Five Major Challenges faced by PM Modi to create Cashless Digital Transaction environment

By Dr Rakesh Goyal

08 December 2016

Prime Minister Narendra Modi has demonetised Rs. 500 and Rs. 1000 notes, exactly a month back. There is a shortage of new replacement currency notes of both Rs. 2000 and Rs. 500 denominations. There can be two hypotheses for this shortage.

First hypothesis for this shortage can due to (a) genuine shortage of new currency notes whereas second hypothesis can be (b) a deliberate attempt by government to keep supply of new notes tights for various reasons.

If it is deliberate attempt to keep the tight supply of new notes, the reasons may be attributed to either (a) to curb illegal conversion of old currency to new currency by various interests such as black money holders, corrupt bureaucracy, industrialists or politicians or terrorist or naxalites; OR (b) denying disruptive forces to pump counterfeit currency in Indian economy; OR (c) forcing people to go for cashless digital transactions (CDT); OR (d) a any partial/full mix of all these three.

On the onset, let me state that I am ardent supporter of PM Modi for his various measures to undertake basic structural changes in Indian economy, society and culture. Some of these measures include demonetisation, IDS, Jandhan, DBTL, give-up subsidy, e-auctions, Swacch Bharat, etc. But the purpose of this article is not to be a blind bhakt of PM Modi but to analyze various issues and challenges, which PM Modi may face in implementing his dream and desired structural changes.

The current focus of this article is only on forcing people to go for CDT. I fully support CDT as it brings transparency in all dealings from individual transactions to commercial transactions to government payments, payment of wages/salaries in unorganized sector, tax collection, tax deployment, etc. If we become even 86%

(size of cash economy catered by official demonetised currency) cashless, my belief is that it will curb 90%+ corruption, black money and 100% of counterfeit currency.

Implementing CDT is not easy. It has many challenges including and not limited to technology, vested interests, resistance to change, education/awareness, risk, cost and legal. In these challenges by vested interests and resistance to change are mostly political, whereas others are technical and logistical. I will discuss here these technical and logistical challenges.

There are five major technical and logistical challenges to implement cashless digital transactions (CDT) in the existing technological, cultural and economic environment. These are –

1. Logistics and infrastructure
2. Cost to users
3. Cyber Security
4. User awareness and ease-of-use
5. Legal issues

Let us discuss these one by one

1. **Logistics and infrastructure**

   Let us consider that all economic adult (age 15+ years) population of current 130 crore Indians will be using CDT in due course. As per 2011 census, population age-group-wise 15-64 and 65+ years is 69.8% (say 70%) of total population. That means approx 91 crore (0.91 billion) Indians will be using CDT. Even if all this mass of people may not use CDT to start with, but the infrastructure need to be planned for all these people scalable to same demographic population after 10 years. Let us derive the dimension of required infrastructure and logistical support system.

   Assumption – Let us assume that a person does 5 CDT per day on an average. That means there will be 910 crore transactions per day considering each debit transaction will have one corresponding credit transaction also. Even if 20% of population is covered in CDT, even then this load will be approx 180 or say 200 crore transactions per day. This load cannot be evenly distributed over the day (24 hours). It may follow some pattern, most probably similar to bell curve. There will be peak and lean period in a day. Nights should be lean period, where as some periods in day will have peak. Average load for 24 hours will be about 7-8 crore transactions per hour or 12 lakh transactions per minute or 20 thousands transactions per second. Peak load may be estimated as 50-60 thousands transactions per second from all over India considering only 20% population. Further, I have assumed 5 CDT per person per day. My wife and some of my friends say it will be minimum 15-20 CDT per day. In that case, the peak load will be 2 lakhs transactions per second. But, this needs some sample survey in all demographies distributed all over India. For 100% population with 15-20 CDT per day, the peak load may be 1 million transactions per second. Even the lower peak load of 50-60 thousands transactions per second is quite huge for any IT infrastructure and it needs lot of logistical and management support.

