VOL. 30 No. 2, October 2021 ISSN 0971-3409

Informatics

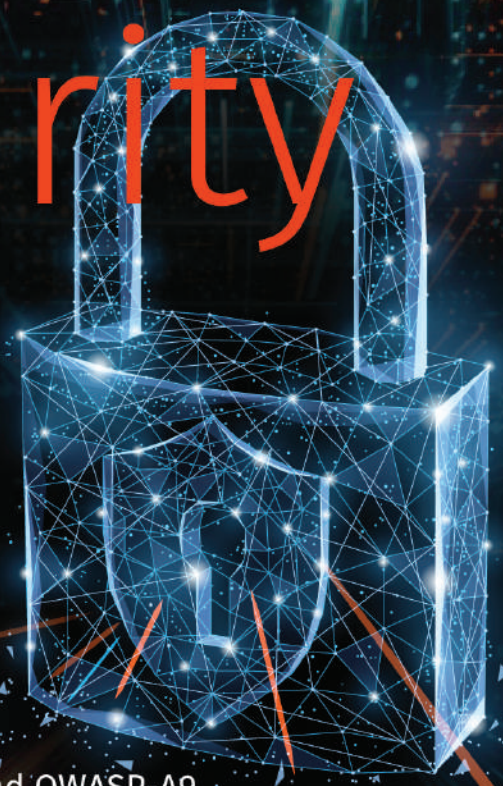
An e-GOVERNANCE PUBLICATION FROM NATIONAL INFORMATICS CENTRE https://informatics.nic.in

States
- Rajasthan
- Tamil Nadu

Districts
- Faridkot
- Mainpuri

Infocus page 18

Cyber Security



- ModSecurity
- Leveraging Big Data
- Defense in Depth
- Start Point of Cyber Security
- DevSecOps
- Preventing Cyber Crisis
- AVART
- Security Audit, Web shell, and OWASP-A9

Digital India
Power To Empower

एनआईसी
NIC

Informatics

Volume 30 No.2, October 2021

PATRON
Dr. NEETA VERMA

ADVISORY PANEL
Nagesh Shastri
Shalini Mathrani
I.P.S. Sethi
Ajay Singh Chahal

EDITOR
Mohan Das Viswam

ZONAL EDITORS
Dr. Dibakar Ray
Reuban K.
Kavita Barkakoty
A. K. Dadhichi

WEB VERSION
Sunil Sunsunwal
Archana Sharma

DESIGN SUPPORT
Mukesh Bharti
Rohit Maurya

PUBLISHED BY
National Informatics Centre
Ministry of Electronics & IT
Government of India
A-Block, CGO Complex, Lodhi Road
New Delhi-110003, INDIA

CONTACT ADDRESS
INFORMATICS
379, A4B4, Floor-3, NIC
A-Block, CGO Complex, Lodhi Road
New Delhi-110003, INDIA
Phone: 011 -24305365
Email: editor.info@nic.in

Editorial

Walls, roofs, doors and locks evolved along with mankind's need to stay safe and sheltered from dangers that lurk in the wild. Today, with the proliferation of internet in everyday life, having the continuous threats of security breaches during the delivery of services and online money transactions in day-to-day life, the need for bringing attention to Cyber Security is of utmost importance and must be a concentrated effort to stay safe and secure online.

The month of October every year is celebrated all over the world as the **National Cyber Security Awareness Month (NCSAM)**. It is important for internet and information technology institutions to take necessary steps and initiatives to dedicate conscious efforts towards ensuring better cyber security hygiene and incorporate stronger security measures. It is a collective responsibility of the government, organisations, employees, consumers and citizens at large to take Security as a priority.

Happy to present you this issue of Informatics which presents an array of interesting articles. **Rajasthan** and **Tamil Nadu** are the States covered in the State in Focus section this time. The two districts; **Mainpuri, Uttar Pradesh** and **Faridkot, Punjab** are featured in the District Informatics. **Securing Endpoints, DevSecOp, Start Point of Cyber Security, Defense in Depth, Preventing Cyber Fraud, AVART** and **National Cloud** are the articles in the Infocus section. Brief information on the prominent mobile applications recently launched by or released with the support of NIC at various States is covered in the Appscape in this edition. **Welfare Schemes for Differently Abled Persons, Kumari e-Sevai Centres, e-Sanvad-Grievance Redressal, SU-SWAGATAM, RoL Ladakh and Sindhudurg District Tourism** are showcased in this section. The regular sections such as Accolades and In The News bring you some interesting reads.

The articles related to Cyber Security updates and initiatives by National Informatics Centre, being the premier institution of the government for ICT Support and Security would be extremely useful for the readers to build awareness and to take necessary precautions at various levels.

Behind the scenes, we the team Informatics continuously enhance the publication by improving the quality, content, and design. The reader's feedback and suggestions are valued most. It would be great if you could take out some time to write to us. Suggestions and feedback may be sent to **editor.info@nic.in**

Wish you a great festive season ahead. Happy reading, and please take care, stay healthy and safe..

Editor

Contents

Editorial 02

Contents 03

From the State

Rajasthan 04

Tamil Nadu 08

District Informatics

Faridkot, Punjab 14

Mainpuri, Uttar Pradesh 16

Infocus

ModSecurity 19

Leveraging Big Data 22

Defense in Depth 25

Start Point of Cyber Security 28

DevSecOp 30

Preventing Cyber Crisis 32

AVART 34

Security Audit 36

Web shell 37

OWASP-A9 38

Appscape 40

In the News 42

Accolades 48

Rajasthan State

Bringing the Government closer to citizen

NIC Rajasthan plays a vital role in implementing major e-Governance projects in the state. Playing a crucial role, it has been instrumental in creating innovative ICT solutions which have not only eased the life of common citizen but have also improved efficiency within the government. In addition to core infrastructure for networks, VC and mini cloud, NIC Rajasthan has established comprehensive solutions like IFMS, PCTS, Shaladarpan, PDS etc., and their integration with different applications has made it possible for the government to function seamlessly and provide continued services.

Tarun Toshniwal
Dy. Director General
& SIO
tarun.toshniwal@nic.in

Amit Agarwal
Sr. Technical Director
amit.agarwal@nic.in

The princely state of Rajasthan is the largest state of the country in terms of geographical area, and is comprised of 33 districts, 352 blocks and 46,000 villages. This is also the border state of India neighbouring Pakistan. The state has a mix of rural and urban population with a literacy rate of 66%. NIC started its operations in Rajasthan in the year 1988. To provide services to various important government entities, NIC established its offices in State Secretariat and in every District Collectorates. It has also established its project offices with many departments and institutions at Jaipur. NIC has established its communication network at secretariat and districts. All 33 district Collectorates have been connected with high speed network. In addition more than 100 institutions have been extended network connectivity from NIC. A regional Centre of Excellence for Application Security (RCOEAS) has also been established at Jaipur, which is catering to ensure application security for applications developed by NIC teams in seven states.

ICT Initiatives in the State

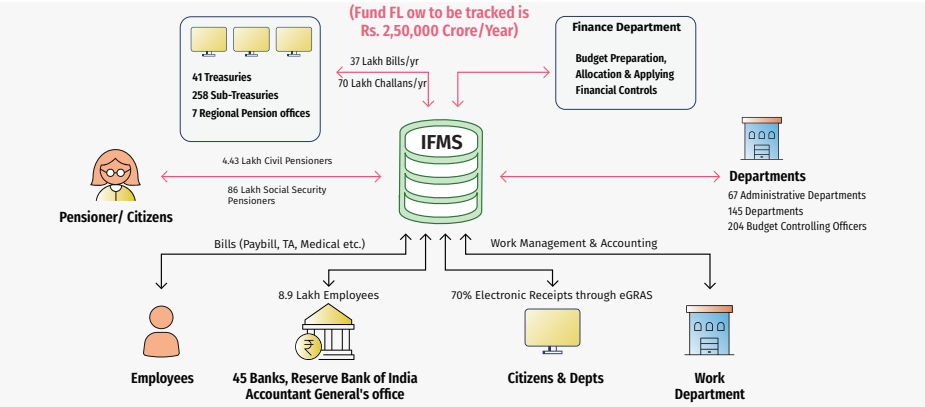
Integrated Financial Management System (IFMS) https://ifms.raj.nic.in

Financial Management of the state is taken care of by Integrated Financial Management System (IFMS), developed by NIC. IFMS is a complete suite of numerous applications related to finance, covering budget, payments, expenditure, receipt, works management and accounting. The system now provides for presentation of paperless budget in the Assembly, which saves almost 50 Lakh papers every year. Online Budget estimation and preparation has saved huge efforts and time which is distributed online to all DDOs. DBT for social security pensioners has saved Rs.300 Crore every year. The state government presents its accounts to the AG, digitally, including all vouchers. This saves 2.5 crore papers every year and the efforts and money in preparation of copies. Integration with e Kuber of RBI saves more than Rs. 100 Crore to the government. Aadhaar enabled Social Security pension system has stopped duplicate payments. The Social Security Pension and Salary system of all employees is completely auto processed without any manual intervention. This has substantially saved the efforts involved in salary and pension processing and has improved service delivery. All A & F sanctions for works are prepared and issued online with a capping of available budget. Since Budget control has been implemented for treasuries, the possibility of excess payment has been eliminated. Civil Pension for all the employees is also automated. Various modules of IFMS have been integrated with numerous applications of other departments. The eGRAS system used for government receipts has been integrated with 42 banks. IFMS provides real time data of all receipts and expenditure to all stake holders. It is supported by mobile apps for various functions.

