

ensuring Digital Sovereignty. In the meantime the simple regulation of open standards, free software, openly available hardware and transparency of algorithms could be developed at least for the state purchases and practices.They increase the risk of surveillance and profiling of disadvantaged populations, because mobile phones in several countries are linked to a registered SIM card.[8] The monitoring and monetisation of all users' activities online is the main motivation for the quasi-philanthropic efforts to connect the next billion, and therefore get hold of their data. User data is the basic raw material for machine learning and artificial intelligence, when combined with sophisticated algorithms and computational power of the concentrated tech conglomerates.

The article " Digital Sovereignty or Digital Colonialism" by Renato Avila Pinto does not mentioned detailed strategy how ICT , AI innovation and the ability to deploy systems and infrastructure rapidly in emerging markets are concentrated in few country can be implemented.

Michael Kolton , in his article "Interpreting China's Pursuit of Cyber Sovereignty and its views on Cyber Deterrence" mentioned that At the 2012 World Conference on International Telecommunications, China (Kolton, 2017)and a majority of attending countries advocated for national governments to boost their control of the Internet. The US and its allies foiled this campaign and upheld the status quo multi-stake holder approach, which invites participation from civil society, private enterprise, national governments, and international organizations. This conflict of ideas remains an ongoing geopolitical dispute that will define the future of cyberspace. China's displeasure with the status quo of Internet governance

When Chinese academic researchers examined the use of social media to organize street protests in Iran and China's Xinjiang, they concluded the US will leverage such technologies to spur regime change in other countries. [12] To mitigate these types of perceived Internet risks, China's Great Firewall blocks sites like Google, Facebook, Twitter, and YouTube. [13] In March 2016, Chinese authorities increased efforts to shutdown virtual private networks (VPNs) that enable citizens and foreign residents to bypass censors. cyber sovereignty as the foundation for a new inter- national code of

conduct for cyberspace in which the principle of sovereignty enshrined in the UN Charter extends to cyberspace. China's vision for cyber sovereignty imagines cyberspace as a new world for nations to stake their claims.

China's cyber strategy appears deter- mined to achieve cyber sovereignty; this end unifies the country's cyber activities. Although the US and China agree on the importance of cyberspace, they fundamentally diverge on the prerogatives a country should enjoy in the virtual world.

In China, the chief goals of its 2015 draft national cybersecurity law are (1) ensure cyber- security, (2) safeguard cyberspace sovereignty, national security, and the public interest, (3) protect the legitimate rights and interests of citizens, legal persons and other organi-zations, and (4) promote the healthy development of economic and social information

After the Stuxnet attack on Iran's cen- trifuges, Colonel Ye and Captain Zhao concluded even China's physically isolated net- works remain vulnerable to US cyber-attack; passive cyber defence alone is insufficient. Therefore, China must achieve parity with the US in cyberspace to deter aggression and protect national sovereignty.

The 2015 Military Strategy affirms the PLA mission to "safeguard China's sovereignty, security and development interests, and provide a strong guarantee for achieving the national strategic goal of the 'two centenaries' and for realizing the Chinese Dream.

Fifth Dimension of war field is CYBERSPACE in addition to AIR, LAND , MARITIME , SPACE. OPEN INTERNET is US strategists interest , the erosion of multi-stakeholder governance should alarm strategists.

Jennifer Holt And S. Malcic in his paper "The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union" (Malcic, 2015)mentioned that now a days the remote data storage in the cloud being practiced by all sectors of

industry, education, government, and culture . As digital content distribution grows increasingly dependent on cloud infrastructure, streaming platforms, and access to "big data" about viewers' personal preferences, concepts of privacy have come to the forefront of citizen and consumer consciousness. Indeed, as access to our digital data increases, so have the cultural concerns, anxieties, and related protectionist movements around digital privacy.

Securely managing and maintaining privacy protections for digital information is extremely complex, due to the wide range of interrelated yet often distinct laws that apply to different types of information and institutions (like health care, global trade, national security, finance, and intellectual property, among others). Moreover, when data is stored in "the cloud" circulates through an infrastructural landscape that is simultaneously local, national, and global. Regulators face a lots of challenges that often defy legal resolutions, as Internet infrastructure extends beyond national boundaries. The global nature of cloud storage has aggravated the challenges of safeguarding digital privacy, due to the gaps and fissures in international data jurisdiction and the attendant difficulties regulating the private sector. The regulation of digital data and cloud infrastructure is in many respects being defined more by the lack of any clear guidelines and regulations.

The challenge for the current global terrain of Internet infrastructure is still remains unclear. The policymakers and governments find too difficult to effectively safeguard digital privacy in the cloud.

A recent European Parliament report on cloud computing raised the issue regarding security of data and lack of interoperability in the cloud space will inevitably stifle innovation and global trade .

The evolving privacy ecosystem is comprised of an intricate combination of citizens' rights and cultural preferences; corporate policies (both formally stated and informally practiced); state, national, regional, and international regulations and laws; as well as input and stewardship from global entities such as the Organisation for Economic Co-operation and development (OECd), the United nations, Internet Corporation for Assigned names and numbers (ICAnn), and the World Wide Web Consortium (W3C). It is a critical arena for the future of Internet regulation. The

privacy ecosystem affects all users, providers, and distributors of digital data and is essentially folded into the layers of content and activities taking place across the Internet.

Whether the fundamental "rules of engagement" in this ecosystem will be determined by government regulations or by private practices such as those employed by digital content platforms (e.g., Google) and Internet service providers (ISPs) remains to be seen. Google's recent assertion that a reasonable expectation of privacy no longer applies to users of their Gmail electronic mail service has certainly called attention to this issue of power and control over "private" data in the digital space.

The privacy ecosystem is ultimately an arena in which the future of infrastructure regulation will be heavily dependent on an international perspective, and accommodations for data security measures that are often determined in multiple jurisdictions. Cloud applications and services provide an excellent case in point. data stored in, processed, and streamed from the cloud is sent across international borders multiple times in the course of reaching its audience or users. As a result, this data passes through a host of different national regimes of privacy laws, intellectual property laws, data processing and protection laws, and other regulations affecting the status of data as it is stored and distributed .

Thus "The Data protection law is largely based on an understanding that where data is located within particular borders, whereas the economics of the cloud is dependent on data being able to flow across borders in fairly seamless way."

In the Journal titled "A three perspective Theory of Cyber Sovereignty " by Hao Yeli stated that Cybersecurity has emerged as a global challenge due to cybercrime and cyber terrorism, and becoming a tier one security threat for sovereign states. Cyber sovereignty has inevitably become the focus of great controversy because of mainly three disputes :- 1. Contradiction between Cyber sovereignty and the spirit of the internet may result to fragmentation of internet 2. Contradiction between Cyber sovereignty and human rights may constrain freedom of speech by State 3. Contradiction between Cyber sovereignty and involvement of multiple stake holders

in governance will provoke controversy on the pattern of internet governance. The concept of cyber sovereignty plays important role in establishing the internationals rules of cyberspace by international consensus and cooperation of issues of disputes. Hao Yeli in his article "A three perspective Theory of Cyber Sovereignty" and stated that the three actors of cyberspace are the State ,the Citizen and the international Community, whose interests and demands are competing. Each of cyberspace actor concentrated on own interest , but routinely ignores those of other two ; thus resulting in situation in which compromise and reconciliation are difficult to achieve. The behind the contradiction of cyber sovereignty and the spirit of internet are the state and the international community.

At the lowest level or the physical level represents cyberspace infrastructure . and is responsible for standardisation in the global cyberspace and interconnectivity. At this level states should be willing to collectively transfer authority in the interest of standardisation and interconnectivity. States with well-developed cyber capacity must take the initiative to extend standardizations and connectivity to less developed states. The middle level represents the application level and includes the many internet platform and internet carriers in the real word to interface different sectors as technology , culture , economy ,trade and e commerce. And at this level the degree of cyber sovereignty should be adopted to local conditions with aim to achieve dynamic equilibrium , multilaterals and multiparty joint administration to balance between freedom and order. The Top or Core level comprises regime ,law , political security and ideology , which is unchallengeable and includes the governing foundations and embodies the core interest of country. At the middle and bottom level cyber sovereignty can be transferred to certain degree , thus allowing multi stake holder governance model. At top level the emphasis on leading role of government. Respect for cyber sovereignty is a prerequisite for international co-operation in this domain and the basis for construction of beneficial cyber space order.

Paul M Schwartz in his issues stated that "Legal Access to the Global Cloud (Lowe, 2019)"Due to persistent requirement of the "cloud computing ", further its international scope of utilisation has raise significant challenges to the traditional legal authorities that permit access to data stored outside the United States. In Article "Legal Access to the Global Cloud", Paul M Schwartz , describe the three models of

cloud computing to provide greater clarity for courts when evaluating international data access requests. These models are namely Data Shard [where service provider stores information in the cloud in multiple international location, the network itself dynamically distributes data to domestic and international servers], Data Localisation Model [Here service provider stores information in a cloud that is restricted to a single country or region] and Data Trust Clouds [In this case company bifurcates network management from the ability to access data]. This article advances two basic principles for a world of omnipresent global cloud computing.

The cloud Act of 2018 , takes major principles to preserve Internet as a Global Space . The basic idea behind the principle is 1. To treat extra-terrestrial data request equally, regardless of location of the cloud provider's headquarters. This approach would provide impetus to Global Cloud Companies and encourages innovation as this approach foster a level playing field for global cloud companies , than balkanisation of the internet. 2. To rely on need for international cooperation to create reciprocity. The cloud Act of 2018, USA also encourages the "Know Your Customer Regime ", where ultimate cost may be paid in users privacy .

Yi Shen in the article titled " Sovereignty and the Role of Government in Cyber Space illustrated that "With the advent of PC, internet cum broadband , Mobile and cloud computing the cyber space is impossible to describe and manage. The concept of cyberspace being a global commons due to its supposed lack of borders is best seen as a wish rather than describe. With the growth of dot-com area in public governance as well as in private sector , the Global economy begins to grows as faster rate than previously. And National Borders become less relevant and national polices became less effective . Thus the erosion of Sovereignty and possible demise of the Westphalian state brought on by globalisation strongly affected the views on internet Governance held by policy makers ,technophiles and internet community.

The three general principles for internet policy emerged in this context viz 1. Technology Neutral , 2. Development of Policy was to be industry led as part of Public -Private Partnership, where Government role would be minimal , predictable legal and regulatory environment 3. Policy solution would need to work in Global Market Place.

The OECD defines that Cyber space is not a commons. The sovereignty completely covers the cyberspace even if nation have not chosen to assert sovereign control . As

cyberspace is a artificial creation which rests on a tangle , physical construct. Most of the interconnected networks that form cyberspace was created for commercial purpose such that any actions in cyberspace take place in context defined in commercial laws and business contract.

The US ideology and culture that has shaped the cyberspace is now under changes as manufacturing spreads to Asia and Americans no longer constitute the largest numbers of internet users The struggle over Domain Name System (DNS) and ICANN , the battles over technology standards and the problems at International Telecommunication Union are symptoms of need of rearchitect of cyber space to better serve the Political and commercial needs . Thus require rethinking the role of Government and recognizing the role of sovereignty. The fact is further becoming the issue with concept of "Data is Oil". Thus securing Digital sovereignty in cyber space has gained enough concept , although different country legislating their respective Data Protection Bill as the issue of data Localization become reasons for exploitation by AI.

The article titled " Cyber Sovereignty and Governance of Global Cyberspace" by Yi Shen address the china's Sovereignty and its possible effect on the evolution of governance of Global Cyber since 2013.Cyber space is logical space that is too difficult to be accurately perceived and managed. Cyberspace is unable to exist without supporting from physical World.

The main challenge of respecting sovereignty in the broad issues of Governance including cybersecurity is that rising of non-state actors produced tough conflict with traditional international law based on rule of sovereignty. In 2015 , Group of government experts submitted a consensus report , named as "United Nations Charter" to UN General Assembly with relating to the development of ICT from the perspective of international security. And principle of sovereignty which is the basis to strengthen the use of ICT security, stating .As per ITU report , initially 40% of global population uses internet , has rise to 50% (now 60%) due to increase in developing country , However low penetration of internet users in underdeveloped and developing country cannot be ignored. Until 2008 , USA and Europe has monopolised the submarine global Optical Fibre Cable. In short todays Global Cyber space developing countries mainly serve as users and while developed countries mainly provides infrastructures and key applications. Also there is asymmetrical

disparity between Developed and developing Countries with respect to capability. But Now developing country have gained corresponding awareness and as a principle of matter intended to implement Cyber Security Strategy. And During recent times Global Cyber space term due Hackers , Country weakening and eliminating the sovereignty of Single Country due its technical incompetence .

Multi stake holder is an operation mode applied by US in 1990 in the process of Internet Commercialization which includes companies , individuals , NGO's and Sovereignties. China prefer more on the multilateral model than the multi-stake-holder model during the negation on how to govern the key information infrastructure that supports global cyberspace represented by the Root DNS server , root file and root file system.

The china main issue is to provide a more precisely defined cyber sovereignty and develop a sophisticated national strategy on cyber security such that it would be taken as a workable guiding principle. As per finding China does not trust the multi-stake-holder approach and of belief that US will abuse its ICT advantages to expand the sovereignty of USA into global space and at same time it has become kind of excuse to avoid other states like china protecting their interest in cyber space. Thus the more constructive theory and practice of International relations and international law in which traditional principle of sovereignty takes high importance in network word.

2 RESEARCH DESIGN AND METHODOLOGY

The present study is more about thought and behaviour exploration on a subject that is comparatively unexplored and even the researcher is not aware of what might emerge, therefore it is essentially qualitative in nature .where exploratory, descriptive and analytical research techniques have been adopted

Since the research is primarily qualitative in nature, the survey tool contains open-ended questions and the responses collected are essentially non-numerical that helps to understand what participants think and also why they think in a particular way Quantitative data collection allows collecting data that on-numeric Such an approach helps to explore the way decisions are made and simultaneously provides with detailed insight into why these decisions have been made. This kind of study therefore needs more rich and varied data that needs to be analysed astutely. The survey tool , therefore is littered with several open ended sentences that do not capture numerical values but instead comprises of several comments / questions which prompts from the respondents to express their opinions.

This chapter presents the objectives of the study, research questions, overall research design, tools and methods of data collection used in the study.

2.1 Objectives of the Study:

Digital sovereignty refers to the degree of control an individual, organization or government has over the data they generate and work with at local or online platform. The principle of Digital sovereignty insists on storage and protection of an individual's personal data in digital form on the cloud1 that is insisted to be hosted within the country in which the individual resides and it subjected only to the laws of that country. In context of India, it is primarily IT Act (2000) and its amendments (2008, 2013) that regulates all digital activities within India. It is supported by National Cyber Security Policy of India 2013 (NCSP 2013) that provides guidelines to build a secure and resilient cyberspace for citizens, business and government in the country. There is another equally important policy - The National Digital Communications Policy, 2018 (Department of Telecom) that seeks to unlock the transformative power of digital communications networks - to achieve the goal of digital empowerment.

2.2 AIM and OBJECTIVES

The aim of the study should had been to understand the dynamics of India's response to international challenges at addressing issue of digital sovereignty For doing so, it was pertinent to understand IT Act and NCSP -2003 and related policy, guidelines , issued by Government of India including Ministry of Communication and IT (MeitY)India within the context of cyberspace, IT infrastructure and Cyber Security. The analysis purports to attempt the following:

- To analyze the issues of privacy being compromised by Botnet /Hardwired Rootkit using secure network element responsible for data-theft or spying. .
- To study how cyber-attacks could affect the Digital Sovereignty
- To comprehend related available mechanisms and models to tackle cyber-attacks. Including Data Shared Model, Data Localisation Model and Data Trust Model.
- Cloud computing uses groups of servers and scalable resources and is accessible remotely through internet Clouds are employed to configure and deploy remote external servers as extensions to a company's local IT network.
- To undertake a comparative study of Data Protection Law of India , China ,Russia , USA and EU.
- To suggest guidelines for ensuring safety of data in State Data Centers.
- To suggest recommendations in the recently tabled Personal Data Protection Bill (PDP , 2019) for robust enactment of Data Protection Law of India.
- To propose a conceptual frame work for Data Security in the environment of Cloud Based Data Storage. i.e. for Data Protection Law

2.3 Research Design

The research design used in this study is exploratory, descriptive and analytical in nature and relies both on secondary sources as well as primary research. Exploratory research is conducted to have a better understanding of the digital sovereignty issues, linked with vulnerabilities and cyberthreats , data storage in cloud , IT equipment security testing mechanism . Descriptive research techniques are used to obtain information concerning the current status of the issues of data security and protection in context to India arisen due to e governance , and existing IT Act , NCSP -2013 and NDCP-2018 , Personal Data Protection bills/ laws (India and elsewhere) , popular prevailing models including (Data Shared Model,Data Localisation Model and Data Trust Model) and Cloud Storage guidelines in India.. The study further analyses the implementation measures required to secure Digital Sovereignty in India . The primary data collected through structured questionnaire deployed using google forms (https://docs.google.com/forms/d/e/1FAIpQLSdMgT-da0KnYe2PQTOi6PBYPC_QvJ5rNizzETQkqcXaRQ4qbw/viewform?usp=sf_link) is analysed using excel to present the findings and recommendations..

2.4 Survey Tool:

The survey tool was presented in four sub sections A, B, C & D.. Section A: Regarding Digital Sovereignty awareness/concept ,Section B: Existing Situation, Challenges and Issues in Digital Sovereignty Section C: Digital Sovereignty is National Issue or Nation Security and Growth Section D: Recommendation for Needful Action to Secure Digital Sovereignty

Section A: Regarding Digital Sovereignty awareness/concept Securing Digital Sovereignty

1.“Digital sovereignty encompasses the idea that users, being citizens or companies, have control over the data they generate”. In the Present day challenges of cyberspace; “Securing Digital Sovereignty “ is national concern to ensure Right of Privacy and Security in the Cyberspace to citizen of India. What is your view?

2.The statement “data is Oil “? What does the statement is implies for?

3.“Securing Digital Sovereignty” is concerned with which of following?

Section B: Securing Digital Sovereignty

(Existing Situation, Challenges and issues in Digital Sovereignty)

4.Personal Data Protection Bill -2020 is sufficient to deal with Digital Sovereignty?

5. Have ever been your data the& while online ?

6.What action you have taken in the past, when your data has been the& or your network was compromised?

7. Why “Securing Digital sovereignty” is important in modern days, because of ?

Section C : Securing Digital Sovereignty

Digital Sovereignty is National Issue or Nation Security and Growth

8.[A] Foreign governments spy on important business deals to benefit their firms.

8.[B] Foreign government interfere in domestic political discussions and elections?

8.[C] Foreign-controlled communication platforms forms ethnic tensions?

8.[D] Foreign government disrupts civilian infrastructure?

8.[E] Large corporations ignoring domestic law and agreements and abusing customer data?

8.[F] Large corporations using their market power to thwart attempts at changing their behaviour?

8.[G] Companies find out from shopping behaviour of customers, if teenagers are pregnant ,then ident them or target teenagers at their most vulnerable time?

8.[H] Companies put hidden microphones in devices and when find out claim they had no idea it was recording users?

8.[I] Commercial data tracking leaks secret military bases ?

8.[J] Commercial firms leaking data allowing people to track heads-of-state?

8.[K] Have you ever have been attempted for financial frauds?

8.[L] Are you confident that your data are secured, Safe and Privacy is ensured ?

8.[M] Are you confident that your Privacy is ensured on cyber space?

9. Securing Digital Sovereignty will affect the GDP growth rate adversely? Section

Securing Digital Sovereignty

10.Digital Sovereignty encompass following aspects

11.Digital Sovereignty faces challenges from

12.Google, Amazon ,WhatsApp, Microsoft & and Facebook data resides are outside India . Can Digital Sovereignty be ensured by Data localization strictly? *

14.Digital Sovereignty can be improved by ensuring Cyber Security and Cyber Safety Awareness?

15.Digital Sovereignty can be secured by

16.Do you think “Government should take needful correctives measures to ensures Digital Sovereignty India “ ?

17.Any suggestion /comment /inputs which you would like to mention on “Securing Digital Sovereignty “

However detailed questions are listed in annexure .

2.5 Tools and Methods of Data Collection

The most important and crucial aspect of any research is data collection, which provides answers to the questions under the study. Data collection relies on the instruments used. There are several tools for collecting data from respondents in social research like-Interview Schedule, Questionnaire, Observation guide etc. Respondent were basically chosen from all section IT savvy citizen of India and ensured homogeneous respondent by equivocal proportionate representation from citizen employed in Government of India , PSU , Private Sector , Students, Others (NRI and employees from MNC's) (Table 2.1). The respondents were ensured to be educated enough to appreciate the content of the survey tool and special consideration was attended

Job and Service Profile detailing of Respondent			
Respondent Job and Service Profile	IT Experience		
	No	YES	Grand Total
Government of India	27	79	106
Others (NRI+MNC)	6	11	17
Private Sector	9	21	30
PSU	4	15	19
Student	16	0	16
Grand Total	62	126	188

Table 2-1 details of Respondent Job and Service

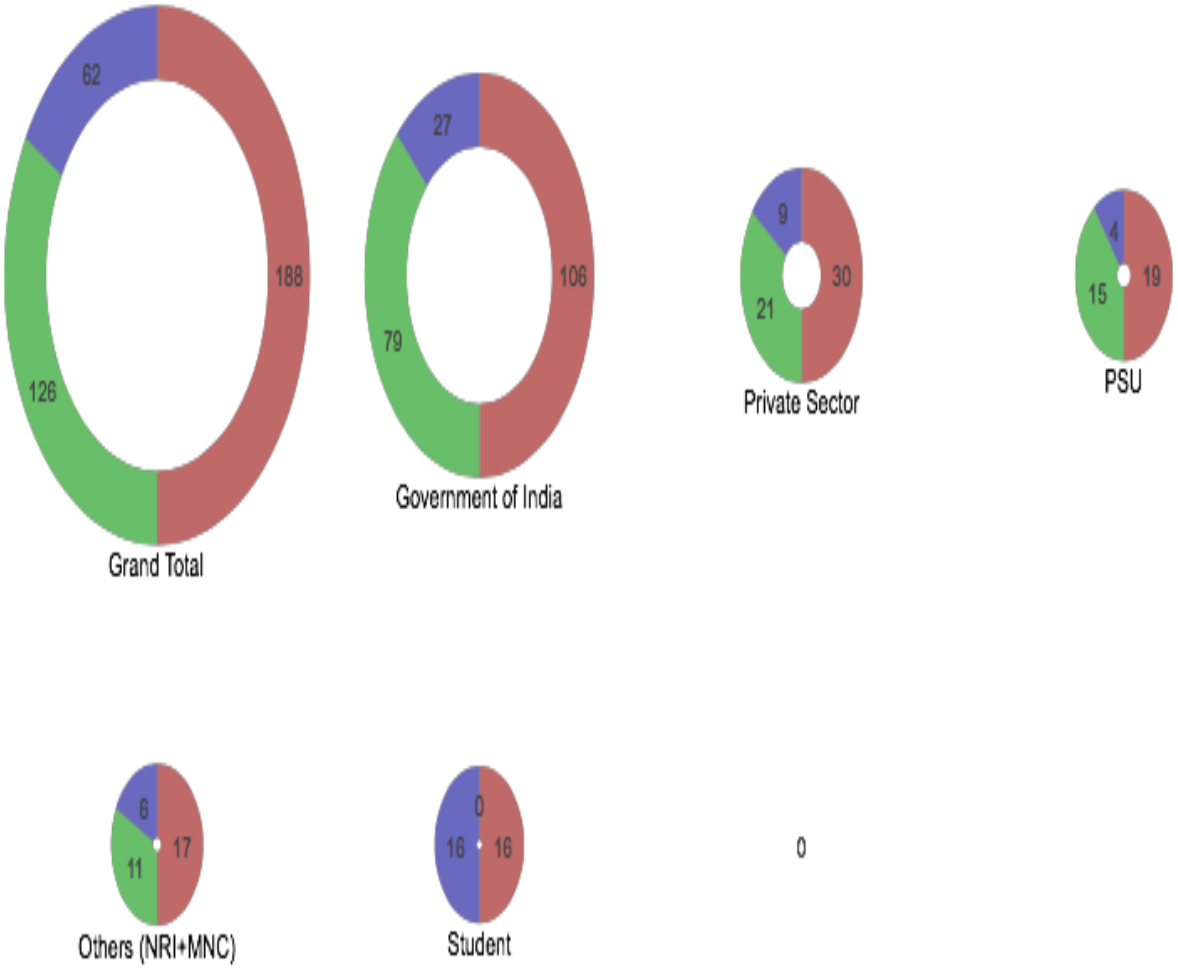


Figure 2-1 Details of Respondent Service Wise Category

Qualification Profile detailing of Respondent			
	IT Experience		
Qualification	No	YES	Grand Total
Doctorate	4	2	6
Graduation [Engineering]	15	48	63
Graduation [Humanities /others]	5	4	9
Post Graduation [Engineering/MBA]	17	70	87
Post Graduation [Humanities/other]	15	2	17
Undergraduate	6	0	6
Grand Total	62	126	188

Table 2-2 Details of IT experience of Respondents

IT experience Profile detailing of Respondent			
Details of Experience in number of yrs.	IT Experience		
	No	YES	Grand Total
< 10 Yrs.		13	13
< 15yrs		12	12
<5 yrs.		33	33
0 yrs.	62		62
More than 15yrs		68	68
Grand Total	62	126	188
Note 1 :// Experience in IT include working in Information Communication Technology & Devise design and development , operation and maintenance of IT environment , Tools & System Note2 :// Basic working knowledge of MS office and Windows does qualify for IT experience.			

Table 2-3 details of IT profile of Respondent

The data was collected by google forms in close groups of senior and middle level public sector officers with special emphasis on officers from Official of Ministry of Electronics , Ministry of Communication , Indian Institute of Public Administration , New Delhi , Abroad Multi National Company , Public Sector Uunit like BSNL,MTNL,PowerGrid, BHEL, and private and student of IIT,Indore , NIT's.

2.5 Interpretation of Data

The interpretation of the data hence collected through the structured questionnaires was undertaken through diagrammatic representation for data like bar graphs, pie charts etc. has been used.

Through these interpretation the gaps/ constraints in securing digital sovereignty were identified that went a long way for proposing the conceptual framework as well as assimilating policy recommendations put forth by the present study .

3 Data Security Policy :Global Context

3.1 Basic Principal of Data Security

3.2 EU :GDPR

3.2.1 Making Europe digitally competitive

It is clear that regulation is a crucial point when thinking about sovereignty in the digital world. Almost 30 years ago, liberalisation in the telecommunications sector started to get rid of borders, exclusive rights, monopolies and protectionism with the aim of promoting the competitiveness of European companies. Why take a step backwards instead of recalling the values that once targeted welfare and growth through embracing competitiveness? The goal to establish a European IT hub and to transform traditional industries into digital champions lags behind reality. At the same time, Europe already is a hub for innovative information and communications technology (ICT) as the Global Information Technology Report 2005 emphasises : Finland (2nd), Sweden (3rd), the Netherlands (4th) and the UK (8th) lead the field in ICT readiness. Combining these facts with Europe's capacity to harmonise a market of 500 million users is one of the biggest advances in this field when it comes to promoting economies of scale. The General Data Protection Regulation, the Directive on security of network and information systems and the Digital Single Market strategy as such are already moving in this direction.