Current state of CDT infrastructure -

CDT means following type of transaction, based on current set of technology and business processes, will replace cash based transactions –

a. Credit / Debit / ATM / Payment / Cash / Similar Cards (cards such as RuPay, Visa, Master, Bank's debit or ATM cards)
b. Internet Banking offered by various banks along with services like NEFT/RTGS/SWIFT. Most big banks are offering internet banking.
c. Mobile payment applications (app) and platforms by some private players (such as PayTM, PayU, JioMoney, Oxigen, freecharge, etc.) with their own back-end infrastructure.
d. Mobile payment platforms offered by banks (Buddy by SBI, Pockets by ICICI, Payzapp by HDFC Bank, etc.)
e. UPI and NUUP (USSD based) offered by NPCIL with front-end by many banks and back-end by NPCIL.
f. Payment gateways by banks for web-portals and used by portals such as IRCTC.

Current back-end infrastructure is either of service provider bank or NPCIL or private mobile app provider. Connectivity is provided by TeleCom operators like MTNL, BSNL, Tata, Vodafone, Idea, Airtel, etc.

Requirement to cater to 50-60 thousands to 1 million transactions per second from all over India -

Let us consider the same set of front-end applications provided by existing set of service providers will continue and may be some new will also join the band-wagon after seeing the enormous potential.

Apart from these above front-end applications and interface, back-end infrastructure requirements will be as below –

a. Integrated single or distributed data acquisition, storage and processing facility / facilities (let me use the word Data Center or DC).
b. If distributed facilities, fail-safe high bandwidth connectivity amongst these facilities.
c. These DC will further have high bandwidth connectivity with various Banks, FIs and other financial intermediataries as defined by RBI or any other regulator.
d. Guaranteed end-to-end connectivity between DC or Bank and end-user as designed in infrastructure architecture. This may be provided by one player or many players. For example BSNL/MTNL/Tata provides connectivity to DC, where as various TeleCom players provide to end-users, including payer and payee. But the connectivity between DC to end-user must be seamless.
e. Interoperability amongst various front-end CDT players.

Current problems -

Interoperability amongst various front-end players except NEFT/RTGS is does not exist. If one person has PayTM and other has freecharge or any other front-end app, they cannot transect payment between them. There is no standard defined for interoperability. Each player has its own standards or non-standards or method of deployment, which is mostly incompatible with rest of other players. Further, most of their infrastructure is planned for low volumes and based on legacy systems, which has evolved organically. For example, 2 banks are using Finacle CBS, compatibility is very limited.

Back-end DC infrastructure to support desired load of CDT has a big capacity gap. Each Bank or operator has its own back-end infrastructure, which is designed to take limited amount of transaction load. There is no backend DC infrastructure, single or distributed, which can take the load of CDT, even if 20% of adult Indian population goes fully cashless.

It will be nightmare for citizens to wait for completion of transaction, especially when CDT is compared with immediate completion of cash based transaction, with no time lost and no wait for connectivity and/or speed. For CDT, backend infrastructure and last mile connectivity both are heavily inadequate. If the existing infrastructure is put to stress test, velocity test, spike test, soak test and endurance test of defined load of CDT, where 20% of “all monetary transactions in India” are CDT, most of infrastructure will fail miserably. Some may even die-down under the stress.

Further, internet connectivity is another big challenge as of now. All devices (mobile phone or any other specific devices) will be connected for CDT through internet data lines, either using mobile data packs or wifi. I have two different internet connections and cannot rely 100% on either of these. The availability of either is never over 90%. There are times, when both are not available simultaneously. The speed is always questionable. In Mobile data, operators talk about 4G, even real 3G speed is a myth. Many times, in 4G, we get a speed less than 2G. Connectivity outage is rampart. While doing internet transaction, many times, getting OTP (one time password) on mobile via SMS as 2FA (2 factor authentication) takes literally few minutes in a city like Mumbai, where I have clearly visible mobile towers just 50 meters across the road. At least minimum 25% times, I need to ask to resend OTP, as it expires in 120 seconds.

This is current scenario, when the penetration of CDT is very limited and may be just less than 2% (my wild guess which may includes net-banking, IRCTC, all card transactions, eWallets, NEFT/RTGS, etc.) of all transactions by volume. Just for clarification, in CDT the value of transaction has no bearing on load on infrastructure. A transaction, whether it is valued for Re 1 or Rs. 100 crores put same load on the infrastructure.

