
Cyber Security and Cyber Forensics (Chapter - 4 : DISSA Course) **Part 3**

Arijit Chakraborty
June 26 , 2021

Computer Networking

- **Micro, Mini (Workstations), Mainframe, Super computers**
- **HLL : C++, JAVA, Visual Basic (VB)**
- **Digital telecom network**
- **Computer network = 2 or more computers, printers & nodes transmit / receive data via wired media - copper cable or OFC or wireless media - WiFi.**
- **Computer network = Internet.**
- **KPI:**
 - ✓ Performance
 - ✓ Reliability
 - ✓ Security

Types of Network Topologies

- **#1) *BUS Topology*:**
- Every network device connected to single cable & transmits data **only in 1 direction**.
- **Advantages:**
- Cost-effective
- Can be used in small networks.
- Very less cable is required when compared to other topologies.
- **Disadvantages:**
- If cable gets faulty then the whole network will fail.
- Slow in operation.
- Cable has limited length.

- ***RING Topology:***
- Each computer connected to another computer in the form of a ring with last computer connected to first one.
- Each device - 2 neighbors. data flow is unidirectional & bidirectional
- **Advantages:**
- Easy to install and expand.
- Can be easily used for transmitting huge traffic data
- **Disadvantages:**
- Failure of one node will affect the whole network.
- Troubleshooting is difficult in a ring topology.

- ***STAR Topology:***
- All nodes are connected to a single network device through a cable.
- **Advantages:**
- If one node fails, then it **will not affect the whole network** and the network will run smoothly.
- Troubleshooting of fault is easy.
- Simple to operate.
- **Disadvantages:**
- High cost.
- If central node gets faulty = whole network will get interrupted

- ***MESH Topology:***
- Every node connected to another one with a point to point topology & every node connected to each other.
- **Advantages:**
- It is robust.
- Fault can easily be detected.
- Very secure
- **Disadvantages:**
- Very costly for Installation & configuration

TCP IP

- IP = how **to address & route each packet to make sure it reaches right destination.**
- Each gateway computer on network checks this IP address to determine where to forward the message.
- **Uses of TCP/IP**
- used to provide remote login over network, for:
 - ✓ interactive file transfer,
 - ✓ to deliver email,
 - ✓ to deliver webpages over the network

Common TCP/IP protocols

- **HTTP (Hypertext Transfer Protocol)**, = communication between web server and web browser;
- **HTTPS (HTTP Secure)**, = secure communication between a web server and a web browser;
- **FTP (File Transfer Protocol)**, = transmission of files between computers.

Types of Transmission Media

- **1. Coaxial Cable:**
 - = 2 conductors which are parallel to each other. Copper used as a central conductor & surrounded by PVC insulation with outer metallic wrapping.
- **Cable TV network** providers also widely use **Coaxial cable in entire TV network.**
- **2. Twisted Pair Cable**
- **Most popular** wired transmission medium. Cheap & easier to install than coaxial cables.
- 2 conductors (copper), each having their **own plastic insulation & twisted with each other.** One is grounded & other **used to carry signals** from sender to receiver.
- used in LAN & telephone landline connections - has high-bandwidth capacity