In order to gain digital sovereignty, it is important to make Europe competitive in a global digital market and not to make the digital market European. Europe cannot create a second Silicon Valley or a European Google; but it can seize the opportunity of a diverse ecosystem, within which new undertakings can grow and established industries can open up to the existing European and even global ICT environment. Therefore, a harmonised digital single market that promotes innovation and fosters legal certainty for all participants is just a first step in encouraging this environment to become a digitally sovereign – that is, a confident and competitive – digital economy in Europe. Europe's economy has nothing to lose but its chance to shape digitalisation.

3.2.2 The Basic Principles of GDPR

The 7 principles of the GDPR listed and explained below:-

Lawfulness, fairness and transparency implies to “Obtaining the data on a lawful basis, leave the individual fully informed and keep your word.”

The concept of lawfulness states that all processes you have that in any way relate personal data of EU citizens must meet the requirements described in the GDPR. That includes data collection, data storing and data processing. The legislation has directions and norms for every step of your data management policy.

Fairness means that your actions – whether a data controller or a data processor – must match up with how it was described to data subject. Simply put, keep the promise you gave your client in the notice before collecting the data. Use personal data only for the purposes and during the time period you indicated.

A clear notice is what the concept of transparency is about. The data subject must stay informed regarding the purposes, the mean and the time period of data processing. You should let your clients know what exactly you are going to do with their data and who will have access to it.

Purpose limitation implies to “Be specific”

In the concept of fairness, One needs to stay true of its promise. The clients should must informed about the “purpose of the data collection”. As stated in the legislation, the purpose must be “specified, explicit and legitimate”. Data can be collected and used only for those purposes that have been transmitted to the data subject and about which the consent was received.

Data minimization implies to “Collect the minimum data you need “

The GDPR is designed to bring data collection to the necessary minimum. Personal data to be collected should be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. Note that under the GDPR you will actually have to justify the amount of data collected, so make sure to design an adequate policy and document it.

Accuracy implies “to Store accurate up-to-date data”

Personal data must be “accurate and where necessary kept up to date”. One must make sure that one does not retain old and outdated contacts and ensure the erasure of inaccurate personal data without delay. Storage limitations implies to ”Retain the data for a necessary limited period and then erase”

This principle relates to Data minimization and states that personal data must be “kept in a form which permits identification of data subjects for no longer than necessary”. You would have to set the retention period for personal data one collects and justify that this period is necessary for one’s specific objectives. Do not forget to document it.

Integrity and confidentiality implies to “Keep data secure”

The principle of integrity and confidentiality requires to be handle personal data “in a manner [ensuring] appropriate security”, which include “protection against unlawful processing or accidental loss, destruction or damage”. One must implement efficient anonymisation or pseudonymisation systems to protect the identity of your clients. You might also consider working towards gaining official certification, such as ISO 27001 to prove one commitment to cyber security.

Accountability implies “Record and prove compliance”.

Policies needed to be ensured, and Data collector are responsible for compliance with the principles of the GDPR. The new legislation requires a thorough documentation of all policies that govern the collection and procession of data. Under the new law, one must be able to demonstrate the documents that prove the compliance with the GDPR when requested by the authorities.

These are the 7 principles of the Data Protection Regulation and now you should have a pretty good idea and understanding of each of them. However, the GDPR is much more than these principles so do not stop here and make sure to explore more about the upcoming law. We wish you best of luck!

3.2.3 Digital Sovereignty and GAFA

- GAFA is an acronym for prime 4 on-line corporations – Google, Amazon, Facebook, and Apple. Microsoft has not been included as .Microsoft was not in a lot manipulating list when the acronym was fashioned.

- It is obvious that GAFA owns the info on the Internet. By GAFA, the quantity not limited to only 4 corporations. Rather on broader sense GAFA, it would relate to all multinational corporations on the Internet that have interaction in end-user knowledge assortment.

- There are two sides of information assortment and utilization. One is industrial and everybody is aware of it and others is People . The different is political the place governments of various international locations lay declare to the info sovereignty. People don't like governments snooping on them, particularly after the Cambridge Analytica fiasco.

  Now a days persons are conscious that they are often conditioned into sure predictable thought patterns simply by utilizing the information that are present in different networks like Facebook, WhatsApp, Ecommerce sites, That's why the difficulty of information sovereignty has turn out to be a mass concern that must be addressed urgently.

Solution to the Data Sovereignty Issue:-

- There are two sides to the activism associated to digital sovereignty — as with every struggle. While one facet advocates retaining knowledge on the datacentres in the identical nation because the person, the opposite desires sovereignty over all knowledge facilities of an organization in order that the federal government or company can entry knowledge at any time when required. This creates pressure as every nation has its personal guidelines and rules relating to .

- The finest resolution for this is to succeed in a standard floor and formulate a robust but related algorithm that apply to all of the datacentres – regardless of the nation the place they function. These guidelines will dictate who owns knowledge and in what kind. The encryption kind must be related throughout international locations, so that very same stage of safety applies to all datacentres. The similar guidelines can inform who can entry what knowledge and the way can knowledge be accessed.

- There is not a lot that the tip customers can do if they're to proceed utilizing the Internet. But there must be an answer in place that defines various things about knowledge sovereignty whilst the info is scattered amongst completely different international locations, all of the whereas, offering safety to the info.

3.2.4 Highlights of GDPR

The GDPR is a set of rules about how companies should process the personal data of data subjects. GDPR lays out responsibilities for organisations to ensure the privacy and protection of personal data, provides data subjects with certain rights, and assigns powers to regulators to ask for demonstrations of accountability or even impose fines in cases where an organisation is not complying with GDPR requirements.

1) Lawful, fair and transparent processing

The companies that process personal data are asked to process the personal data in a lawful, fair and transparent manner. Lawful, fair and transparent means :

i. Lawful means all processing should be based on a legitimate purpose.
ii. Fair means companies take responsibility and do not process data for any purpose other than the legitimate purposes.
iii. Transparent means that companies must inform data subjects about the processing activities on their personal data.

2) Limitation of purpose, data and storage

The companies are expected to limit the processing, collect only that data which is necessary, and not keep personal data once the processing purpose is completed. This would effectively bring the following requirements:

i. forbid processing of personal data outside the legitimate purpose for which the personal data was collected
ii. mandate that no personal data, other than what is necessary, be requested
iii. ask that personal data should be deleted once the legitimate purpose for which it was collected is fulfilled

3) Data subject rights

i. The data subjects have been assigned the right to ask the company what information it has about them, and what the company does with this information. In addition, a data subject has the right to ask for correction, object to processing, lodge a complaint, or even ask for the deletion or transfer of his or her personal data.

ii. There are 8 data subject rights according to GDPR

iii. As and when the company has the intent to process personal data beyond the legitimate purpose for which that data was collected, a clear and explicit consent must be asked from the data subject. Once collected, this consent must be

documented, and the data subject is allowed to withdraw his consent at any moment.

iv. Also, for the processing of children's data, GDPR requires explicit consent of the parents (or guardian) if the child's age is under 16.

5) Personal data breaches

i. The organisations must maintain a Personal Data Breach Register and, based on severity, the regulator and data subject should be informed within 72 hours of identifying the breach.

ii. There are 5 steps to handle a data breach according to GDPR.

6) Privacy by Design

Companies should incorporate organisational and technical mechanisms to protect personal data in the design of new systems and processes; that is, privacy and protection aspects should be ensured by default.

7) Data Protection Impact Assessment

To estimate the impact of changes or new actions, a Data Protection Impact Assessment should be conducted when initiating a new project, change, or product. The Data Protection Impact Assessment is a procedure that needs to be carried out when a significant change is introduced in the processing of personal data. This change could be a new process, or a change to an existing process that alters the way personal data is being processed.

There are 5 phases of the EU GDPR Data Protection Impact Assessment.

8) Data transfers

The controller of personal data has the accountability to ensure that personal data is protected and GDPR requirements respected, even if processing is being done by a third party. This means controllers have the obligation to ensure the protection and privacy of personal data when that data is being transferred outside the company, to a third party and / or other entity within the same company.

There are Implementing 3 main accountability principles under the EU GDPR.

9) Data Protection Officer

When there is significant processing of personal data in an organisation, the organisation should assign a Data Protection Officer. When assigned, the Data Protection Officer would have the responsibility of advising the company about compliance with EU GDPR requirements.

10) Awareness and training

Organisations must create awareness among employees about key GDPR requirements, and conduct regular trainings to ensure that employees remain aware of their responsibilities with regard to the protection of personal data and identification of personal data breaches as soon as possible.

Conclusion: GDPR principles are key for understanding the GDPR

To conclude, there are a significant number of requirements that relate to EU GDPR. It is important to understand these requirements, and their implications for your company, and implement them within the context of your company. Such implementation would require a dedicated effort, like that of running a project.

3.3 Data Protection and Privacy Laws for the United States in 2020

The internet is rapidly evolving and so are the guidelines by which it operates. There many are the data protection and privacy laws for the United States in 2020.The global internet usage hit 3.8 billion by mid last year. The internet is changing life as we know it in a significant way.

Most of these changes are positive. However, the world has seen instances where the internet has shown its ugly side. As such, there must be an enactment of progressive laws to deal with emergent internet-related threats.

Privacy remains one of the most significant concerns for the billions of online users. To address this developing concern, the United States continues to enact privacy laws. These regulations seek to protect internet users and their information against unauthorized access or interference.

What Are Privacy Laws?

A majority of Americans believe that the security of their data is no longer guaranteed. Half of USA populations believe that five years ago, their personal information was safer than it is today.

.

With such emerging concerns over the security of personal information, Consequently, the U.S. government, through the two chambers of Congress, device legislative solutions to this concern. Information privacy laws refer to legislation that addresses the regulation, storage, and use of personal information. The bills address the extent of the right to obtain such information by the government, organizations, or individuals.

In the context of the internet, such laws govern the legal right to privacy in your routine activities online. Some of the rules are listed as below:-

Electronic Communication Privacy Act

With the changing scope of internet usage and privacy in the United States without discussing the ECPA. This Act came into operation in the year 1986. However, it still affects online use and data privacy in the United States to date.

The ECP Act allows the government the right to access your communication on various channels, including but not limited to emails, social media, and any other digital communication platform.

The U.S. government has come under pressure on the use of this Act and the consequence this has on privacy. However, following the 9/11 attacks and the need to improve on surveillance, the government still reserves this vital privilege. Internet providers such as Google must turn in personal information about you on request from the government.

The Electronic Communication Privacy Act often affects the application of most other subordinate laws that have been passed since the year 1986.

Cyber Intelligence Sharing and Protection Act (CISPA)

With the security and terror in mind, the government has been keen to enhance its authority to access or to demand information on issues of national security.

But for most people, this Act has a fundamental legal pitfall related to the definition of the term "cyber threat."

The federal government also has an obscure right to coerce anyone to share information on potential cyber threats regardless of their willingness to cooperate. Most of the opposition to this Act is based on the presumption that the government is using cyber-security as a tool to gain access to private information against the public will.

The Health Insurance Portability and Accountability Act

This law recognizes "covered entities" under HIPPA as part of the need to acknowledge "protected health information." Covered entities recognized in the Act include hospitals and insurance companies.

The HIPPA now defines the standards that ought to be in place to ensure the utmost safety for your information as you seek health or insurance services. At the State level, there've been other more recent privacy laws that supplement the privacy laws at the federal law.

The California Consumer Privacy Act

The CCPA, law handles digital privacy in the State of California according to member's unprecedented access to data collected by companies or businesses.

Any business that sells consumer's information is under obligation to publish the names of such individuals online.

As a consumer, having the right to opt-out of allowing the sale of such personal information. With the growing demand for consumer information, citizen have the right to decide on whether their data should be commercial. The CCPA defines personal data and provides critical stipulations on the scope of use of such data.

Most other states have moved to imitate this approach to data privacy and access in California. States such as Massachusetts are looking forward to enacting similar laws by the year 2023.

Nevada Chapter 603A Security and Privacy of Personal Information and SB 220

Other states such as Nevada already have rules in place that deal with the issue of data privacy. This chapter covers the definition of private information.

The legislation also covers the scope of use of this information by third parties. Such information covered in the section includes the primary role by institutions. Such organizations include health care providers and businesses that must institute measures to protect such information from access and misuse.

Understanding Personal Identifiable Information PII

PII refers to the unique data used to identify a specific person. Such information includes full names, the social security number, bank account information, driver's license, or passport. This information is critical when deciding on whether there's a breach of data privacy.

In the European Union, the General Data Protection Regulation has been an essential tool in the definition of personally identifiable information. The Expedited Policy Development Process (EPDP) remains a critical approach for the process of balancing the government's right to access information and privacy laws.

Ignorance of the Law Is No Excuse

The enactment of privacy laws seeks to ensure a balance between citizen right to information privacy while online and national security. Right to privacy is a legal guarantee as long as this freedom does not put the security of the United States in jeopardy. Knowing and understanding these privacy laws is essential in 2020.

3.4 China Data Protection Law

Under the new Cybersecurity Law, collecting any user's personal information requires the user's consent and network operators must keep collected information strictly confidential. Personal information is defined as information that can be used on its own or with other information to determine the identity of a natural person, including the person's name, date of birth, ID card number, biological identification information (e.g. fingerprints and irises), address, and telephone number. Once such information has been de-identified, it is no longer subject to the requirement for personal information under the law.

According to the new Cybersecurity Law, network operators are subject to the following requirements when collecting and using personal information:-

- Collection and use of personal information must be legal, proper and necessary.
- Network operators must clearly state the purpose, method, and scope of collection and use, and obtain consent from the person whose personal information is to be collected; personal information irrelevant to the service provided shall not be collected.
- Network operators shall not disclose, alter, or destroy collected personal information; without the consent of the person from whom the information was gathered, such information shall not be provided to others.
- In the event of a data breach or a likely data breach, network operators must take remedial actions, promptly inform users, and report to the competent government agencies according to relevant regulations.

- In case of an illegal or unauthorized collection and use of personal information, a person is entitled to ask a network operator to delete such personal information; when information collected is wrong, an individual can request correction.
- Owners of networks, administrators of networks, and network service providers. Telecom and Internet service providerrs.
- Networks are systems consisting of computers or other data terminal equipment and relevant devices that collect, store, transmit, exchange, and process information according to certain rules and procedures (Article 76 of the new Cybersecurity Law). If you have a couple of computers at home that can share files, and perhaps a printer connected to them, you technically have a network. The law is not likely to go that far, but the generic definitions of network and network operators leave a lot of room for interpretation, which is exactly how the Chinese government wants it.

The new Cybersecurity Law also requires critical information infrastructure operators (CIIOs) store within China personal information and important data gathered and generated within China and conduct annual security risk assessments regarding their data. Though the definition of CIIO is yet to be clarified, we already know China's yet to be finalized Measures for Security Assessment of Personal Information and Important Data Leaving the Country will likely require foreign companies doing business in China make big changes in how they handle data. The Cyberspace Administration of China (CAC) published a draft of Measures for Security Assessment of Personal Information and Important Data Leaving the Country back in April, raising many concerns for foreign businesses operating in China.

These Measures for Security Assessment would expand the data localization requirement to all network operators. This would mean that pretty much all personal information and important data collected by network operators within the PRC must be stored within China and not leave China, other than for "genuine business need" and after a security assessment.

Since the new Cybersecurity Law does not differentiate between internal and external networks, it is broad enough to include any company that owns an internal network. Will your China WFOE be able to transmit employee information back to its overseas headquarters? In China's Cybersecurity Law and Employee Personal Information, we set out best practices for doing this, but that was written before publication of the Draft Measures. Should the Draft Measures become effective — as expected — our views on data transfers will almost certainly toughen. Foreign companies are already setting up data centres in China so as to be able to keep data local and many of our clients are looking at doing the same.

4 Data Security Policy :Indian Context

4.1 IT Act and Data Protection Law

4.1.1 Right to Privacy

The nine judge bench of supreme court, headed by Justice DY Chandrachud overruling the principles evolved in the Habeas Corpus case in the case Justice Puttaswamy (Retd.) V. Union of India , evolved as a landmark judgment in the history of India with regards to the status of Right to Privacy and reiterated that Privacy is constitutionally protected right which not only emerges from guarantee of life and Personal liberty in Article 21 of Constitution of India, but also arises in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental right contained in part III of Constitution of India. This article shall envisage on the origin privacy and judicial developments on privacy.

I. ORIGIN OF PRIVACY

In 1859, John Stuart in his essay "On Liberty" gave expression to the need to preserve a zone within which the liberty of the citizen would be free from the authority of the state. In late 1890, Samuel D Warren and Louis Brandeis stipulated the need of right to enjoy life which included 'right to be alone'. The right "to be let alone" thus represented a manifestation of "an inviolate personality", a core of freedom and liberty from which the human being had to be free from intrusion. It justified the need of being left alone with the early developments in technology, photography, and newspaperization.

The intention behind it introduction of such a principle was to protect personal writings and personal productions, not only from theft and physical appropriation but against publication in any form which might not be consensual in nature. Hence, at the time when development and technology change started threatening the individual in public gaze, many eminent jurists regarded the right to be let alone as an added chapter in the law of privacy.

II. GOLDEN TRILOGY OF CASES ON PRIVACY

Early developments in the history of privacy saw two landmark judgments – the 8-judge bench decision in M.P. Sharma v. Satish Chandra (1954 SCR 1077) and the 6-judge bench decision in Kharak Singh v. The State of U.P. (1964 (1) SCR 332). In

M.P. Sharma, the process of search and seizure was challenged as it violated Article 20(3) of the Constitution of India. In Kharak Singh, the court dealt with UP Police Regulations which provided for secret picketing, domiciliary visits, periodical inquiries, reporting of movements and collection of records of history-sheeters, violating Article 21 of Constitution of India. In both the cases, the court dismissed the existence of the fundamental right to privacy envisaged in the constitution.

However, it shall be noted that in both the cases the petitioner's arguments relied on the A. K. Gopalan Case which enumerated that Article 19 and Article 21 are mutually exclusive. The case has been overruled and considered bad in law after the landmark R. C. Cooper Case ((1978) 1 SCC 248) in which the court discarded the theory that fundamental rights are water-tight compartments. Hence, by virtue of this, principles enumerated in Kharak Singh and M. P Sharma should also be overruled.

This was also re-strengthened by Maneka Gandhi v. Union of India (1970) 1 SCC 248), in which court ruled that enumeration in Article 19 does not deprive Article 21 of its expansive ambit. While analyzing the discordant view in the ADM Jabalpur case, the court held that the constitution is not the sole repository of life and liberty. Even if the rights were not granted under Article 21, the state would not be permitted to suspend such rights. For example, as under the 44thAmendment, Article 359, even in an emergency, the power to move to the court for enforcement of rights shall not be suspended for Article 20 and 21.

III. LATER DEVELOPMENTS ON PRIVACY IN INDIA

Later, three judgments saw and acknowledged privacy as a constitutionally protected fundamental right, namely, Gobind v. State of Madhya Pradesh (1975 2 SCC 14), PUCL v. Union of India (telephone tapping case) and R. Rajagopal v. State of Tamil Nadu ((1994) 6 SCC 632)(Court dealt with a conflict between the freedom of the press and the right to privacy). However, all three judgments were of smaller benches and left the stakeholders in dilemma with regards to interpretation of Privacy under Article 21 of the constitution of India or not. In Rajagopal Case the court held that the right to privacy has two aspects: the first affords an action in tort in damages for the unlawful invasion of privacy, and the second is a constitutional right.

In the Puttaswamy case the arguments before the courts (Respondent) were [A] very few people are affected by the right to privacy [B] Privacy was rejected as a fundamental right in constitutional debates [C] the statutory protection to privacy

exists, and hence there is no need to make it a constitutional right [D] Privacy is still an elitist construct [E] Privacy is common law right, not a fundamental right [F] Substantive due process is not granted in the Indian Constitution and [G] Privacy is civil liberty, not a" personal liberty" as in Article 21.

However, petitioner's arguments on the same were that privacy is a natural and inalienable right, individuals have right to informational privacy, privacy is a concern against the state and non-state actors and privacy have always been legislatively recognized in India vide section 5, Indian Telegraph Act of 1885; Section 26,Indian Post Office Act 1898 and Section 8(1)(i) of Right to Information Bill, 2011 to much later, Privacy Bill,2011.

IV. CRITICISMS OF THE DOCTRINE OF PRIVACY

There have been many criticisms of the said doctrine, Thomson's Reductionism theory stipulates that right to Privacy has been derived from other rights such as the right to property and bodily security, so it should be best understood as a derivation of other rights and must be interpreted accordingly. Early few articles, published in Havard Law Review also saw the idea that the scales of balancing state and personal interest must tip in favor of the national need for knowledge, innovation, and development.

Thus, there shall be no such hindrances like privacy which is tilted towards personal interest over national need. The idea of privacy was also criticized by the feminist saying that privacy should not be a cover to asset patriarchal mindset and state must take issues like domestic violence in the private sphere seriously. These ideas left the status of interpretation and extent of use of the idea of privacy in dilemma.

However, Supreme Court while giving the directions in the said judgment relied on the literature which as defined some specific principles on privacy such as decisional autonomy, spatial control, and informational control. On analyzing the diagram, in the Indian context, fundamental right to privacy should ideally deal with [A] privacy of the person and body;[B] informational privacy and [C] autonomy in consonance to the Articles 19(a)to (c), 20(3), 21 and 25.

V. CONCLUSION

All in all, the court didn't find any contravention with regards to international conventions and the national legislative decisions and recognized the need for constitutional validity of the said right. India is already a signatory to 1948 UN Declaration of Human Rights, wherein Article 12 speaks on Right to Privacy. Treaties

must be respected vide directive principle 51(c). The preamble to 'Necessary and Proportionate Principles' also insist on this right.

However, post the judgment the judicial system of India still needs to deal with the subject like Aadhar and application of the said right. It will now be easier for courts to decide on factors like usage of biometrics, phones in light of privacy, however, another pertaining question to it is whether the concept of Aadhar is violative to the right of privacy or the way government has planned to implement it. These questions will be dealt in the case which Supreme Court shall be hearing soon.

4.1.2 Personal Data Protection Bill

The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. The highlight of PDPB are as follows:-

i. Applicability:

The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India. Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator.

ii. Obligations of data fiduciary:

A data fiduciary is an entity or individual who decides the means and purpose of processing personal data. Such processing will be subject to certain purpose, collection and storage limitations. For instance, personal data can be processed only for specific, clear and lawful purpose. Additionally, all data fiduciaries must

undertake certain transparency and accountability measures such as: (i) implementing security safeguards (such as data encryption and preventing misuse of data), and (ii) instituting grievance redressal mechanisms to address complaints of individuals. They must also institute mechanisms for age verification and parental consent when processing sensitive personal data of children.

iii. Rights of the individual:

The Bill sets out certain rights of the individual (or data principal). These include the right to: (i) obtain confirmation from the fiduciary on whether their personal data has been processed, (ii) seek correction of inaccurate, incomplete, or out-of-date personal data, (iii) have personal data transferred to any other data fiduciary in certain circumstances, and (iv) restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.

iv. Grounds for processing personal data:

The Bill allows processing of data by fiduciaries only if consent is provided by the individual. However, in certain circumstances, personal data can be processed without consent. These include: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency.

v. Social media intermediaries:

The Bill defines these to include intermediaries which enable online interaction between users and allow for sharing of information. All such intermediaries which have users above a notified threshold, and whose actions can impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.

vi. Data Protection Authority:

The Bill sets up a Data Protection Authority which may: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Bill. It will consist of a chairperson and six members, with at least 10 years' expertise in the field of data protection and information technology. Orders of the Authority can be appealed to an Appellate Tribunal. Appeals from the Tribunal will go to the Supreme Court.

vii. Transfer of data outside India:

Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as critical personal data by the government can only be processed in India.

viii. Exemptions:

The central government can exempt any of its agencies from the provisions of the Act: (i) in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and (ii) for preventing incitement to commission of any cognisable offence (i.e. arrest without warrant) relating to the above matters. Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as: (i) prevention, investigation, or prosecution of any offence, or (ii) personal, domestic, or (iii) journalistic purposes. However, such processing must be for a specific, clear and lawful purpose, with certain security safeguards.

ix. Offences:

Offences under the Bill include: (i) processing or transferring personal data in violation of the Bill, punishable with a fine of Rs15/- crore or 4% of the annual turnover of the fiduciary, whichever is higher, and (ii) failure to conduct a data audit, punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher. Re-identification and processing of de-

identified personal data without consent is punishable with imprisonment of up to three years, or fine, or both.

x. Sharing of non-personal data with government:

The central government may direct data fiduciaries to provide it with any: (i) non-personal data and (ii) anonymised personal data (where it is not possible to identify data principal) for better targeting of IT services.

xi. Amendments to other laws:

The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data.

The Personal Data Protection Bill, 2019 ("PDP Bill") was introduced in the lower house of the Parliament on December 11, 2019. The "Committee of Experts on Data Protection" chaired by Justice B.N. Sri Krishna submitted its report along with the draft bill ("2018 Bill") on 27th July 2018. The PDP Bill is largely based on the 2018 Bill and seeks to protect the personal data of individuals.
The PDP Bill governs the processing of personal data:

i. where such data has been collected, disclosed, shared or otherwise processed within the territory of India,
ii. the State, any Indian company, any citizen of India association of persons, and
iii. by foreign entities dealing with personal data of individuals in India. As this PDP Bill is in line GDPR so take care of all intricacy,

However Bill contains the provision Data Localisation may be ensured.

4.1.3 Potential Impacts of Draft India PDPB -2018 on Global Capability Centres

Since late 1990s, there has been a significant rise in the establishment of Global Capability Centres (GCCs) within India. There are currently GCCs operating across numerous sectors including information technology (IT), financial services, telecommunication, manufacturing, oil & gas, aerospace, healthcare, automobile, and biotech.

The Personal Data Protection Bill (PDPB) needs to be applicable to organisations operating in India and abroad that process personal data of Indian data principals . Thus, GCCs will also come under the purview of PDPB as they process the personal data (or may be in some cases, sensitive personal data) of their employees based in India and/or any other individuals within the territory of India. This will trigger GCC to revisit their current ecosystem (across people, process, and technology layers) to align with the requirements under the PDPB.

Given the nature of the industry structure and operations carried out by GCCs, a large volume of personal and sensitive personal data is collected, stored, processed, retained, and disposed in India. For this reason, the PDPB would impact many areas of GCCs such as legal, IT, human resource, sales and marketing, procurement, finance, and information security, etc.

PDPB's key requirements and potential impact on GCCs

- Notice: PDPB requires data fiduciaries to provide notice about its personal data processing activities and associated purpose at the time of collection. This needs to be in a clear, concise, and easy to read language. Hence, organisations would be required to update their website privacy policy to include elements such as consent, purpose of processing personal data, and security controls for protecting personal data etc., with respect to transactions related to Indian data principal.

- Cross-border transfer and data localisation: PDPB requires organisations to store at least one serving copy of personal data on a server or data centre located in India. Localisation of personal data would affect organisations due to the additional costs involved in the establishment of servers and data centres to store

the data. In addition, by the way of enhanced vulnerability considering that there would be multiple copies of personal data at multiple locations. Organisations need to incorporate standard contractual clauses (data privacy oriented contractual language) and obtain explicit consent of the data principals for certain categories of personal data.

- Privacy by design: PDPB requires data fiduciaries that launch new services, products, innovative technologies or expand into new geographies to include data protection from the very onset of the designing of systems. Organisations would have to incorporate privacy into design, operations, and management of their systems and business processes.

