Cyber Security Policy for Digital India- Roadmap for Secure Cyber Space

Jagdish Chander Sharma (IAS), Shailender Kaushal, Ajay Singh Chahal,
Principal Secretary (IT), Senior Systems Analyst/Scientist-C, State Informatics Officer/Scientist-F
HP Secretariat, Government of HP, National Informatics Centre, Himachal Pradesh, HP Secretariat, Shimla-171002 (HP)
jagdish.chander22@ias.nic.in, kaushal.shailender@nic.in, ajay.chahal@nic.in
9418000066, 94184-57724, 94182-75076

Abstract

Sun is essential to all lives on earth, but too much exposure to Sun can also be harmful similarly connectivity is essential in contemporary world but excessive exposure to cyber world can also be risky. Cyber security is very crucial not only for individual but equally important for the economy and security of our country. Cyber security cannot be left to the Government alone to solve. Organizations and Individuals play equally important role in minimizing cyber security threats. India is growing rapidly and Information Technology has played major role in the development of India. In order to keep the momentum going, we need to ensure all Information & Communication Technology (ICT) services and infrastructure present in the country must be protected. Well defined Cyber Security Policies will ensure the protection of our ICT infrastructure from the natural, accidental or intentional threats.Threats will continue in the long run. Private sector and individuals must understand and implement the new policy. Implementation of such policies will provide resistance to any major cyber-attack. In case anyattack occurs, these polices will ensure to minimize the risk and recovery should be possible in a reasonable time frame.

Keywords- Digital India, cyber security, security policies, cyber threats, security audit.

1. Introduction

The Government of India is committed to enabling innovation, growth and prosperity for all Citizens through implementations of programs like Digital India, Smart Cities, BharatNet, Digital Locker, Jan Dhan and many more. These programs will bring more and more people connected through internet and also expose them to the threats of Cyber world. India is increasingly a target for cybercrime and espionage. All of our Governments, businesses and individuals need to work together to build resilience to cyber security threats and provide more services online.

IT sector has been one of the most significant growth catalysts for the Indian economy in the last decade. In addition to the economic growth, it is also influencing the lives of individuals directly or indirectly. If an organization is connected to the Internet, it is vulnerable to compromise. As people and systems become ever more interconnected, the quantity and value of information held online has increased, so have efforts to steal and exploit that information, harming our economy, privacy and safety. Cyberspace, and the dynamic opportunities it offers, is under persistent threat. Malicious cyber activity is a security challenge for all. Allorganizations across the Government, public and private sectors have been compromised by state-sponsored or non-state actors. Overseas, large multinational companies and government organizations have been targeted, losing substantial amounts of sensitive commercial and personal information or incurring major damage to their business and reputation. To grow our cyber security capabilities and to anticipate and respond to cyber threats, we must identify our weaknesses and address ourconcerns. It is critical that we build our nation's stock of cyber security skills, which are becoming increasingly essential for life and work in our connected world. Ultimately, to deal with all these challenges, we need to understand the kind of cyber threats that are taking place in the cyber-world, as shown in Figure-1. It shows the trend of attacks in recent years. As we can see, numbers of incidents are increasing every year. It is the right time for us to be proactive and define our priorities and polices for cyber world.

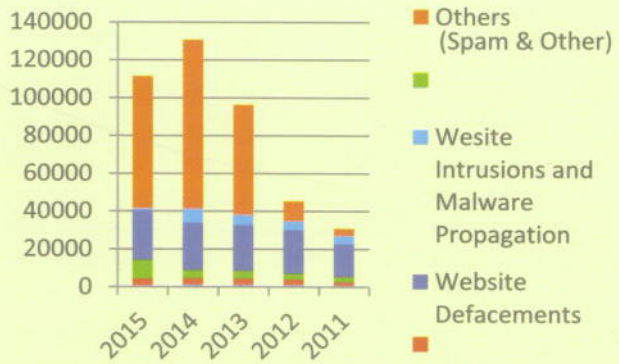


Figure-1:Year-wise incident report of cyber attacks in India.

2. The Role of Government

The Government is a key player in the whole cyber scenario, but it has to be a collective effort by all stakeholders, be it businesses, organizations or

individuals. Government around the world has begun to develop policy and standards to protect themselves against cyber threats while trying to promote the benefits of cyber enabled world. Implementation of Smart cities will bring the details of infrastructure to the cyber world. Government of India plans to shortly issue a RFP to set up the national cyber coordination Centre (NCCC) which will safeguard India's cyberspace against potential threats. The process has been fast tracked since the government runs many critical websites, with DigiLocker being one of online schemes wherein users upload their personal information and documents. NCCC will also be critical to the success of the government's Digital India programme.It comes in the backdrop of many government websites, mainly state departments or ministries, being hacked recently.The security of cyber space is not optional, but mandatory in view of its impact on national security, public safety and economic impact [1]. The key considerations for securing the cyber space include following points.

- To improve the resilience and robustness of critical information infrastructure in Government sector like State Data Centers and State Wide Area networks and similar infrastructure in public and private sector.
- To continue coordination with international partners and international organizations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development.
- To raise awareness of the responsibilities of businesses and of private individuals around securing their networks, devices and information and to support them in this by means of information, training and voluntary codes of practice.
- Use of adequately trained and qualified manpower along with suitable incentives for effective results in highly specialized field of cyber security.
- To ensure that the State has a comprehensive and flexible legal and regulatory framework to combat cybercrime by protection of sensitive or personal data.
- To ensure that the regulatory framework that applies to the holders of data, personal or otherwise, is robust, proportionate and fair.
- To build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents.