> **The state of Rajasthan has taken major strides towards implementing e- Governance systems. NIC Rajasthan has been key technology partner of Rajasthan Government in development and implementation of many innovative and successful systems. The integrated Financial Management System (IFMS), Pregnancy & Child Tracking System (PCTS), Asha Soft, PDS computerisation, Pehchan, Works Management, Integrated Shala Darpan, Apna Khata, e Panjiyan, Social Security Pension System and many IT based DBT schemes are among very successful projects. NIC Rajasthan's team is very enthusiastic and always ready to take new challenges. I am happy to note that Informatics October 2021 issue is specially showcasing the e governance initiatives by NIC in Rajasthan. I congratulate and wish success to the entire team and look forward to many more e-governance initiatives by NIC.**
>
> **AKHIL ARORA, IAS**
> **Principal Secretary, Finance & Medical Government of Rajasthan**

Apna Khata https://apnakhata.raj.nic.in

Apna Khata is implemented as part of DILRMP for Land records computerization across the state in all tehsils and all villages. Digitally signed Record of Rights can be obtained from Apna Khata portal by making online fee payment. This has eased the process of obtaining RoR which are also given with the khasra map. The citizen is also provided with the facility to submit online applica-



▲ IFMS - The Financial Manager of Government of Rajasthan

tion for mutation. The entire process flow for mutations is online which can be accessed through mobile as well. Apna Khata portal shares land records information with property registration portal, crop insurance, Raj Kisan, Jan Soochna, e Mitra and many other portals.

ePanjiyan https://epanjiyan.nic.in

ePanjiyan is the online portal for property registration. Integrated with Apna Khata, the system provides for auto mutation of the property at the time of registration itself. All the 539 Sub Registrar Offices of the state are using the portal which provides for online assessment and payment of stamp duty. Excessive stamp value if any is also refunded online. e Panjiyan Mobile App facilitates on the sport verification of the property by Sub Registrar offices. The system also provides interface for property registration at the offices of Urban Local bodies which issue the land holding PATTAs. More than 60 Lakh property registrations have taken place through the system. The citizen can take prior appointments on the system. It also provides facility for anywhere registration which gives lot of convenience to the citizen.

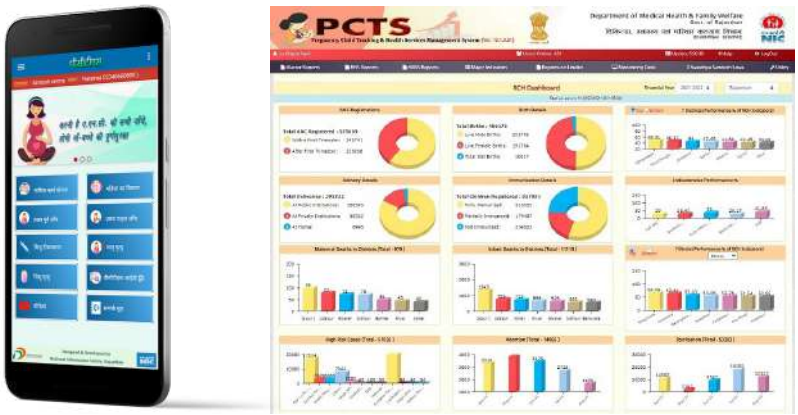
PCTS https://pctsrajmedical.raj.nic.in

Pregnancy and Child Tracking System (PCTS) has become government's arm for delivering services related to reproductive and child health programmes of medical department in Rajasthan. The system is used in providing services related to ANC, delivery, PNC, sterilisation, immunisation, child health, mother's health, institutional infrastructure management etc. It provides for name based tracking of pregnant women and their children. Large scale process re-engineering had seen a successful implementation of the project which covered every government health institution. Today ANMs use PCTS mobile App for first-hand information updation from field. PCTS has also bagged National e Governance Award among other recognitions. The system has been integrated with RCH portal of GoI. With excellent mechanisms for monitoring of individuals, it has been used by Rajasthan government as an effective tool for bringing down Maternal and Infant mortality and improving immunisation and institutional delivery. Integrated with large number of applications, today birth certificate is also provided through PCTS app as it is integrated with Pehchan portal.

AshaSoft https://ashasoft.raj.nic.in

AshaSoft is the one stop solution for the ASHAs (Accredited Social Health Activist) posted anywhere in the state. Facilities includes, performance measurement and Direct Benefit Transfer (DBT) for ASHAs for services provided in 48 activities, Online sanctions by each MoIC (Medical Officer In charge), Payments released by CMHOs using his digital signatures. This Software has also been shared with few other states. Since the performance on each parameter can be monitored through the system, the system has resulted in substantial improvement in service delivery.

▼ Pregnancy and Child Tracking System (PCTS) – Mobile App and Dashboard



"e-Governance in Rajasthan has steadily evolved. With a focus on improving public services delivery, many projects have been implemented harnessing technology. The state has also created IT infrastructure reaching down to the remotest of villages. In this journey of growth, NIC has played a pivotal role in development and implementation of major applications which have given end-to-end solutions to the citizen and the government. Moving with the ever-changing technology and creating new IT enabled facilities, NIC team has collaborated very well with the state government because of which applications developed by state government could be integrated with national portals. It is a pleasure to note that Informatics October 2021 issue is focusing on e-governance initiatives by NIC Rajasthan. I would like to appreciate the efforts and spirit of NIC Rajasthan, and wish them success in their future endeavours."

ALOK GUPTA, IAS
Principal Secretary, IT&C
Government of Rajasthan

Online JSY, Rajshree and ShubLaxhmi Payment System (OJAS)

https://ojspm.raj.nic.in

OJAS is the DBT system for online payments for beneficiaries of various government schemes related with welfare of women and children such as JSY, RAJSHREE & SHUBHLAXMI. All payments of JSY are done online within 48 hours of discharge from hospital. So far approximately Rs. 1820 crore have been transferred to the bank account of more than 1 crore beneficiaries using the system.

Integrated System for Monitoring of PCPNDT Act (IMPACT) https://pcpndt.raj.nic.in

The system helps in effective implementation of PCPNDT Act. Since the system provides powerful surveillance mechanism, it has successfully

▲ Hon'ble education minister Shri Govind Singh Dotasra lanching ShalaSamblan Mobile App at Jaipur.

▲ D-Flow - The Enterprise Framework for Data Management

contributed in curbing girl child foeticide in the state. it has also helped to improve sex ratio at birth in Rajasthan. Online record of every sonography of each pregnant woman is maintained online. Presently the system Covers all 3790+ registered sonography centres (Government and private). Records of more than 2.5 crore sonographies is available online.

Integrated ShalaDarpan

https://rajshaladarpan.nic.in

ShalaDarpan is a comprehensive portal for information related to students, teachers and infrastructure of government schools. This covers all 66 thousand government schools with online information of 91 Lakh Students, 4.5 Lakh Teachers / Staff. The portal caters to various tasks, such as school admission, student academic performance, result preparation, Student Transfer Certificate, Pre-Post Matric Scholarship distribution, State Board Exam Management (5th & 8th standards), Staff recruitment, posting, joining and relieving, Staff Leave & Attendance. With the help of the system, the state has been able to rationalise the deployment of teachers which has resulted in availability of concerned subject teachers in every school. The system is also used for online Annual Performance Report (APR), ACP (Annual Career Progression) of all teachers. The system works as the back-bone for the education department in Rajasthan. All major beneficiary schemes for students are administered through ShalaDarpan.