Another characteristic is that there are heterogeneous types of mobile phones and operating systems. Citizens use featured (smart) phones and basic phones. Out of claimed approx 100 crore phone connections, smart phone are estimate is about 25% and rest as basic functional phone, which just have facilities of talking and SMS without internet connectivity. In smart phones also the operating system may be android or iOS or windows or blackberry or some other. The challenge will be to cater to all this heterogeneous jig-saw puzzle blocks in seamless manner so that a basic phone can transact business with so-called smartest phone seamlessly in defined quality parameters.

Thus, the first challenge for PM Modi will be to create and ensure robust and reliable back-end IT infrastructure, WAN connectivity and last mile connectivity with defined and measurable quality parameters. The quality parameter of the whole infrastructure setup must be a reliable transaction within a specified time of say 2 seconds when the peak load will be from 50-60 thousand to 1 million transactions per second.

2. Cost to users

Another critical factor is cost of transaction to users. We Indians are quite sensitive to price elasticity. We always believe in saving cost, sometimes even at the cost of quality.

Let us compare cost of CDT with cost of existing cash transaction.

Cost of cash transactions

Cash transaction has three players. First player is payer, second is payee and third is currency note. Currency note can be considered as representative of RBI (which issues and guarantees), which again represents Indian government. Thus the third player is government (frontend by RBI), which issues the real rupee (one rupee).

In any cash transaction, the cost of transaction to both payee and payer is NIL. The transaction cost is incurred by government (frontend by RBI). RBI prints currency; stores currency in currency chests; moves it to banks; collects back, stores, destroys mutilated/returned/demonetised currency. Cost is borne by RBI for all these activities. This cost includes direct cost, indirect cost and overheads for all these activities. I am not considering opportunity cost because cash has been a mandatory activity for our economy. Now, in CDT environment, cash transaction cost will be reduced so opportunity cost of part of the total cost may be considered but let us ignore it for this paper.

To understand it easily, let us assume that all these cost for one currency note is Rs. 10 and the currency note life is 100 transactions. Then, the cost per transaction per note becomes 10 paise, which is incurred by RBI or the government. A person buys goods/services worth Rs. 20 and gives a note of Rs. 100 to shopkeeper and shopkeeper returns back 8 notes of Rs. 10. There is an exchange of 9 notes in the deal. Thus the cost of transaction becomes 90 paise, borne by RBI. This cost is not real but illustrative. It will be different, based on real data. But there will be a cost. For coins, the cost will be different based on their higher cost of minting and also much higher life.

Cost in CDT environment

In CDT, there is paradigm change upside down. Currently, the cost to government is nil. The cost to payer may be smaller but not nil. Major cost is incurred by payee. All cards payments, mobile app payments, UPI charges payee. Sometimes, payee transfers this cost to payer directly or indirectly. This cost varies from 0.5% to 3% of transaction value. Payer will also be paying for internet/mobile data and/or SMS, as applicable. Thus, both payer and payee pay the cost of CDT. We cannot calculate this cost per transaction in a simple manner as cost of cash transaction can be calculated. This cost will be based on value of transaction and not number of notes exchanged.

It can be considered as a monetary penalty to payer and payee for using CDT compared to cash transaction.

There will be resistance from many payees and even from payers that why should they incur this cost, especially when cost in cash transaction is nil to them and there is no delay.

An average pre-paid Indian mobile user is so much cost conscious that after every call, s/he verifies the balance available. Missed call is an Indian jugaad to save cost with number of rings in missed call is the code for some action.

Thus, the second challenge for the PM Modi will be – who will incur the transaction cost in CDT environment. He needs to invent ways to incentivize the CDT and not penalize the payee and/or payer. If RBI / government save a lot of money in CDT, PM must use this saved money to create reliable, robust and secure infrastructure, connectivity and last mile and let payee and payee incur no cost as in cash transaction. Else, the resistance may continue.

3. **Cyber Security** –

Cyber Security is another serious challenge and concern, which can make or break CDT mission. Current service providers including banks, payment companies, etc. do not guarantee cyber security to either cashless digital payer or payee.

Cyber security can be defined as achieving minimum baseline of basic security criteria including (a) assuring "Confidentiality" of all data; (b) maintaining "Integrity" of all data and infrastructure; (c) assuring "Availability" of services in desired quality parameters; (d) assuring protection of "Privacy"; (e) "Non-repudiation" of person and/or transaction; (f) maintaining "Incident response" with defined service level parameters and; (h) availability of "Customer protection functionalities" in end-to-end IT infrastructure.