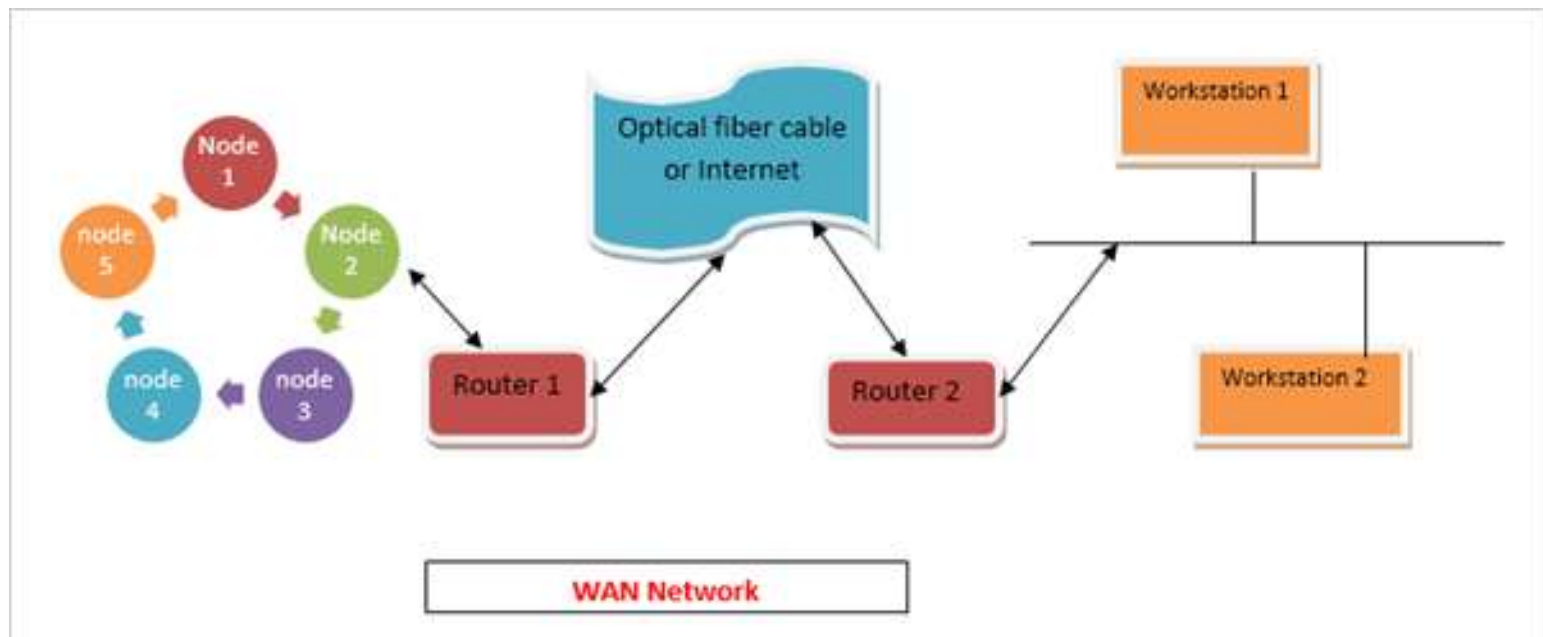
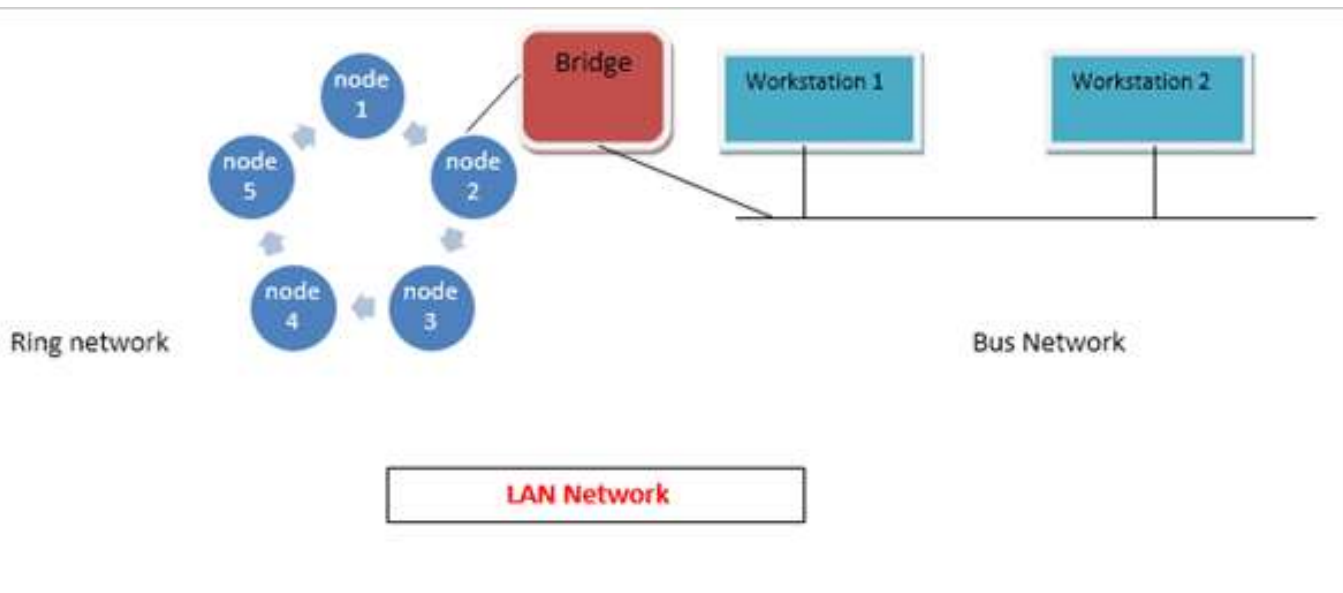
3. Fiber Optic Cable:

- made up of a **core surrounded by a transparent cladding material**
- It uses **properties of light for signals** to travel between them.
- used in WAN
- Optic fiber = flexible & transparent fiber - consists of **silica glass** or plastic.
- Optic fibers transmit signals in form of light between 2 ends of fiber = **they permit transmission over longer distances & higher bandwidth** than coaxial & twisted pair cables or electrical cables.

Network components

- **1. Ports:**
- Port identifies- connection b/w network devices.
- Each port = identified by a number.
- If IP address as comparable to address of hotel,
- ports = suites or room numbers within that hotel.
- **2. Routers**
- To establish connection between 2 locations = use routers at both ends & connected by fiber optic cable through high bandwidth
- **Components of routers** = CPU, flash memory, non-volatile RAM, RAM, network interface card & console.
- **3. Switches:** connects other devices & manages node-to-node communication within network,
- ensuring data packets reach their ultimate destination.
- Router sends information between networks, switch sends information b/w nodes in a single network.

LAN & WAN



Google Fibre network

- Dunant subsea cable, connecting US & mainland Europe = ready for service
- Google = **used 4,000 miles of cable**, underwater, to connect US to Chile
- Delivering **record capacity of 250 TB** per second (Tbps) across Atlantic
- Enables **more fibres** within cable, providing **higher system availability**.
- Each cable expected to **last up to 25 years**.
- **Google's subsea cable** = Grace Hopper - run between US , UK and Spain = expected to be completed in 2022.
- Nearly **750,000 miles of cable connect continents** = for communication and entertainment
- Demand for undersea cables **will only grow** = more businesses rely on cloud computing services

- **De-militarized Zone – (DMZ)**
- "neutral zone" between internal network & outside extranet network.
- Small network = **lies between trusted internal network (LAN) & un-trusted external network (Internet).**
- DMZ is isolated **using security gateway** (i.e., firewall) to filter traffic between DMZ & private network.
- DMZ itself **has security gateway in front** to filter incoming traffic
- DMZ contains devices accessible to Internet traffic, such as Web, FTP, SMTP & DNS servers
- **Goal of DMZ = allow access to resources** from untrusted networks while keeping **private network** secured
- **DMZ server** = resides in DMZ & used to externalize resources to public network

Firewall

- Firewall = **software or hardware device** - examines data from several networks & either permits it or blocks it to communicate with user network
- Governed by predefined security guidelines. Defends from internal & external threats
- Supervises flow of traffic between distinctive parts of network.
- Firewall always exists between private network & Internet - filters packets coming in & out.
- **Next Generation Firewall (NGFW)** =seamless & centrally managed control of network traffic - physical, virtual or cloud.

2FA

- Two-factor authentication (2FA) = security system requires **2 separate, distinct** forms of identification in order to access.
- F1: password
- F2 : text with a code sent to smartphone, or
- biometrics using fingerprint, face, or retina.
- 2FA improves security, but not foolproof

2 FA

- Google account settings & enable 2FA feature.
- Google Authenticator app to ensure no one else can access account without permission.