- Choice and consent: PDPB requires data fiduciaries to describe the choices available to the data principal. In addition, obtain implicit or explicit consent for the collection, use, and disclosure of personal information. Therefore, organisations would have to update their standard operating procedures (SOPs). They also need have to identify the personal data collection points to implement the privacy requirement to provide choice and consent to data principals.

- Data protection impact assessment (DPIA): PDPB requires data fiduciaries to conduct a data DPIA. This is done to evaluate risks that result from data processing, particularly when large volumes of personal data and/or sensitive personal data are processed.

- Rights of data principals: PDPB provides data principals with rights such as right to access their data, right to seek correction of their data, right to portability of their data from one entity to another, and the right to be forgotten, wherein an entity can be prevented from further disclosure of personal data. Hence, organisations need to update their processes and technical controls to comply with data principal's rights in a timely and efficient manner.

- Data breach notification: PDPB requires data fiduciaries to notify the Data Protection Authority within a reasonable period of time. They need information related to nature of the personal data affected by the breach, the number of individuals affected by the breach, the possible consequences of the breach, and the mitigating measures taken by the organisation. Organisations would be

required to develop procedures to identify and report data incidents by implementing process and technical solutions.

- Culture and communication: PDPB requires organisations to develop a culture of privacy by making employees aware about the best practices to handle personal data including disclosure to only authorized recipients. Therefore, organisations would be required to undertake specific privacy trainings that allow employees to understand all privacy-risks related to the personal data they process.

- Third party compliance: PDPB requires organisations to expand the scope of due diligence of third parties by adding privacy-related requirements and conducting a data privacy impact assessment while on-boarding new third parties. Therefore, GCCs need to make sure their third parties comply with privacy requirements and follow strict policies and controls, aligned with their policies and controls.

- Data disposal: PDPB requires that personal data should only be stored for a time period necessary for its processing and thereafter, it should be securely destroyed. The end of data lifecycle requirement would obligate organisations to prepare a data lifecycle procedure, data retention and secure destruction procedure, and update contracts to govern the data disposal obligations in a timely and secured manner.

4.2 National Digital Communication Policy -2018

With a view to cater to the modern needs of the digital communications sector of India, the Union Cabinet on Wednesday approved the National Digital Communications Policy-2018 (NDCP-2018). The new telecom policy has been formulated in place of the existing National Telecom Policy-2012 and aims to facilitate India's effective participation in the global digital economy. The policy aims to ensure digital sovereignty and the objectives are to be achieved by 2022. Under the new telecom policy, the government aims to provide universal broadband connectivity at 50 Mbps to every citizen. It has kept a target of providing 1 Gbps connectivity to all Gram Panchayats by 2020 and 10 Gbps by 2022.

Here are the key features of the policy:

- Provide universal broadband connectivity at 50 Mbps to every citizen.

- Provide 1 Gbps connectivity to all Gram Panchayats by 2020 and 10 Gbps by 2022.
- Ensure connectivity to all uncovered areas.
- Attract investments of USD 100 billion in the Digital Communications Sector.
- Train one million manpower for building New Age Skill.
- Expand IoT ecosystem to 5 billion connected devices.
- Establish a comprehensive data protection regime for digital communications that safeguards the privacy, autonomy and choice of individuals.
- Facilitate India's effective participation in the global digital economy.
- Enforce accountability through appropriate institutional mechanisms to assure citizens of safe and secure digital communications infrastructure and services.

One of its objectives is to ensure connectivity to all uncovered areas and attract investments of $100 billion in the Digital Communications Sector. Besides this, one million manpower will be trained for building New Age Skill. It also aims at expanding IoT ecosystem to 5 billion connected devices. The IoT is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity. This enables these things to connect, collect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems. IoT results in efficiency improvements, economic benefits, and reduced human exertions.

4.3 NCSP-2013 and NCSS 2020

Government of India formulated National Cyber Security Policy in the year 2013. The policy may have been apt for that era of time, but the present scenario of Cyber Threat and Cyber Crime Proliferation, demands a more exhaustive Policy.

The National Security Council Secretariat (NSCS), Government of India, had met and decided to Revise the National Cyber Security Policy, and bring out a more exhaustive and meaningful National Cyber Security Strategy 2020. Following are the agenda of National Cyber Security Strategy 2020:-

1. National Cybersecurity Strategy is to secure the national cyberspace, which has been subjected to privacy breaches and hacks in the past.
2. The government aims to strengthen the infrastructure and processes that are connected to the internet.
3. The government aims to synergise the resources available through cooperation and collaboration with different players.

The Government further decided to come out with the National Cyber Security Strategy 2020 (NCSS 2020). NCSS 2020, is under preparation with the co-operation and feedback from three pillars of cyber security: secure (national cyberspace), strengthen (structures, people, processes, capabilities), and synergise (resources including cooperation and collaboration).

The Need for National Cyber Security Strategy 2020 (NCSS 2020)

India was one of the first few countries to propound a futuristic National Cyber Security Policy 2013 (NCSP 2013). Since the adoption of NCSP 2013, the technologies, platforms, threats, services and aspirations have changed tremendously. The transformational Digital India push as well as Industry 4.0 is required to be supported by a robust cyberspace. However, Cyber intrusions and attacks have increased in scope and sophistication targeting sensitive personal and business data, and critical information infrastructure, with impact on national economy and security. The present cyber threat landscape poses significant challenges due to rapid technological developments such as Cloud Computing, Artificial Intelligence, internet of Things, 5G, etc. New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime & cyber terrorism, and so on. Threats from organised cybercriminal groups, technological cold wars, and increasing state sponsored cyber-attacks have also emerged. Further, existing structures may need to be revamped or revitalised. Thus, a need exists for the formulation of a National Cyber Security Strategy 2020.

What is Ahead

"5G will change the entire scope of cybersecurity in India. There are new aspects like ransomware, and IoT was not there. So with these changes, there is going to be a new strategy for dealing with cybersecurity.

A task force, under NCSS, is responsible for formulating a five-year strategy (2020-25). The NSCS-2020 is supposed to includes cloud computing and AI, too. It also raises issues of "include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, and international cooperation on cybercrime & cyber terrorism".

The step taken by the Indian government, and its concerns towards cybersecurity in India, was not been enough; yet this present strategy of inviting comments from the Indian Citizens (and others) is the need of the hour. The loss to businesses and also to the common citizens' due to lack of Cybersecurity measures had affected multi fold. The New National Cybersecurity Strategy is likely to play a crucial role in helping businesses overcome security challenges in the Indian context where the common man is affected. "Cyber Secure India" thus encourages each one of Indian Citizen.

4.4 State Data Centre and Cloud

Background:-

In order to utilize and harness the benefits of Cloud Computing, Government of India embarked upon an ambitious initiative – "GI Cloud" which has been coined as 'Meghraj'. The focus of this initiative is to accelerate delivery of e-services in the country while optimizing ICT spending of the Government.

MeitY has empanelled the Cloud Service offerings of CSPs in the form of Bouquet of Cloud Services. The Bouquet of Cloud Services comprises of Basic Cloud services which are mandatory services under CSPs various Cloud offerings. The CSPs has to offer the "Basic Cloud Services" to the Government Organizations under at least one of the Cloud Deployment Models defined by MeitY which are Public Cloud, Virtual Private Cloud and Government Community Cloud. The details of such Cloud offerings are mentioned as below-

MeitY Empaneled CSPs Basic Cloud Service offering Detail with Datacenter location							
Cloud Service Provider	Data Center Location		Deployment Models for Basic Cloud Service offering*			ST QC Audit Status	Empanelment Validity
	For Public Cloud and VPC	For GCC	Public Cloud	VPC	GCC		
Amazon Internet Services Pvt. Limited	1) Mumbai -03	Not Applied	√	√	NA	Audited	24/10/2022
Bharat Sanchar Nigam Limited (BSNL)	1) Ahmedabad -01 2) Faridabad-01	1) Ahmedabad -01 2) Faridabad-01	√	√	√	Audited	12/09/2022
CtrlS Data Centers Limited	1) Hyderabad-01 2) Navi Mumbai -01	1) Hyderabad-01 2) Navi Mumbai -01	√	√	√	Audited	12/09/2022
Cyfuture India Private Limited	1) Noida-01 2) Jaipur-01	1) Noida-01 2) Jaipur-01	√	√	√	Audited	12/09/2022
ESDS Software solution Pvt. Limited	1) Nashik-01 2) Mumbai- 01 3) Bengaluru- 01	1) Nashik-01 2) Mumbai- 01 3) Bengaluru- 01	√	√	√	Audited	17/09/2022
Microsoft Corporation (India) Private Limited	1) Chennai-01 2) Mumbai-01 3) Pune -01	1) Chennai-01 2) Mumbai-01 3) Pune -01	√	√	√	Audited	12/09/2022
Netmagic IT Services Private Limited	1) Mumbai-02 2) Bengaluru- 02	1) Mumbai-02 2) Bengaluru- 02	√	√	√	Audited	12/09/2022
Nxtra Data Limited	1) Bengaluru- 01 2) Noida- 01	1) Bengaluru- 01 2) Noida- 01	√	√	√	Audited	24/10/2022
Reliance Corporate IT Park Limited	1) Mumbai-01 2) Jamnagar-01	1) Jamnagar-01	√	√	√	Audited	04/12/2022
Sify Technologies Limited	1) Bengaluru- 01 2) Navi Mumbai- 01	1) Bengaluru- 01 2) Navi Mumbai- 01	√	√	√	Audited	12/09/2022
Tata Communications Limited	1) Bangaluru-01 2) Mumbai -01 3) New Delhi-01	1) Mumbai -01 2) New Delhi-01	√	√	√	Audited	12/09/2022
Web werks India Pvt. Limited	1) Mumbai -01 2) Pune-01	1) Mumbai -01 2) Pune-01	√	√	√	Audited	17/09/2022

***With mandatory inclusions as per Bouquet of Cloud services**

Table 4-1 details of CSP Empaneled

MeitY (Ministry of Electronics and Information Technology) has invited the bid documents from the prospective Cloud Service Providers with reference to the RFP for “Provisional Empanelment of Cloud Service Offerings of Cloud Service providers (CSPs)” dated 30th December 2015.

The envisaged implementation model is depicted in the below figure:

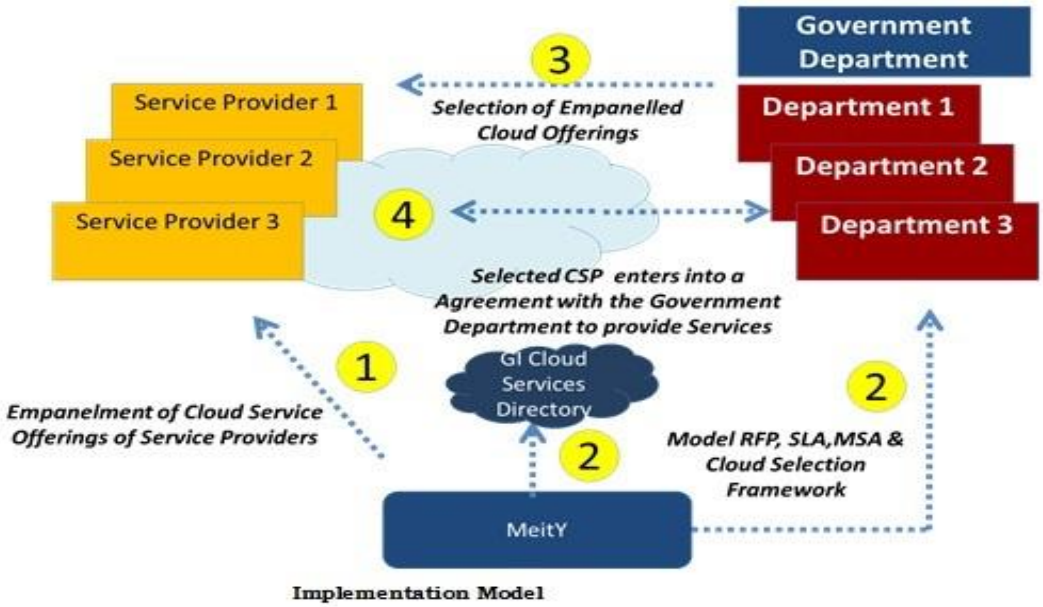


Figure 4-1 Cloud Implementation Model

The empanelment of the Cloud service offerings of CSPs has been done for a combination of the Cloud Deployment models and Service offerings as mentioned below:

Deployment model

1. Public Cloud
2. Virtual Private Cloud (VPC)
3. Government Community Cloud (GCC)

Service Offerings

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Disaster Recovery as a Service (DRaaS)
4. Dev / Test Environment as a Service (DevOps)
5. Virtual Desktops as a Service (VDaaS)

The Audit Criteria Documents have been approved by MeitY for Auditing the empanelled CSPs

MeitY has completed the provisional empanelment of the Cloud Service Providers (CSPs) in September 2016. Subsequent to this empanelment, it is proposed to conduct

the audit of these CSPs. A detailed audit criteria has been approved comprising of the following documents for auditing the empaneled CSPs:

1. Application form for Cloud Service Provider - This is the form that CSPs need to fill and submit to STQC to get themselves audited.
2. Audit Criteria for CSPs - This document covers specific requirements for cloud service providers to comply with for the purpose of conformity.
3. Audit Report – Audit Report format is to provide information for audit decision (or otherwise) in a uniform presentation. This makes easy to correlate with the audit criteria.
4. Vocabulary – This is the list of definitions of various terms/terminologies used in the various audit documents.
5. Schedule of Charges – This document highlights the charges for application, audit and evaluation and statement of conformity fees.

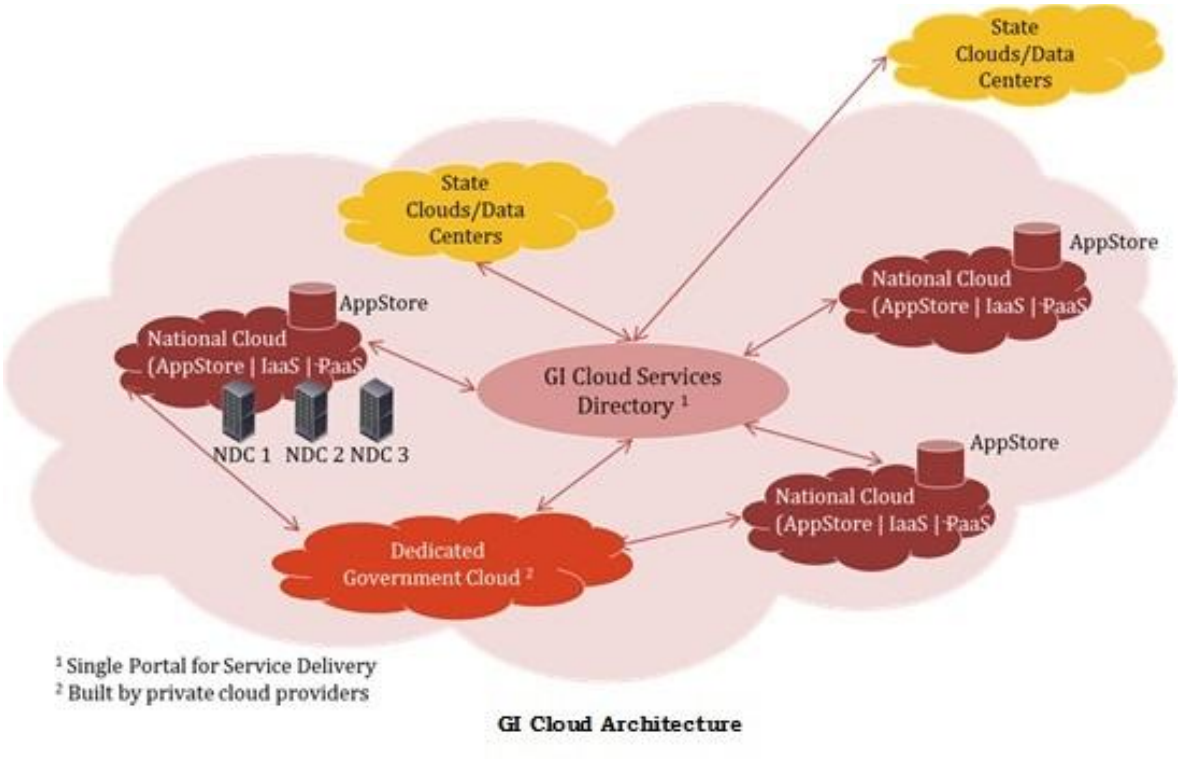


Figure 4-2 GI Cloud Architecture

The architectural vision of GI Cloud as mentioned above consists of a set of discrete cloud computing environments spread across multiple locations, built on existing or

new (augmented) infrastructure, following a set of common protocols, guidelines and standards issued by the Government of India.

The first National Cloud implemented by NIC was launched in February' 2014 where a large number of government departments are already using cloud services

4.4.1 Cloud Data Centre and their issues

Data center and cloud, both serve as the storage of a large amount of data. The basic differences between a data center and a cloud storage are:

Data Center:

- A data center is an on-premise hardware.
- It accumulates data within the local network of an organization.
- Data centers are run by in-house technological departments.
- Data center has the capacity of storing servers.
- Data center is a fully secured program without the intrusion of any third party.

Cloud:

- Cloud is an off-premise form of computing.
- It accumulates data on the Internet.
- Cloud services are run by general cloud servers.
- Cloud-based resources need to be housed in data centers.
- Cloud resources will be shared with the other users of the same provider, if the private cloud is not used.

Data centres in India mainly operate on two models. The first one is known as a captive data centre model, in which an organisation builds, operates, and manages its own data centre. The other is the outsourced or a "co-location "model, where organisations purchases data centre hosting services from external providers. Under

this arrangement, the external provider offers power, security and cooling needs for the datacentre, while the customers use the leased space to deploy their servers.

Initially, captive data centres enjoyed a significant market share, but gradually, they have ceded their ground to third-party service providers. Third-party data centre service providers are tipping the scales in their favour with their value-added services, innovation, and high opportunity costs of real estate and electricity.

As a result, business verticals such as BFSI (banking, financial services, and insurance), telecom, retail, media and entertainment are increasingly leveraging third-party hosting functionalities over in-house data centre services.

4.5 A SECURE ELEMENT and IOT

The Secure Element contains a certified microcontroller and embedded software. It is secure, personal and portable and comes in multiple form factors : smart card, USB token, microSD, etc. Generally India imports from China, USA, Singapore and other country , they manufacture and personalize such secure elements, as well as the software and secure infrastructure around it. Secure elements have a strategic role in protecting digital identities and are vital to ensure digital security and privacy. Generally secure elements are divided into 5 main areas:

I. Telecom: SIM cards (secure elements with a SIM application)
II. Payment & banking: cards issued by banks and retailers for payment services (debit, credit, prepaid schemes…); cards issued by retailers or service providers for loyalty services; and social cards with payment application
III. Government & healthcare: cards likely to be issued by governmental bodies for citizens identification (travel, ID and healthcare documents) and online services and cards issued by private health insurance companies
IV. Device manufacturers: mobile phones, tablets, navigation devices and other connected devices including an embedded secure element without SIM application

V. Others: cards issued by operators, for transport, toll or car park services (i.e. “Transport”); cards issued by pay-tv operators for decrypting TV signals (i.e. “Pay TV”); physical and logical access cards.

The Mobility and contactless transactions are key drivers for growth, thanks to the convenient and secure user experience they enable.

5 Finding and Observation

5.1 What is “Digital Sovereignty” ?

The notion of digital sovereignty appeared around 2010. This concept concerns the storage and protection of individuals personal data in its digital form. Digital sovereignty addresses the issue that personal data is collected by different business’ across the web and held with or without the users consent. It is designed to give individuals control and ownership of their presence and representation in the digital world.

The idea is that personal data stocked on the internet must be kept in the country in which the person resides and must therefore be subject to the law of the country in question. Hence cyberspace must be protected in the same way that we protect territory such as the land, sea and air , space.

5.2 Why Do we need to have Secure Digital Sovereignty ?

Objective regarding Digital Sovereignty

Their objective is to secure India Digital Sovereignty , and it is well established fact that

“The digital ecosystem is controlled and shaped by the most powerful stakeholders, digital giants whom are mostly American, (notably we referrer to GAFA, that is to say Google, Apple, Facebook and Apple), but not only that, it is those whom put pressure on the market and put us in a position where we are dependent on technology, addicted to their way of being, following their objectives and subjecting ourselves to their interests”

Another book called “Digital sovereignty” by Pierre Bellinger stated that “Digital sovereignty is commanding our present day and our futures through the high-usage of technology and computer networks … as a Frenchman, our data, our memory, our projects, our way of thinking, our communication and our documents must without a doubt stay within our national territory under the protection of our laws and our court system.”

Due to cyberthreats and hacking , one of the major concerns of digital sovereignty is the question about where to store your data.

I. Strategic concerns

It is imperative to avoid the India's data leak to foreign countries, notably to the USA, China. It is important to maintain our autonomous capacity in decision making and action.

Finally, it is vital to preserve our national sovereignty as we face new threats generated by societies growing digitalisation.

II. Economic concerns

No society is sheltered from scientific, economic or commercial espionage; The protection of India businesses and the confidentiality of their data is therefore essential. Hence it is of great importance to ensure that this data remains housed on India soil. Digital sovereignty is equally a way in which to fight against the purchase and usage of data for commercial and marketing reasons without consent of those concerned.

III. Political concerns

Digital sovereignty is a way for governing bodies to recreate citizens confidence in the state, whilst acting to protect them by protecting their private lives and private data. It must equally enable the protection of infrastructure critical to the state.

IV. National security Concerns

Cybercrime, hacking, manipulation, sabotage, terrorism etc. today data security has become a serious National Security concern. Every day, countries, businesses and citizens are confronted with major threats, such as identity theft, fraud and coercion. We often think of the Cambridge Analytica scandal since user data was unknowingly collected and used to influence the elections.

Therefore, one of the major concerns regarding digital sovereignty is to make the cloud safer and more geared towards the needs of citizens than those of businesses and the state.

5.3 Finding and Observation

5.3.1 Introduction :-

“digital sovereignty is the mastery of our present and our fate as expressed in the use of tech and computer networks”. “No national sovereignty is possible without digital sovereignty. The Internet is a global network entirely controlled by the USA and China. US companies are most often dominant. Dependence and the transfer of wealth caused by this imbalance should lead the government to implement specific internet industrial policies”,

The profile of 188 respondents are below:-

From total 188 respondent , their assessment has been taken, as in the India digital transformation stage of e commerce and e-governance has been done at very fast rate, simultaneously internet / broadband penetration has also increased .

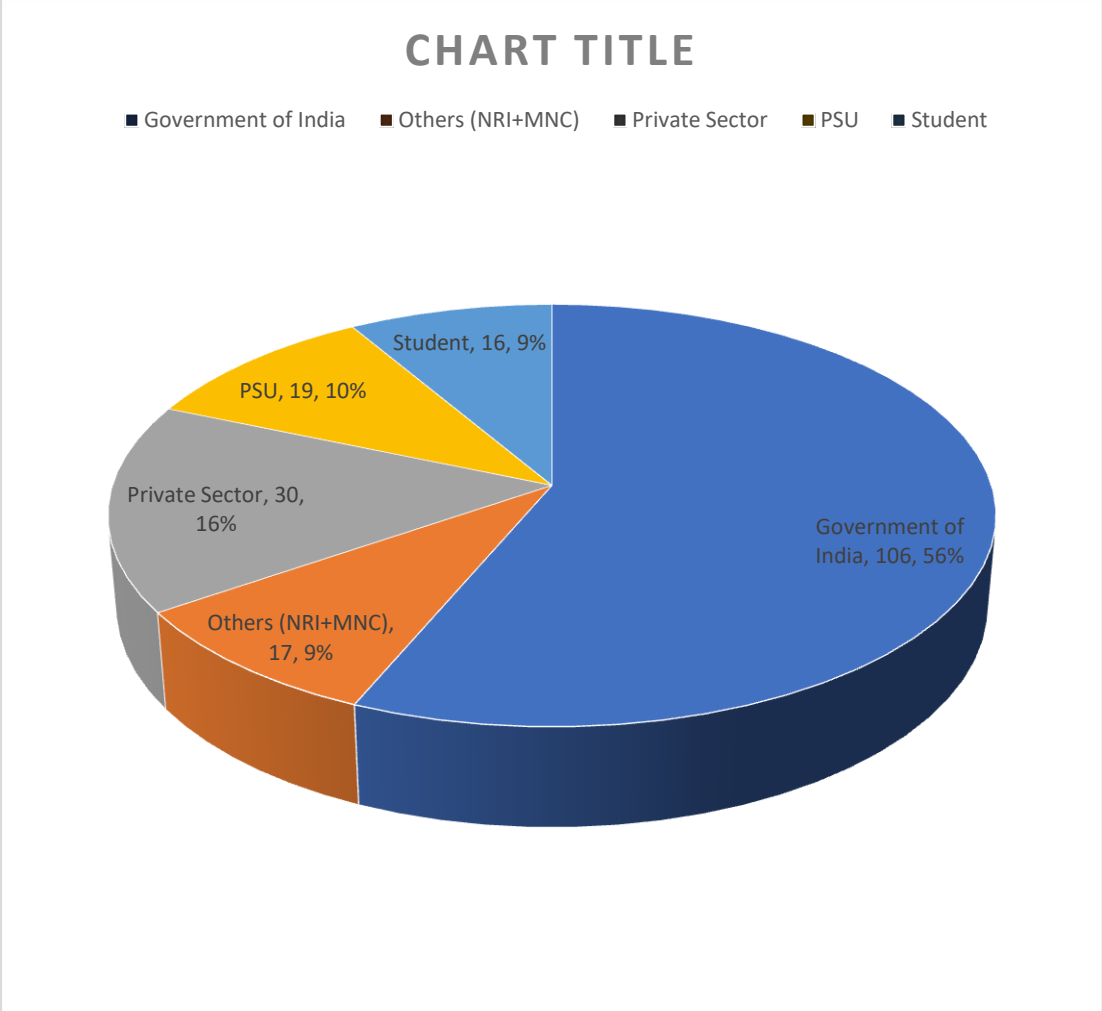


Figure 5-1 Pie chart of Respondent Service Profile

Out of total respondent 188, 126 are IT experience of up to 20yr or more , but 62 have only experience of working in IT platform and understand IT . The breakup of IT and Non IT are tabulated picture wise in accordance with their Job / service profile.