Barring a few exceptions (just to save me of prejudice), almost all IT infrastructure of all transaction service providers will fail on more than one of the basic cyber security (apart from transaction load) criteria like Confidentiality, Integrity, Availability, Privacy, Non-repudiation, Incident response and Customer protection functionalities for CDT requirements.

We read regularly cases of data theft, hacking, loss of money, software malfunction, hardware malfunction, data center outage, denial of service, delays, etc. The list is long. Few years back a big Indian bank was offline for 50 hours during week-days. Most of the times, all these are conveniently covered under the wrap as technical glitch (as happened with Jet Airways few days back).

Internet banking applications are not tested for many customer oriented risks and vulnerabilities such as and not limited to man-in-the-middle attack, malware, business intelligence, information leakage, etc. In some cases, it is observed that even very basic requirement are missing, for example SSL/TLS is not used; password storage in browser not blocked; auto-complete is enabled; cookie is not secured; security patches are not applied; to name a few from a long list. Having security vulnerabilities such as SQL-Injection, Cross Site Scripting, CSRF, unsafe transport layer, session hijacking, etc. is another major concern. These vulnerabilities are hacker’s gateway to compromise the user demographic, logon and transaction data. Any compromise violates the basic cyber security criteria like confidentiality, integrity, privacy, etc. and exposes the citizen to risk of various losses including and not limited to financial, regulatory, credibility, image, identity hijack, etc. Very limited web-portals are rigourously tested for cyber security vulnerabilities.

Similarly, in mobile apps, very few apps are rigorously tested for cyber security. Examples exist that the app is made available without even complete functionalities and security testing. Hack of NaMo app, which is basic and simple app, for online voting on demonetizing demonstrate the level of cyber security posture in unsecure apps and lack of cyber security awareness in developers/ programmers. In at least one of the currently available and fairly used mobile payment apps, the session do not end after a transaction or after specified time, thus risk of user session hijacking exist.

Further, in featured (smart) Mobile phone environment, installing any app will ask you almost all permission such as (a) take pictures and record videos; (b) read, add and modify contacts; (c) Approx and precise location; (d) record audio; (e) read phone status and identity; (f) directly call phone numbers; (g) read, receive, send, view your SMS and MMS; (h) read, modify or delete contents on your SD card; (i) full network access; (j) activity recognition; (k) control vibration; (l) run at startup; (m) view network connections; (n) control NFC; (o) install shortcuts; (p) receive data from internet; (q) read google service configuration; (r) prevent phone from sleeping; (s) measure app storage space; (t) change audio/video settings; (u) pair with blue tooth devices; (v) view and connect wifi connections; (w) change network connectivity; (x) send sticky broadcast. Most of the app asks either for all these permissions or most of these permissions. The user, without reading and understanding, permits all permissions. S/he has the option either install app with permissions or forget it.

I have downloaded a Hanuman Chalisa app. It asked for over 10 permissions including reading SMS, making phone calls, video/audio recording. Ideally, only permission was required for this. i.e. playing audio. So, you decide whether it a strategy to steal my information in return of providing some desired service?

Now, in some operating systems, the user has an option to deny certain permissions. But, very few citizens are aware of it and even after that there is no guarantee that the app is not be reading the data even after permission is off.

Further, many apps also read data, which is not in permission list. This data includes and not limited to (a) reading data from buffer/cache/RAM; (b) specially read authentication (user-id and password) data; (c) sending data to defined IP address/server; etc. There is no check or control or regulation over this tendency.

Given all above permissions and read of data, in mobile phone, especially smart phones, the citizen data is totally naked. The data used by payment app, including authentication (user name and password etc) is totally exposed to many other apps, which are loaded on mobile and reading everything with permission and even without permission.

This has absolute potential for stealing citizen credentials and misusing by criminals.

Phishing and vishing attack are another area of great concern in both mobile and PC environment.

In Credit/Debit/ATM cards, the risk of card cloning and skimming exists in POS terminals and ATMs. I know few e-commerce sites, which have glaring security vulnerabilities and it is 100% guaranteed in these sites that your data will be exposed to some hacker (this word loosely used).