The Figure-2 shows the various stages of data in cyber world from where data can be stolen or manipulated. We need to ensure that all the layers of network are protected from the known threats in cyber world [3]. All data needs to be encrypted and proper access control systems should be implemented. Second layer is application, where application hardening and antivirus solutions is required. Next layer is host, which can be protected using HIDS, HIPS and Operating system hardening and patches should be done regularly to ensure all vulnerabilities are removed from the host. Network layer can be protected using Network based Intrusion detection systems and secure network protocolsImplementation of firewalls, VPNs, IPS and IDS at perimeter network. Physical security is also very important for these tracking devices, locks and deployment of security agencies at all data centers is important [4].

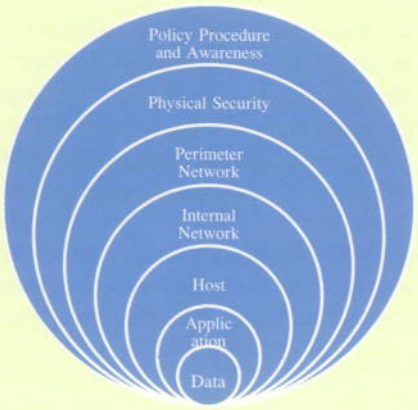


Figure-2: Information life cycle in cyber world.

At the top level, we need to make aware all the users about the policies and procedures to ensure protection of their data. Most of these layers will be taken care by technology. Government role is in the formation of policy and procedures and to bring awareness among the people about the importance of cyber security.

3. Indian Cyber Security Key Agencies

Some of the most important agencies that are involved in cyber surveillance or dealing with cyber crime in India are working under Ministry of Information and Broadcasting, Ministry of Home affairs and Ministry of Electronics and Information Technology. Some of the important agencies functional in India are [2]:

a) *National Information Board*

The National Information Board is the highest policy making body for cyber security. It was set up in the year 2002 and is chaired by National Security Advisor. It acts as the highest policy formulation body at the national level and periodically reports to the cabinet committee on security of the Government of India headed by the Prime Minister.

The NIB consists of 21 members and most of them are the secretaries of the Government of India of various Ministries. The National Technology Research organization (NTRO) provides technical cyber security and the intelligence.

b) *National Security Council*

The National Security Council (NSC) of India is an executive government agency tasked with advising the Prime Minister's office on matters of national security and strategic interest.The National Security Council Secretariat (NSCS) is the apex agency looking into the political, economic, energy and strategic security concerns of India and act as the secretariat to the National Information Board.

Besides the National Security Advisor (NSA), the Deputy National Security Advisor (DNSA), the Ministers of Defence, External Affairs, Home, Finance of the Government of India, and the Deputy Chairman of the now NitiAyog are members of the National Security Council. Other members may be invited to attend its monthly meetings, as and when required.

c) *NATGRID*

The National Intelligence Grid or NATGRID is the integrated intelligence grid connecting databases of core security agencies of the Government of India to collect comprehensive patterns of intelligence that can be readily accessed by intelligence agencies.

NATGRID is an intelligence sharing network that collates data from the standalone databases of the various agencies and ministries of the Indian government. It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel. This combined data will be made available to 11 central agencies, which are: Research and Analysis Wing, the Intelligence Bureau, Central Bureau of Investigation, Financial intelligence unit, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Enforcement Directorate, Narcotics Control Bureau, Central Board of Excise and Customs and the Directorate General of Central Excise Intelligence.

d) National Technical Research Organisation

The National Technical Research Organisation, originally known as the National Technical Facilities Organisation (NTFO), is a highly specialised technical intelligence gathering agency. While the agency does not affect the working of technical wings of various intelligence agencies, including those of the Indian Armed Forces, it acts as a super-feeder agency for providing technical intelligence to other agencies on internal and external security. The agency is under the control of India's external intelligence agency, Research and Analysis Wing, although it remains autonomous to some degree. The organisation does hi-tech surveillance jobs, including satellite monitoring, terrestrial monitoring, internet monitoring, considered vital for the national security apparatus.The agency develops technology capabilities in aviation and remote sensing, data gathering and processing, cyber security, cryptology systems, strategic hardware and software development and strategic monitoring.

The National Critical Infrastructure Protection Centre, an agency under the control of National Technical Research Organisation, has been created to monitor, intercept and assess threats to crucial infrastructure and other vital installations from intelligence gathered using sensors and platforms which include satellites, underwater buoys, drones, VSAT-terminal locators and fiber-optic cable nodal tap points. The officials have identified countries from where such gadgets could be procured but refused to reveal them due to 'security and other implications'.

e) The National Cyber Coordination Center

National Cyber Coordination Centre is a proposed cyber security and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Some have expressed concern that the body could encroach on Indian citizens' privacy and civil-liberties, given the lack of explicit privacy laws in the country

Some of the components of NCCC include a cyber crime prevention strategy, cyber-crime investigation training, review of outdated laws, etc. Indian and U.S. intelligence agencies are also working together to curb misuse of social media platforms in the virtual world by terror groups

f) National Information Infrastructure Protection Centre (NIIPC)

NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. They would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defense and Law enforcement agencies with a view to protecting these agencies' ability to collect, analyze and disseminate intelligence. NIIPC would interact with other incident response organizations including CERT-In, enabling such organizations to leverage the Intelligence agencies' analytical capabilities for providing advanced information of potential threats.

g) National Disaster Management Authority (NDMA)

The National Disaster Management Authority (NDMA) is the Apex Body for Disaster Management in India and is responsible for creation of an enabling environment for institutional mechanisms at the State and District levels. NDMA envisions the development of an ethos of

Prevention, Mitigation and Preparedness and is striving to promote a National resolve to mitigate the damage and destruction caused by natural and man-made disasters, through sustained and collective efforts of all Government agencies, Non-Governmental Organizations and People's participation.

h) CERT

CERT-In (the Indian Computer Emergency Response Team) is a government-mandated information technology (IT) security organization. The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

CERT-In was created by the then Indian Department of Information Technology in 2004 and operates under the auspices of now MeitY. According to the provisions of theInformation Technology Amendment Act 2008, CERT-In is responsible for overseeing administration of the Act.Table-1 shows the year wise incidents handled/ reported to CERT India [5].