The Graphical presentation 188 respondent as per their education qualification are pictured as below:-

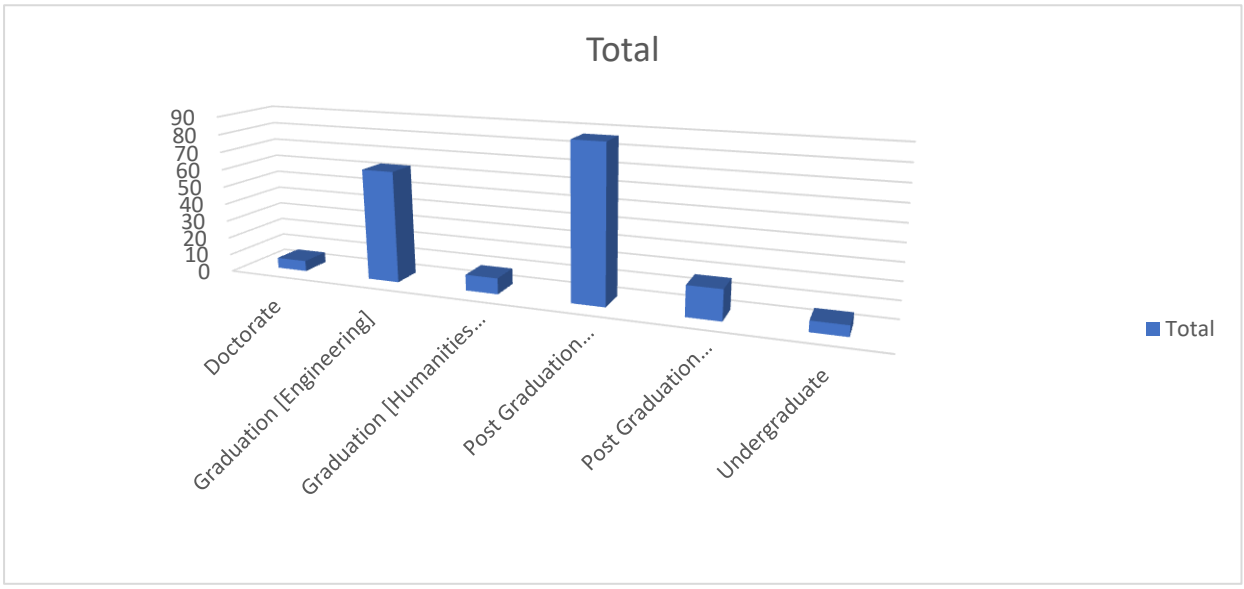


Figure 5-2 Educational Profile of Respondent

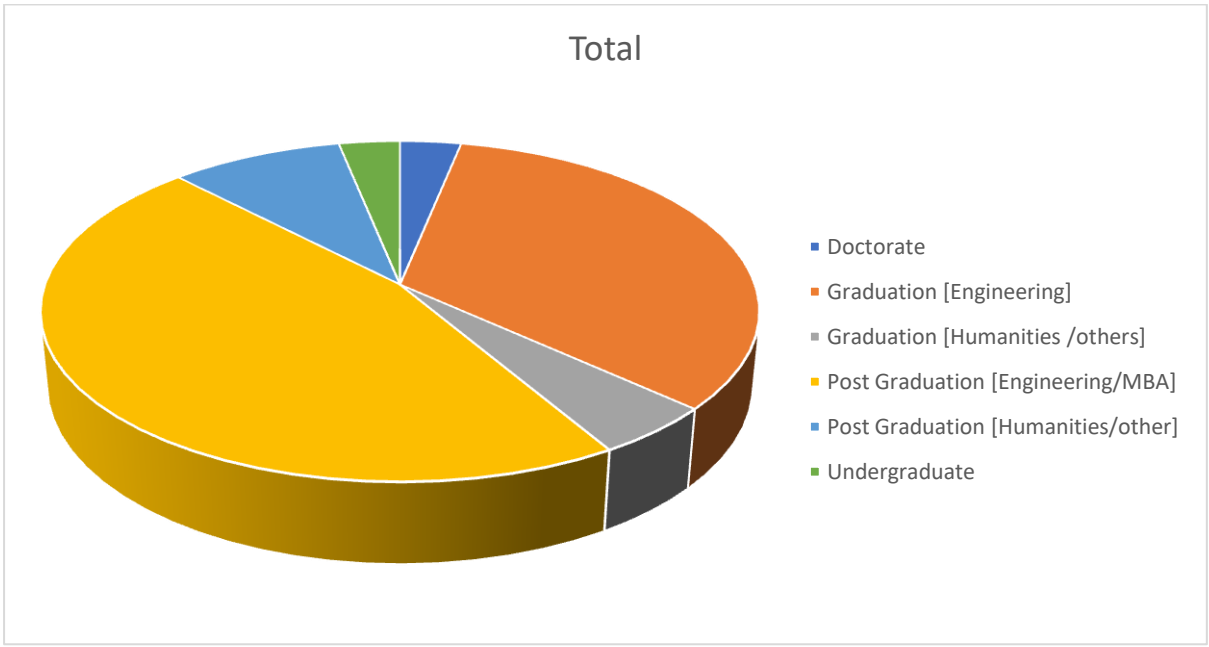


Figure 5-3 Pie Diagram of Educational Profile of Respondent's Educational Qualification

And Digital initiatives. Has changed the velocity of life . It is already been established that the Growth rate of ICT directly affect the % growth rate of GDP. But. simultaneously lot of problems like data theft and technological dependence , also arises which is directly or indirectly being faced by India, And thus Digital Sovereignty is being compromised . So with regard to various question relating to following heading for assessment of uprising problem /issues :-

1. Digital Sovereignty Concept and Awareness
2. Existing issues and Challenges in Present context of Cyber Space
3. Digital Sovereignty is National Issues
4. Recommendation for needful action to Secure Digital Sovereignty

5.3.2 Digital Sovereignty Concept and Awareness

Question No. 1://

1.“Digital sovereignty encompasses the idea that users, being citizens or companies, have control over the data they generate”. In the Present day challenges of cyberspace; “Securing Digital Sovereignty “ is national concern to ensure Right of Privacy and Security in the Cyberspace to citizen of India?

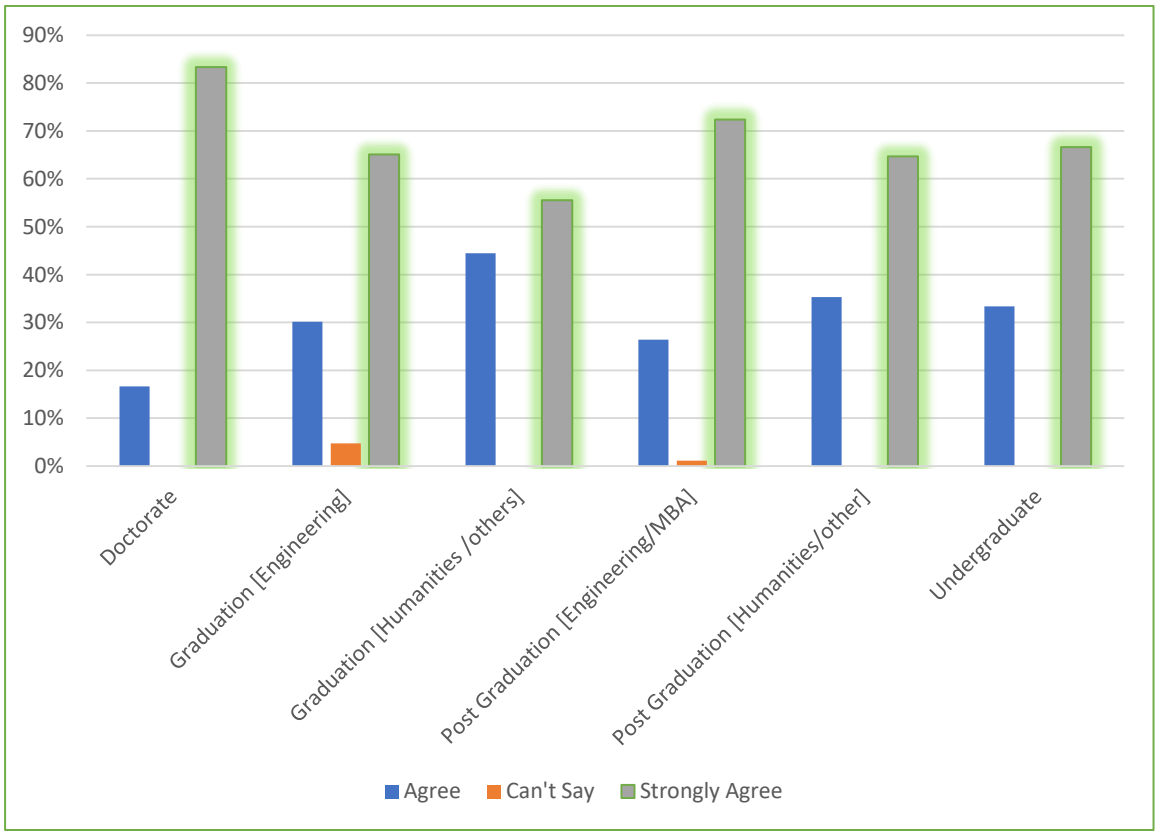


Figure 5-4 Educational Profile of Respondent

Row Labels	Agree	Can't Say	Strongly Agree	Grand Total	% count
Doctorate	1		5	6	83.33%
Graduation [Engineering]	19	3	41	63	65.07%
Graduation [Humanities /others]	4		5	9	55.55%
Post Graduation [Engineering/MBA]	23	1	63	87	72.41%
Post Graduation [Humanities/other]	6		11	17	64.70%
Undergraduate	2		4	6	66.66%
Grand Total	55	4	129	188	

Table 5-1 Respondent educational details

Row Labels	Agree	Can't Say	Strongly Agree	Grand Total	% maximum Strongly agreed
Government of India	34		72	106	68%
Others (NRI+MNC)	4	1	12	17	71%
Private Sector	6	1	23	30	77%
PSU	5		14	19	74%
Student	6	2	8	16	50%
Grand Total	55	4	129	188	

Table 5-2 Respondent responses to Concept of Digital Sovereignty

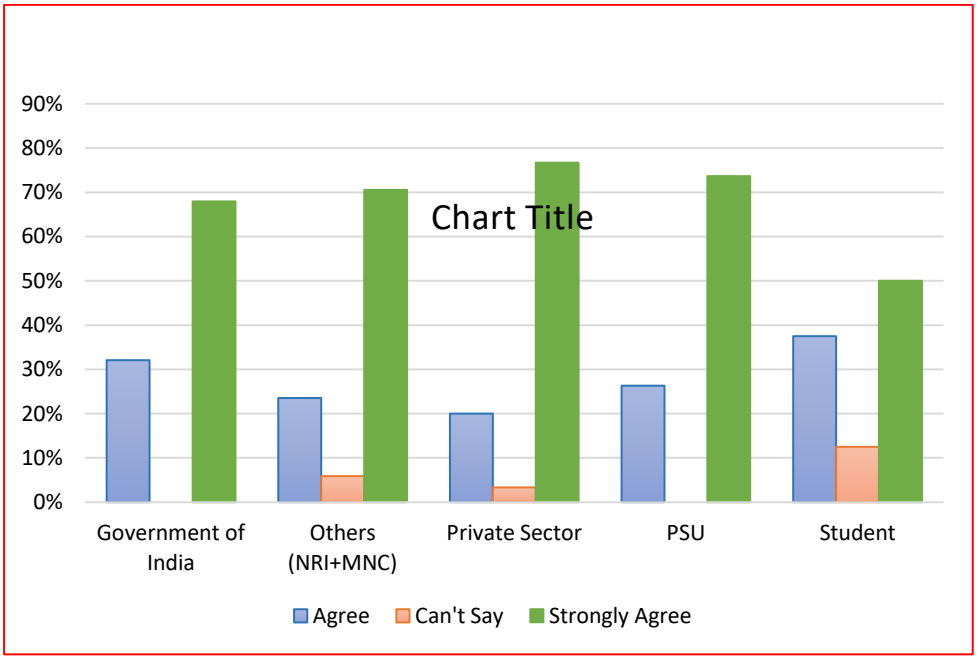


Table 5-3 Bar diagram(%) responses to question of digital sovereignty

Remark ://

1. Majority of Officer of GoI (68%) , Others(MNC+NRI) 71% , Private Sector (77%) , PSU(74%) ,Student(50%) are of strongly agreed to concept of "Securing Digital Sovereignty " is national concern to ensure Right of Privacy and Security in the Cyberspace to citizen of India
2. 83.33% of Doctorate , 72.41% of Post Graduate [Engineering +MBA] ,65.07% of Graduate [Engineering] , 64.70% of Postgraduate [Humanities /others] ,55.55% of Graduate [Humanities /others] and 66.66% of Undergraduate strongly agreed to opinion opinion of "Securing Digital Sovereignty " is national concern to ensure Right of Privacy and Security in the Cyberspace to citizen of India
3. It can be inferred that more % this engineering background and more qualified made stronger voice for of "Securing Digital Sovereignty " is national concern to ensure Right of Privacy and Security in the Cyberspace to citizen of India

QUESTION 2: The statement “data is Oil “?

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering/MBA]	Post Graduation [Humanities/other]	Undergraduate	Grand Total	% Count
AI application and Data Analytics application	1	10	1	12	4	1	29	15.4 %
Can’t Say	1	3	3	7	1	1	16	8.5%
Data having money equivalent conversion	2	42	3	51	11	4	113	60.1 %
Data is Gold	1	7	1	14	1		24	12.8 %
Data is oil	1	1	1	3			6	3.2%
Grand Total	6	63	9	87	17	6	188	100.0 %

Table 5-4 Respnses of Respondent to data is oil

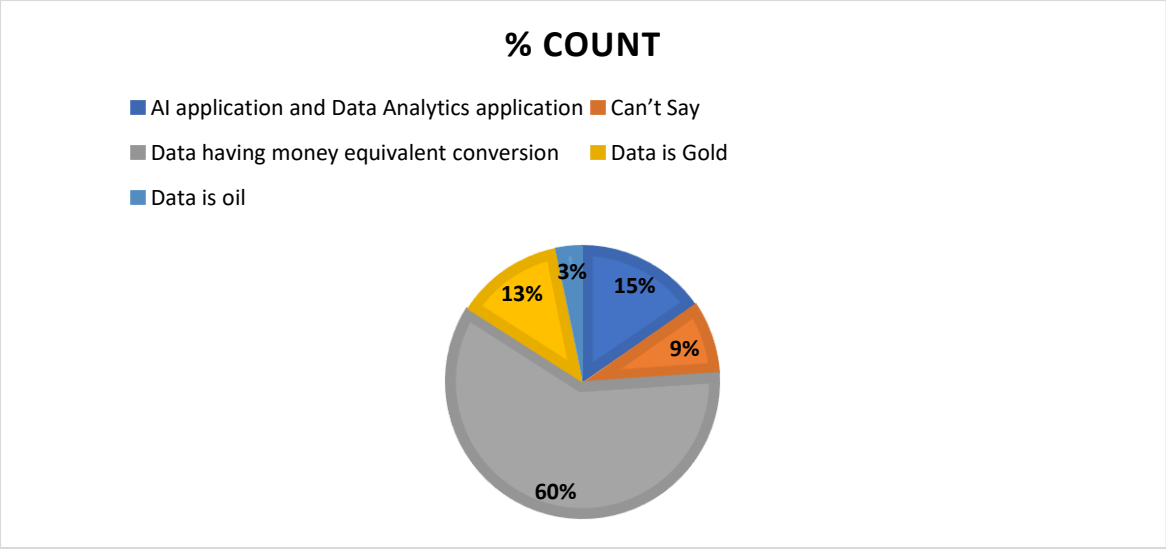


Figure 5-5 Pie chart : data is oil

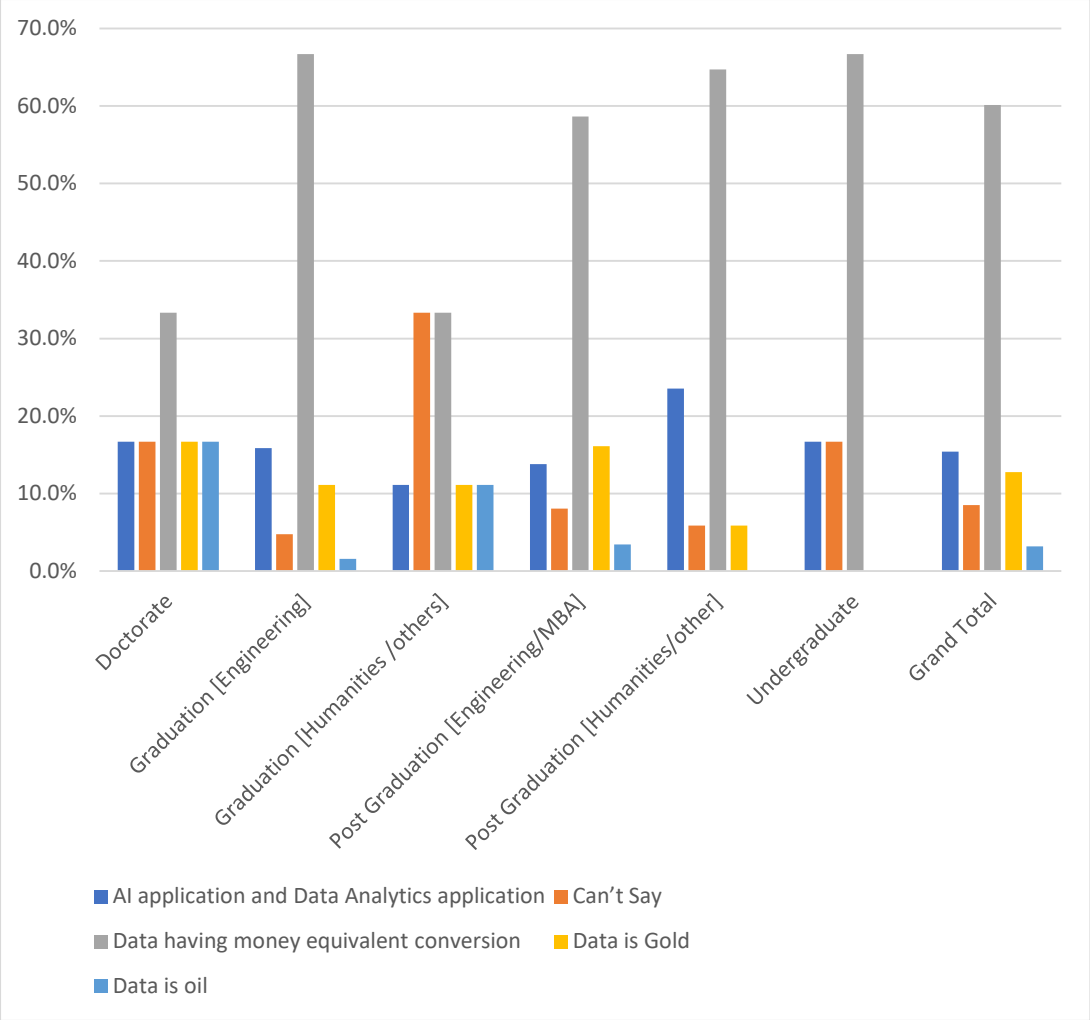


Table 5-5 Bar diagram of Responses to "Data is Oil"

Remarks:// :: Here the respondent is not clear of concept and Data is gold statement is misleading because true understanding of use of others personal Data , Statement "Data is Gold " because of AI application and Data Analytics software can be made on Data for predicting human future behaviour and physical phenomenon . That's why the respondent having 15% of all educational qualification registered for AI application and Data Analytics.

Question No.3“Securing Digital Sovereignty” is concerned with which of following? *

A. Data Security
B. Network Security
C. Both of A and B
D. Information Management System
E. Can’t Say

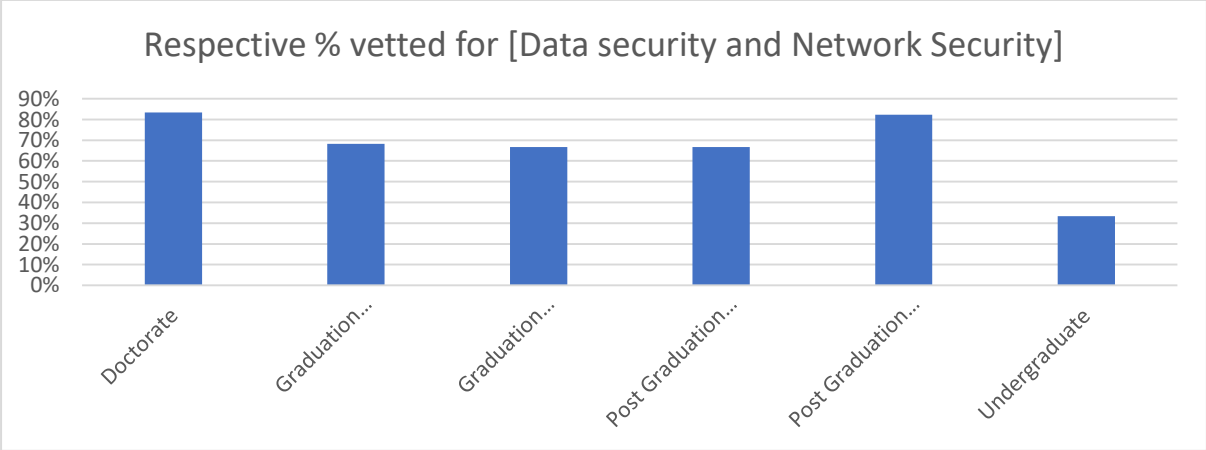


Figure 5-6 Securing Digital Sovereignty: % of responses vetted for Data and Network Security

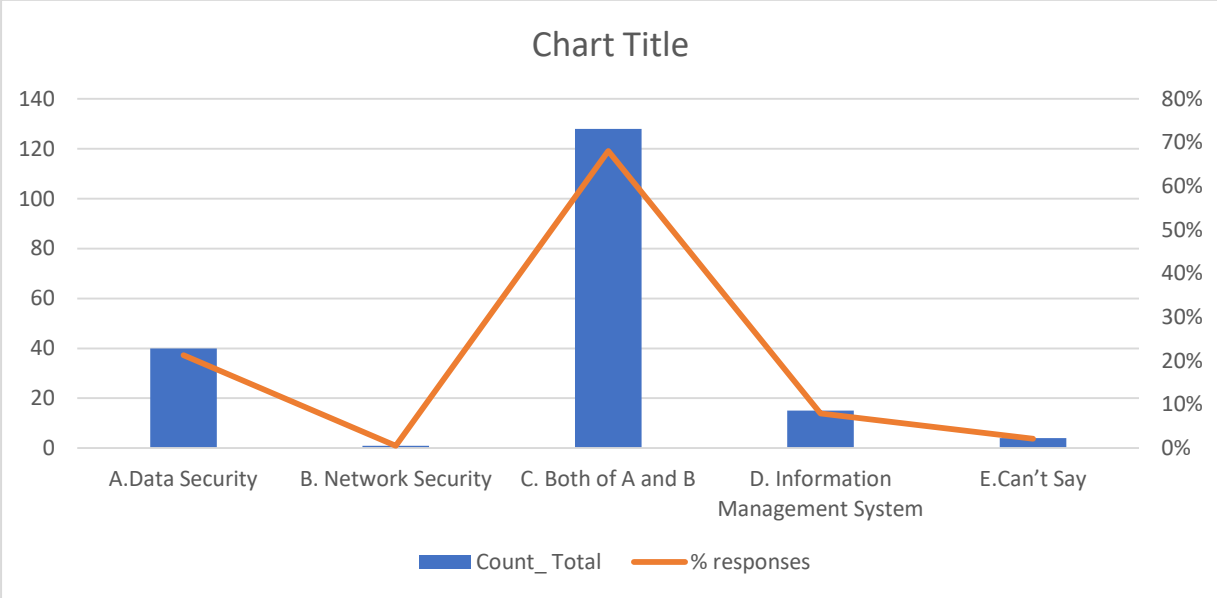


Figure 5-7 Respondent Responses for Securing Digital Sovereignty qualification wise

Conclusion:// Here. the maximum respondent has vetted for both Data Security and Network security as measures for securing the digital sovereignty , that too maximum by respondent having highest qualification of Doctorate , Post-Graduation (Engineering +MBA). Now on % percentage analysis the as above. Hence Network Security is also of utmost importance to secure Digital Sovereignty apart from Data Security.

5.3.3 Existing issues and Challenges in Present context of Cyber Space

Section B: Securing Digital Sovereignty : Question related to Existing Situation, Challenges and issues in Digital Sovereignty has to respondent .

4.Personal Data Protection Bill -2020 is sufficient to deal with Digital Sovereignty? *

A. Strongly Agreed
B. Agreed
C. Can't Say
D. Disagree
E. Strongly Disagreed

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering /MBA]	Post Graduation [Humanities /other]	Undergraduate	Grand Total	% Count
Agreed		20	1	28	4	3	56	30%
Can't Say	4	33	5	42	11	3	98	52%
Disagree		4	1	6	2		13	7%
Strongly Agreed	2	5	2	9			18	10%
Strongly Disagreed		1		2			3	2%
Grand Total	6	63	9	87	17	6	188	100%

Table 5-6 Qualification wise responses to Personal Data Protection Bill -2020 is sufficient to deal with Digital Sovereignty

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering/ MBA]	Post Graduation [Humanities/ other]	Undergraduate	Grand Total
Agreed	0%	32%	11%	32%	24%	50%	30%
Can't Say	67%	52%	56%	48%	65%	50%	52%
Disagree	0%	6%	11%	7%	12%	0%	7%
Strongly Agreed	33%	8%	22%	10%	0%	0%	10%
Strongly Disagreed	0.0%	1.6%	0.0%	2.3%	0.0%	0.0%	1.6%

Table 5-7 :Qualification wise responses to Personal Data Protection Bill -2020 is sufficient to deal with Digital Sovereignty

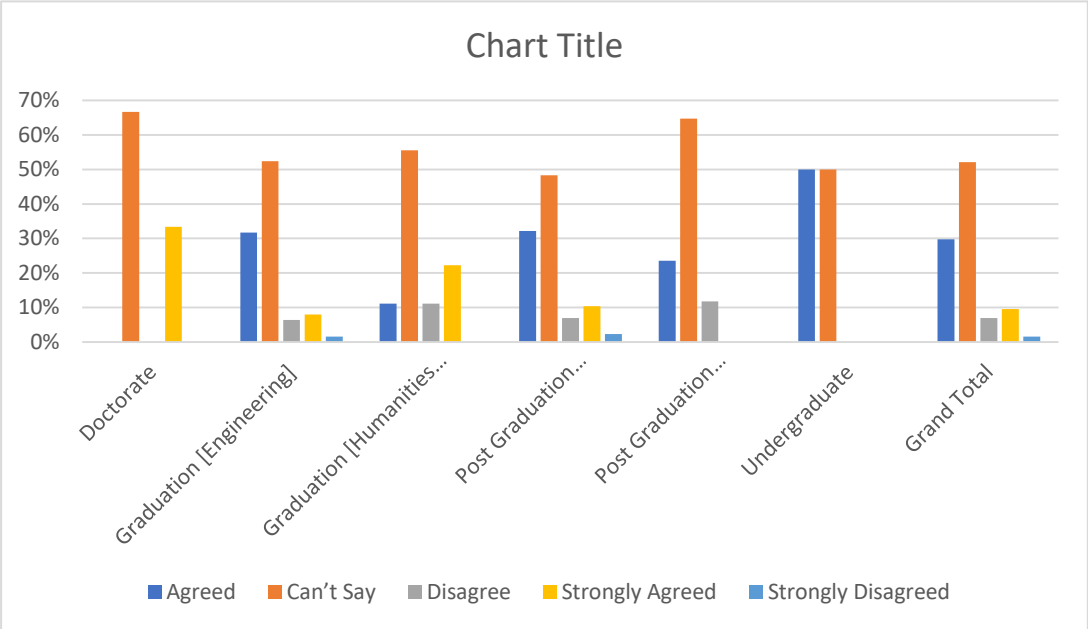


Figure 5-8:Qualification wise responses to Personal Data Protection Bill -2020 is sufficient

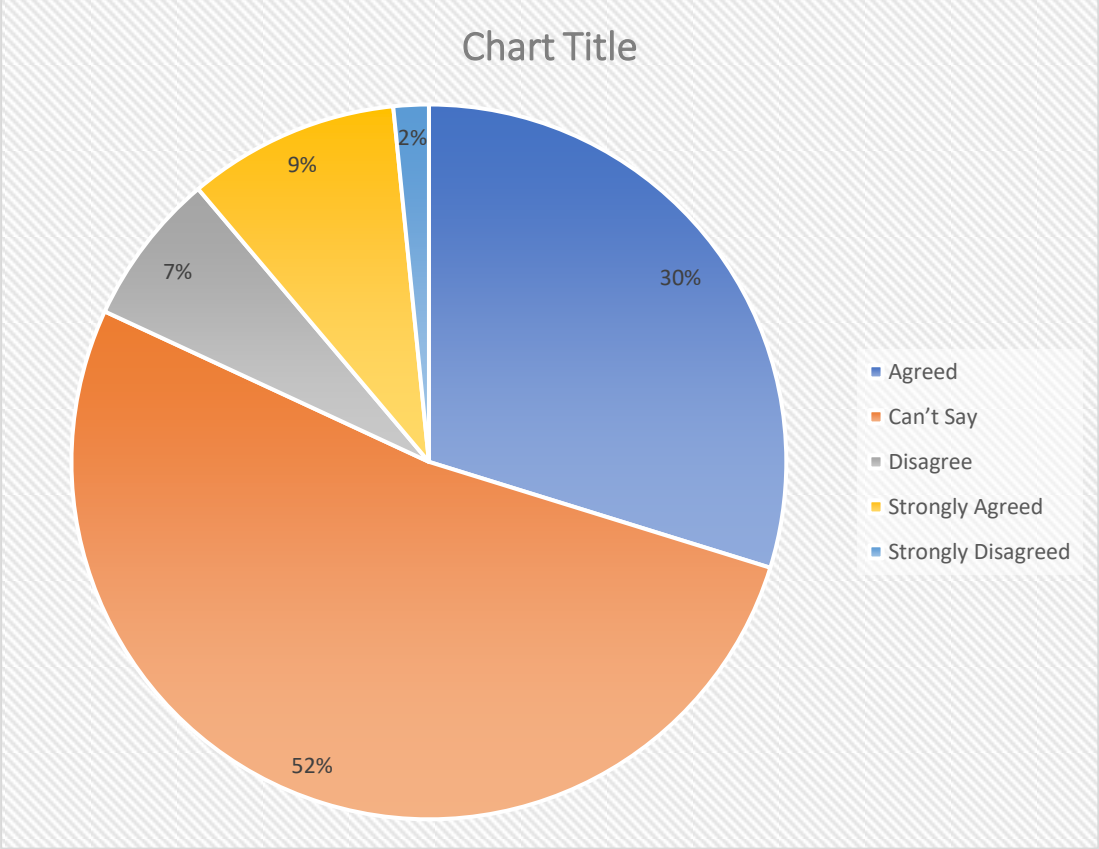


Figure 5-9 :Qualification wise responses to Personal Data Protection Bill -2020 is sufficient

Remark :// 52% of respondent are not in a position to make view that tabled bill PERSONAL DATA PROTECTION BILL is sufficient to deal with Digital Sovereignty while only 9% strongly agreed and 2% simply agreed . While analysis the reason it has been seen that all section of respondent of 68% of doctorate , 48% of Post Graduate [Engineering +MBA] , 65% of Post Graduate[Humanities +others], 52% of Graduate[Engineering], 48% of Graduate[Humanities +others] and 50% of undergraduate are not in a position to make view. This simply states that proper knowledge and awareness programme has to organised for proper imparting of training and As PERSONAL DATA PROTECTION BILL 2020 is one step forward for securing the digital sovereignty.