Pushing CDT forcibly without rigorously tested and properly certified apps along with reliable and cyber secure infrastructure is exposing the citizen, without any shield, before the demon called cyber criminal. Lot of cyber crimes are expected to happen. For a common man, even a loss of Rs. 100 will be big. Citizens will lose faith in CDT and PM Modi.

Thus, the third challenge for PM Modi will be to make sure that cyber security parameters - confidentiality, integrity, availability, privacy, non-repudiation, incident response and customer protection functionalities are guaranteed. The infrastructure and apps are rigorously tested and properly certified and de-risked before asking the citizen to use.

4. **User awareness and ease-of-use** –

   Assume that robust and secure infrastructure exist; reliable connectivity exist; costing is not an issue and cyber security is assured, if the citizen do not know the usage, the mission will fail.

   Any user need to know following –

   a. Why s/he need an application (app) or a service?
   b. What the app or service is suppose to do?

c. Is there any better and/or cost-effective solution exist?
d. How to load or install the app (includes web, mobile, card, ATM, etc)?
e. How to use the app?
f. Does app has an user-friendly user manual in my language?
g. What all facilities are available and what are limitations?
h. What care and precautions to take?
i. Dos and Don’ts / FAQs
j. How to protect him/her from attacks from hackers, phishing/vishing agents, call center frauds, money mule and other frauds?
k. In case of operational problem, where to report and how to get these resolve? This must be a single point contact, hearing patiently in his/her own language.
l. In case of legal and/or fraud, what to do and whom to contact?
m. What are his/her duties, rights, liabilities?
n. How his/her money is safe and/or secured and/or protected?

The current status is that the user awareness or education is extremely low up to the extent that it is almost nil or non-existent. With my limited sample size, I have seen that even most of the operational bankers in branches have limited or no awareness or education about cashless digital banking/ transaction, i.e. internet banking or mobile app. Branch Manager refer the problem to IT or some other department to resolve some basic issues in internet banking.

Another aspect of user awareness is language. Almost all instructions and data to fill, are in English, which is used by a miniscule minority. Further, given the standard of education, many graduates cannot understand the “instruction of install” or FAQ, provided on websites of banks. The user instructions and awareness material must be in local language harnessing different print/audio/video/multimedia/animation modes and channels. User must get clear educational data either written and/or visible and/or audible examples or instructions and guidance, just by pressing a predefined button/key (similar to F1) at every step, while using the app.

PM Modi is banking on the fact that there are more mobile phones in India than Indian adult population. But most of these mobile phones are non-smart category; while in smart-phone category, the phones are used for low hanging applications such as whatsapp, facebook, youtube, with almost all permissions, apart from talking and SMS. Installing and using in secure manner, a CDT app needs some higher consciousness level of education and awareness.

Further, it is widely seen that any general purpose application like Windows or Linux is mostly installed by hardware engineers or are self installed, where default settings are on, which are dangerous for cyber security. They do not customize the installation to suit the need of the person and security. The same will be repeated in CDT apps, if user himself is not properly educated and that will be big risk for security of data and money.

In case of UPI apps, most of these offered by banks are non standard and often user-hostile to install. Coupled with slow or broken data lines and slow response, even the informed user, who has spent at least 30 minutes to read the instructions, also gives up. Further, the configuration and security features are not defined clearly. High risk exist that the current versions of apps are offered in haste, may be due to pressure from PMO or RBI or other such body. This puts off the user. As and when few users will have problems, the bad reputation spreads like wild fire.

Thus, the fourth challenge before PM Modi is to create simple, user-friendly, standardize educational material. He needs to create mechanism to educate the users in installing, configuring and using in user-friendly manner.

5. **Legal issues** -

Legal issues in CDT are another critical challenge to avoid future problems.

Over a period of 210 years of modern banking, many laws, acts, rules, guidelines, practices are created, streamlined and followed. There are over 80 laws, acts, rules, guidelines for banks to follow. Some examples of these laws, acts, rules, etc. are Banking Regulation Act, Negotiable Instruments Act, Bankers Book Evidence Act, Indian Evidence Act, SARSAESI Act, FEMA, etc. apart from other specific acts like RBI Act, SBI Act, SIDBI Act, etc. Then there are other well established controls such as maker-checker control, physical control, Security items (accountable documents), etc.