Table-1: Incident-wise Details of Cyber Incidents in India

Incidents/Year	2015	2014	2013	2012	2011
Phishing	534	1122	955	887	674
Network Scanning and Probing	3673	3317	3239	2866	1748
Virus/ Malicious Code	9830	4307	4160	3149	2765
Website Defacements	26244	25037	24216	23014	17306
Wesite Intrusions and Malware Propagation	961	7286	5265	4591	4394
Others (Spam & Other)	69841	89269	58161	10567	3720
Total	**111083**	**130338**	**95996**	**45074**	**30607**

CERT organizations throughout the world are independent entities, although there may be coordinated activates among groups. The first CERT group was formed in the United States.Following are the roles and functions of CERT-IN:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

In addition to these organizations, with an objective to make India, a Global Information Technology Super Power and a front-runner in the age of Information revolution is the key Ministry of Electronics & IT, to promote and run e-Governance services and infrastructure. All critical eGovernance infrastructure of Government is managed by MeitY, as given in Figure-3. Its various agencies are responsible for managing the cyber security aspects in the country on a regular basis.

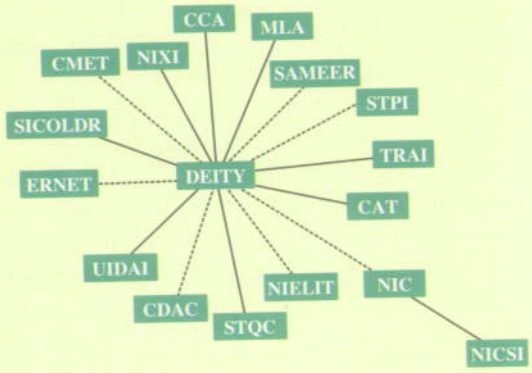


Figure-3: Structure of MeitY, GoI.

Figure 3 shows the structure of MeitY and its organizations which have mandate to promote eGovernance for empowering citizens and ensure a secure cyber space. MeitY has already taken many important initiatives to secure government services. Many of its originationsare following ISO 27001 standards to ensure international security standards. The Chief Information Security Officers (CISO) has been identified and regular training sessions are conducted for its employees.

4. Recommendations

Government must coordinate different efforts, manage stockholders interests and educate the public to establish cybersecurity as a priority. This can be incredibly effective but ultimately the case might be made for stronger government intervention through policies and regulations. In addition to the policies Government must identify critical computer infrastructure and ensure such infrastructure is safe from such cyber attacks. We have critical Government infrastructure in shape of NKN, State Data Centers, State Wide Area Network All types of infrastructure face some level of risk associated with various threats. Threat can be natural, accidental or intentional. Regardless of the nature of threat, these must be identified and necessary prevention mechanism must be defined. We must ensure that all known vulnerabilities are removed. We must enhance the capacity of critical ICT infrastructure to resist any major cyber attack. In case of an attack on infrastructure, we must be able to minimize

it and recovery should be possible in reasonable, shortest possible time frame. The key actions to reduce security threats and related vulnerabilities are:

- Identify and classify critical information infrastructure assets.
- Use of latest and secure products, protocols and communication system.
- All Internet Service Providers would be closely associated in providing secure information flow through their networks and gateways by implementation of Multiple Protocol Label Switching (MPLS) or VirtualPrivate Network (VPN) technology.
- Process for national level security threat and vulnerability assessments to understand the consequences.
- Identification of national level security organizations to act as a nodal agency and co-ordinate all matters related to information security in the country, with clearly defined roles & responsibilities.
- Emergency preparedness and crisis management (Mirror Centers, Hot/warm/cold sites, communication, redundancy, and disaster recovery plans, test & evaluation of plans etc
- Periodic as well as random verification of the level of emergency preparedness of critical information infrastructure facilities in resisting cyber attacks and minimize damage & recovery time in case cyber attacks do occur.
- Development of comprehensive repair and maintenance policy so as to minimize false alarms and increase cyber resource availability to all users efficiently.
- In order to effectively deal with targeted cyber attacks on sensitive sectors. Different teams must be formed to deal with different critical sectors such as finance, defense, energy, transportation, telecommunication etc.
- Establish public-private architecture for responding to national level cyber attack.
- Cyber security drills and exercises in IT dependent business with continuity plans to access the level of emergency preparedness of critical information infrastructure facilities in resisting cyber attacks with minimum damage and recovery time in case any attack happens.

5. Conclusion

The initiatives taken by the Government of India to make cyber space more secure have been analysed thoroughly in this paper. However, actions for securing information and information systems are required to be done at different levels within the country. In addition to the actions by Government, other stakeholders such as Internet Services Providers (ISP), large corporate and small users/home users are also required to play their part to enhance the security of cyber space within the country. Role of Government should be restricted to make policies and procedures and educate citizens about cyber security. All of us should understand our responsibilities for our own cyber space and should at least take care of safety of our personal devices.

Community in cyberspace is based on the interaction between people and society. All key agencies formed by Government must support each other and with the huge growth in the number of Internet users in the coming years, the security of data and its proper management will play a vital role for future prosperity and potential. Threats on IT systems have made Governments to re-think about regulatory solutions but care must be taken not to disturb privacy and ease of existing systems that are supported by IT and above all, we should aspire for more computer literacy to understand the safety issues related to our cyber space. At the same time we need to utilize the specialization of private sector in the field of cyber security and government should promote more PPP projects for the national cyber space. The Law & IT, Minister, GoI has stated recently that companies with information technology as significant part of their business should get their cyber security audit by third party and appoint an officer to manage their IT security. This is a significant step towards ensuring national cyber security [6].