Private School Portal https://rajpsp.nic.in

Integrated portal for Private Schools of Rajasthan State working as bridge between private Schools and School education department. The portal provides facilities for RTE admissions including Online application, lottery and school allotment, Generation of installment wise automated Claim bill of verified students and Claim reimbursement in School's Bank Accounts, More than 8 Lakh students have been benefitted so far. Payment to participating schools is made online.

GyanSankalp https://gyansankalp.nic.in

This is an online platform for CSR funding, donations and voluntary contributions to raise funds for the schools in Rajasthan. Funding is accepted under various categories such as Support a Project, Donate to a School, Mukhyamantri Vidyadaan Kosh, Adopt a School, etc. More than Rs. 219 Crores have been collected through this portal with the help of around 2.2 Lakh supporters for supporting around 60+ thousands Government school in the state. Tax exemption receipt is generated through the system. Donor may propose / create a project to support any number of selected schools.

OASYS (Online Assembly System) for Rajasthan Legislative Assembly

https://rlaquest.raj.nic.in

OASYS is a workflow-based system for transaction of information between hon'ble members, assembly secretariat, government departments and citizen. All questions and motions are submitted online, after scrutiny the notices are served online to concerned departments, which again reply online along with all annexures. The system has helped in saving a substantial amount of time, effort and paper. more than 1 Crore paper sheets are saved every year. The system is also used for publishing and searching Assembly proceedings online. Starting from the year 1952, proceedings of all houses are available online. The system has been shared and replicated with other states as well.

eMulakat for Prisoners

eMulakaat is implemented under ePrisons project for all Jails of Rajasthan. The system facilitates jail inmates to communicate their family members by video call at home. Approximately 1.25 Lakh eMulakat sessions have been conducted for prison inmates in various jails of Rajasthan.

Quarantine Tracker for COVID

Quarantine Tracker is a mobile based system which is useful in monitoring of quarantined persons. The mobile app tracks the movement of the person who are quarantined and are advised isolation. It provides a monitoring mechanism which ensures that the patient/ person does not move to any other place during the quarantine period and generates alerts for administration. Quarantine Tracker has been implemented in districts.

Rajasthan High Court

https://hcraj.nic.in

Technical services in the judiciary by NIC Rajasthan have been immensely useful for a large section of the society. From High court to District courts, NIC has extended its services at all levels. The Case Information System (CIS 3.1) facilities for Case Filing, Scrutiny, Cause List and Order Preparation available on portal. This has been integrated with National Judicial Data Grid. Case Status, Orders and Judgments are available in public domain. More than 15 lakh judgments of High Court and 10 lakh judgments of subordinate courts are available online. Facility of display board within the court campus and its integration on mobile app is also quite useful for advocates. The Rajasthan High Court mobile app also provides quick access to cases repository which also facilitates advocates and litigants to maintain their case di-

▼ Mobile App of Pehchan

aries in the mobile app.

Vehicle Location Tracking System, (VLTS) for ambulances https://vlts.parivahan.gov.in/rj

VLTS is a real time application for vehicle tracking integrated with National and State Emergency Response System. The system has been implemented for ambulance tracking in Rajasthan. All ambulance vehicles are fitted with VLT device and PANIC button. The system provides for alert dashboard and real time tracking of vehicle status.

Public Distribution System (PDS) https://food.raj.nic.in

A complete supply chain-based system of Public Distribution has been implemented in Rajasthan with end-to-end computerization. All Ration Cards (2.06 Crore) are digitized in the state. Aadhaar seeding is done for 95 % NFSA cards. One nation one card scheme has been implemented in the state. Citizen can apply online for ration card through any eMitra kiosks. Allocation from State HQ to FPS is based on real time information of beneficiaries and stock position at FPS. The system facilitates monitoring of supplies, truck challans, lifting from FCI Godowns, delivery at FPS and receipt acknowledgment by FPS dealers through mobile based service. The system has helped the state in minimizing leakages from the PDS cycle.

Civil Registration System, Pehchan https://pehchan.raj.nic.in

Unified portal for Birth, Death and Marriages Registration in Rajasthan, is the single source of truth for all civil registrations in the state. Used by all 12,500 Registrars and 3000 Sub registrars (Government Hospitals, CHC / PHC), the system is also accessible to 1,600 private hospitals and 80,000 eMitra kiosks. A citizen can also apply online either through the web portal or Pehchan mobile app. Digitally Signed Certificates are generated and delivered to citizens. All certificates have QR code implementation which is useful for insurance agencies and citizens for authentication. So far about 2.27 crore Registrations have been done on the portal. Pehchan is integrated with applications of Medical & Health, Settlement, Palanhar Scheme, Aadhaar and Jan Aadhaar, etc. No manual certificate is being processed in the state.

Rajasthan Business Register https://br.raj.nic.in

Business Register Portal is used for the online registration of Business enterprises and NGOs of Rajasthan. It has been made mandatory in Rajasthan to register on portal for Organized and Unorganized sector. The registration process is having no manual intervention. The system facilitates the government to keep an eye on new business activities and NGOs in the state and it can be an useful tool for the government for planning.

Public Health Engineering Department https://phed.raj.nic.in

NIC is computerising PHED department for Work flow based A & F sanction generation, Monitoring of physical and financial progress of projects, Photographs of work at site can be viewed online, Online stocks of Division stores, Requisition from divisions, Supply order & receipt online, Water quality test reports (Chemical, Bacteriological, Residual Chlorine, etc.), Alerts for water impurities.

Video Conferencing Session of Hon'ble Prime Minister with Hon'ble CM Shri Ashok Gehlot at CM Office, Jaipur

Integrated Works Monitoring System (IWMS) https://rdprwms.raj.nic.in

The system is implemented for rural development department. All civil works are carried out under various schemes using this system. Starting with work proposal, administrative, technical and financial sanction, the system is used for monitoring work execution on regular basis. UC and work completion certificates are also generated with the system. More than 1.3 Lakh works have been sanctioned and monitored through the system, so far. With geotagging, the system also has the facility to upload period photographs from project site. It has been useful in ensuring timely completion of works.

Rajasthan Electricity Regulatory Commission https://rerc.rajasthan.gov.in

NIC Rajasthan has developed Case Information System for the commission in which advocates, organisations and citizen may register online for case filing. Petition may also be filed online with the requisite fee payment. A web portal for the RERC is also been developed and hosted by NIC Rajasthan.

eNagar Suite

This is an integrated Suite of applications for local bodies. The citizen can apply online for land and property mutation, building permission, 90 A conversion, Community centre booking and sale permission. The system also comprises of Document Scanning system, e engineering and e Auction of properties, online accounting, file monitoring, online lottery, court cases monitoring, citizen care centre etc. The system is implemented in few districts. Online delivery of such citizen services has improved transparency and efficiency and has saved lot of hardships for the citizen.

Regional Centre of Excellence for Application Security (RCEoAS)

RCoEAS has been established at Jaipur to cater to application security requirements of applications developed by NIC. The centre caters to eight states viz ; Rajasthan, Gujrat, Maharashtra, Goa, Daman & Diu, Dadra & Nagar Haveli, Madhya Pradesh, Lakshadweep. The centre audits web applications, APIs and mobile applications of these states. It regularly conducts penetration testing in production environment to improve security posture of NIC.

NICCI Chatbot Service https://niccicms.raj.nic.in

NICCI is the smart Chatbot developed by NIC Rajasthan as a generic service, which can be plugged in any portal without any programming. Using proximity rules, bot rules, and language rules NICCI looks for maximum weighted reply. It is also voice-enabled where a user can seek assistance by speaking to the Bot. NICCI is enabled with interfaces in English and Hindi language. NICCI is also equipped with a user friendly Content Management System (CMS) for knowledge enhancement. It is implemented with many portals which also includes portals of other states.

D-Flow- The enterprise Framework for Data Management https://dflow.raj.nic.in

D-Flow is an innovative and generic e-governance tool from NIC Rajasthan. The application is extremely useful in cases where data is to be collected from large number of cascaded field locations either on an ad hoc basis or as a regular schedule. The system permits user at any level to create its own data collection form, name it and circulate it to any number of users for data collection. The form can be scheduled for reporting on one time basis or any frequency of collection, such as one time / weekly / monthly / annually etc. The user is also given the facility to attach scanned sheets which can be merged automatically while compiling the data forms received from various users. Presently implemented in Rajasthan Police department for approximately 2000 users ranging from state level users to the police station level. It is a generic application which can be used by any department without the need of coding and can be rolled out immediately.