Many of these laws, rules, and guidelines were framed when there was no concept of CDT. These laws cannot handle digital transactions, even in cash based environment. For operating in digital environment, the nearest law is Information Technology Act-2000, amended in 2008 (say IT Act-2000).

Let us take an example. As per Banking Regulation Act and other related acts, any financial transaction or instrument is valid only if it is physically signed in ink on paper. Further, as per section 3, 4 and 5 of IT Act-2000, any digital transaction is considered equivalent to paper based signed transaction, only if it is digitally signed using “Digital Signature” issued by licensed Certifying Authority (CA), licensed by Controller of Certifying Authorities (CCA). Apart from these, any other transaction is legally illegal. Thus, theoretically and technically, all internet banking transactions and payments done using mobile, which are not digitally signed using “Digital Signature” issued by licensed CA are illegal. This may create legal issues at some point of time in future.

Further, in case of crime / fraud, creating and collecting evidence in digital environment is radically different compared to paper based or physical environment. In physical environment, the evidences are generated and available on paper. Thus hard copy evidence exists. Creation of chain of custody is easy. Laws support this. Forensic analysis of paper based evidence is an established science. In digital environment, many times, logs are unavailable or deleted or corrupted or tampered; the storage is corrupted or deleted or tampered; evidences are scattered over different places/jurisdictions, in some cases even in other countries; law to define and accept digital evidences does not exist. These and similar issues need to be addressed before courts will be further loaded with CDT related cases over and above 3 crore cases, already pending in various layers of Indian courts.

Another legal issue that will come in cash environment that transactions are done by minors also and they are considered valid. Will transactions done in CDT environment by minors be legally binding and valid? As per banking law and practices, minor can have a bank account only under the guardianship of a major, mostly either of the parents. What will be the status of transaction by a minor in CDT environment using that account?

Another important legal issue is of protection of citizen in case s/he is victim of cyber crime in CDT. Currently there is no protection to citizen, in case of cyber fraud, where the citizen is pure victim and not responsible for the crime. As per IT Act-2000, all cyber crimes / frauds are to be adjudicated by Cyber adjudication officer, who is mostly Secretary/Principal Secretary of IT department of the respective state. Currently, most of the Cyber adjudication officers are non-functional. The appeal is to be filed with Cyber Appellate Tribunal, located at Delhi. Cyber Appellate Tribunal is non-functional for last 5 years. Both these remedies are created under IT Act-2000/2008, which is an act of parliament. Civil / Criminal courts has no jurisdiction in cases related to cyber frauds. What is the recourse open to cyber crime victim citizen?

Further, there exists no cyber liability insurance in India. For banks, RBI has published draft “limited liability circular” on 11 August 2016, asking for comments by 31 August 2016. Even after 3 months, this notification is still pending and citizens are not even partly protected. It is speculated that this may be due to lobbying by banks.

Thus, the citizen is totally unprotected and no working forum to get his/her grievances redressed.

There may be more legal issued, which needs brain storming and PM Modi need to find workable solutions to those legal issues.

Thus, the fifth challenge before PM Modi is to create and review the existing legal framework to address the above and other legal issues related to CDT. He need to change/amend/create laws aligned to technology and business requirements. Further he has to ensure that in case of cyber fraud, the citizen is (a) protected and (b) gets fast and immediate remedy/justice, for which the basic legal framework is available but not implemented.

What to do now –

I do not want to finish this paper with problems and challenges. This issue needs lot of brain storming. There can be many stand-alone and/or combined cost-effective and appropriate solutions. Even then, I would like to make few suggestions, which are neither exhaustive nor fit-all type. These further need more deliberations and debate –

Administrative measures -

1. Government should consider making mandatory all B2B, B2C, B2G, G2B and G2C payment transaction using CDT. B2C transactions for small petty expenses below Rs. 100 can be allowed using cash with a certain limit of either daily expenses or turnover. (B=Business, G=Govt and C=Citizen)

2. Government should make mandatory or at least encourage with incentive, all C2B and C2G over Rs. 5000 using CDT. This limit may gradually be reduced to 2000 in 6 months and 1000 in 1 year, as maturity level and infrastructure increases.

3. Similarly, even C2C can be considered. Transactions under Rs. 100 with small vendors (Chai wala, vegetable wala, etc) can be considered as C2C.