There will be debate about the merits and drawbacks of government involvement in controlling cyber security. With respect to cyber security regulations, we are still in early days of what the government role should be, what tools are available. Policymakers and stakeholders should take security risks seriously, but be careful that attempts to strengthen one system do not irreparably harm other systems.

References

1. *Ministry of Electronics and Information Technology website* at http://meity.gov.in/content/strategic-approach accessed on 21 October 2016.
2. *Article on "An overview of India's cyber security agencies"*http://www.medianama.com/2016/04/223-indias-cyber-security-agencies/ accessed on 21 October 2016.
3. *Coverage on "Cyber Security and Related Issues" at* http://www.insightsonindia.com/2014/11/25/cyber-security-related-issues-comprehensive-coverage/
4. National Cyber Security Policy 2013 at https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013 accessed on 23 October 2016.
5. *Annual report of Cert, India available at https://cert-in.org.inaccessed on 28 October 2016*
6. http://economictimes.indiatimes.com/tech/ites/ravi-shankar-prasad-for-cyber-audit-of-firms-in-it-business/articleshow/55376609.cms*accessed on 11 November 2016*

Digital Transformation in Himachal Pradesh Transport Department: Reaching out to Last Mile Rural Population

Dr. Sunil Kr. Chaudhary, IAS, Bhupinder Pathak, Ajay Singh Chahal

Commissioner-cum-Director Transport, Scientist-D/District Informatics Officer, Scientist-F/State Informatics Officer
Transport Department, Govt. of HP, National Informatics Centre, Himachal Pradesh, HP Secretariat, Shimla-171002 (HP)
transport-hp@nic.in, 94184-67676, pathak.b@nic.in, 94181-11012; ajay.chahal@nic.in, 94182-75076

Abstract

e-Governance is the effective use of Information & Communication Technology to improve the system of governance that is in place, and thus provide better services to the Citizens. eGovernance is considered as a high priority agenda of the Digital India program, as it is considered to be the only means of taking Information & Communication Technology (ICT) based services to the "Common Public" through Digital Transformation. The paper discusses the role, these ICT systems play in providing various Transport sector services Online at the doorstep of rural/urban community or individual by bringing all services related to the Driving License, Learner's License and complete relevant information about the existing Driving License on single web portal. In Himachal Pradesh, it has been achieved where all the information is available in a single web portal covering all the Transport department offices and is accessible online on a 24x7 basis. This contact-less SAARTHI system has simplified the processes, reduced the visits of citizens to Transport offices, reduced footfalls, enabled online payment of fees and has put a check on corrupt practices. The system has helped to consolidate the databases into a centralized platform and deliver core services upto village level.

Keywords: digital transformation, last mile connectivity, transport, Sarathi, driving license, common service centre

1. Introduction

With a view to computerizing all the Regional Transport Offices (RTOs) in the country and bringing about uniformity in the Driving License and Vehicle Registration documents issued by the Regional Transport Offices, the web-enabled Saarthi project has been conceived and implemented. Previously, although the citizens were getting their licenses through a computerized system, they had to visit the Regional Transport Offices-RTO/ Registration & Licensing Authorities-RLA offices personally, multiple times, resulting in cost and time of the citizens in addition to various corrupt practices. In order to offer better services, the web-enabled SW was developed by the NIC Central Team and Himachal has been the first State in the country to roll it out in all RTO/RLAs of the State of Himachal Pradesh, ahead of other States, offering the service of driving licenses to citizens from the comfort of their homes. This new web based system has been rolled out in all the 70 RLAs & RTOs in Himachal Pradesh in a period of six months and has been implemented on the backbone of a robust HIMSWAN data network with adequate bandwidth and built-in redundancy to facilitate acceptable standard of speed, information security and fault tolerance. This last mile connectivity has been an important factor in the implementation of the SW at the remotest locations of the State and the BSNL has proved its worthiness for providing the connectivity at remote/ hard/ difficult to access locations, which will remain un-serviceable by other private services providers for years to come. The data and application for the whole country is being maintained in a National level data centre backed up by a Disaster Recovery Centre – both of which have the latest hardware, software and control infrastructure to achieve optimum operational performance, safety and security.

At the national level, the new system will consolidate the database and applications for all RTOs in all States into a common, centralized platform and deliver the core services of Sarathi throughout the country upto village level. Himachal Pradesh is having a Population of 68 Lakhs, 10.03 % is Urban and 89.97% is Rural Population. The 89.97% of the Rural including Tribal Population is being served. 50% of the applications have been submitted online and the 3700 Common Service Centres established at the last mile at the village level are or the Transport Service Providers are serving the people of Himachal Pradesh. These CSCs/LMKs are bridging the gap of digital divide in rural areas.

Total RTOs	70
RTOs Covered	70
Population Urban Rural	10.03%
	89.97%
Area	55673 Sq. Kms
Application Submitted	195988

The RTO and RLA authorities throughout Himachal Pradesh now operate computerized counters/offices to help citizens to obtain driving licenses. The re-engineered online process now takes less than 24 hours instead of two/ three days, as was necessary under the earlier system. The lack of transparency under the old system resulted in a flourishing business for agents and middlemen leading to corruption. The individual driving License holders can now track the status of their applications online from the Sarathi service portal. Such a State wide Internet based solution and its implementation would have raised many eye-brows few years back. But it has been actually achieved.