Core Infrastructure

NIC Rajasthan is well equipped with state-of-

the-art digital infrastructure to cater to exhaustive needs of the state. More than 5000 NICNET nodes have been established in the state which includes State Secretariat, Collectorates, other government offices and educational institutions etc. HD Video Conferencing facilities have been established in Secretariat, High Courts principal seat Jodhpur and Jaipur Bench, all 33 District collectorates and 35 District Courts. More than 15,000 NIC email accounts are maintained. NIC also maintains more than 100 web portals / applications of Rajasthan state. To cater to the computing requirements, NIC mini cloud has also been established. NIC has also extended its support at state data centre. High speed connectivity has been extended to large number of user departments and educational institutions like IIT Jodhpur, IIM Udaipur, AIIMS Jodhpur, MNIT Jaipur as well as RSDC and RSWAN.

CSI SIG eGovernance Award to Rajasthan Business Register, received by SIO Rajasthan, NIC and Economics and Statistics Department team

Other Important Projects

Project Name	Implementation Status
eTransport	Implemented in State
eHospital	Implemented in AIIMS Jodhpur and National Institute of Ayurveda, Jaipur
Sandes	Implemented in PHED and DoIT&C
Jeevan Pramaan	Implemented and integrated with eMitra
e-Prison	Details of 22 Lakh old inmates and 21,000 current inmates captured. About 9000 eMulakaat done.
e-procurement	More than 1 Lakh tenders floated every month.
Saar	Implemented for 80 Departments
Index of Industrial Production (IIP)	Implemented in the State and index generated
Price Statistics in Rajasthan (PSR)	Implemented in all Districts and Krishi Upaj Mandi Samitis
Rajasthan Agriculture Statistics (RaJAS)	Implemented in all districts
RAJPOSHAN	Implemented up to block level in all districts.
Media Management System	Implemented for DES and NIC Rajasthan
DREAMS	Implemented for Police, Revenue, Transport and Medical department for all field units of these departments in Rajasthan
E Office	Implemented at Rajasthan Legislative Assembly

Important Mobile Apps

App Name	Users
Shala Samblan	Government
Budget Rajasthan	Citizen, Government
Civil Registration System, Pehchan	Citizen
Rajasthan Business Register	Citizen
Pregnancy & Child Tracking System (PCTS)	Government
Rajasthan Legislative Assembly	Hon'ble MLAs, Media and Citizen
RajFood	Government
Rajasthan High Court eservices	Citizen, Advocates
e-Gras	Citizen
eCounselling Assistant	Citizen
Arogya Sathi	Citizen, Government
i-Lens	Government
eSAJAG	Citizen, Government

Accolades

NIC Rajasthan has won many national and state awards for its projects.

- National eGovernance Award for Pregnancy and Child Tracking System (PCTS)
- National e Governance Award for OASYS (Online Assembly System)
- National e Governance Award for Asha Soft
- CSI awards for PCTS App, Price Statistics portal, Civil Registration System, Business Register, Gyan Sankalp portal, Integrated Shala Darpan
- GEMS of Digital India Award for excellence in e-Governance in the field of Finance Sector
- Various other awards such as Skoch Award, Manthan Award, e-India, e-World, eGov Rajasthan also been conferred to different projects of NIC Rajasthan

Way Forward

- Development of AI based systems for the applications related to the sectors of Finance, Medical and Education
- Development of Data Analytics
- Development of mobile applications to help implement m-Governance
- Transition to micro services based architecture in major applications

For further information, please contact:

STATE INFORMATICS OFFICER
NIC Rajasthan State Centre
8318, NW Block, Secretariat
Jaipur, Rajasthan - 302 005
Email: sioraj@nic.in, Phone: 0141-2227992

Tamil Nadu State

A Pioneer in Digital Governance

NIC Tamil Nadu State Centre provides consistent support to the Government of Tamil Nadu, Central Departments and PSU's situated in Tamil Nadu, in their endeavours to fully develop e-governance solutions, specifically citizen centric solutions, for the benefit of the common man, and to ensure improvement in Government services and wider transparency of both state and central Governments.

K. Srinivasa Raghavan
Dy. Director General & SIO
ks.raghavan@nic.in

Beena C
Sr. Technical Director
beena.tn@nic.in

Tamil Nadu, located in extreme south India, is bounded by the Indian Ocean to the east and south and by the states of Kerala to the west, Karnataka to the northwest, and Andhra Pradesh to the north. The tourism industry of Tamil Nadu is the largest in India, with an annual growth rate of 16 percent. The region was ruled by several regimes, including the "three crowned rulers" – Chera, Chola and Pandyan states, which shape the region's cuisine, culture, and architecture. The economy of Tamil Nadu is the second-largest in India. Tamil Nadu is the most urbanised state in India, and one of the most industrialised states; the manufacturing sector accounts for more than one-third of the state's GDP.

NIC Tamil Nadu has provided consistent support to the Government of Tamil Nadu, Central Departments and PSU's situated in Tamil Nadu, since 1988 in their endeavours to fully develop e-governance solutions for the benefit of the common man. NIC Tamil Nadu has provided NICNET connectivity, more importantly in recent days, high speed Gigabit Network National Knowledge Network (NKN) connectivity to IIT's, various premier Universities in Tamil Nadu and reputed Institutions of National importance for research purposes, apart from Government of Tamil Nadu and its State Data Centre Operations for day to day activities. NIC Tamil Nadu has specialised divisions for Mobile Development and Open Source Technology Group (OTG) for all open source development & research activities across the country.

ICT Initiatives in the State

Vahan & Sarathi https://parivahan.gov.in/

Web based version of Vahan and Sarathi (version 4) has been implemented successfully in all 145 RTO Offices located across Tamil Nadu.

m-Vahan (Fitness App)

m-Vahan App has been successfully implemented in all 145 RTOs of Tamil Nadu for conducting Fitness Check by authorized Motor Vehicle Inspectors. An average of 5000 to 10000 FCs being done every Month.

e-Challan

e-Challan is a Centralised Application consisting of Android based Mobile App and web Application. Mobile App is used by the Enforcement Officials of Transport Department and Traffic Policemen for booking Challan against Traffic Violators. More than 14 Lakhs Challans being booked every month by the enforcement Officials of Police and Transport Departments and an average fine amount of Rs 5 Crore being collected every Month.

"NIC Tamil Nadu State has been the technology partner with the Government of Tamil Nadu in all the citizen centric applications. The State achieved laurels in many e-initiatives, thanks to NIC for technical support. Revenue Services, Social Security Schemes, Grievance Day Petition, MIS PDL, DBT, e-Office are some of the important web based software applications with which the citizens, business community and Government at large are benefitted. The team at NIC Tamil Nadu has vast domain knowledge in all key areas of Government and the technical competency to offer solutions. I am very happy to note that Informatics October 2021 is showcasing the e-initiatives of NIC in Tamil Nadu State. I wish the NIC Tamil Nadu team the very best in all their future endeavours and look forward to their continued support for the State in e-Governance initiatives."

THIRU K. PHANINDRA REDDY, IAS
Principal Secretary Revenue Administration, Government of Tamil Nadu

Traffic Violators can pay the fine amount through Net banking, Debit Card, UPI and post Office.

Intelligent Traffic Management System (ITMS)

ITMS System is app cum web application for booking challans for the traffic violations on road/ traffic signals junctions through ANPR Cameras / ANPR based CCTV Cameras, installed at various locations, for the Police Department.

The violations captured through different media are processed in the ITMS system and challan issued to the violators. The system is integrated with Vahan and Sarathi to get the

Dashboard showing the statistics on Vehicle registration and revenue collection

details of the vehicle owner /Licence holder.

The ITMS system has been implemented in the major traffic signals of the following districts of Tamil Nadu :

- Coimbatore: 17 Traffic Signal Junctions
- Salem City: 1 Traffic Junction
- Tiruchirappalli: 5 Traffic Signal Junctions
- Chennai: 2 Traffic Signal Junctions

Implementation of ITMS in other Traffic Junctions of remaining Districts are in progress.

Computerisation of Tamil Nadu Local Body Elections

NIC TN helped in the Computerisation of Tamil Nadu Local Body Elections by developing modules for Preparation of Photo Electoral Roll for 6.5 Crore Voters for Tamil Nadu Local Body Elections, Randomization of Polling officials (8 Lakh) for polling duty by collectors, Randomization of EVMs for Urban Local body Election. Nomination details entry of Candidate, Online Result Dissemination.