5. Have ever been your data theft while online ?.

A. YES
B. NO
C. Can't Say

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering /MBA]	Post Graduation [Humanities /other]	Under graduate	Grand Total
Can't Say	2	21	2	25	8	1	59
NO	2	28	6	46	6	4	92
YES	2	14	1	16	3	1	37
Grand Total	6	63	9	87	17	6	188

Table 5-8 Responses to Have ever been your data theft while online ?

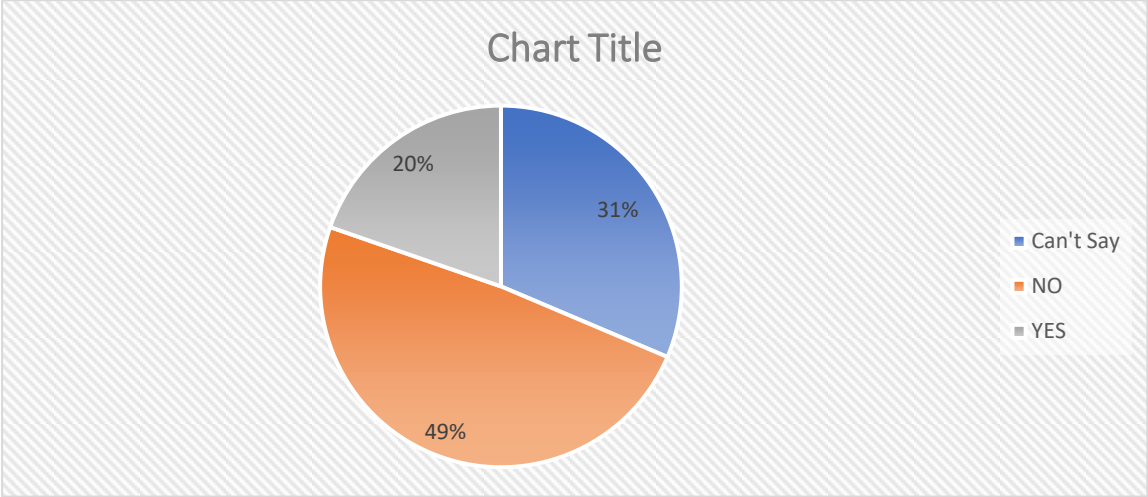


Figure 5-10 Pie chart of responses to Have ever been your data theft while online

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering /MBA]	Post Graduation [Humanities /other]	Undergraduate	Grand Total
Can't Say	33%	33%	22%	29%	47%	17%	31%
NO	33%	44%	67%	53%	35%	67%	49%
YES	33%	22%	11%	18%	18%	17%	20%

Table 5-9 % responses toHave ever been your data theft while online ?

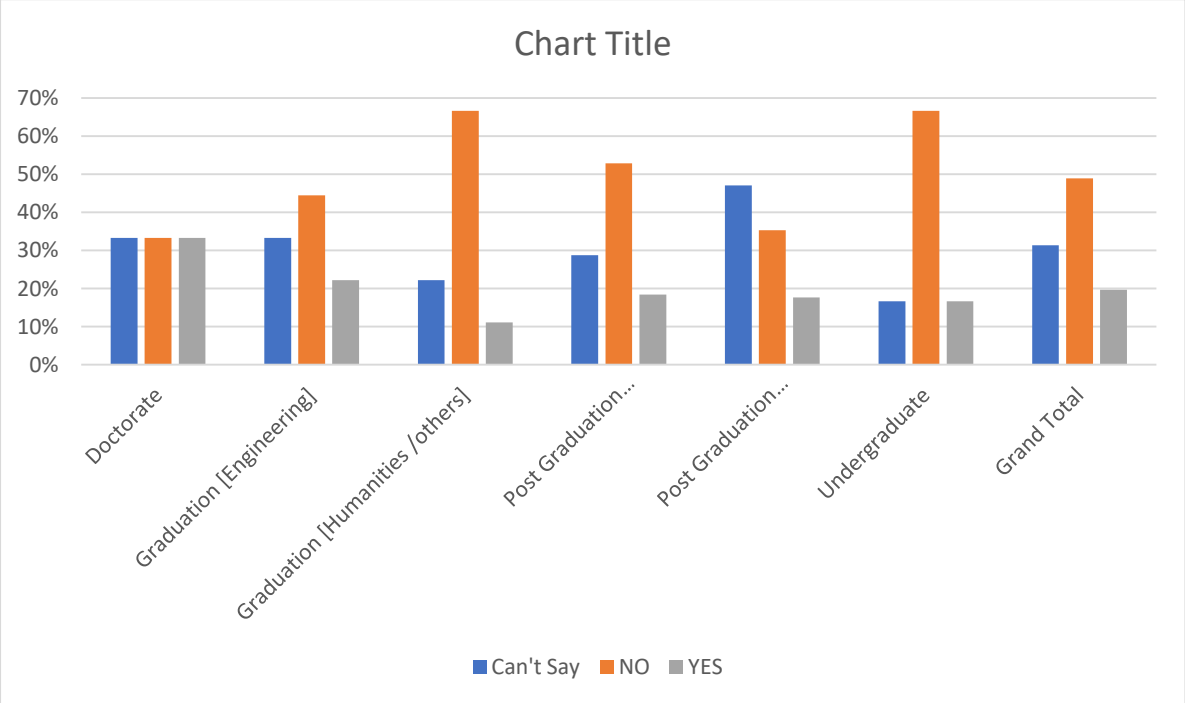


Figure 5-11 Bar diagram of responses:Have ever been your data theft while online

Remark :// 31% of respondent can not figure out whether their has. Been stolen or not while online while 49% says “No”where as 20% says” Yes “. While on detailed analysis it has been observed that 67% of respondent with Graduation [Humanities /others] background registered for “No” . And “Yes” is contributed by engineering graduate and Postgraduate and Doctorate . This implies the proper understanding of concept of data theft is required.

6.What action you have taken in the past, when your data has been theft & or your network was compromised?

A. Logged FIR to nearest Police Station
B. Format my device
C. Did not do anything
D. Lodge complain to Secretary (IT)
E. Complain to consumers redressal Authority

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering /MBA]	Post Graduation [Humanities /other]	Under-graduate	Grand Total
Complain to consumers redressal Authority		5		12	1		18
Did not did anything	5	26	6	38	8	3	86
Format my device		26	1	22	6	2	57
Lodge complain to Secretary (IT)		3	1	1	1		6
Logged FIR to nearest Police Station	1	3	1	14	1	1	21
Grand Total	6	63	9	87	17	6	188

Table 5-10 Responses to Action taken when data is left or network is compromised ?

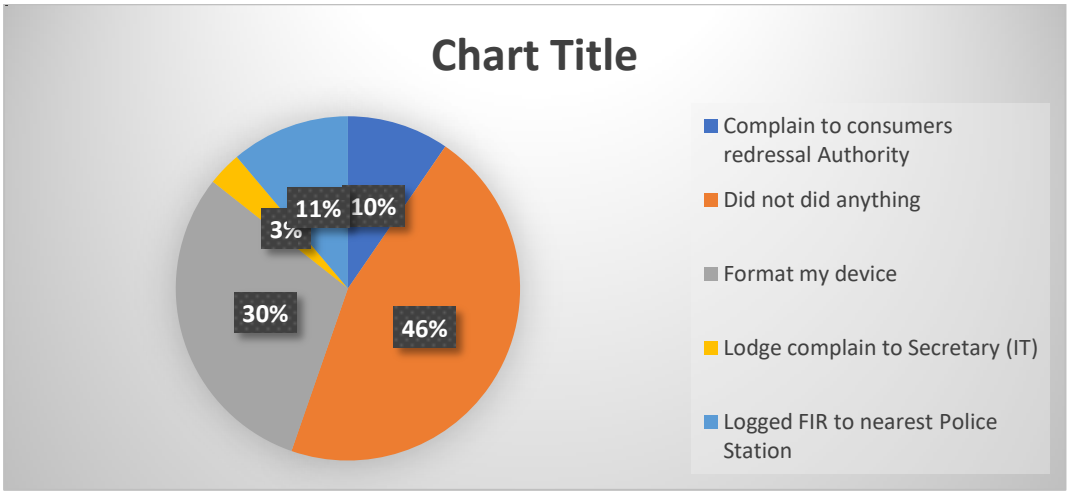


Table 5-11 Pie Chart :Responses to Action taken when data is left or network is compromised

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering /MBA]	Post Graduation [Humanities /other]	Under-graduate	Grand Total
Complain to consumers redressal Authority	0%	8%	0%	14%	6%	0%	10%
Did not did anything	83%	41%	67%	44%	47%	50%	46%
Format my device	0%	41%	11%	25%	35%	33%	30%
Lodge complain to Secretary (IT)	0%	5%	11%	1%	6%	0%	3%
Logged FIR to nearest Police Station	17%	5%	11%	16%	6%	17%	11%

Table 5-12 (%) Responses to Action taken when data is left or network is compromised

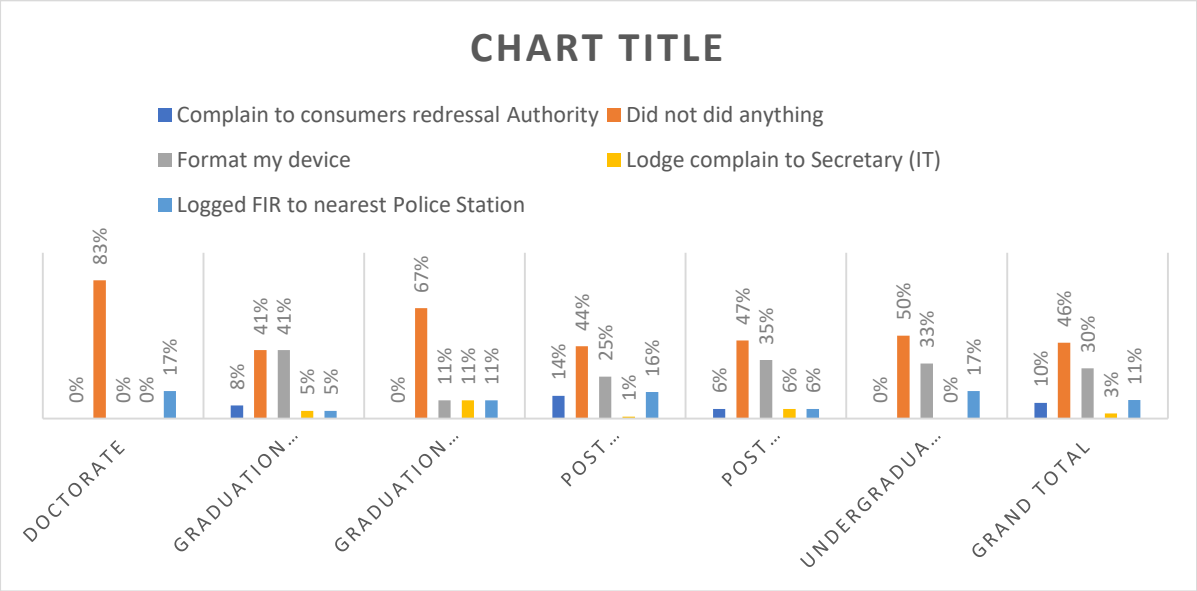


Table 5-13 Bar diagram :Responses to Action taken when data is left or network is compromised

Remark:// 46% of Respondent did not any thing and 30% Format their devices . only 3% and 11% Lodge complain to Secretary (IT) and Logged FIR to nearest Police Station respectively. On detail analysis it learnt that Lodge complain to Secretary (IT) and Logged FIR to nearest Police Station means has been resorted by Engineering and Post Graduate [Engineering /MBA] qualified individual mainly. So proper Cyber

Awareness and Capacity Building programme mechanism has adopted for better Digital Aware Citizen and Cyber knowledgeable Citizen .

7. Why “Securing Digital sovereignty” is important in modern days, because of ?

* Mark only one oval.

A. Right of privacy
B. AI based on Data analytics
C. GDP
D. As any economic and other allied activities on internet generate huge data.
E. All of the above.

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering /MBA]	Post Graduation [Humanities /other]	Under-graduate	Grand Total
AI based on Data analytics		3		3			6
All of the above.	2	29	6	47	8	3	95
As any economic and other allied activities on internet generate huge data.		7		9	2		18
Right of privacy	4	24	3	28	7	3	69
GDP							
Grand Total	6	63	9	87	17	6	188

Table 5-14 Responses : Why “Securing Digital sovereignty” is important in modern days?

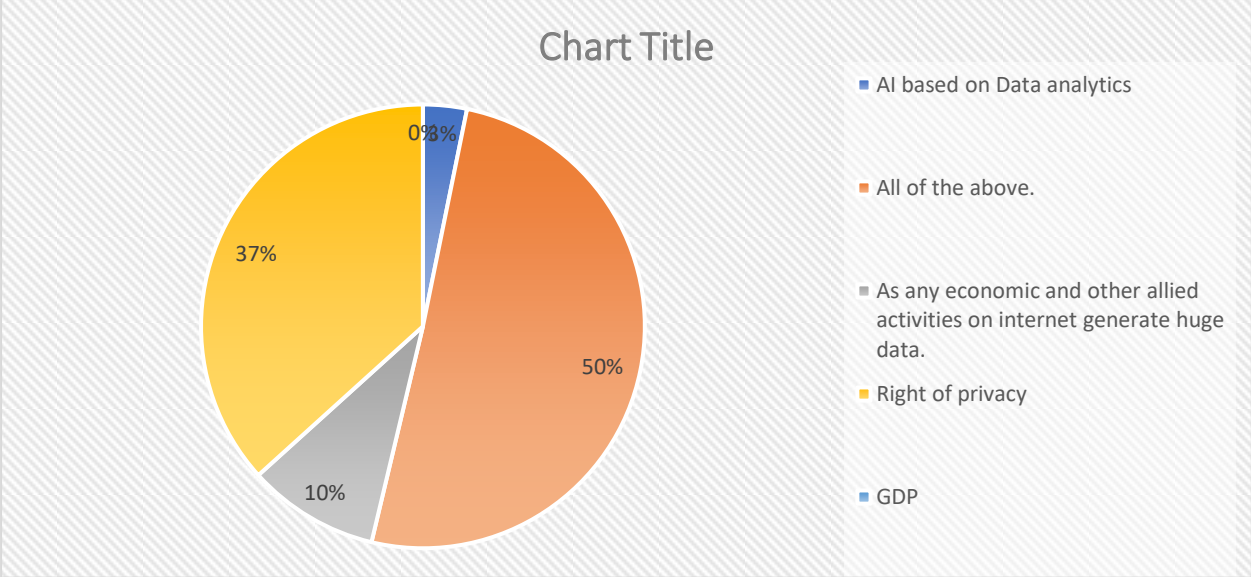


Figure 5-12 Pie Chart :Why "Securing Digital sovereignty" is important in modern days,

Row Labels	Doctorate	Graduation [Engineering]	Graduation [Humanities /others]	Post Graduation [Engineering /MBA]	Post Graduation [Humanities /other]	Under-graduate	Grand Total
AI based on Data analytics	0%	5%	0%	3%	0%	0%	3%
All of the above.	33%	46%	67%	54%	47%	50%	51%
As any economic and other allied activities on internet generate huge data.	0%	11%	0%	10%	12%	0%	10%
Right of privacy	67%	38%	33%	32%	41%	50%	37%
GDP	0%	0%	0%	0%	0%	0%	0%

Figure 5-13 % Responses :Why "Securing Digital sovereignty" is important in modern days,

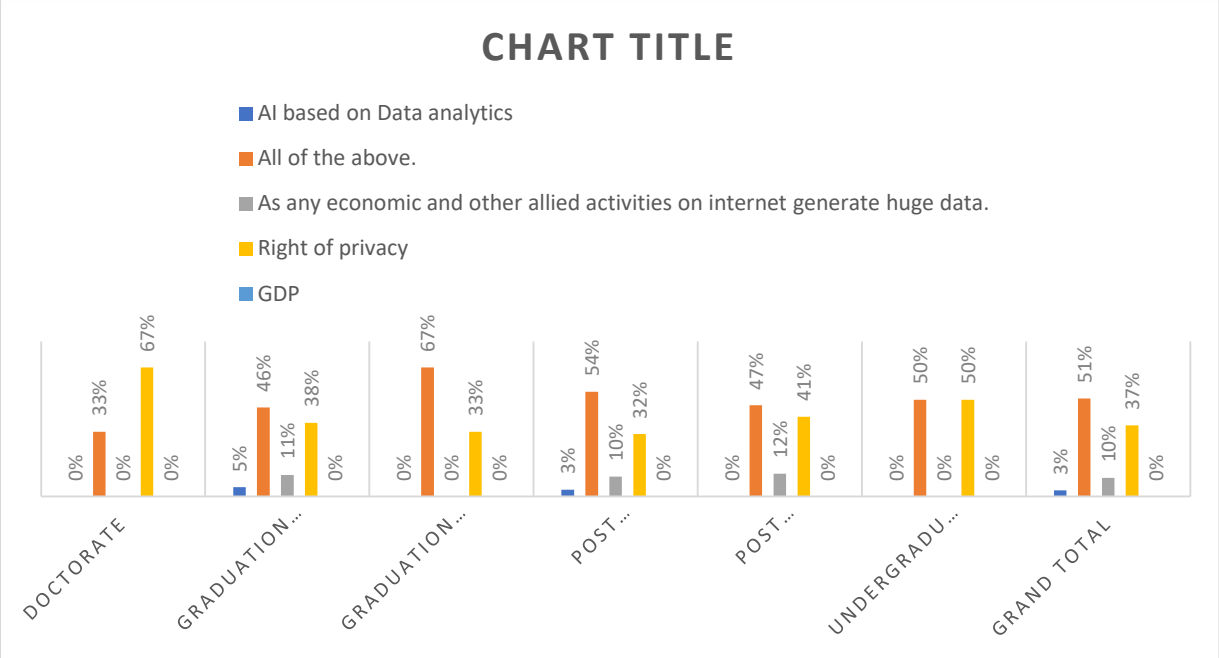


Figure 5-14 Bar Diagram :Why "Securing Digital sovereignty" is important in modern days.

Remark://

51% of respondent stated that Securing Digital sovereignty" is important in modern days, because of all of four listed factor-

1. Right of privacy
2. AI based on Data analytics
3. GDP
4. As any economic and other allied activities on internet generate huge data.

The majority of respondent from Engineering Background.

While 37% shows their consent for Right of Privacy and major contribution from Graduate [Humanities /Other] background.

Thus Cyber awareness programme along with its impact on Digital Sovereignty is to be heighted . Also Capacity building in Cyber Security is to be taken up on top priority in academic compulsory Programme.

5.3.4 Digital Sovereignty is National Issues

8.[A] Foreign governments spy on important business deals to benefit their firms.? *.

A. YES
B. NO
C. Can’t Say

	Count of IT Experience		
Question No. 8A	No	YES	Grand Total
Can’t Say	21	31	52
NO	6	7	13
YES	35	88	123
Grand Total	62	126	188

Table 5-15 Responses :Foreign governments spy on important business deals to benefit their firms.

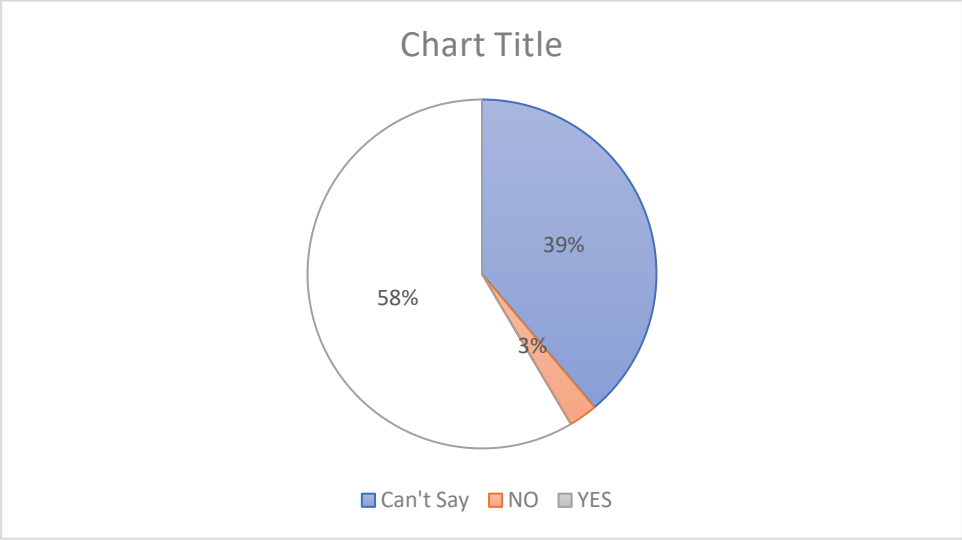


Table 5-16 Pie Chart :Foreign governments spy on important business deals to benefit their firms.

8.[B] Foreign government interfere in domestic political discussions and elections? *

Mark only one oval.

A. YES

B. NO

C. Can’t Say

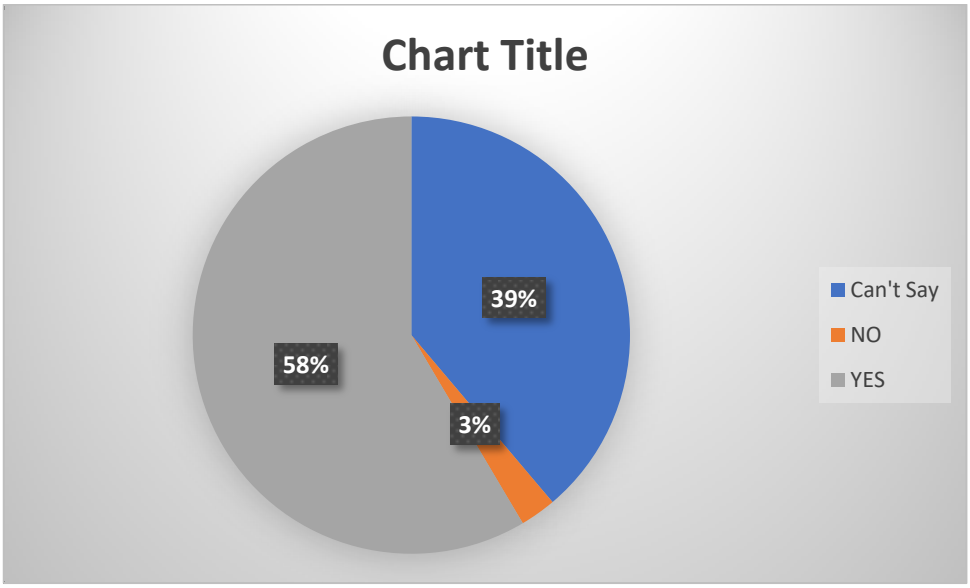


Figure 5-15 Pie Chart: Foreign government interfere in domestic political discussions and elections

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	21	31	52
NO	6	7	13
YES	35	88	123
Grand Total	62	126	188

Table 5-17 Responses: Foreign government interfere in domestic political discussions and elections

8.[C] Foreign-controlled communication platforms forms ethnic tensions? YES

A. NO
B. Can’t Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	28	49	77
NO	4	10	14
YES	30	67	97
Grand Total	62	126	188

Table 5-18: Responses :Foreign-controlled communication platforms forms ethnic tensions

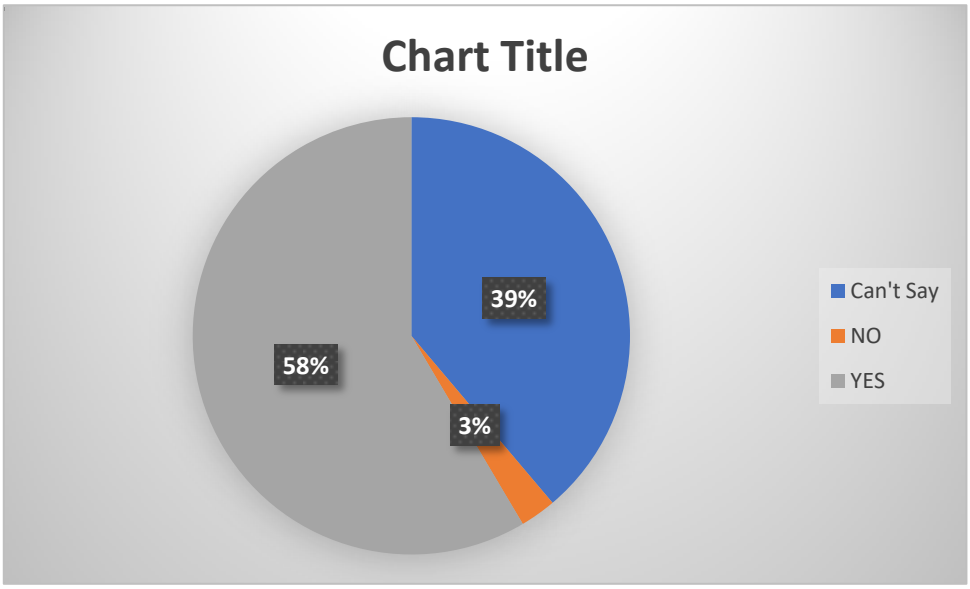


Figure 5-16 Pie Chart: Foreign-controlled communication platforms forms ethnic tensions

8.[D] Foreign government disrupts civilian infrastructure?.