2. Objectives

The primary objective of implementing this project in Transport Department is to:

- To provide transparent, timely and citizen centric delivery of services by using ICT.
- Reduction in Time For Delivery of Service
- Re-engineer the entire processes by eliminating non value adding steps and
- Convenience to the citizens
- Anytime Anywhere 24x7 service for application submission and e-payment.
- SMS service to the Driving License Holder from application submission to the approval of Driving License.
- Improve citizen perception about the department
- Citizen Interface with the Department more friendly
- Increasing the Satisfaction Level of Citizens
- Providing information to the applicant about the application status through web tracking.
- To provide the service to other stake holders viz. Insurance companies, Police, RTOs/RLAs of India, MORTH, Courts, Banks and other Govt. Agencies for the verification of Driving License.

Digital Transformation under Digital India

Dr. APJ Abdul Kalam, Former President of India, had visualized e-Governance in the Indian context to mean – "A transparent smart eGovernance with seamless access, secure and authentic flow of information crossing the interdepartmental barrier and providing a fair and unbiased service to the citizen." [2]

The Govt. of India's Digital India initiative is an umbrella programme that covers multiple Government Ministries and Departments. It weaves together a large number of ideas and thoughts into a single, comprehensive vision so that each of them can be implemented as part of a larger goal. Each individual element stands on its own, but is also part of the larger picture. Digital India is to be implemented by the entire Government with overall coordination being done by the Ministry of Electronics and Information Technology (MeitY). Digital India aims to provide the much needed thrust to the nine pillars of growth areas. In 5th Pillar of Digital India is e-Kranti, which is an essential pillar of the Digital India initiative. Considering the critical need of e-Governance, mobile Governance and Good Governance in the country, the approach and key components of e-Kranti have been approved by the Union Cabinet on 25.03.2015 with the vision of "Transforming eGovernance for Transforming Governance". There are 44 Mission Mode projects under e-Kranti under which Transport Sector is one of the project for the delivery of services. [3]

E-Governance in India has steadily evolved from computerization of Government Departments to initiatives that encapsulate the finer points of Governance, such as citizen centricity, service orientation and transparency. Lessons from previous e-Governance initiatives have played an important role in shaping the progressive e-Governance strategy of the country. Due cognizance has been taken of the notion that to speed up e-Governance implementation across the various arms of Government at National, State, and Local levels, a programme approach needs to be adopted, guided by common vision and strategy. This approach has the potential of enabling huge savings in costs through sharing of core and support infrastructure, enabling interoperability through standards, and of presenting a seamless view of Government to citizens.

The National e-Governance Plan (NeGP), takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision, a shared cause. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is evolving, and large-scale digitization of records is taking place to enable easy, reliable access over the internet. The ultimate objective is to bring public services closer home to citizens, as articulated in the Vision Statement of NeGP.

"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realize the basic needs of the common man"

In addition, prior research has also suggested that the main rationale for the use of government and eGovernance is that it can reduce costs and delays in processing and delivering services, expand citizen's access to public

sector information, increase transparency and public accountability, and weaken authoritarian tendencies. The relationship between e-government and corruption was also studied to infer that as the use of ICT or e-government increases the level corruption decreases. The study suggests that a 1% increase in the government Index may have resulted in a 1.17% decrease in corruption [1].

3. Challenges

The main challenge faced in starting Online Sarathi4.0 service was:

- How to migrate from existing Sarathi1.0 to Sarathi4.0
- Porting of existing data from Sarathi1.0 to Sarathi4.0
- Porting of subsequent pending data to Sarathi4.0 for which transactions were pending in Sarathi1.0 after initial porting of data.
- How to tackle the old transactions which were not completely processed in Sarathi1.0
- Part of the payment done in Sarathi1.0 after migration.
- Same DL records was available in different RLA/RTO authorities because of previous transactions done. How to take the valid updated records during porting for RLA/RTO data to Sarathi4.0.
- The Last Mile Connectivity in all the RLA/RTOs and even RLA/RTOs of remote tribal areas was a challenge and is a challenge, even today!
- Mapping of different master tables used in Sarathi1.0 & Sarathi4.0
- The master tables codes were not same in all the RLA/RTOs and mapping of such table of different RLA/RTOs to Sarathi4.0
- Testing of software on staging server for different types of transactions and issues faced in tackling such cases in Sarathi4.0
- Issues faced during the pilot run at two pilot sites.

4. Services Offered

The Sugam Kendras are offering many services under one roof in a time bound manner. The services being offered are diverse in nature, so is the delivery associated with it. The software implemented in these centers are role based work flow applications and responsibility associated with one task is assigned to the individual operator assigned for that activity.

The applications are basically on-line transaction processing wherein the information is taken from the applicant on standard government prescribed formats/ forms and then same is filled and if required his/ her photographs, Digital Signatures and finger prints impressions are taken on spot beside acceptance of cash at the cash counter. If the approving authority is available in the office and no further field verifications are required, immediately the services are provided. Otherwise the applicant is given a date by which the activity would be completed. The main services have been listed in Figure-1.