WEF's view

- *Cyberattacks are one of the top 10 global risks of highest concern in the next decade, with an estimated price tag of USD90 trillion if cybersecurity efforts do not keep pace with technological change.*
- *- World Economic Forum*

Cyber Security –Survey

- 4.1 billion estimated records breached in H1 of 2020
- 34% of reported cybersecurity breaches involved internal actors
- Every 14 seconds, a ransomware attack carried out on businesses in 2020
- 71% of reported breaches = financially motivated

Key cyber trends- 2019-20

- **1. Airtel - Data: Names, date of birth,**
- emails, residential addresses and IMEI number
- Quantum: More than 300 million users
- Cause: Unprotected application programme interface (API)
- **2. NPCIL**
- Data: Administrative function of power plant
- Quantum: One power plant
- Cause: Undetected malware in system
- **3. Banks :**
- Data: Customers' debit and credit card information
- Quantum: More than 1.3 million credit/debit cards
- Cause: Unprotected database

Impersonation on Social media

- Government mandated that top companies -Twitter, Facebook, Instagram & YouTube have to remove accounts with fake profile pictures of known personalities & businesses, & general subscriber, **within 24 hours** of being notified of same by user or someone on his/her behalf.
- **IT ministry's diktat** : grievance redressal mechanism prescribed for social media platforms,
- *Makes it contingent on firms to remove any content around obscenity, Vulgar act or conduct within 24 hours after receiving complaint*

Fraud incident

- Media reports – 2000 affected in Mumbai with fake vax
- Deb : free mask & sanitizer distributed, Yaas relief - to gain popularity
- KP: 250 people received 'shot' at fake Kasba centre - 6 days.
- Investigations : Deb organised fake camps - Kolkata, City College, CHS
- Fraudulent documents : KP seized fake ID cards, vax labels;
- 1. IAS officer posted with Ministry of Information & Culture
- 2. Joint Municipal Commissioner of KMC.
- His car fitted = beacon & sported KMC stickers.
- Risk : Adhar card copies of recipients retained, PII stored by fraudster
- Aadhar fraud call: One Victim's bank account targeted – Phishing : UID linking with mobile no
- Demand for CBI enquiry , scan on other vax camps
- KP : Fraudster's office raided & laptops / IT equipment , documents seized
- Cyber forensic Auditor – steps in such environment

Digital Forensics- Audit steps

- **Digital Forensic** = *“Process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law).”*
- **Digital Evidence** = any information, data of probative value stored in binary form, transmitted , received by an electronic devices.

Evidence Collection –

1. Consult with investigator to determine **details of case & potential evidence to be collected.**
2. Determine **necessary equipment** to take to the crime scene.
3. **Review legal authority to collect evidence**, restrictions are noted
4. When evidence from scene cannot be removed, it **should be copied or imaged on-site.**
5. All individuals not involved in collection process **should be removed** from proximity of digital evidence.
6. Individuals with relevant information (e.g., user names, passwords, OS & network credentials) **should be identified & interviewed.**
7. Crime scene **should be searched systematically.**

Safety Advisories , Best practices (Guidance)

- **Forensic & Cyber / IS Auditors** - engaged in public practice or employed by insurance companies, banks, police forces, EOW, ACB, government agencies etc
- **Minimum Safety SOP** =external threats / risks

Personal Hazards, safety & protection issues : Cyber Auditor

- Risk of personal / physical threat to forensic auditor/ team
- Report of forensic auditor = presentation as evidence.
- Investigation = lead to legal (criminal) proceedings against suspect,
- Members of Forensic audit team = involved in resultant court case.
- Forensic audit team members = called to court to describe evidence & explain how suspect was identified.
- If chargesheet filed against accused found valid, penal consequences on accused , hence substantial chance that suspect /accused may try and prevent the forensic auditor from achieving his intended audit result.
- Attempts to prevent forensic auditor such that he is unable to expose illegal or unethical acts of suspect before Court of law.
- Forensic audit evidences may also be tampered or damaged.
- Forensic auditor face direct personal threats endangering his safety & security. = personal safety risk to forensic auditor.