C. YES

D. NO

E. Can’t Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	35	61	96
NO	4	17	21
YES	23	48	71
Grand Total	62	126	188

Table 5-19 Responses :Foreign government disrupts civilian infrastructure

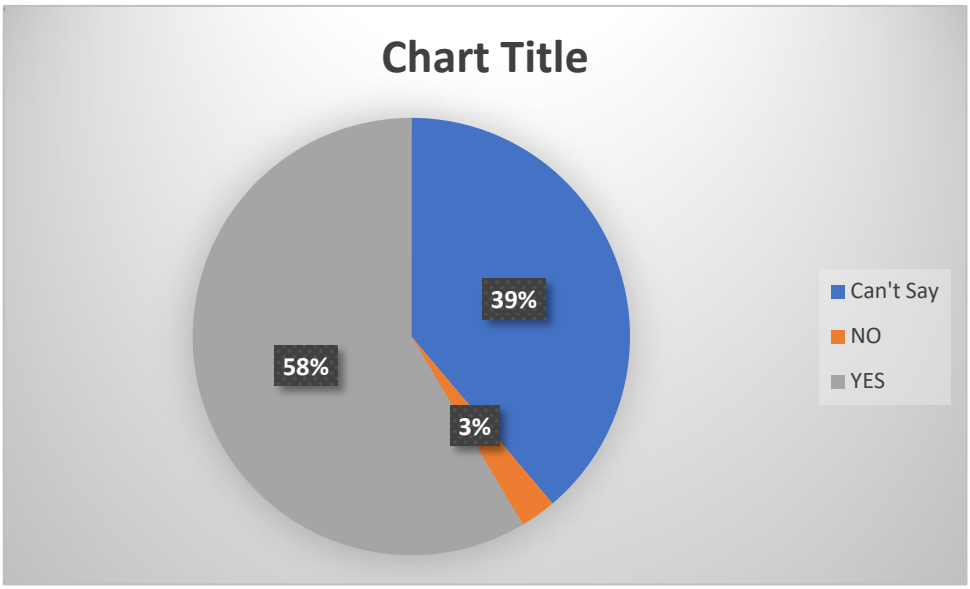


Table 5-20 Pie Chart: Foreign government disrupts civilian infrastructure

8.[E] Large corporations ignoring domestic law and agreements and abusing customer data?.

A. YES
B. NO
C. Can’t Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	17	24	41
NO	8	10	18
YES	37	92	129
Grand Total	62	126	188

Table 5-21 Large corporations ignoring domestic law and agreements and abusing customer data

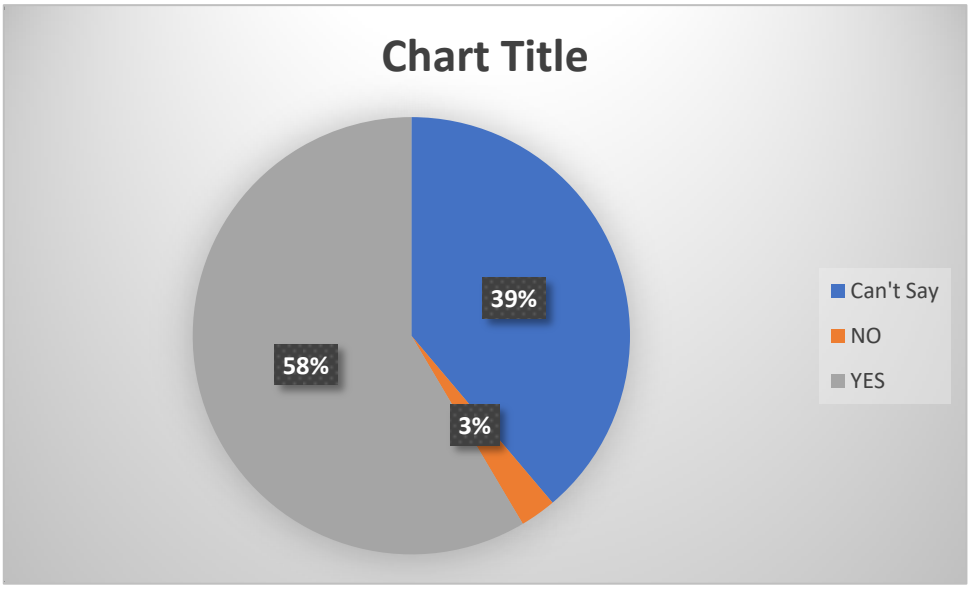


Table 5-22:Large corporations ignoring domestic law and agreements and abusing customer data

8.[F] Large corporations using their market power to thwart attempts at changing their behaviour?

A. YES
B. NO
C. Can’t Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	17	22	39
NO		2	2
YES	45	102	147
Grand Total	62	126	188

Table 5-23 :Large corporations using their market power to thwart attempts at changing their behaviour.

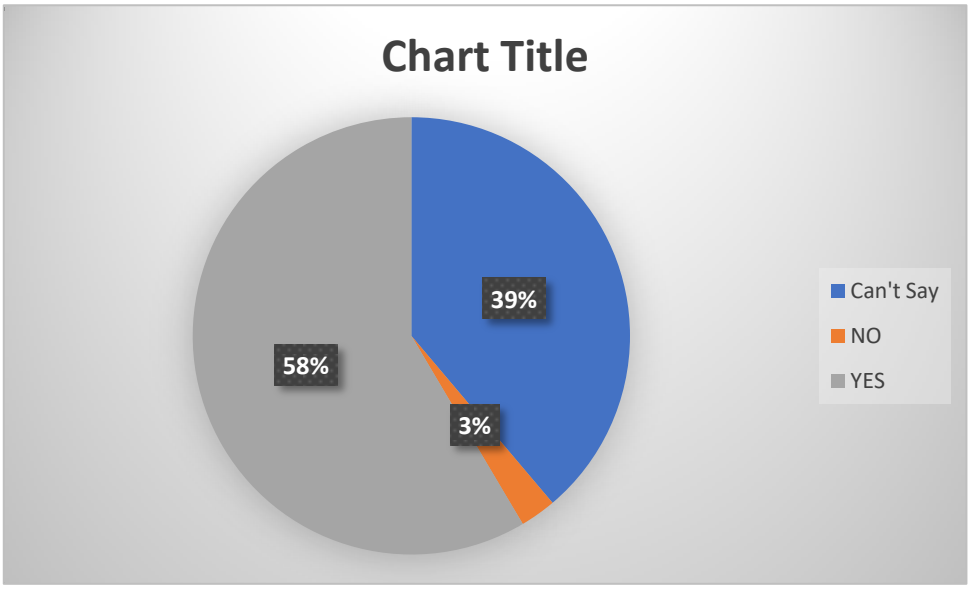


Figure 5-17:Large corporations using their market power to thwart attempts at changing their behaviour

8.[G] Companies find out from shopping behaviour of customers, if teenagers are pregnant ,then ident them or target teenagers at their most vulnerable time? *

Mark only one oval.

A. YES

B. NO

C. Can’t Say

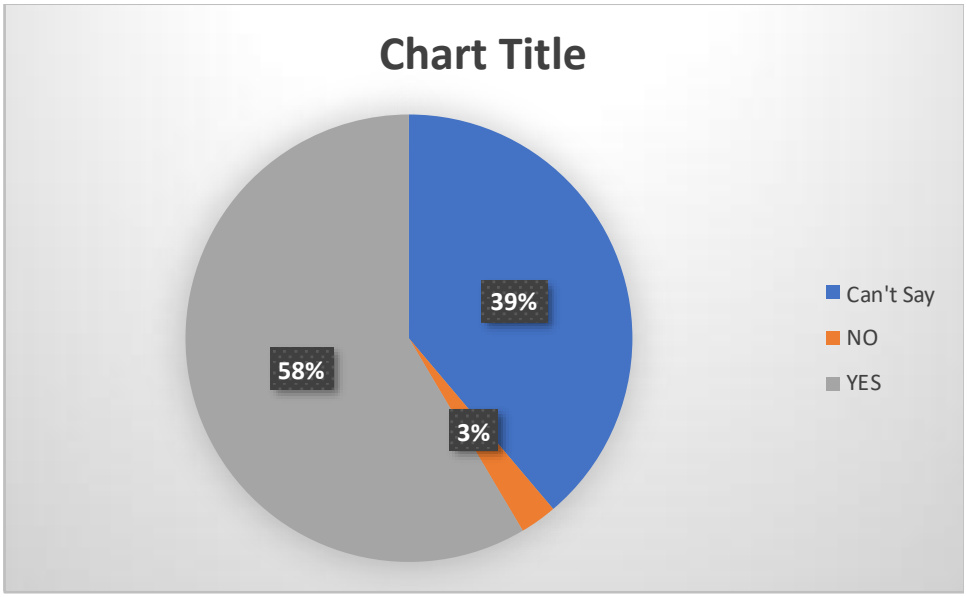


Figure 5-18 Companies find out from shopping behaviour of customers like teenager

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	28	45	73
NO	1	4	5
YES	33	77	110
Grand Total	62	126	188

Table 5-24:Companies find out from shopping behaviour of customers like teenager .

8.[H] Companies put hidden microphones in devices and when find out claim they had no idea it was recording users? *

Mark only one oval.

A. YES
B. NO
C. Can't Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can't Say	37	80	117
NO	4	7	11
YES	21	39	60
Grand Total	62	126	188

Table 5-25 Responses :Companies put hidden microphones in devices

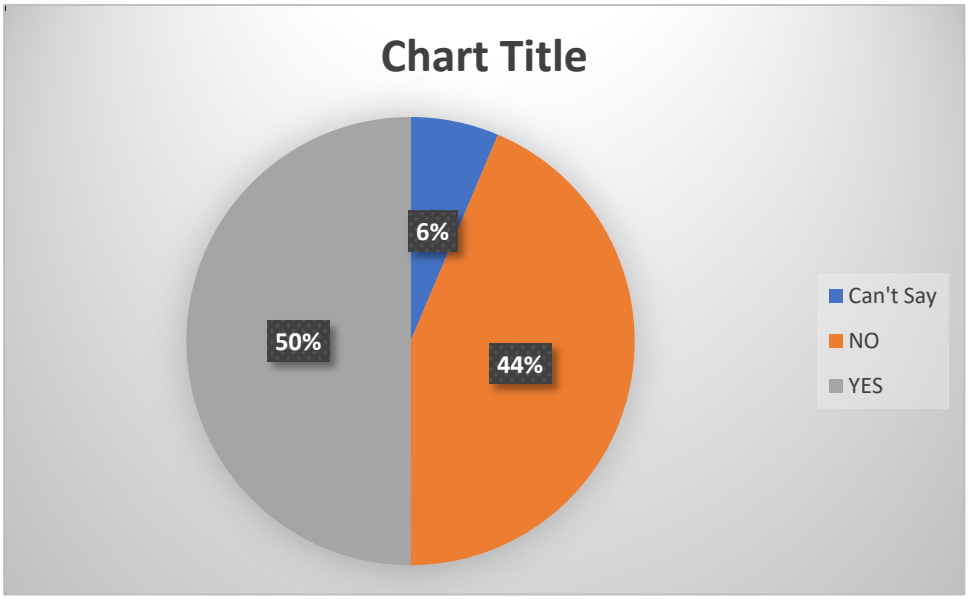


Figure 5-19 :Companies put hidden microphones in devices

8.[I] Commercial data tracking leaks secret military bases ? * Mark only one oval.

A. YES

B. NO

C. Can’t Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	31	62	93
NO	4	15	19
YES	27	49	76
Grand Total	62	126	188

Table 5-26 Responses :Commercial data tracking leaks secret military bases

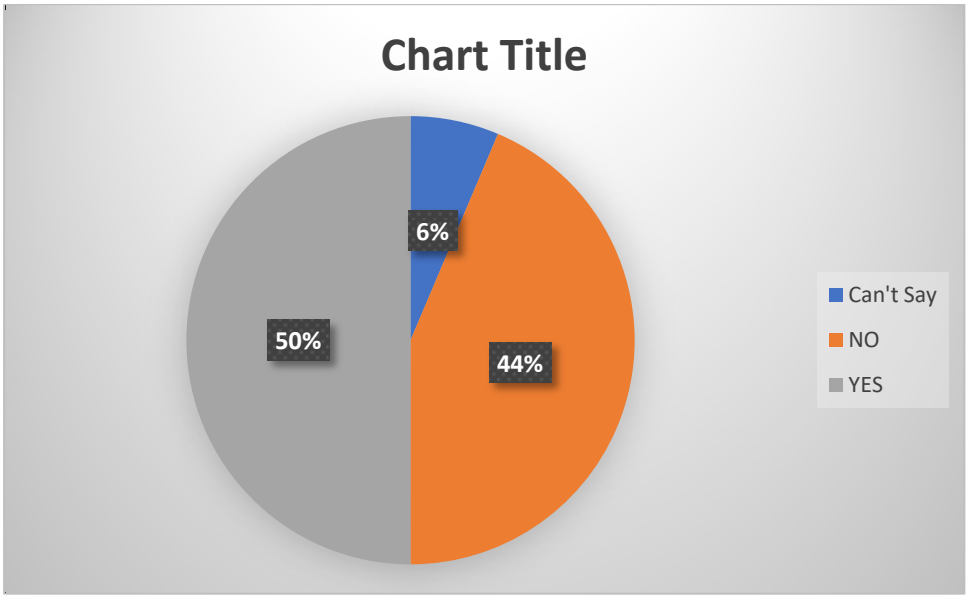


Figure 5-20 Pie Chart :Commercial data tracking leaks secret military bases

8.[J] Commercial firms leaking data allowing people to track heads-of-state? * Mark only one oval.

A. YES
B. NO
C. Can’t Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	33	61	94
NO	3	14	17
YES	26	51	77
Grand Total	62	126	188

Table 5-27 Responses:Commercial firms leaking data allowing people to track heads-of-state

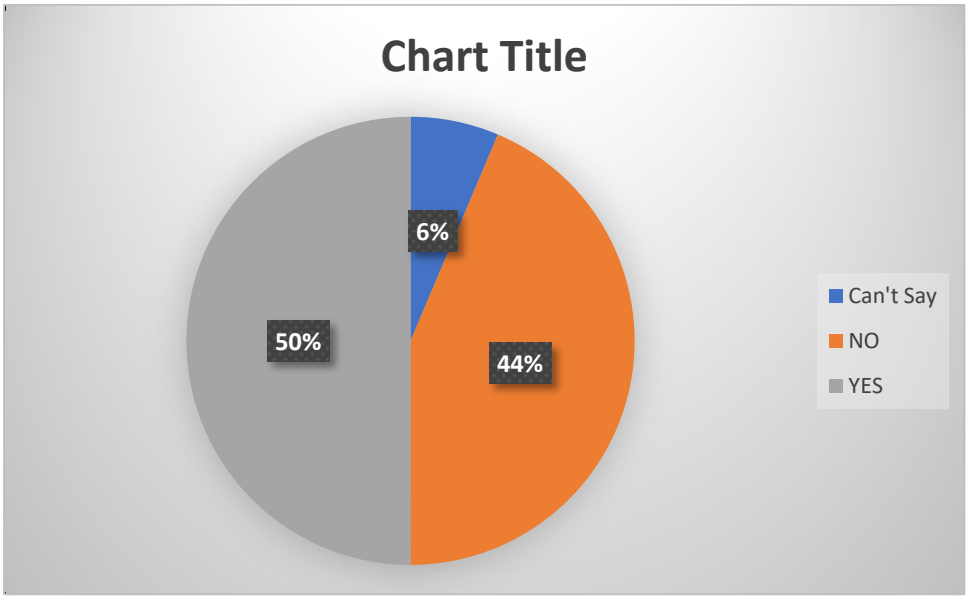


Figure 5-21 Responses :Commercial firms leaking data allowing people to track heads-of-state

8.[K] Have you ever have been attempted for financial frauds? * Mark only one oval.

A. YES
B. NO
C. Can’t Say

Count of IT Experience	Column Labels		
Row Labels	No	YES	Grand Total
Can’t Say	7	5	12
NO	27	55	82
YES	28	66	94
Grand Total	62	126	188

Table 5-28 Responses :Have you ever have been attempted for financial frauds

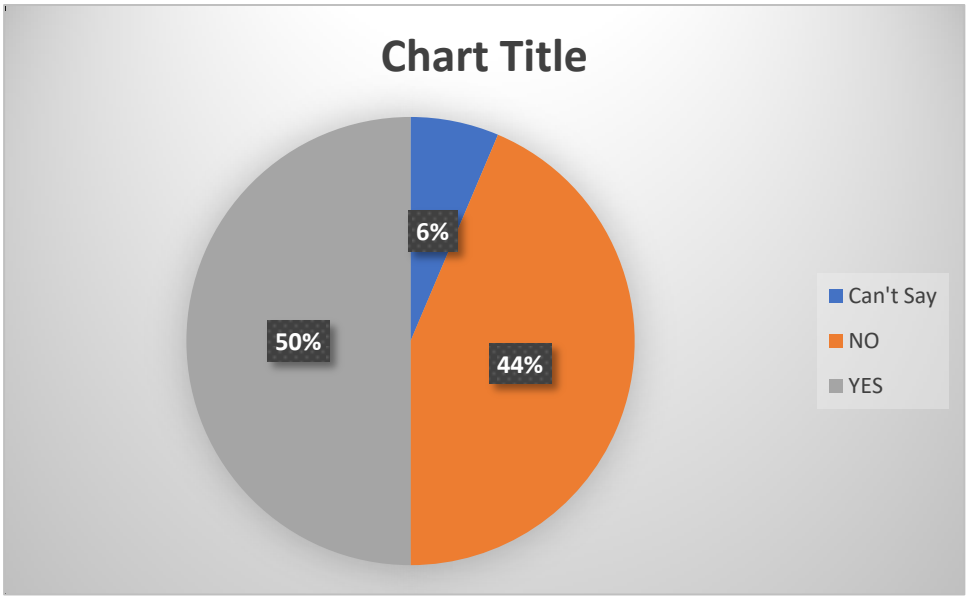


Figure 5-22 :Responses :Have you ever have been attempted for financial frauds

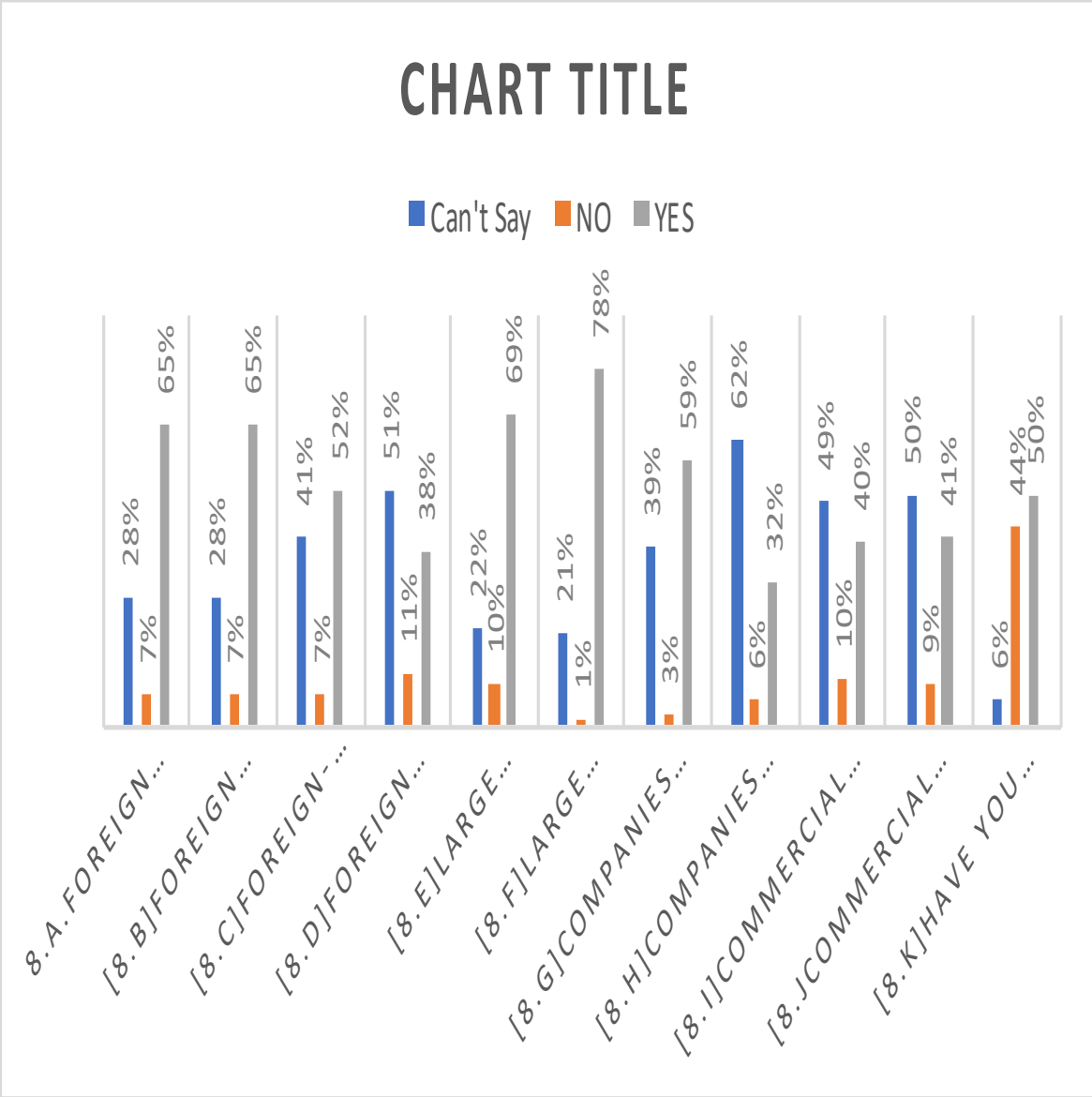
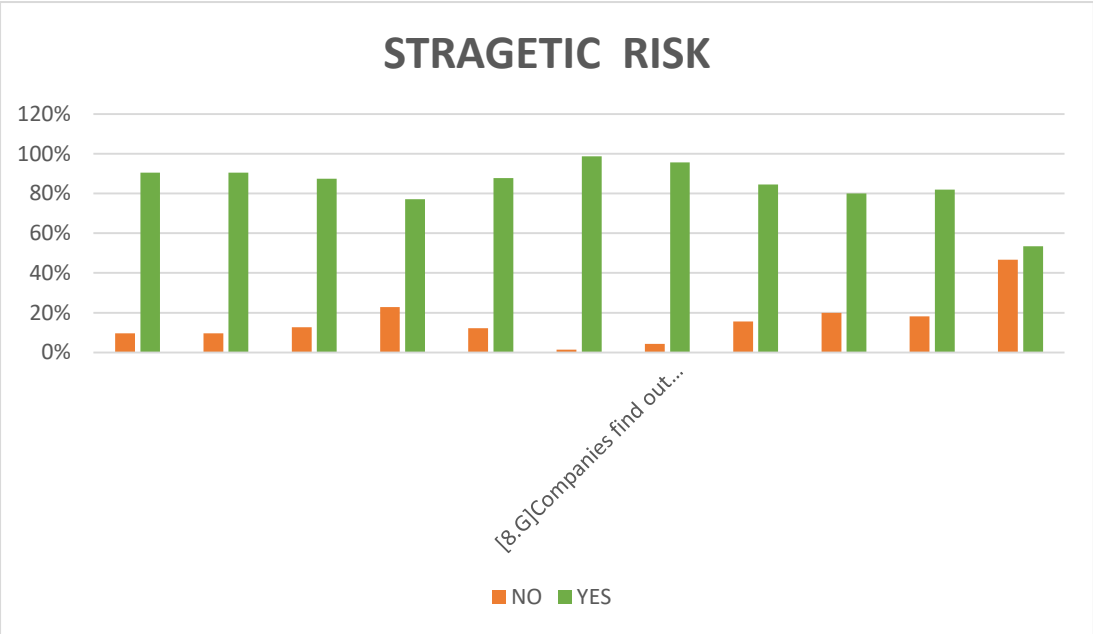


Figure 5-23 Responses to all strategic question in Bar diagram



On data analysis the primary date following observation has been acknowledge

What could happen?

	Scenario	Majority Ans for Yes	% of Respondent given "Yes"	% of Respondent given "No"
8A	Foreign governments spy on important business deals to benefit their firms	YES	90%	10%
8B	Foreign government interfere in domestic political discussions and elections	YES	90%	10%
8C	Foreign-controlled communication platforms foment ethnic tensions	YES	87%	13%
8D	Foreign government disrupts civilian infrastructure	YES	77%	23%
8E	Large corporations ignoring domestic law and agreements and abusing customer data	YES, YES	88%	22%

8F	Large corporations using their market power to thwart attempts at changing their behaviour	YES	99%	1%
8G	Companies find out from shopping behaviour if teenagers are pregnant and out them, or target teenagers at their most vulnerable time	YES, YES	96%,96%	4%,4%
8H	Companies put hidden microphones in devices and when find out claim they had no idea it was recording users	YES	85%	15%
8I	Commercial data tracking leaks secret military bases	YES	80%	20%
8J	Commercial firms leaking data allowing people to track heads-of-state	YES	82%	18%
8K	Have you ever have been attempted for financial frauds?	YES	53%	47%
	What is next?	Need Action	Call for for strengthen digital infrastructure	
Note : Can answer option are excluded to understand the problem				

8.[L] Are you confident that your data are secured, Safe and Privacy is ensured ? *

A. YES

B. NO

C. Can't Say

Count of IT Experience	Column Labels			% Count
Row Labels	No	YES	Grand Total	
Can't Say	21	28	49	26.06%
NO	37	86	123	65.42%
YES	4	12	16	8.51%
Grand Total	62	126	188	

Table 5-29 Responses :data are secured, Safe and Privacy is ensured

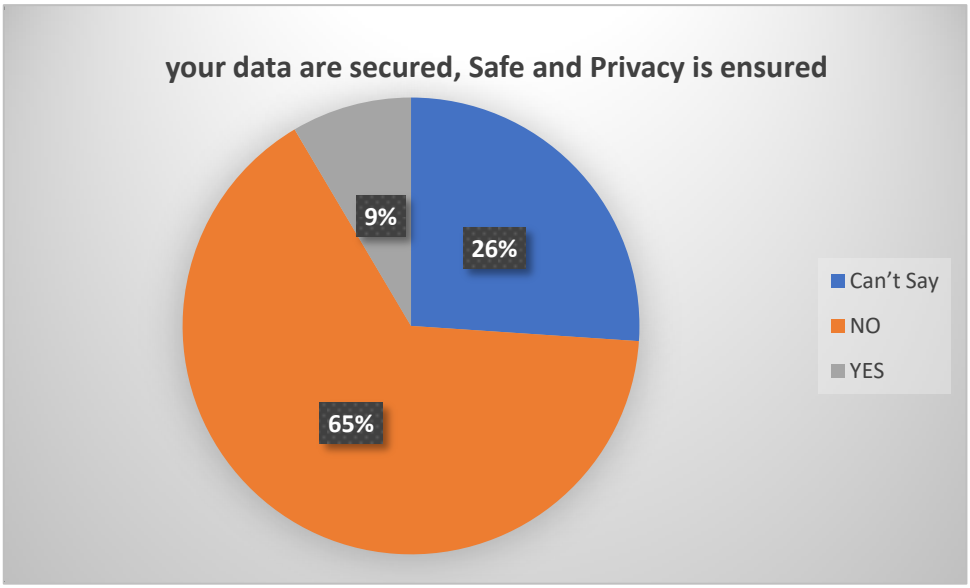


Figure 5-24 Pie chart of responses if your data are secured, Safe and Privacy is ensured

Remark :// 65% of respondent stated that data are not secured, Safe and neither Privacy is ensured . While 26% of respondent stated that their data are secured, Safe and Privacy is ensured . This simply implies needful action is to be ensured for digital sovereignty.