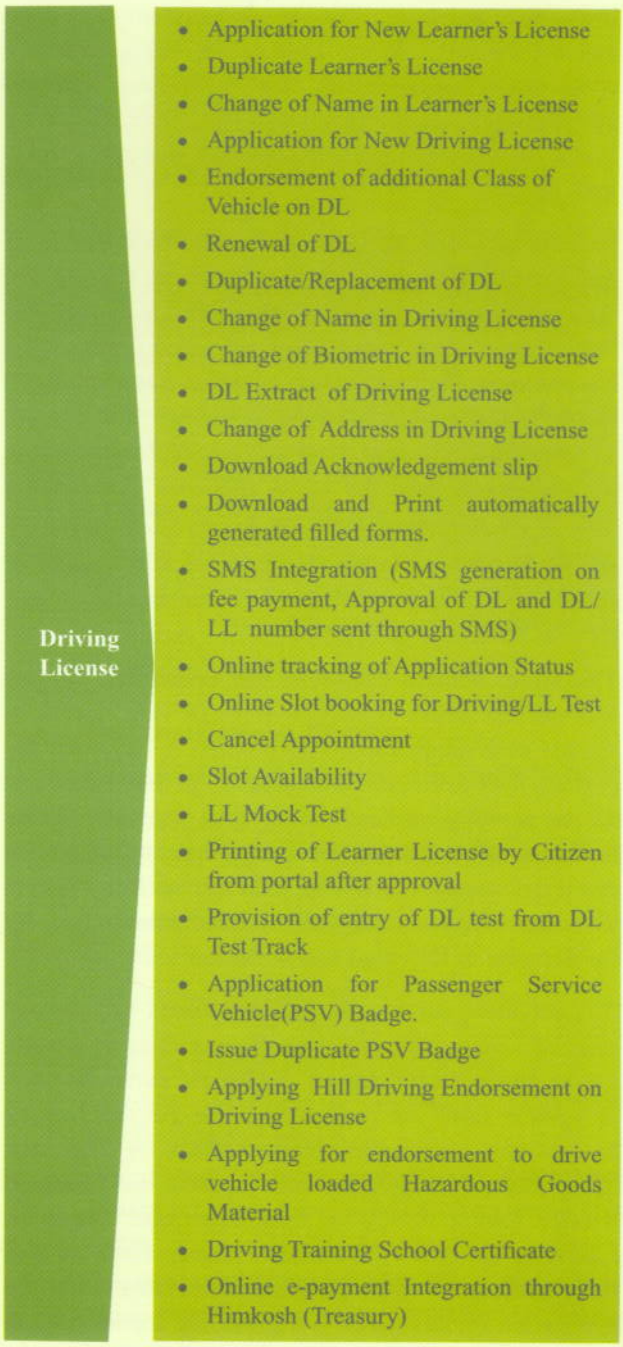


Figure-1: Sarathi Services List

5. Implementation

The new version of Sarathi4.0 facilitates the citizen to file their application online along with uploading of necessary documents. A unique Application Number is generated for each application filed, which can be used by the citizen to track the status of the application. The online Learner's License Test (STALL) slot booking and e-payment integration with HIMKOSH (HP Cyber Treasury) for payment of license fees and various other services are available through this new system. This web application can be accessed through other devices such as mobiles, tablets, etc. The SMS integration is also there and the Driving License holders are being intimated about the action taken and when it has been approved and the LL/DL number generated. The e-mail integration is also there for sending the updates of application to the individual.

In existing system, the public can search their Driving & Learner License details online and also see the status of their applications. The application status will show the flow of application in the office and which dealing hand has processed their application on which date and when it has been approved, printed and dispatched. The Learner License holder can download the Learner Licenses from the web portal once the LL is approved. The SMS is sent to the individual once the LL or DL is approved alongwith the LL/DL number. In earlier system, general public had to visit or contact concerned RLA/RTO office for applying and payment of fees etc.

The Motor Vehicle Inspectors can update the Driving License Test results directly from the Driving Test tracks against each application. The RTO/RLA can track the pending application at different levels in their office and all the pending applications for final approval will be available. Any applicant, if coming for any of the service and if the renewal is also due, then automatically system takes care of the same and alert the individual to pay for the Renewal of Driving License fee too.

An individual passing the driving ground test for one class of vehicle and failing in another class of vehicle has an option to withdraw a service for particular class of vehicle from the public portal to get the Driving License or to wait and pay for the balance fee. The Govt. of Himachal Pradesh has also opened the Common Service Centre (CSC) up to Village level known as LokMitra Kendras in Himachal Pradesh. They are also the stakeholder in this project and are submitting the application on this portal and providing the services to the public living in rural areas of Himachal Pradesh.

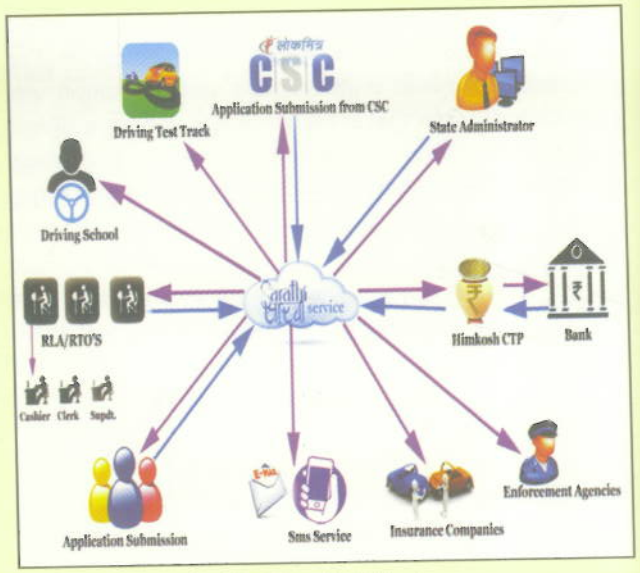


Figure-2: Saarthi 4.0 Flow Architecture

The "Sarathi Service Portal"[5] provides various types of services to all stakeholders namely, citizens, general public, Driving School business enterprises, students, employees, Drivers, special category people etc. Therefore, coverage of the stake holders and targeted population is 100%. The online system has been hosted at NIC National Cloud 'MeghRaj' and available to all stakeholders 24x7 and accessible from anywhere, anytime throughout the State, India and abroad using Internet.