Photo Electoral Roll

Integrated Temple Management System (ITMS)

https://hrce.tn.gov.in

An Integrated Temple Management System (ITMS) has been designed and developed for Hindu Religious and Charitable Endowments (HR & CE) Department to monitor the complete information about the Temples, its attached properties, the revenue earned from various sources, physical and financial progress of New temple and Temple Renovation works (Tirupani), Budgets, Audits, provide various online Temple Services to Devotees, etc.

ITMS is a unique Product that can be replicated in other States / UTs. Comprehensive Bilingual Web Portal developed completely using Open Source Tools using PHP and PostgreSQL. ITMS has been replicated in Puducherry UT for 233 Temples of HRI & Wakf Board (URL is https://hri.py.gov.in)

Karnataka Hindu Religious Institutions and Charitable Endowments Department has accorded in principle approval for implementation of ITMS in the State of Karnataka.

Discussion with Uttar Pradesh is in progress.

Benefits

- ITMS portal provides services to all the Devotees / Citizens and the officials with its G2G, G2B and G2C Services.
- Dynamic Websites of 44,000+ Temples in a single Portal.
- eServices : Online Ticket Booking for Darshan during Covid19 strictly on SOP.
  - Online Collection: Rs.5.90 crores through Online Darshan Tickets and more than Rs.1.25 crore towards donation through ePayment Transactions with 100% reconciliation
- Modular Dashboard Services
- GIS Integration
- Mobile Apps developed:
  - To capture the Geo-location of Temples across the State by Temple Officials
  - QR Code verification of Online Tickets for Temple Officials
  - App for dissemination of Temple Information such as Temple Deities, timings

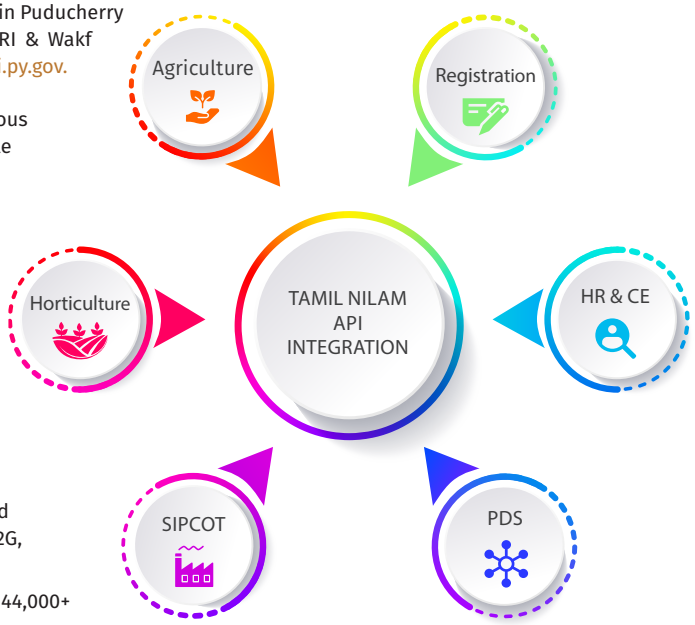
TamilNILAM

https://tamilnilam.tn.gov.in/Revenue/

Web Based TamilNILAM (Tamil Nadu Information system on Land Administration and Management) is role based, work flow based application which aims to modernize management of Land Records, minimize scope of land/ property disputes, enhance transparency in the Land Records maintenance system. The ultimate objective of Land Records Computerisation is Automatic Mutation and conclusive Titling which was enabled from 23rd February, 2021.

Benefits

- The app facilitates instant generation of Record of rights without any manual intervention.
- Citizen view of ROR is available in 'Any Time Any Where' citizen Portal
- The Web Based TamilNILAM is implemented in 294 Taluks from October 2014



Land Record secured Data Sharing across various online applications

▲ The Integrated Temple Management System won award under Exemplary Product category from Digital India Awards 2020 from the Hon'ble President of India

- Total Number of Application Processed 1,11,25,385
- Nearly 6000 Patta transfers are done on a daily basis using this application.
- RoR Viewed (Daily)
  - Chitta: 2 Lakhs
  - Register: 1.5 Lakhs
- No. of Land Parcels 4,00,70,973
- No. of Land Owners 4,78,08,674

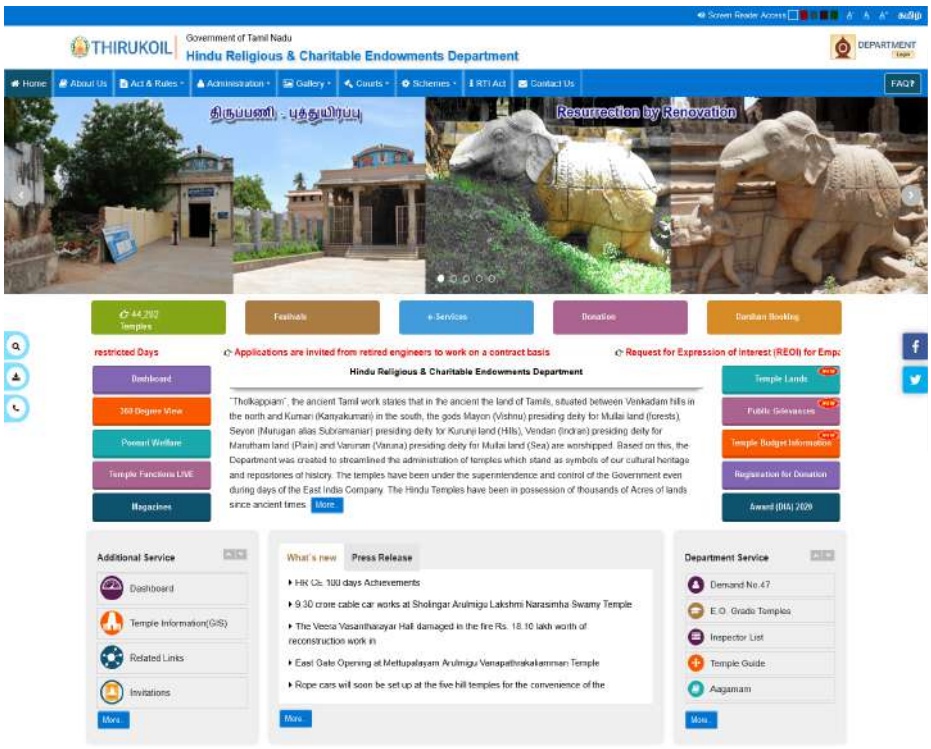
Crime & Criminal Tracking Network & Systems (CCTNS)

https://eservices.tnpolice.gov.in

Crime and Criminal Tracking Network & Systems (CCTNS) aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing. CCTNS is intended to ensure that Police maintains all its Crime and Criminals data through an online system and to provide Citizen access to Police Services online. CCTNS is a Mission Mode Project under the National e-Governance Plan (NeGP) of Govt. of India. The State Crime Records Bureau (SCRB), is the nodal agency for implementing the CCTNS project and NIC is acting as the Application Development Agency.

The CCTNS system is integrated with various pillars of MHA/ NCRB/ ICJS to exchange information. It is successfully integrated with NCRP Portal (Cyber Crime), ICJS, NAPIX (BharatAPI), iRAD, eTaal, CSC, UMANG and FRS Apps.

▼ Home Page of Integrated Temple Management System



Benefits

- This service of CCTNS project shall enable Citizens to send their requests for services to Police through online citizen service portal and track status of registered service requests
- The web based workflow system facilitates the officers of the Tamil Nadu Police, right from the Police station to the top level officials to process the online applications, monitor and record the case status and generate various MIS reports on the CCTNS data
- The TNPolice Citizen mobile app facilitates the citizens in filing the online complaints and view the status of FIR/CSR and verify the vehicle details
- The Officers Mobile App facilitates them in viewing FIR/CSR details, monitoring the case progress, Session case trail and NBW pending cases etc. The Mobile App for SI & SSI officers facilitates them in Accused name search, Vehicle search, Scene of crime details and IMEI search

Common Integrated Police Records Updation System (CIPRUS)

CIPRUS is a comprehensive software solution in monitoring the day-to-day activities of the Police Station. This work-flow and role based application has the modules for Case Registration, Investigation, Prosecution and Admin/Staff Management. It provides a dashboard with

major information for Station House Officer (SHO) and facilities to generate various MIS reports. The DMU (Data Migration Utility) helps in migrating/ transferring the Police Station level CIPRUS application data to the National level Core Application Software (CAS) maintained by National Crime Records Bureau (NCRB). The CIPRUS Application is successfully implemented in all 63 Police Districts across all 1952 Police Stations including Special Units. On an average, 75,000 FIRs and 80,000 CSRs are getting registered monthly in the state.