8.[M] Are you confident that your Privacy is ensured on cyber space? * Mark only one oval.

A. YES
B. NO
C. Can't Say

Count of IT Experience	Column Labels			% Count
Row Labels	No	YES	Grand Total	
Can't Say	16	13	29	15.42%
NO	40	101	141	75.00%
YES	6	12	18	9.54%
Grand Total	62	126	188	

Table 5-30:Responses :Are you confident that your Privacy is ensured on cyber space

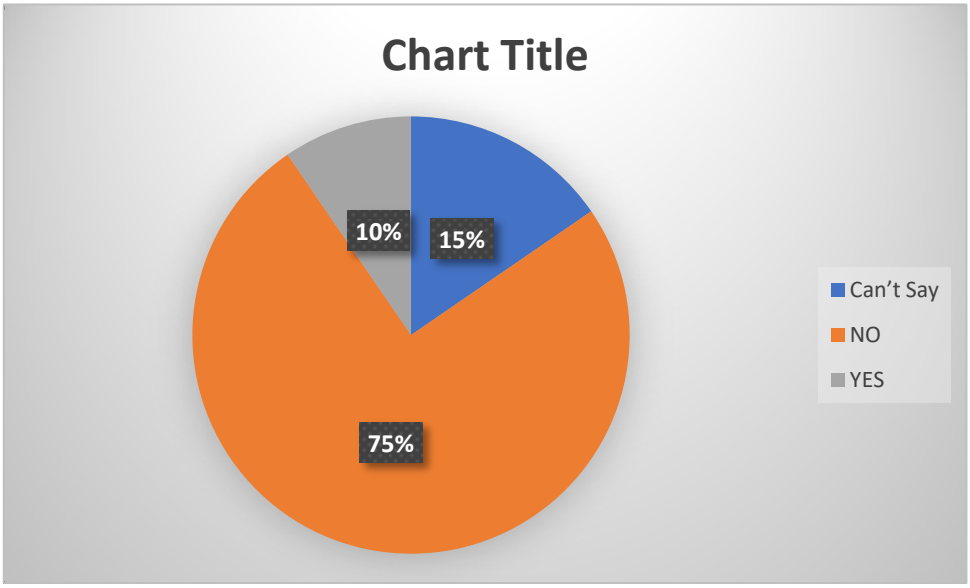


Figure 5-25 Pie chart : Are you confident that your Privacy is ensured on cyber space

Remark:// When respondent was asked directly about Privacy is ensured on cyber space or not . 75% of respondent stated with "No" and Only 10% "Yes". This simply implies PDP Bill 2020 should be enacted earliest to ensure Privacy of Citizen.

9. Securing Digital Sovereignty will effect the GDP growth rate adversely? .

A. YES
B. NO
C. Can’t Say

Securing Digital Sovereignty will effect the GDP growth rate adversely?	Non IT Experience	IT experience	Grand Total
Can't Say	18	32	50
NO	20	56	76
YES	24	38	62
	62	126	188

Table 5-31Response :Securing Digital Sovereignty will effect the GDP growth rate adversely

Securing Digital Sovereignty will effect the GDP growth rate adversely?	Non IT Experi	IT experience	Grand Total
Can't Say	29%	25%	27%
NO	32%	44%	40%
YES	39%	30%	33%

Table 5-32 Response (%):Securing Digital Sovereignty will effect the GDP growth rate adversely

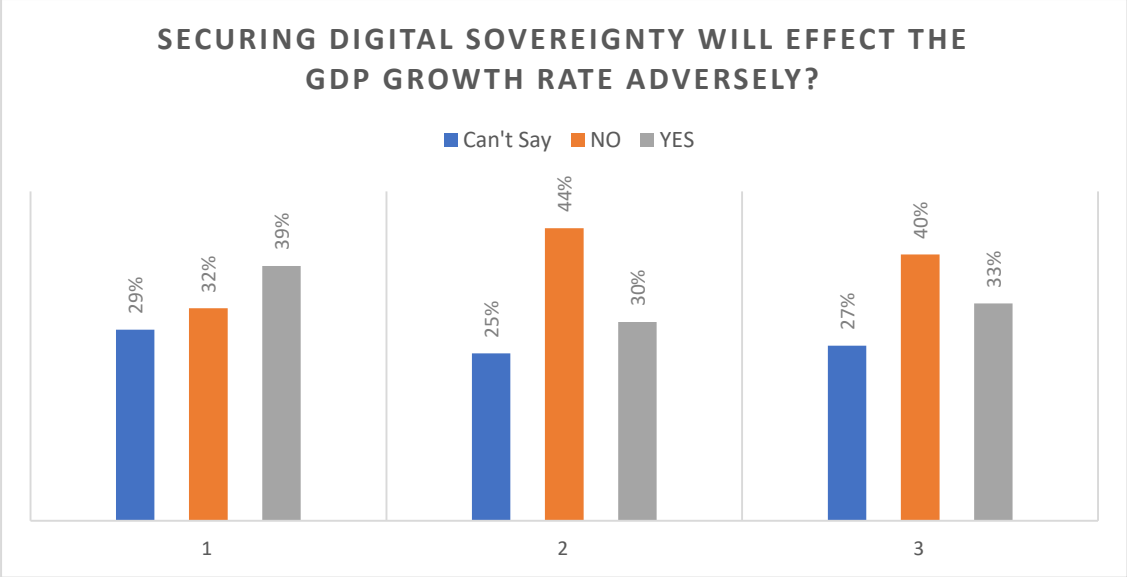


Table 5-33 Pie Chart: Response showing securing digital Sovereignty will affect GDP

Securing Digital Sovereignty will effect the GDP growth rate adversely?	Non IT Experience	IT experience
Can't Say	29%	25%
NO	32%	44%
YES	39%	30%

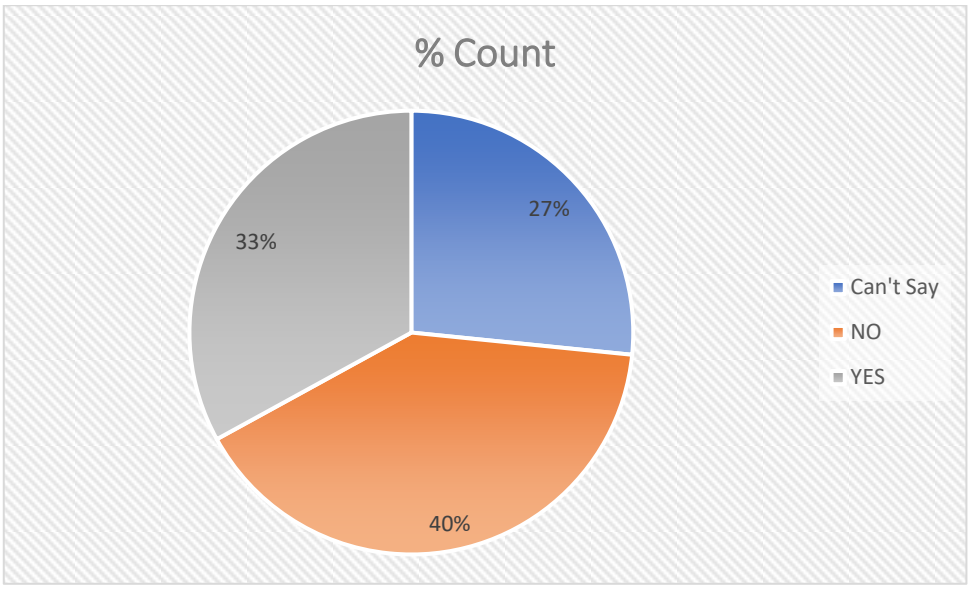


Figure 5-26 Pie chart:Securing Digital Sovereignty will effect the GDP growth rate adversely

Remark :// 33% of respondent stated that Securing Digital Sovereignty will effect the GDP growth rate adversely while 40% negated . as securing digital sovereignty will requires the huge investment for creation of Data Centre, IP infrastructures and R&D so likely to affect adversely., however on long run it will effect GDP growth positively. However on details analysis it learnt that IT experience give responses for No effect and Non IT experience registered response for affecting adversely.

5.3.5 Respondent opinion for securing Security Digital Sovereignty

Recommendation for needful action to Secure Digital Sovereignty

Qus.10. Digital Sovereignty encompass following aspects * Mark only one oval.

A. Security of Data
B. Protection of Data
C. Both A & B
D. None of these
E. Can't say

Row Labels	< 10 Yrs	< 15yrs	<5 yrs	0 yrs	More than 15yrs	Grand Total	% count
A. Security of Data				1	2	3	2%
B.Protection of Data				1	1	2	1%
C. Both A & B	12	12	32	60	65	181	96%
D.None of these			1			1	1%
E. Can't say	1					1	1%
Grand Total	13	12	33	62	68	188	

Table 5-34 : Response :Digital Sovereignty encompass

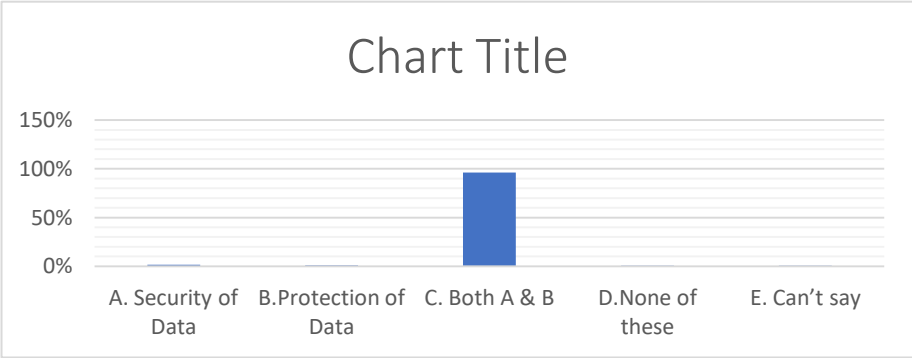


Table 5-35 Pie chart : responses showing Digital Sovereignty encompass both data protection and Security

On analysis >> It is analysed that 96 % of respondent stated that Digital Sovereignty encompasses both 1. Security of Data

2. Protection of Data

Thus the Strong Data Protection law is not enough and sufficient measure but certainly necessary for ensuring Digital Sovereignty in India

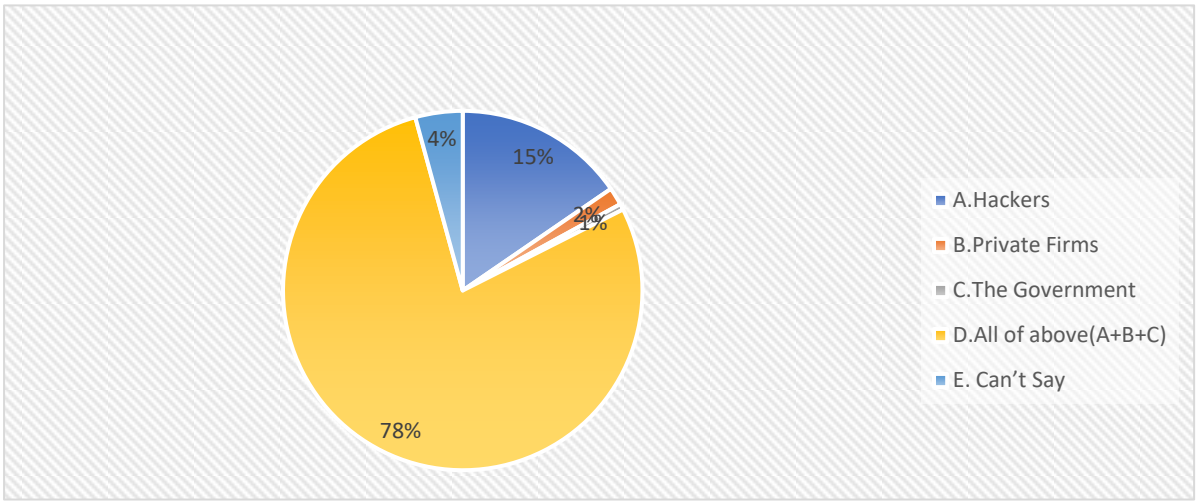
Qus11. Digital Sovereignty faces challenges from ?

A. Hackers
B. Private Firms
C. The Government
D. A,B and C [all of above]
E. Can't Say

Digital Sovereignty faces challenges from ?						
Row Labels	< 10 Yrs	< 15yrs	0 yrs	More than 15yrs	Grand Total	% count
A.Hackers	3	2	10	12	29	15%
B.Private Firms			2	1	3	2%
C.The Government			1		1	1%
D.All of above(A+B+C)	10	8	46	53	147	78%
E. Can't Say		2	3	2	8	4%
Grand Total	13	12	62	68	188	

Figure 5-27 Responses :Digital Sovereignty faces challenges from

Figure 5-28 Pie chart :Digital Sovereignty faces challenges from



Remark :// 76 % of respondent has stated that Digital Sovereignty faces challenges from Hackers , Private Firms, Government. Thus respondent are concerned about Privacy , hacking and data illegal selling or reutilisation without permission.

Qus12.Google, Amazon ,WhatsApp, Microso& and Facebook data resides are outside India ? Can Digital Sovereignty be ensured by Data localization strictly? *

A. YES
B. NO
C. Yes ,but secured Data Centre requrired
D. Do not Know
E. None of these

Row Labels	< 10 Yrs	< 15yrs	<5 yrs	0 yrs	More than 15yrs	Grand Total	% count
A. YES		1	8	10	19	38	20%
B. NO	3	3	6	9	14	35	19%
C.Yes ,but secured Data Centre required	10	8	15	32	32	97	52%
D.Do not Know			3	11	3	17	9%
E.N.one of these			1			1	1%
Grand Total	13	12	33	62	68	188	

Table 5-36 Responses :Sovereignty be ensured by Data localization

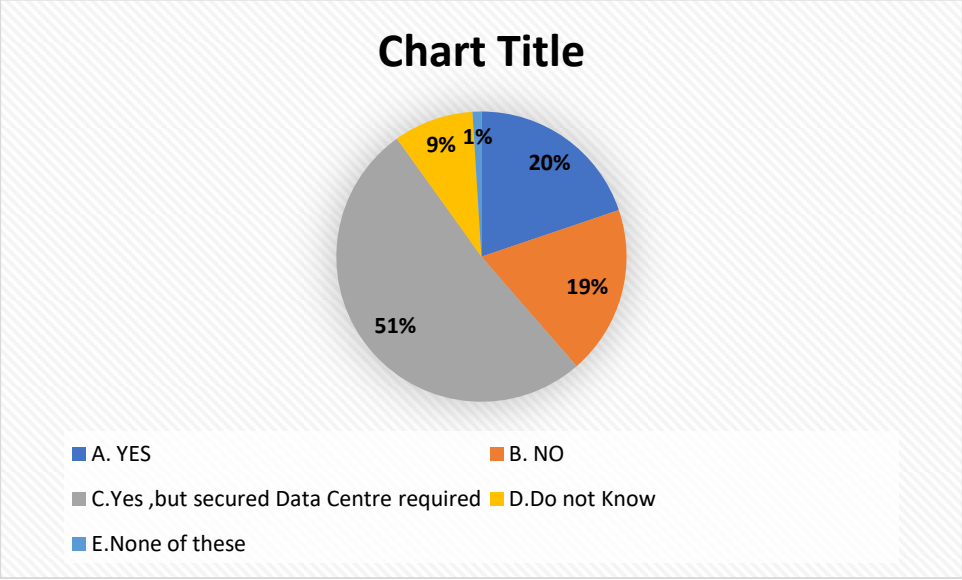


Figure 5-29 : Pie chart :Sovereignty be ensured by Data localization

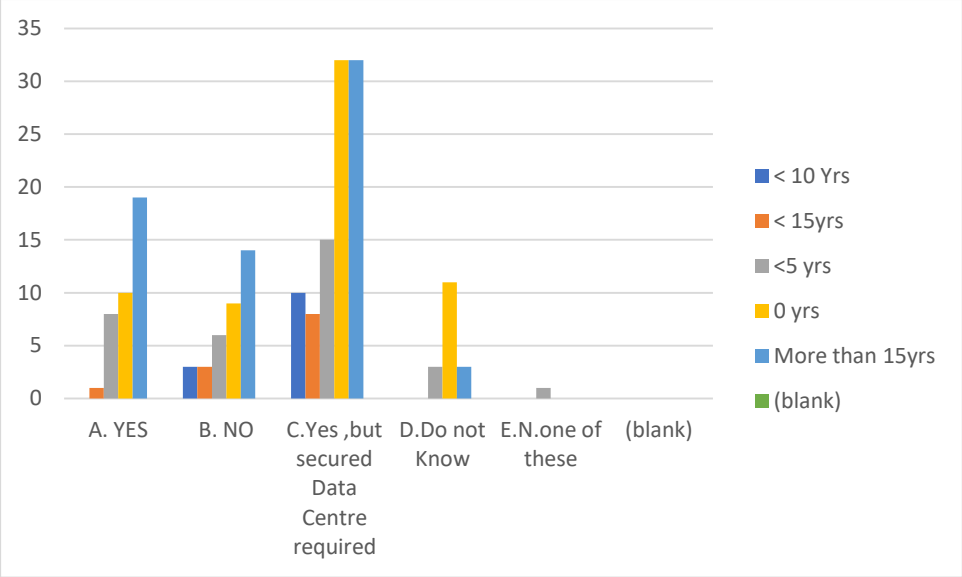


Figure 5-30 Pie chart :Sovereignty be ensured by Data localization (Secured but Data Centre is required)

Remark : On analysis of data it can be concluded that 20% of respondent are stating data is secured "Yes" and in agreement that data is stored on foreign (land) data centre with Facebook ,Amazon, Microsoft and WhatsApp considering them to more rule following and their data is secured on par with foreign national Country law but 51% respondent, majority of respondent are conditionally stating that Data is secured and 19% are stating "No "about but inhouse Data Centre is required to be more precisely Thus data localisation issue is referred with70% of respondent and felt for More inhouse Data Centre.

Qus13..Which of following is/are the major hurdles in ensuring the digital sovereignty? * Mark only one oval.

A. Data localization
B. Technological Competence
C. Strict Data Protection Law
D. A,B and C [all of above]
E. Can’t Say

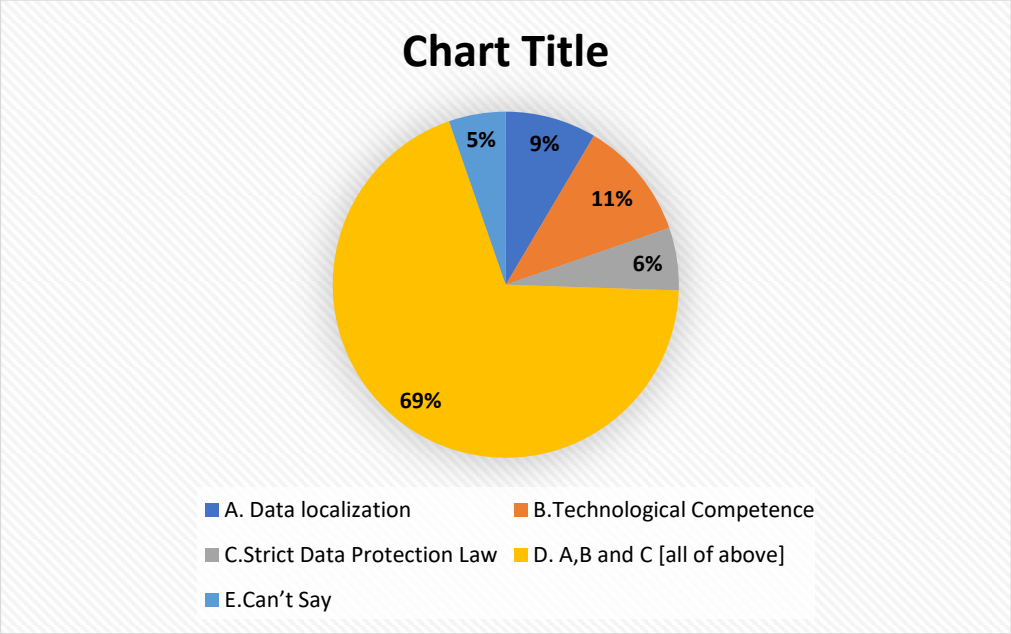


Figure 5-31 Pie chart :major hurdles in ensuring the digital sovereignty

Row Labels	< 10 Yrs	< 15yrs	<5 yrs	0 yrs	Grand Total	% count
A. Data localization	1	1		6	16	9%
B.Technological Competence	3	1	4	7	21	11%
C.Strict Data Protection Law	2	1	1	4	11	6%
D. A,B and C [all of above]	6	9	27	42	130	69%
E.Can't Say	1		1	3	10	5%
Grand Total	13	12	33	62	188	

Table 5-37 Responses: major hurdles in ensuring the digital sovereign

Remark // 69% of respondent stating the major hurdles in securing digital sovereignty are 1. Data localization 2. Technological Competence 3. Strict Data Protection law. With the PDP bill is already tabulated so one of the hurdles will resolved as PDP Bill is made in conformity with GDPR.

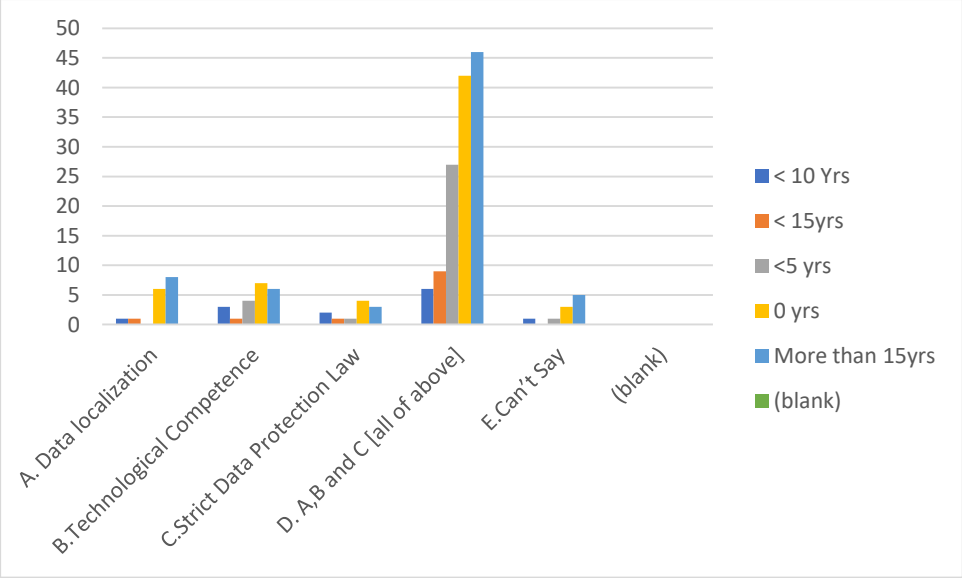


Figure 5-32 Pie Chart illustrating major hurdles in ensuring the digital sovereignty [IT Experience wise]

Qus.14. Digital Sovereignty can be improved by ensuring Cyber Security and Cyber Safety Awareness ? *.

A. Strongly Agree
B. Agree
C. Can’t Say
D. Disagree
E. Strongly Disagree

Count of Total No of years' experience in IT field									
	No	No Total	YES				YES Total	Grand Total	% count
Row Labels	0 yrs		< 10 Yrs	< 15yrs	<5 yrs	More than 15yrs			
A. Strongly Agree	32	32	9	8	21	40	78	110	70%
B. Agree	25	25	3	4	12	27	46	71	27%
C. Can’t Say	4	4						4	2%
D. Disagree						1	1	1	1%
E. Strongly Disagree			1				1	1	0%
Grand Total	61	61	13	12	33	68	126	188	

Table 5-38 Responses :Digital Sovereignty can be improved by ensuring Cyber Security and Cyber Safety Awareness

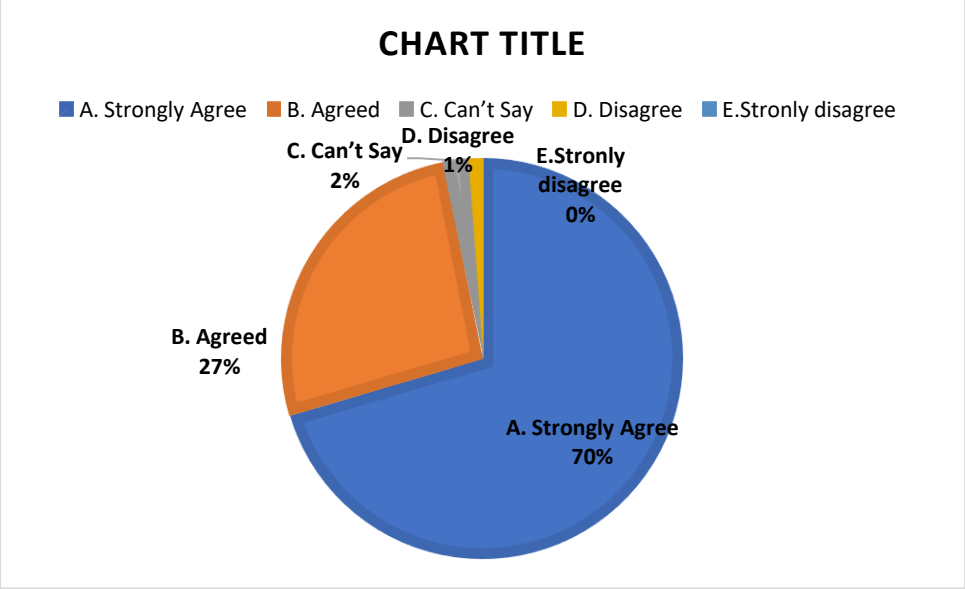


Figure 5-33 Pie Chart :Digital Sovereignty can be improved by ensuring Cyber Security and Cyber Safety Awareness

Remark :// 70% of Respondent strongly agreed and 27% Agreed , i.e. 97% of respondent agreed with view that Digital Sovereignty can be improved by ensuring Cyber Security and Cyber Safety Awareness as any data theft or hacking , initially individual unknowingly get trapped to vulnerabilities and threats . So Cyber Security and Cyber Safety Awareness along with capacity building in society , institutions and Industry by NGO , Govt and Government approved Policy and Act can improve and secure Digital Sovereignty one step forward.