The stakeholders' geographical coverage is mostly with in Himachal Pradesh State except those who are going out of the State and getting their licenses renewed in other states. The other stake holders are Insurance companies who are getting the verification of the genuineness of Driving License, banks who are verifying the authenticity of the DL where the public is giving the Driving License as proof of address and identity for opening bank accounts. The CSCs provide these services in rural areas on payment basis. However stakeholders residing temporarily anywhere in India o abroad can also access the service from their respective places 24x7. Beside this, the Transport Department ha given the License to Transport Service Providers fo rendering the various services to the public for onlin submission of various applications especially for driver who are Matric passed and are not well versed with I system. These TSPs are now stake holders in this projec

The public at large viz. General public and taxi drivers Public and Private Bus Drivers have been helped an benefited most, by implementing the online systen The application status will show the flow of applicatio in the office and which dealing hand has processe their application on which date and when it has bee approved, printed and dispatched as shown in Figure-

The Learner License holder can download the Learner Licenses from the web portal once the LL is approved. The SMS is sent to the individual once the LL or DL is approved alongwith the LL/DL number. In earlier system, general public had to visit or contact concerned RLA/RTO office for applying and payment of fees etc.

SARATHI 4.0
Implementation in Himachal Pradesh

The software is uniformly implemented in the State of Himachal Pradesh covering all the 70 RLA/RTO who are issuing Driving Licenses. Himachal Pradesh is the first state in India who has implemented this software covering entire area of the state. The coverage aspect as a service is beyond the State too as the Driving License holders residing outside Himachal Pradesh can view / verify their Driving License details in Public Domain.

- Total Driving License issuing RLA/RTOs: **70**, Solution implemented in all **70** RLA/RTOs,
- Population: 68 Lakhs, 10.03 % is Urban and 89.97% is Rural Population and Rural Literacy is 81.85%.
- 89.97% of the Rural including Tribal Population is being served.
- Area : 55,673 square KMs including Trans Himalayan arid zone having toughest terrain in the world.
- The dispersed population having density of 123 people per Sq Km are being served.
- Total Application submitted so far: 1,95988 since October 2015 till 20th September 2016.
- Half of the applications (50%) are submitted online.

6. Last Mile Connectivity

In Himachal Pradesh the HIMSWAN is providing reliable network through BSNL for vertical and horizontal connectivity throughout the State and has reduced the cost of communication between Government Departments at different locations and is providing secure network infrastructure to enable electronic transfer of sensitive data, payments etc. with improved capacity for disaster management. HIMWAN is a highway of connectivity between G2G, G2C and providing round the clock connectivity of minimum 2 Mbps between districts and Sub.Division/Blocks/Tehsils. The key highlights of HIMSWAN are:

✓ Data Communication, Voice over Internet Protocol (VoIP), Video Conferencing (VC) and selective Internet available at all Locations.

✓ Last mile connectivity through Lease line or VPNoBB.

✓ Last mile connectivity through wireless wherever wired line is not available.

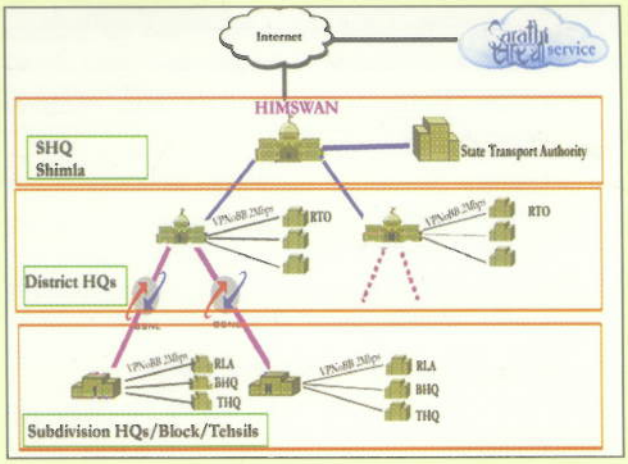


Figure-3: HIMSWAN Architecture

Presently in all the 70 RTOs and RLAs of Himachal Pradesh, 2Mbps VPNoBB connectivity has been provided by the Department of IT, Govt. of HP. The District HQs RLAs and RTOs are connected through NICNET on NIC LAN wherever they are near NIC Offices.

The Common Service Centres/Lok Mitra Kendras are using BSNL, AIRTEL connectivity and in the remote tribal hard areas of the State the, VSATs have been provided to the Offices and CSCs. In Himachal 3000 CSCs are providing services to the citizens. The Transport Service Providers (TSP) appointed by the H.P. Department of Transport are working at the Block and Village level, who are providing the services to the Citizens who don't have access to Internet.[4]

7. Post Deployment Benefits

✓ One can submit applications online for New DL & LL

✓ Online e-payment integration with HimKosh Cyber Treasury.

✓ The online slot booking for the appointment for DL and LL test.

✓ Services of LL and DL e.g. Renewal of DL, Endorsement of Additional Vehicle Class, Duplicate DL etc. are available online.

✓ Uploading of Scanned Documents, Photograph and Signature of Applicant.

✓ User friendly website with all the information needed for anyone including all the web-fill able forms.

✓ The address of the license holder is being captured using the e-Governance standards by taking Census 2011 data having State, District, Tehsil/ Town, Village, Ward & Pin code.