भारत सरकार Government of India
रेल मंत्रालय Ministry of Railways
(रेलवे बोर्ड) (Railway Board)

Office Order No. 10 of 2021

National Cyber Security Strategy

The current pandemic has introduced a greater reliance on electronic modes of communication in official working. It is, therefore, necessary that all officials take responsibility and follow adequate procedures when using Information Technology (IT) infrastructure for ensuring confidentiality, privacy, etc. in dealing with official information. This can be achieved to a great extent by following internet ethics, cyber hygiene and following best practices on use of IT equipment viz., Desktops, Laptops, Mobile devices, etc. While many Officials are aware of these and other related practices, there are still a number of officials who are unaware of the same.

A number of incidents have come to notice regarding breaches in various IT applications of IR. These incidents have seen a spike in recent times as electronic working gets further proliferated. While a majority of these are application related, there are also incidents which have occurred due to improper handling of the IT assets by the personnel in general.

2. It has been observed that, in recent times, an alarming increase has been seen in the number of breaches/attempted breaches to ICT infrastructure of Govt Organisations. The Government of India, at the highest level, is also seized of the need for adequately and appropriately securing the ICT infrastructure. In keeping with this need, the Government has been working on the subject strategy.

3. Now, Hon'ble Prime Minister has given the following directions for action by all Ministries:

“Every Ministry has some personnel with technical aptitudes. These are to be identified and trained in Cyber Security Courses within six months. These should then form the cyber security nucleus of that Ministry.”

Therefore, in order to create awareness and educate the employees, the Government of India, at the highest level, has decided that all Officers and Staff may be imparted a generic training in Cyber Security. Accordingly, C-DAC, an organization under the Ministry of Electronics & Information Technology, GoI, has been tasked with providing these trainings. Each training session will last 4 hours and the calendar for the same will be advised by C-DAC to the registered attendees.


All Unit Heads are advised to encourage the Officers and Staff working under their control to enroll and attend these training sessions. **On successful completion, the participation certificates may be placed in their respective service records.**

All Officers and Staff are requested to avail of this opportunity for enhancing Cyber Security Awareness.

This issues with the approval of Chairman & CEO, Railway Board.

No. A-20003/2/2020-RBCC

Dated : 16.02.2021


16.2.2021
(Rajnesh Singh)
Director ME (C&IS)

National Cyber Security Strategy 2020-

Data Security Council of India

- India is **second-fastest digital adapter among 17 of most-digital economies globally**, rapid digitisation require forward-looking measures to boost cybersecurity.
- **National Cyber Security Strategy 2020** is being formulated by the Office of National Cyber Security Coordinator at the **National Security Council Secretariat**.
- **Cyber Security** is *protecting cyber space including critical information infrastructure from attack, damage, misuse and economic espionage*.
- The **National Security Council (NSC)** of India is a 3-tiered organization that **oversees political, economic, energy & security issues of strategic concern**.

National Cyber Security Strategy 2020:

Aim: To improve cyber awareness and cybersecurity through stringent audits.

- ✓ Empanelled cyber auditors – Review security features
- ✓ **table-top cyber crisis management exercises** regularly to reinforce the idea that cyber attacks can take place regularly.
- ✓ **Index of cyber preparedness**, & monitoring of performance.
- ✓ **Separate budget for cybersecurity** suggested, + synergise role & functions of various agencies with domain knowledge.
- ✓ **Most developed cyber warfare capabilities = United States, China, Russia, Israel & United Kingdom.**

- **Increased Digital usage Post-Covid:**
Critical infrastructure = digitised—
**financial services, banks, power,
manufacturing, nuclear power plants,**
- **For Protecting Critical Sectors:**
- Increasing interconnectedness of
sectors & proliferation of entry points
into internet, further grow **with adoption
of 5G.**
- **6.97 lakh** cyber security incidents
= first 8 months of 2020,