Online Examination System (OESNIC)

An examination portal for conducting both descriptive and Objective type questions. Salient features are Multilingual Support, Multi Tenant Architecture, Mobile Friendly Responsive Web Design. More than 150 Exams are conducted for NIC, other Central and State Government Departments.

▲ OESNIC interface

Monitoring of Swachh Bharath Mission Activities through Online Application and Mobile App

An Integrated Monitoring System for Swachh Bharath Mission Activities has been developed by NIC Tamil Nadu State Centre for Rural Development and Panchayat Raj Department, Government of Tamil Nadu. A web based Software has been developed for monitoring the activities of Thooimai Kaavalars (Swachhta Dhoots – Clean Village campaigners) numbering about 13,000.

e-Taxation - Directorate of Town Panchayats, Tamil Nadu

Tax collection modules related to Property Tax, Water charges, Profession Tax, Non Tax and Trade License for all 528 Town Panchayats have been developed. Salient features include Masters and Business Logic is Customizable at local Town Panchayat, Multilingual Support. Service requests can be handled through a customizable workflow methodology.

Department of Industries and Commerce

New Entrepreneur-Cum-Enterprise Development Scheme (NEEDS)

New Entrepreneur–cum-Enterprise Development Scheme (NEEDS) was introduced from the year 2012-13 onwards to assist the educated youth to become first generation entrepreneurs. The objective of the NEEDS system is to enable the Online Filing of NEEDS Application and to computerize the entire flow involved in the processing of NEEDS Application.

Benefits

- Educated youth will be assisted in getting entrepreneur training, preparing their business plans, tie up with financial institutions to set up new business ventures and assist to avail terms loans from Banks/ Tamil Nadu Industrial Investment Corporation (TIIC)
- So far 25,623 Applications received on NEEDS and 6,506 Applications Sanctioned by Bank

Unemployed Youth Employment Generation

A web based system for online filing of UYEGP and to manage the entire process flow involved has been designed, developed and implemented.

Benefits

- Applications received on UYEGP: 65,094
- Applications Sanctioned by Bank: 17,316

Integrated Court Case Monitoring System (CCMS)

The main objective of CCMS is to establish a new management system and procedure to expedite resolution of all cases and to actively monitor the cases in which Government is a party, till timely conclusion.

Benefits

- Enables fetching the details of Court cases filed before High Court of Madras on real time basis and that helps the Government for responding the directions of the Court by improving management of Court Case in a systematic way
- Ensure the filing of Counter Affidavit and necessary follow up action to monitor the Court cases effectively
- Provisions for fetching the Next Hearing Date, Judgements/Orders, etc. will help the Department/ HODs concerned, to get prepared for taking necessary action to avoid the disdain of Court if any

TN-IAS Intra

https://agaram.tn.gov.in/ias

TN-IAS Intra Application is a Computer based system for maintenance of the Service Register to provide an accurate picture of man power, service particulars, deputation details, etc., It has now been reengineered, so that the application software will get merged with the existing Application for the Administration of Carded Civil Servants (IAS Officers) in the State to accommodate further requirements in tune with emerging technical advancements and support in terms of current technology. Revamping the IAS Intranet envisages bringing out the automation of process flow in e-Tour, e-leave, e-Foreign Tour and e-LTC modules of the system.

RTI Online Information System

RTI Online Information System is an ICT based tool that facilitates/ empowers the citizens to File RTI Requests online, File first Appeal online, Track and Monitor the status and Receive Reply online. It facilitates the Departments of Tamil Nadu to e-Manage & e-Monitor the RTI request & First Appeal.

Benefits

- Monitoring at the level of Nodal Officer for all PIOs and FAAs
- System maintains the history of all the actions chronologically in the life cycle of a RTI Request and first appeal

▼ Property Tax Receipt

Do not waste water, use it economically.

Achirapakkam Town Panchayat, Chengalpattu District

Receipt of Property Tax

Assessment Number : 2468 | Name of the Owner : M.Pathrilal

Receipt Number : 2021-2022/200046/1/672 | Date : 22-09-2021 02:01 PM

Street Name : Door No-7, ST-01-(ACHARAPAKKAM WEST MADA STREET) | Ward No : WD-13

Mode of Payment : Cash | Usage Type :

Demand detail	Taxation period	Amount in Rs			Note
		Arrears Amount	Current	Total	
Property demand	2021-2022 (1st Half)	0	79.00	79.00	
Property demand	2021-2022 (2nd Half)	0	79.00	79.00	
SWM demand	2021-2022 (APRIL-MARCH)	0	24.00	24.00	
			Total	182.00	

Rupees(₹) :One Hundred and Eigthy-Two

kpmtpadmin kpmtpadmin

Bill Collector

Executive Officer
Achirapakkam Town Panchayat

▲ Dashboard of Secretary level Login

- Citizen can track the status of RTI request or first appeal

eGov Application for Department of Ex-Servicemen

https://esmwel.tn.gov.in/

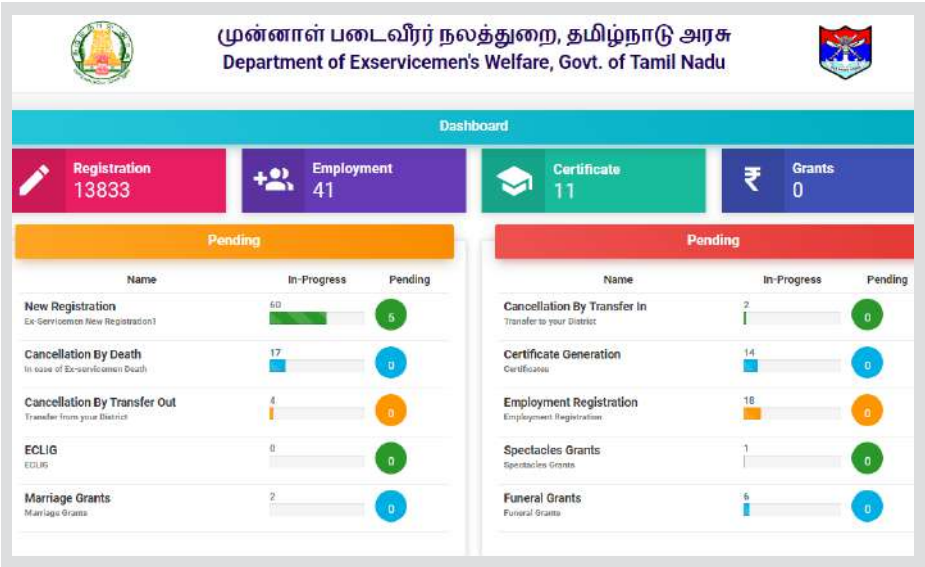
The Department of Ex-Servicemen's Welfare is responsible for resettlement of Ex-Servicemen, family and of the families of serving Defense Personnel in the State. Major Activities of the Department are Registration of Ex-Servicemen, Employment related activities, implementing various welfare schemes like grants, etc. and Miscellaneous activities related to Ex-Servicemen.

It also covers activities like Registration of Employment, Generation of Primary and Secondary Employment Card, Issue of Priority Certificate, Employment Renewal, Modification, Add Qualification, Add Priority and Remove from Live. This application is being replicated in Chhattisgarh.

Online Contributory Pension Scheme (CPS)

A complete system to maintain and process the CPS details of the State Government Employees recruited on or after 01/04/2003. It is a web based system for carrying out the complete workflow involved in the processing of contributions under the Contributory Pension Scheme (CPS).