Qus.15. Digital Sovereignty can be secured by * Mark only one oval.

A. Regulatory and license regime on Cloud Data Centre
B. IT device Equipment Security Compliance Mechanism
C. Strong Data Protection Law
D. Securing Cyber Space from Hackers
E. All of them
F.

Count of IT Experience	Column Labels						
Row Labels	< 10 Yrs	< 15yrs	<5 yrs	0 yrs	More than 15yrs	Grand Total	% Count
A. Regulatory and license regime on Cloud Data Centre			1	5	5	11	6%
B.IT device Equipment Security Compliance Mechanism					2	2	1%
C. Strong Data Protection Law		2	1	6	5	14	7%
D.Securing Cyber Space from Hackers				3	1	4	2%
E. All of them(A,B,C &D)	13	10	31	48	55	157	84%
(blank)							
Grand Total	13	12	33	62	68	188	

Figure 5-34 responses :Digital Sovereignty can be securing Action

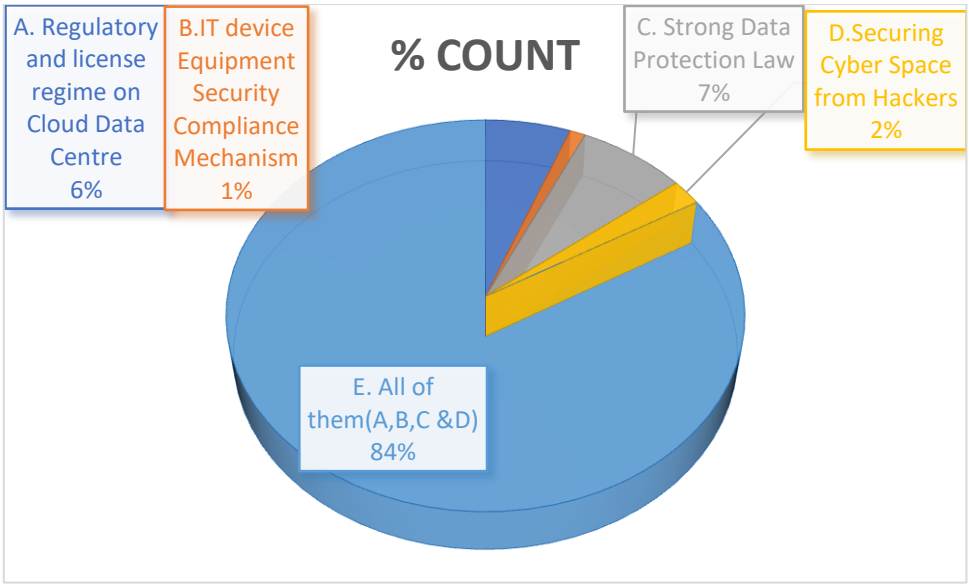


Figure 5-35 Pie Chart: Digital Sovereignty can be securing Action

Digital Sovereignty can be secured by	Count	% count
A. Regulatory and license regime on Cloud Data Centre	11	6%
B.IT device Equipment Security Compliance Mechanism	2	1%
C. Strong Data Protection Law	14	7%
D. Securing Cyber Space from Hackers	4	2%
E. All of them	156	84%

Remark :// 84% of respondent has vetted strongly for all of the four action for securing digital sovereignty :-

A. Regulatory and license regime on Cloud Data Centre
B.IT device Equipment Security Compliance Mechanism
C. Strong Data Protection Law
D. Securing Cyber Space from Hackers

Which requires 1.the Security Testing Compliance Mechanism for ICT Equipment and Devices , 2. IT infrastructures creation like data Centre 3. Strong data Protection Act and 4. Educating and capacity building with respect to network and cyber security in society , Industry and Institution.

Qus.16. Do you think “Government should take needful correctives measures to ensures Digital Sovereignty India “ ? *

A. Strongly Agree
B. Agreed
C. Can’t Say
D. Disagree
E. Strongly Disagree

Count of IT Experience2	Column Labels						
Row Labels	< 10 Yrs	< 15yrs	<5 yrs	0 yrs	More than 15yrs	Grand Total	%
A. Strongly Agree	12	9	24	38	50	133	71%
B. Agreed	1	3	9	20	17	50	27%
C. Can’t Say				4		4	2%
D. Disagree					1	1	1%
Grand Total	13	12	33	62	68	188	100%

Table 5-39 Responses: Government should take needful correctives measures to ensures Digital Sovereignty India

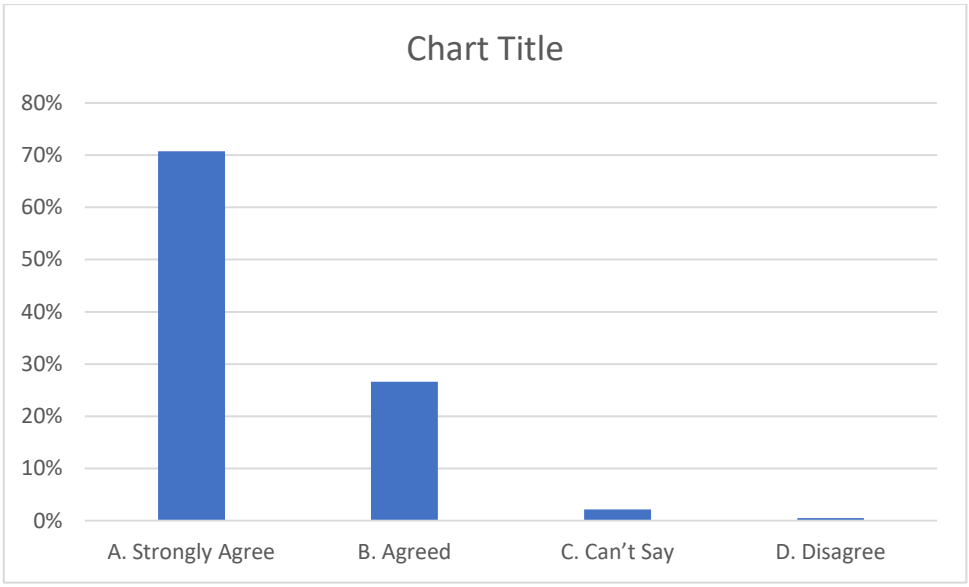


Figure 5-36 Bar diagram: Government should take needful correctives measures to ensures Digital Sovereignty India

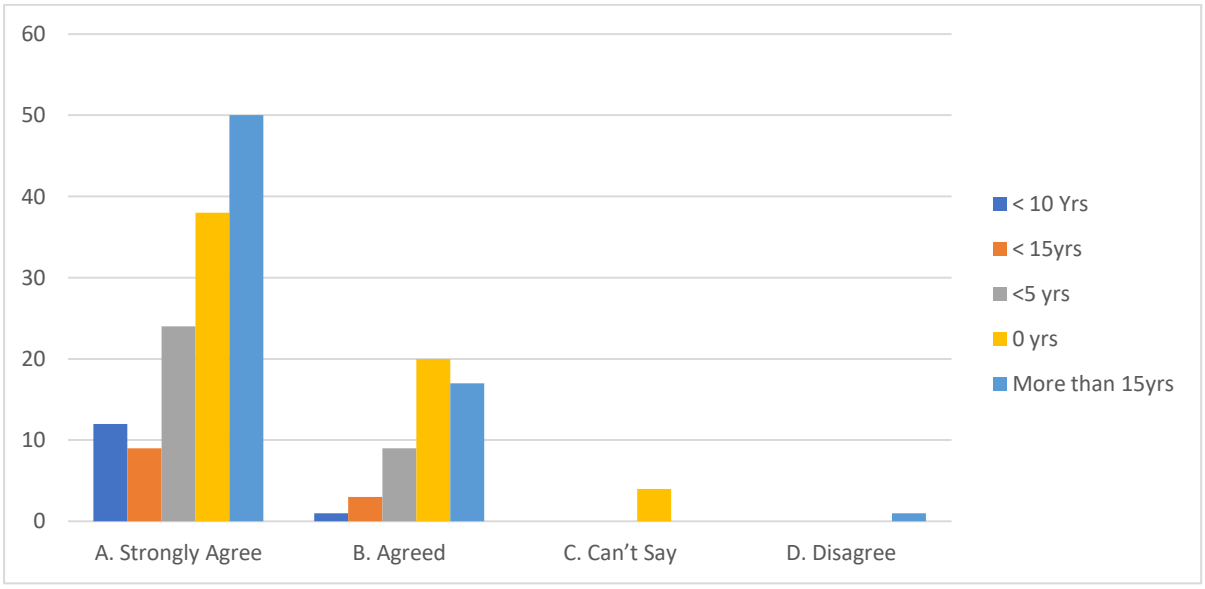


Figure 5-37 % bar diagram :Government should take needful correctives measures to ensures Digital Sovereignty India

Remark :// 71% of respondent strongly and 27% agrees to mandate, i.e. total 98% of respondent wants the Government for taking needful corrective action to ensures digital sovereignty in India in best possible manner.

6 Recommendation

6.1 Digital Sovereignty : Concern

The internet has greatly (profoundly) changed our citizen and society of economically, socially and culturally. Up until recently, the issue regarding the collection and usage of users' personal data had not ever really been resolved.

However, since the Snowden scandal and rise in cybercrime, this situation has evolved. Following a number of hacking scandals and data theft (Facebook, Yahoo, TV5, the American elections etc.), internet users are now very worried about their

1. private lives'
2. confidentiality and
3. their personal data's security.

Consequently, cybersecurity has become a dominant concern of Digital Sovereignty.

And thus maximum of world population do not trust Social Media Networks to manage and protect their personal data. And thus presented the challenge, the term "Securing Digital Sovereignty" has been burning topic now days in all country irrespective of developing or developed or underdeveloped.

6.2 Strategic risks

Loss of control over data represents a strategic risk for our society. individuals, businesses and governments are surveilled and their data is monetized by foreign corporations using AI and data analytics . When societal debates take place on platforms owned by corporations and hosted in countries with a vested interest, how can we trust the results?

When nearly all commerce flows through a few select platforms these platforms control the prices and capture most value. Innovation on new technologies in machine learning and big data analysis depend on vast data treasures that are not available to India , in General.

I. Long term innovation

Each nation/territory that does not own or have control over platforms will ultimately have to follow the rules of somebody that does. Those nations will at best become “app-developers” where they are dictated what they can and cannot do. Data from the platforms will ultimately allow those nation whom owns them – to gain insight that others do not have.

II. Lack of choice or complete dependency on one or few companies of Foreign Country

Already today there are immense dependencies on a few companies services. As always – monopolies or even oligopolies are not preferred for any buying party. To lower these dependencies on these few companies will require bold decisions and change in what people are used to run on their desktops.

III. National security

When one person can have power to affect a nation or a continent with a press of a button – it is never a secure situation. Many countries in World have decided to be self-sustaining when it comes to food. Certain data really ought to be treated the same way.

IV. Environmental aspects

With the rise of AI, Big Data and other modern ways of analysing data – our mark on the environment will continue to rise in multiples. 99% of the world is in danger of falling behind (even more) and risk not being able to control one or more of the above aspects of our data.

All large platforms are concentrated to one or a few countries. Those will have companies that amass data like no others. Those owners of that data have better insight which in turn will allow for greater possibility of continued innovation.

On data analysis the primary date following observation has been acknowledge

What could happen?

Q.No.	Scenario	% of Respondent given "Yes"	%of Respondent given "No"
8A	Foreign governments spy on important business deals to benefit their firms	90%	10%
8B	Foreign government interfere in domestic political discussions and elections	90%	10%
8C	Foreign-controlled communication platforms foment ethnic tensions	87%	13%
8D	Foreign government disrupts civilian infrastructure	77%	23%
8E	Large corporations ignoring domestic law and agreements and abusing customer data	88%	22%
8F	Large corporations using their market power to thwart attempts at changing their behaviour	99%	1%
8G	Companies find out from shopping behaviour if teenagers are pregnant and out them, or target teenagers at their most vulnerable time	96%,96%	4%,4%
8H	Companies put hidden microphones in devices and when find out claim they had no idea it was recording users	85%	15%
8I	Commercial data tracking leaks secret military bases	80%	20%
8J	Commercial firms leaking data allowing people to track heads-of-state	82%	18%
8K	Have you ever have been attempted for financial frauds?	53%	47%
	What is next? Ans. Call for strengthen digital infrastructure and design IT equipment by ensuring Security and Privacy by Design		

6.3 Recommendation

Becoming 100% digital sovereign is quite a challenge, if not impossible. Governments (but also companies and private persons) are becoming increasingly aware of the importance of data ownership . But if any country determined to succeed, know that by making the right choices in the areas described above, India definitely moving in the right direction, but lot more to do.

Considering the claim for digital sovereignty by different Nation like USA ,China ,France ,Germany , Canada , Russia , South Korea by enacting Data Protection Act but still the sovereignty is compromised at different instance of time in the past. France is proclaiming that as they are technical incapable to Secure true Digital Sovereignty . Understanding the respondent majority suggestion to secure digital Sovereignty, and as different steps taken by different country in steps forwards towards achieving Digital Sovereignty in cyber space Cyberspace with its characteristic of (dematerialisation, de-temporalization and reterritorialization) can cross borders and the territory of state despite of all precautions to protect its sovereignty. Hence the absolute digital sovereignty is difficult to achieve. However the level of Digital Sovereignty in the country can be evaluated and categorised as

1. Low means high dependency or
2. Medium or
3. High means no dependency

based on performance or achievement of country on criteria variables . These different criteria variables parameter for evaluating level of Digital Sovereignty (low or Medium or High) is evaluated is proposed as below

1. Data (Data Protection Law and law of Privacy)

First and foremost, it is need to make sure that citizen should have full control over their data. It is important to have data control does not mean intellectual property. Rather it's not just about short-term commercial risks. It's also about the possible future implications of leaving your data in the hands of others.

If the service provider , not the user decides which data is at the disposal of whom and how he uses them ,then it low .The Country has complete control over who has

access to data and can delete them at any time , then Medium. Data can be stored, read, changed and deleted, independently of the software solution that is used then high.

2. API [Software and IT Competence]

Open standards and open APIs are also very important when it comes to digital sovereignty as they enable a smooth transition to alternative solutions. An open API gives your developers easy access to data used by an application, without offering a lot of limitations. Another good thing about open APIs is that they are often based on open standards and protocols such as OpenID Connect for identity management. By choosing software vendors that rely on open standards and open APIs, it can be certain that citizen can retrieve their data at any time, in a format that the other applications they intended use can recognize.

No or only proprietary APIs available, then level of Digital sovereignty is low. Support of a high number of open standards and APIs then level of Digital sovereignty is medium .
The level of Digital Sovereignty qualifies for high if access to all data and functions via open, freely usable APIs with open source reference implementation

3. Source Code [IT equipment Designing Capability]

In an ideal, digitally sovereign world, all the software your company uses is open source. In this way, citizen know precisely what happens to their data and be certain there are no backdoors built in the software you are using. Open-source software also allows you to modify the code so you can easily change it to your needs. This may come in handy if, for example, citizen plan to switch vendors and need to replace one piece of software with another. With open-source software, they can make sure the new software integrates easily in their existing software stack.

Level of Digital Sovereignty is low , if Source code not available , other wise medium. While the level of Digital Sovereignty qualifies for high if Source code testable/source code available in case of manufacturer’s failure . i.e .Source code changeable/usable modified

4. Hardware Designing

Yes, hardware. This is a tough one since, if they want to keep full control over your hardware, they have to build your hardware of their own . Usually, this is not really an option. Open-source hardware does exist but is far from being as mainstream as open-source software. Whenever possible, purchase hardware that is produced in the India. This gives a little bit more control over IT than using hardware that is produced in, for example, European China or the United States. Just think about what happened with Huawei and US trade Ban and with the backdoors in Cisco software

If the hardware is purchased as black box , then low . otherwise medium Existing solutions can extended with own hardware. While the level of Digital Sovereignty qualifies for high if all hardware components can be produced and influenced by the organization of particular country.

5. IT Products as Solution

Remotely Control is what digital sovereignty is all about. It's not about you sitting on your knowledge, but about you being the owner of your data, because your data is your knowledge. It's about knowing where your data is at all times and what happens to it at this very moment. And it's about the freedom to make changes and, for whatever reason, to choose a different solution. It's about knowing that your sensitive information is safe with the software vendors that process your data for you.

The IT solution is only available from a single vendor, there are no control or migration options qualifies for low level of Digital Sovereignty,
Any advancement from earlier qualifies for medium if Important parts can be controlled and migrated to other suppliers, the structure of a solution operated by the organization itself is possible. While the level of Digital Sovereignty qualifies for high if User organization operates solution itself, has control over all components (source code, hardware, …) and may change / replace them.

6. IT Skills : Security ,Safety Awareness Citizen

All of the above is just talk if you do not have the right skills in-house. If people want to change code or customize and integrate different applications, they need people who can do that. We never said becoming digitally sovereign is easy.

No understanding of processes and data use, no skills to make adjustments available. The level of Digital Sovereignty if improved to medium if Understanding of data and processes is present, possibilities for adjustments are limited. While the level of Digital Sovereignty qualifies for high if Skills for changing data, program code and processes are available.

7. Fabrication of Secure Element and IoT element :

Secure elements contains Telcom SIM, banking Card, Government & healthcare As Industrial, any automation Card. As Policy of Matter because in India these FPGA cards are not manufactured rather only programmed. As Industrial Policy Matter the Government should take enough measures to manufactures these secure card as recent time spying on network by Hardwired-Rootkit has noticed, and it is difficult to detect and mitigate . Recent days with implication IoT devices are integrated in India , whole network are venerable and thus Digital Sovereignty is compromised without any commission or omission of users. Security and Privacy by Design should this means that manufacturers and providers should be held responsible for the security and privacy of the entire product life-cycle from design to distribution and use. This is particularly true for connected devices (IoT) aimed at consumers.
If country is able design IT equipment by ensuring Security and Privacy by Design , then level of digital sovereignty is high , Medium if Fabricate and programming And otherwise low if outsourced or import.

8. Cloud Policy [Cloud Computing]

The basic idea behind the principle is

i. To treat extra-terrestrial data request equally, regardless of location of the cloud provider's headquarters.

ii. To rely on need for international cooperation to create reciprocity. This approach would provide impetus to Global Cloud Companies and encourages innovation as this approach foster a level playing field for global cloud companies , than balkanisation of the internet.

These models are namely

1.Data Shard : where service provider stores information in the cloud in multiple international location, the network itself dynamically distributes data to domestic and international servers

2.Data Localisation Model: Here service provider stores information in a cloud that is restricted to a single country or region and

3.Data Trust Clouds: In this case company bifurcates network management from the ability to access data.

If cloud policy is Data Shard , the Digital Sovereignty is high , If data stored in Data localization model , then medium , else low if Data Trust Clouds is used.

Thus India's Digital Sovereignty lies at medium level , needed to be done lot with respect to strengthen Digital Infrastructure and to encourages IT equipment development by ensuring Security and Privacy by Design.

And Moving ahead in Present Circumstances

Open source enables businesses to be digitally sovereign.

Firstly, only open source can guarantee full control and transparency over their application and data. Crucially, with open source there is no vendor lock-in. Citizen have freedom to choose who hosts your data (on premises or in the cloud) or choose to support yourself.

By providing standard open source software for standard services and problems, we reduce the effort to provide 'commodity' services. The open communities around software share knowledge and skills, reducing pockets of proprietary knowledge.

More generally, India and public institutions need to assess their IT strategy and look at opportunities to embed open source to maximise innovation and enhance data security. At a government level, it doesn't make sense to fund the development of proprietary software and create dependencies that we can't easily escape.

If, instead, government funding was devoted to investing in open source projects, public money would be spent for public good, providing more control and removing our growing dependencies on overseas technical giants that consume huge volumes of private data as a business model.

As a regulatory powerhouse, PDP Act 2020 will a great stride into the direction of digital sovereignty but there's more to be done. India should be looking at open source not only to reduce their total cost of ownership but also as an enabler of digital sovereignty and data privacy. Government of India is Committed for securing "Digital Sovereignty" and GoI India seems to be on a mission toward digital sovereignty. As long pending PDP Act 2020 talks of data localisation and strong compliance mechanism for Data Security on par with GDPR of European Model .

Further also cloud policy is missing in India , which should be on par with Cloud Policy of USA, And will thus competition for Data Centre will increase with transparency , and will thus stimulus for investment or FDI on Data Centre in India. Government of India, must utilize the brain power of technocrats, motivate the IT brain of IIT for innovation and research and must ensure the long pending the industry issue of setting up of VLSI fabrication lab as consumer IT markets supports and is one of the motivating factor for setting up fabrication industry , and will thus reduce imports bill of Government of India by ensuring the Hardware competences on far with China . Digital sovereignty

"In order to guarantee our digital sovereignty, India need to reduce dependencies on individual IT service and infrastructure providers. In addition, parallelly India examining alternative programs in order to replace certain software and IT infrastructure with Compliance and Security Certification Mechanism with Research and innovation by Start-up , these start-up should be well supported by Govt of India and Private Industries.

And thus India should strive hard to enhance and upgrade their IT competence to improve the ranking on digital Sovereignty to higher side by above listed action and suggestion in following agenda :-

[A] Compliance Mechanism:

1. Data Security
2. Cloud Policy [Cloud Computing]

[B] Software Capability and Competence

3. Source Code [IT equipment Designing Capability]
4. Hardware Designing API [Software and IT Competence]

[C] Hardware Fabrication & Production

5. Designing IT Products as Solution
6. Fabrication of Secure Element and IoT element :
7. Hardware Designing for Fabrication

[D] IT competence in Human Resource Development

8. IT Skills : Security ,Safety Awareness Citizen

Till proper competence is developed , India should work with open source software and Hardware designing and production competence improved , India should managed with standard IT Equipment Standardisation Testing Schedule before induction of IT equipment and system . Thus proper investment in structural Institutional Setup and Industry for Education ,Innovation , Research in IT and security should be encouraged with aim to achieve 100% Digital Sovereignty means Absolute Sovereignty.

6.4 Suggestion from respondent for "Securing Digital Sovereignty "

Access to all Government data in equitable manner will improve digital sovereignty. All the data going in and out of licensed ISP servers should be mirrored and monitored by security agencies for lawful interception and monitoring. Any individual can be manipulated basis how the world or any organisation or government wants them to change and react...we have live examples from Delhi riot case. As long as the data centres for all internet traffic is located offshore, securing digital sovereignty is a pipe dream. Awareness is the key. For example people keeping simple passwords is not a platform issue but an awareness issue. How many people exercise their right to provide limited permissions to apps on their phones. Awareness needs to start from schools and organizations. Make sure all websites seeking personal information have a module

on data security and privacy - module provided by govt. Awareness to citizens and transparent digital policies in India required. Having indigenous applications & data network equipment, Strict enforcement of relevant rules & regulations. Awareness, Strong law, Block chain can be used in network .it should be mandatory Data need to be stored in the country. Punish agencies which leak individual data. Data security and protection mechanism both should be made universal and mandatory for all online transactions, be it commercial or social. Digital Sovereignty has to accepted as an extension of right to privacy as well as the Government's duty to protect it. Foreign companies have strict data laws - am not sure if our government can do that. Important people should try to reduce use of internet so that they don't give digital signatures. India cannot secure its digital sovereignty by keeping behind in the technology race. We need to develop our own technology solutions for our IT needs. Government is expected to play a important role in this regard.

It's important but is an evolutionary concept and will take time to regulate, both in terms of law and behaviour. It's now emerged as a mad elephant. Requires a lot of strength to tame it.Law on digital security is needed but competition in e-commerce should not be adversely affected.. Many of local companies are worst in data security then multinational. Multinational companies approach depends on its origin. Network security along with strong data protection bill is to be ensured, with lot of measures about cyber safety awareness programs should be ensured. Niti Ayog seems to be already working in AI and ethics, especially concerned by the data of young children on digital platforms of learning. It is not anonymized. Not ensuring Digital sovereignty will lead to compromising with sovereignty of the state. Not only the main data centre but also the disaster recovery center must be within the national boundaries. No mirroring of any personal data to be allowed beyond country boundaries. Personal data at rest or in motion must be always be with better encryption. None of these digital assets must be allowed to be accessed from outside the national boundaries. These digital assets holding organization s must be sought to be registered under country laws and are to be subjected to audit. Only Trusted applications must be allowed to fetch the users data. Securing digital security will boost online transactions, more purchasing and overall improvement in country economics. Securing digital sovereignty is a must and needs to be ensured uncompromisingly. Separate department of networks

security is essential for Data sovereignty. Similar recommendations as are there in GDPR to be made effective. If a company/organisation which can not protect data should not be allowed to collect data including mobile number Strict data privacy laws should not create hurdles for provisioning of services for common men. Strict Data Protection Laws, stringent actions for not following them and User Awareness are most important. Strict protection law but with minimum intervention areas. Strong data privacy law, rigorous implementation, trained staff, aware public and alert Government are required for data protection and digital sovereignty. This is the domain where future prosperity and security of a nation depends. There should be good training in this field and general awareness should be high. Strong implementation of decisions taken. Country should have their own servers for storing critical data. Strong regulation by government on data protection and cyber space security Strong regulatory regime and adequate data protection mechanism are essential components of digital sovereignty. There has to be international treaty to protect data from large corporate, government agencies and hackers. There is very thin boundary between data theft and data used. With AI, churning data, its for sure a threat. There should be global guidelines for data protection as internet is a wide spread thing. Use of legal and regulatory frameworks to data sovereignty

7 Conclusion

“Digital sovereignty cannot be undermined and should be seen first step for the success of Digital India, Make in India, various poverty eradication schemes and creation of a digitally empowered society and knowledge based economy” . And thus

Securing digital sovereignty implies to ensure digital security and sovereignty; thus enables community to thrive (develop and prosperity) . viz.

“Digital Sovereignty will mean not merely that the individual are owners of own data but also they have effective autonomy ,control, choice , integrity, security in context present day state of Cyber space. as there are four guiding principles in connection with digital sovereignty: freedom of choice, self-de- termination, self-control and security. “

8 Annexure : Questionnaire and filled Reply.

9 Reference

Arnd Weber, S. ,. (March 2018). *Soverignity in Information Security.*

Ayers, C. E. Rethinking Soverignty in the context of cyber space. U S Army College.

Dar, J. A. (2019). *Privacy and data ProfectionLaws in Indai,USA and European Union.* Walnut Publication india.

Gueham, F. (n.d.). *Digital soverignty - Steps towards a new system of internet Governance.* Retrieved from fondapol.org.

Jackson Adams, M. A. (Nov-Dec,2016). cyberspace: A new Threat to the Soverignty of the state.

Kolton, M. (2017). *Interpreting China's Pursuit of Cyber Soverignty and its views on Cyber Deterrance.*

lewis, J. A. (2010). Soverignty and the Role of Government in Cyber space. *Spring /Summer* .

Lowe, S. D. (2019). *Multi Cloud Security* . John Willy & Sons .

Malcic, J. H. (2015). The Privacy Ecosystem:Regulating Digital identity in the United states and European Union. JSTOR.

Neil Robinson, L. V. *The Cloud.* JSTOR.

Pinto, R. A. (2018). Digital Soverignty or Digital colonisation . *Inernet and Democracy* .

shen, Y. (2016). Cyber soverignty and the Governance of Global Cyberspace.

Srikrishna, J. B. *A free and Fair Economy Protecting Privacy ,Empoering Indians.*

TIM MAURER, R. M. (November 2014). *Technological Sovereignty: Missing the Point?* Washington, DC: New America and GPPi.