CYBER SECURITY HIERARCHY IN INDIA (1/2)					
PM OFFICE/CAB INET SECY (PMO/CAB SEC)	MINISTRY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Security COuncil (NSC)	National Cyber Corrd Centre (NCCC)	Ambassadors & Ministers	Tri Service Cyber Commad	Department Of Information Technology (DIT)	Cyber Security And Anti Hacking Organisation (CSAHO)
National Technical Research Org (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecom (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre (NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (NI)	Indian Computer Emergency Response Team CERT- IN	Centre of Excellence for Cyber Security Research & Development in India (CECSRDI)
Joint Intelligence	Central Forensic Science Lab (CFSLS)		Air Force (AFI)	Educational Research Network (ERNET)	Cyber Security of India (CSI)

PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTRY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research & Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center			Defence Research Dev Authority (DRDO)	Standardisati on, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

HDFC Bank case update - June 24,2021

- HDFC Bank MD & CEO Sashidhar Jagdishan apologised for **technical glitches - resulted in RBI freezing issue of new credit cards** & putting on hold **its digital strategy**.
- AR 2020-21 : CEO promised action to ensure that HDFC bank keeps –
- Culture, Conscience & Customers at forefront

Background of RBI action

- **December 2020** : RBI banned HDFC Bank from new digital launches, + issuing new credit cards & proceeding with Digital 2.0 plan
- **Reason**: series of technical glitches reported over last 2 years.
- **Prime reason**: lack of capability in Bank data centre
- RBI initiated 3rd party audit of HDFC bank's IT systems.
- HDFC Bank - 56 million customers = individuals, SME & corporate entities.
- *“This audit is now over and the report has been submitted to the regulator. We now await the decision from the RBI,”*
- - CEO

HDFC Bank IS Control initiatives

- Strengthened **disaster recovery resiliency**,
- build a "**digital bank** within bank
- To scale up infrastructure to **handle potential load** for next 3/5 years.
- In process of **accelerating cloud strategy** to be on cutting edge leveraging best-in-class cloud service providers
- Intensified **security enhancements** over IT systems
- **Strengthened firewalls**
- CEO said :
- *“We have strengthened our process of monitoring our Data Centre (DC) and have shifted key applications to a new DC. This includes key consumer facing ones. We have strengthened the Disaster Recovery trials and processes so as to bounce back to serve our customers faster and quicker,”*

HDFC Bank

- Business continuity in pandemic times
- Technology Interventions
- Employee safety and Productivity
- Maintain operational stability



Maintain operational stability

1. DR site at Kanjurmarg used as contingency site to ensure continuity of critical Treasury Department
2. Enhanced internal communication mechanism further;
3. Set up a crisis group on mobile platform for faster communication, action and response
4. BCP Strategy for Retail Branch Banking further being enhanced with plans to include a :
 - ✓ Comprehensive BCP Manual,
 - ✓ Table Top on BCP,
 - ✓ Periodic Preventive Checks,
 - ✓ BCP during Branch downtime,
 - ✓ E-Learning Module for Branch Banking

VPN deployment

- HDFC Bank procured sufficient additional licenses for VPN & has segregated those basis priorities
 - – Priority 1. Branches facing frequent complaints/isolation
 - – Priority 2. Single branch cities
 - – Priority 3. Vulnerable geographies
- **Status** : Process is being defined with help of IT. Pilot run has been completed.

Directors Report 2021

- *Business Continuity Planning (BCP)*
- *Your Bank has an ISO 22301 certified Business Continuity Plan (BCP) in place to minimise service disruptions and potential impact on its business, employees and customers during any unforeseen adverse event or circumstances. The central Business Continuity Office works towards strengthening the continuity preparedness. The plan is designed in accordance with regulatory guidelines & reviewed regularly.*
- *The implementation is overseen by the Information Security Group and the Business Continuity Steering Committee which is chaired by the Chief Risk Officer (CRO).*
- *The Business Continuity Policy and Procedure defines roles for Crisis Management, Business Recovery, Emergency Response and IT Disaster Recovery Planning teams*
- *Ensuring Business Continuity during COVID 19*
- *Team HDFC Bank rose to the challenge of delivering banking services during the outbreak of the COVID-19 pandemic. Your Bank emerged successfully from the nationwide lockdown and adopted a hybrid approach of working from home, nearby location as well as base location in accordance with pandemic protocols that have been periodically released by the Government.*

Thank you