▼ Dashboard depicting ex-servicemen activity details



Benefits

- Total No. of S1 Forms filed Online: 2,24,955
- No. of Applications Approved & Allotted: 2,21,511
- No of Application Returned back to DDO: 657
- No of Application yet to be processed: 2,787
- CPS Account slip for the Financial Year 2019-2020 disseminated for 4,97,894 Subscribers

Visit of VIPs to NIC State Office or NIC Events

- The third round of online auctioning of the gift items received by our Hon'ble Prime Minister is conducted from 17-Sep-2021 to 7-Oct-2021 through the portal https://pmmementos.gov.in developed by NIC. The gift items include sports gear and equipment of the medal-winning Olympians and Paralympians. The proceeds of this auction will go to the 'Namami Gange' initiative
- Hon'ble Chief Minister, UP presided over 18th CSI SIG eGovernance awards 2020 function held on 12.02.21 at Lucknow and conferred Award of Excellence to Central Public Procurement Portal and PM Mementos Portal
- Chief Minister of Tamil Nadu launched 'Auto Mutation of Land Records' on 23rd Feb 2021

Accolades

- NIC Tamil Nadu won gold award under Excellence in Digital Governance – State/ UT category from Digital India Awards 2020 from the Hon'ble President of India
- The Integrated Temple Management System won silver award under Exemplary Product category from Digital India Awards 2020 from the Hon'ble President of India
- Government eProcurement System of NIC © (GePNIC) application won silver award for NIC Data Quality Challenge
- "Mobile App as a Service for District Administration" developed by DIO Nilgiris, won the Best Mobile App under Innovation Category competing more than 400 apps developed across the country

Way Forward

Dedicated officials at State and District centres work together, discover ideas to drive innovative solutions and provide better next-generation digital services for state and central Government.

For further information, please contact:
STATE INFORMATICS OFFICER
NIC Tamil Nadu State Centre
E2A, Rajaji Bhavan, Besant Nagar, Chennai
Tamil Nadu - 600 090
Email: sio.tn@nic.in, Phone: 044-24902580

Faridkot District, Punjab

Transforming the Rural District into Advance Digital One

Since its inception in late 80's, the District Unit is a pioneer in designing, developing and implementing many e-Governance Projects with an objective to use electronic means to support and stimulate good governance. NIC Faridkot is instrumental in rolling out the ICT awareness in the district for greater transparency and efficiency leading to governance for the people, by the people. Now NIC Faridkot is moving ahead with m-Governance and implementing innovative technological solutions for citizen-centric services and promoting Digital India Programme for easing the lives of citizens.

Ajay Rampal
Dy. Director General
& SIO
sio-punjab@nic.in

Anil Katiyar
Scientist-C & DIO
katiyar.anil@nic.in

Faridkot is a royal and historic city located in the south-western part of Punjab. The district is named in the honour of the revered 13th-century Sufi saint, Baba Fariduddin Masud Ganjshakar. Population of district is 6 lakh. The Gurudwara Tilla (Chilla) Baba Farid, Gurudwara Godari Sahib, Royal Palace, Clock Tower and Bir are some of the renowned historical places located in the district. The district houses State Medical University Baba Farid University of Health Sciences and also is a Divisional Headquarters.

ICT Initiatives in the District

M-Nivaran

The Mobile Based Citizen Centric Solution, M-Nivaran was designed to provide an umbrella platform starting from panic button for the females in danger and to all Government Popular Schemes, Grievances, Janbhagidari (helped administration by civic participation) to Covid Crises Management including Vaccination, Covid Dashboard, and real time update to the citizens about various restrictions imposed during partial lockdown etc.

Modules of M-Nivaran App

Other Key Initiatives

Covid-19 Management MIS

NIC Faridkot, under the leadership of Sh. Kumar Saurab Raj, IAS developed and implemented Online portal developed to ensure smooth management of demand and supply chain.

Modules of Covid Management MIS

Automated mechanism created to impart information about lockdown/ curfew/ containment zone was ensured.

SMS based information dissemination module was developed for migrant labour to get accurate information.

All district level meetings were organized through virtual mode to avoid gathering of officers.

Besides the technical support, donations worth ₹ 75 Lakh were collected in in-kind forms and ensured to reach the same in write hands and acted as a Central Custodian for all Covid-19 donations and its disbursement.

Drug Abuse Study MIS

An online portal was developed and study has been made at all OOATs Clinics of District. Report was prepared after analyzing Socio- Economic, Demographical Parameters data to conclude on the factors for drug addiction and submitted to state government to fight with Drug Maniac.

Baba Farid Aagman Purav

To strengthen the Deputy Commissioner vision to conduct "feast" according to world class standards, ICT is widely used. Over 10 lakh people visited the feast.

NIC-Wi-Fi

In one of the major Step towards Digital India, the outstanding initiative of implementing High Speed NIC Wi-Fi services in all the offices of

Our recent innovation the Mobile Based Citizen Centric Solution, M-Nivaran was launched to provide an umbrella platform to touch every aspect of citizens needs starting from panic button for the Citizens in danger, to all government popular schemes, grievances, suggestion, Janbhagidari to Covid crises management including vaccination, Covid dashboard, and real time updates to the citizens.

I congratulate the entire team of NIC, Faridkot who have been working tirelessly and relentlessly providing sustainable support and services to District Administration and I hope to carry forward e-Governance to reach at the unreached in the district.

VIMAL KUMAR SETIA, IAS Deputy Commissioner, Faridkot, Government of Punjab

NIC Faridkot has been instrumental in prevailing and leading the pace of e-Gov activities in district. One of these innovations was launch of High Speed NIC Wi-Fi services in complex, which was first of its kind in entire state. This endeavor has ensured seamless connectivity to district officials/general public anywhere and anytime within premises and enable them to access E-Governance application through Wi-Fi enabled devices

RAJIV PRASHAR, IAS Special Secretary, Transport, Government of Punjab

During high times of Pandemic, Faridkot is one of the districts where IT has made inroads down to the grass roots level which needs to be highlighted for meeting people's aspirations.

To ensure access to essential items to each household in district, grocery/food/transportation facility for migrant labourers, ensuring essential movement during curfew/lockdown, Technology based Framework consisting of Modules Online Demand Supply Portal, e-Pass, Migrant Labourer Transportation SMS Service, Online system for Sector Magistrates for ensuring door to door ration supply has helped immensely to manage implement monitor and control the situation. During my tenure as Deputy Commissioner every other day we do excellent work with the such IT based Solutions of NIC Faridkot.

KUMAR SAURABH RAJ, IAS Deputy Commissioner, Barnala, Government of Punjab

▼ Awarded by Shri Sadhu Singh Dharmsot, Hon'ble Cabinet Minister on 26th januay 2020

the district which makes District Faridkot to be the second district in entire country to have it implemented.

NIC Faridkot has integrated with District NOC of NIC for enhanced bandwidth of 34 Mbps. The Wi-Fi connectivity at complex has extinguished old LAN structure and also act as a secondary link, results in saving revenue in terms of Broadband bills etc.

Other Implemented Projects

- eOffice, iHRMS ,NDAL, IVFRT, RCMS, IFMS, VMS, NGDRS, VAHAN & SARTHI, E-Abkari

Events organized

- National Teacher's Award ceremony (Chief Guest: Hon'ble President of India) held virtually using NIC-VC facility
- Visit of Smt. Vini Mahajan IAS, Chief Secretary, Government of Punjab on June 2021
- Visit of Shri S. Rana Gurmeet Singh Sodhi, Minister of Sports, Govt. of Punjab on 26th januay 2020 (Republic Day celebration)
- Visit of Shri Hussan Lal, IAS, Principal Secretary to Chief Minister, Govt. of Punjab

Accolades

- DGMC Bronze Award for M-Nivaran Mobile App
- Award by Hon'ble Cabinet Minister, Shri Sadhu Singh Dharmsot on 26th januay 2020 (Republic Day celebration)
- Award for best Departmental Services

▼ Awarded "Bronze" for M-Nivaran Mobile App in DGMC by Dr. Neeta Verma, DG, NIC

Way Forward

Abreast with the advancements in various technologies, NIC Faridkot is spearheading to leverage the potential of Digital Twins, Blockchain, IoT, Augmented Reality and Cloud Application. Focusing on solutions based on mobile app, the upcoming project is modular M-Nivaran. Other initiatives taken are IHRMS & Attendance system.

For further information, please contact:
DISTRICT INFORMATICS OFFICER
Room No 232-235, First Floor
Mini Secretariat Faridkot
Punjab - 151203
Email: punfdk@nic.in, Phone: 01639-250659

Mainpuri District, Uttar Pradesh

The haven for migratory birds showcases its marvelous use of ICT for e-Governance

Since its inception in 1989, National Informatics Centre (NIC), Mainpuri has played a pivotal role in implementation of various ICT Projects in the district. NIC is playing key role in extending technical expertise to District Administration in ICT initiatives and implementation of various G2C, G2G and G2E projects. Dr. Neeta Verma, Director General NIC awarded NIC, District Centre Mainpuri with certificate of commendation for the development of cross platform mobile app "m-Nirikshan" under the National level challenge- District Governance through Mobile Challenge (DGMC).