4. These amounts and time limits are not sacrosanct and can be debated and modified.

Infrastructure and logistics -

5. Government must either create or facilitate a robust and secure backend infrastructure, which will take peak load, considering 80% of adult population goes for CDT. This can be government's own or under PPP model or assigned to some experienced Indian organisation with proven track record. It must be ensured that no alien entity will have access to this infrastructure as it contains one of the most super critical national assets. This must not fall into bureaucratic red tape else failure is guaranteed.

6. TeleCom operators must guarantee WAN and last mile connectivity availability and speed, with penalty clause.

7. Web applications and Mobile app must be simple, user-friendly and secure with robust testing and certification. In case of failure, the certification agency must be answerable. They must follow standard front-end and have back-end standards.

8. In case of more than one service providers, interoperability must be ensured with no cost to user.

9. Government must work on single UPI/USSD app, which must be used by all banks connecting to their backend using API. This UPI service must be free and compatible with smart phone as well with ordinary phones. This must be available on various operating systems. This must be thoroughly tested and certified for functionalities and security. The government must guarantee protection of personal, access and transaction data.

10. Government must ensure service level quality parameters such as completion of transaction in 2 seconds.

Cost of transaction -

11. Cost of CDT transaction to payee and payer must be NIL.

12. Government must incentivize CDT against current penalize model for payer and payee. It may consider subsidizing all CDT against saving accrued to RBI by reduction in cash transactions and thus currency cost.

13. Government must incentivize and promote CDT in rural areas through gram panchayats, zila panchayats, etc. There must be some visible benefit to village, if they go CDT.

14. There can be fiscal and tax incentives for citizens. For example rebate u/s 80 on some percentage of total digital transactions or percentage of digital transactions in a year. Rebate in indirect taxes may be considered.

Cyber Security –

15. It must be ensured that the whole end-to-end CDT IT eco-system is secure on basic and advanced security parameters. There must be on-going audits and assurance to citizens that their operations, money and data are safe and secure.

16. This must be done using qualified, experienced, specialized and certified empanelled IT Security auditors. Auditor must be answerable in case of any breach or glitch or vulnerability.

17. The end-user apps must have functionalities to block any attempted data leak from PC and mobile phone.

18. The user-interface must be user-friendly, available in all languages defined in eighth schedule of Indian constitution. It must allow minimum data entry on prompts with provision for audible prompts.

19. A periodic report on cyber security and incidents must be published.

20. Citizens must be regularly updated on cyber security.

Awareness and education -

21. User-friendly user/operating manuals and other related material must be created ASAP.

22. A big push must be given to user awareness and education in their own language using different kind of media for different demography. This will be a full time task in itself.

23. Students of 9th and 11th class can be trained and mobilized to further train, create awareness and implement CDT with citizens. These students must be awarded extra incentive such as performance certificates or 2-5 marks for social work in their 10th and 12th exam based on their tangible and measurable performance.

24. Indian NGOs with no foreign funding and agenda must be encouraged to create mass awareness and education. RBI or government can engage, encourage and fund creditable Indian NGOs for this awareness with accountability and performance parameters.

Legal issues -

25. Required laws must be created and existing must be amended, with due checks and controls, to facilitate CDT to become legally valid.

26. Citizen must be protected from losses in case of loss of money or data or privacy. It can be done using insurance and limiting the liability of citizen with defined time frame. DICGC or insurance companies must be encouraged to underwrite these losses at a predefined premium.

27. Adjudication process must be reactivated and function in time bound manner. It may require more Adjudication Officers, who can be appointed other than state IT Secretaries.

28. Other legal issues must be address. This may require one or more bills in parliament. This can be part of finance bill, thus require passing by Lok Sabha only.

29. CDT must be implemented in mission mode. A separate nodal officer or CEO at PMO/RBI may be appointed, who will have powers to take action and bypass bureaucratic red tape. His/her performance must be measurable.

Dr Rakesh Goyal is perpetual student of cyber security since 1991. He is PhD is Cyber Security, Gold Medalist Engineer, Gold Medalist PGDM from IIMB. He is MD of Sysman Computers Private Limited, Mumbai, one of the 23 IT security audit organisations empanelled with CERT-In, Min of IT, GoI to audit cyber security of critical national infrastructure/assets. He can be contacted at rakesh@sysman.in.