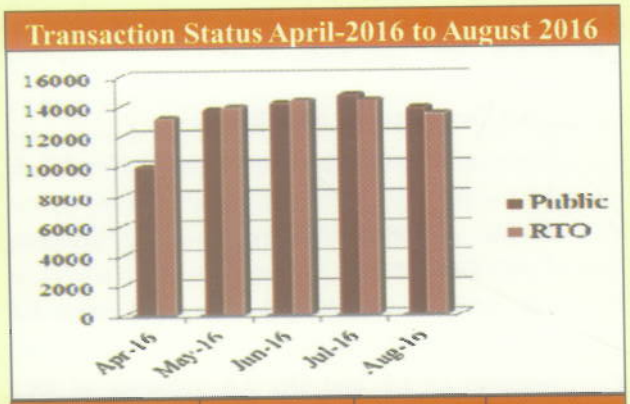
✓ Real-time Services to the Citizens

- ✓ Tracking of Application Status
- ✓ Automated Alerts to Citizens
- ✓ Elimination of NOC and Clearance Certificate
- ✓ Onetime submission of documents
- ✓ Online sharing of data by RTO, State transport department & DoRTH
- ✓ Online sharing of relevant information by Insurance agencies, banks
- ✓ Use of relevant information by Police department
- ✓ Computerized test for learner's licence and online booking for service.
- ✓ Online Mock test for learning license
- ✓ Online NOC verification of license issued by any authority
- ✓ Single source of all Information for MIS for office

These above are some of the initiatives that have made the department not only responsive but also provide services in a transparent manner. The department maintains a central database and provides services to the police and other departments upon request.

8. Key Learnings

After implementation of online services, RTO department has become much transparent and user friendly resulting in faster licence issue and application turnaround process time. The applicant can apply for a license online by visiting the online portal of Sarathi service



Month Year	Public	RIO	Total
Apr-16	9896	13158	23081
May-16	13725	13884	27609
Jun-16	14160	14320	28480
Jul-16	14681	14353	29034
Aug-16	13825	13399	27224
Total	**66287**	**69141**	**135428**

49% of the applications have been recetved online through protal or through Transport Service Providers/CSCs and 50% applications have been entered through RTO/RLA staff.

Figure-4: Transaction status from April to August 2016

It is evident from the figures given in the diagram that out of the total applications received from April to August 2016, 48% of the applications have been received from the public portal. One can see the success and response of the public in getting the service. It has definitely reduced the number of visits to the RTO/RLA office and waiting time in RLA/RTO office in getting the service with lesser footfalls in their offices.

The learner licence holder need not to visit the office as immediately after the Learner License screen test aid for Learner License (STALL), the result is flashed on the screen and if candidate is passed the LL is approved and applicant is intimated about the Learner Licence on his/ her mobile. The individual can take the Learner License print from the Sarathi Service Portal.

The Insurance and Bank companies applying online for the DL extract need not to visit to any of the RLA/RTO office in Himachal Pradesh. They can apply online and make online payment for the fee specified as per the rules and the system will calculate automatically and after payment of fee they can print the DL extract by giving the application number.

One person holding multiple Driving License from different authorities in the past are being stopped when they are coming for any of the transaction. On the basis of Name, Father's Name & Date of Birth each person is being given unique BIOID internally.

Cost effectiveness

The implementation of the web portal of Sarathi services in all the 70 RLA/RTOs of Himachal Pradesh has been appreciated by Govt. Of India and this process re-engineering initiative has benefitted all stakeholders. Now that all services are online, it is saving the time and cost to citizens and hydrocarbon fuel used in motor vehicles on part of the State and Country and contributing towards of clean environment. On part of the Government, there has been huge saving of revenue by eliminating the processes of procurement of paper, printing forms, transporting these forms to various office locations throughout the State, storing, managing inventory and finally issuing/ sending of the Forms to citizens as per their requirements/ requests. The time required to complete the above processes and officials working on these processes has also been saved, which may be seen in terms of revenue saving on part of Government and the State.

Green Digital Governance

Green Initiative: IT has been used to enable paper-less transaction to the extent possible. All the forms as defined in Central Motor Vehicle Rules are being submitted online and the requirement of manual submission of all those forms will be stopped.

Smart & Green Solution: The saving of time and costs to citizens and hydrocarbon fuel used in motor vehicles on part of the State and Country is contributing towards of clean environment.

Paperless office: By utilizing the online services the Government of Himachal Pradesh is aiming to achieve a Paperless Governance and Cashless transactions. This indirectly has impact on reducing the extra Green House Gases that would have been released, had the citizen travelled multiple times to avail the service.

Digilocker: The Driving License has now integrated with Digi locker under the Digital India programme. With this integration people will no longer need to carry around physical copies of Driving Licenses. They can instead access digital copies of the same on their mobile phones via the Digi Locker mobile app.

9. Conclusion

The successful implementation of the Saarthi4.0 web-enabled software in a hilly and difficult State like Himachal Pradesh ahead of all other States of the country signifies the fact that citizens are eager to utilize online services which deliver definite outputs (DL in this case), in difficult to connect scenarios too. The role of user (Transport Department), implementing agency (NIC) and CSCs (LokMitra/TSP) is very important. Of course, there are issues like last mile connectivity, change management, resistance to change, quick software solution up-gradation as per feedback provided are essential elements in such a large scale State wide roll-out of online services. Connectivity issues need to be addressed through a combination of ISPs like VSATs, VPNoBB, LL, private ISPs, WiFi from nearest connectivity point, inclusion of multiple private service providers, based on ground realities of the locations/ offices being covered. Some suggestions like mandatory capturing of Aadhaar number, to capture enrolment from the private driving training schools for accountability, mandatory ePayment of fees, capturing DL test results from driving tracks will further enhance the value of these services to the citizens and Government alike.

References

1. Mistry J.J.; Jalal Abu, "An empirical analyses of relationship between e-Government & corruption"; The International Journal of Digital Accounting Research Vol. 12, 2012, pp. 145 – 176
2. Article on E-Governance Big Challenge: Abdul Kalam, http://www.cxotoday.com/story/e-governance-big-challenge-abdul-kalam
3. http://www.digitalindia.gov.in/
4. The CSC/Lok Mitra Kendra in Himachal, http://hp.gov.in/csc/
5. www.parivahan.gov.in/sarathiservice
6. https://sarathi.nic.in National Register Sarathi portal