R.H. Khan
Dy. Director General
& SIO
rh.khan@nic.in

Mayank Lal Sharma
Scientist 'C' & DIO
mayank.sharma@nic.in

Mainpuri district is one among the 75 districts Uttar Pradesh state. The district is famous for its more than a dozen wetlands and bird sanctuary having biggest population of Sarus cranes in India. Mainpuri's Sarus circuit tourism is a major attraction for eco-tourists. In the District, there is Saman Bird Sanctuary (designated as a protected Ramsar site) which is a place of stay of the world-famous Siberian Crane which comes here in its migration cycle and stays here for 3-4 months during November to February. Mainpuri is also well known for its TARKASHI handicrafts.

ICT Initiatives in the District

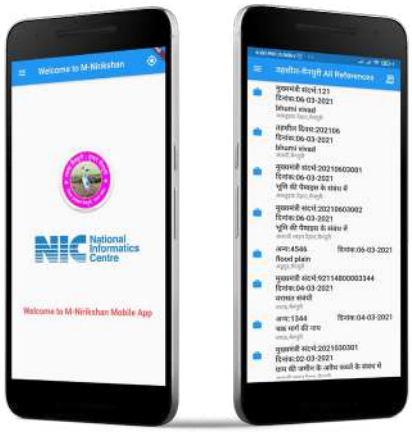
"m-Nirikshan" Mobile App

"m-Nirikshan" mobile app aims to improve quality in public grievance redressal system by expediting complaint transfer and real time GPS based grievance redressal. The Mobile App was designed and developed by NIC Mainpuri (U.P) under District Governance Mobile Challenge (DGMC).

Using this "m-Nirikshan" mobile app, the district and tehsil administration can monitor the field visit of the lekhpal/ field officers so that transparency can be bring out among citizens and district administration.

Advantages of "m-Nirikshan" App

- Field employees will get enough time to resolve the complaint.
- They will be able to ensure his presence with photographs, which will prevent the repetition of false complaints.



▲ "m-Nirikshan" Mobile App interface

"NIC, Mainpuri has played a pivotal role in implementation of various government schemes and channelizing the power of e-Governance to the masses. NIC, Mainpuri is providing ICT support and services to various departments of District Administration. NIC helps the District Administration through a mobile app "m-Nirikshan" to improve the quality in existing public grievance redressal system. I sincerely appreciate the efforts put in by the NIC District Unit in promoting Sarus Circuit Tourism of District Mainpuri. The District Administration also appreciates NIC for providing round the clock ICT support during Covid-19 Pandemic period."

MAHENDRA BAHADUR SINGH, IAS
Collector & District Magistrate
District Mainpuri

- Now redressal of any complaint will be possible through the app only when the concerned employee will go to the site and upload the disposal report along with his location and photographs.
- In this way quality disposal of complaints will be ensured which will further improve the existing Public Grievance Redressal System of state.

Sarus Circuit Tourism, District Mainpuri

To promote District Mainpuri's Sarus Tourism, NIC Mainpuri designed and developed a responsive website http://sarustourism.in/, along

▲ Sarus Circuit Tourism, District Mainpuri website

▲ Hon'ble Minister of UP, Shri Girish Yadav presenting award to DIO, NIC Mainpuri for the outstanding contributions in UP Farmers Loan Waiver Scheme

with done commendable job in publishing Sarus Circuit wetlands' locations on Google Map. The website is also listed under important websites column on UP Tourism web portal.

Other Key Initiatives in the District

NIC Mainpuri has been successfully carrying out all the major mission mode projects (MMPs) of national and state level, which include e-District, Land Records Computerization-UPBHULEKH, Integrated Road Accident Database, Jansunwai Portal, CM Help Line 1076, Anti Bhu Mafia Portal, Rahat Portal, e-Pass application during Covid-19 lockdown, e-Lottery for liquor shops, e-Public Distribution System, PRoperty Evaluation & RegistratioN Application, Social Welfare Schemes, U.P. Rani Laxmi Bai Mahila Evam Bal Samman Kosh, Arms Licensing Computerization System, Dashboard for Analytical Review of Projects Across Nation (DARPAN), Inter-operable Criminal Justice System (ICJS), e-Prosecution, training and support in implementation of various government schemes like UP Farmer Loan Waiver Scheme, various applications on Board of Revenue Portal like revenue court computerization system (RCMS), General Elections related Applications & Mobile Apps etc. Mainpuri is also the first district in Uttar Pradesh, to migrate its district website (https://mainpuri.nic.in/) on Secure, Scalable & Sugamya Website as a Service (S3WaaS) platform. Conducted VC sessions on regular basis and various VVIP's live webcast arrangements at various locations in the District. During COVID-19 lockdown period, to minimize the physical interaction among the officers, conducted VC sessions using NIC Vidyo Desktop VC solution. Necessary IT support is being provided to the District Administration in recruitment process of various posts under different departments. Computer awareness cum capacity building training programs are also undertaken regularly to facilitate effective implementation of e-Governance projects / applications.

Events

Launch Event of "m-Nirikshan" mobile app

"m-Nirikshan" mobile app is launched by Shri Mahendra Bahadur Singh, IAS, District Magistrate, Mainpuri on 4th March 2021.

Accolades

- Dr. Neeta Verma, Director General NIC awarded District Mainpuri with certificate of commendation for development of cross platform mobile application "m-Nirikshan" under DGMC on date 28th May 2021.
- Hon'ble Minister of UP, Shri Girish Yadav present award to DIO, NIC Mainpuri for the outstanding works & contributions in UP Farmers Loan Waiver Scheme implementation in District Mainpuri.
- Shri Pramod Kumar Upadhyay, IAS, Former District Magistrate present award of appreciation in form of Demi Official letter to DIO, NIC Mainpuri for the outstanding and extended IT support in Lok Sabha General Election 2019.

▲ Certificate of Commendation

▼ Shri Mahendra Bahadur Singh (IAS), DM Mainpuri launching "m-Nirikshan" app

Way Forward

In order to realize the dream of 'Digital India', NIC Mainpuri is committed to provide efficient and total ICT support to the District Administration and field level offices of the State and Central Governments in the District. The dedication and zeal towards achieving excellence in the area of ICT has made NIC Mainpuri a household name in the district.

For further information, please contact:
DISTRICT INFORMATICS OFFICER
NIC - Mainpuri District Centre
Collectorate Campus, Mainpuri
Uttar Pradesh - 205001
Email: upmai@nic.in, Phone: 05672-234183

Cyber Security

19 ModSecurity

22 Leveraging Big Data and AI-ML for Security Analytics

25 Defense in Depth through Layered Security

28 Endpoint: The Start Point of Cyber Security

30 DevSecOps

32 Preventing Cyber Crisis

34 Automated Vulnerability Analysis & Reporting Tool

36 Security Audit, Web shell, and OWASP-A9

ModSecurity

Open Source Web Application Firewall

With the increasing threats and attacks on web applications, organizations require a more effective concept of web application security. Web Application Firewall (WAF) is such a concept that can be used to prevent various threats and attacks on web applications. WAF has the ability to filter packets, block malicious HTTP requests, and also do logging. The open-source WAFs are highly flexible and customizable. With full access to the source code, Open source WAF offers the freedom to WAF administrators, web administrators and developers to apply rules as per individual application and provides flexibility to customize and extend the tool itself to fit as per application requirements. ModSecurity is a popular open source Web Application Firewall.

ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. It provides protection from a range of attacks against web applications such as Cross Site Scripting (XSS), SQL Injection, Cross Site Request Forgery, Local File Inclusion, Path Traversal, Session Fixation etc. and allows for HTTP traffic monitoring, logging and real-time analysis. ModSecurity excels at virtual patching contributed by its reliable blocking capabilities and the flexible rule language that can be adapted to any need.

Ratnaboli Ghorai Dinda
Scientist-G & HOG
(Application Security)
ratnaboli@gov.in

R. K. Raina
Scientist-F
rk.raina@nic.in

Rajeev Kumar Yadav
Scientist - B
yadav.rajeev@nic.in

ModSecurity gives access to the HTTP traffic stream in real time, along with the ability to inspect it. It can be deployed in embedded mode or in reverse proxy mode. ModSecurity excels at virtual patching because of its reliable blocking capabilities and the flexible rule language that can be adapted to any need. ModSecurity works with OWASP ModSecurity Core Rule Set (CRS), CRS is a set of generic attack detection rules for use with ModSecurity or compatible web application firewalls. The CRS aims to protect web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts. ModSecurity along with CRS provides protection against many common attack categories, including SQL Injection, Cross Site Scripting, Cross Site Request Forgery, Local File Inclusion, Open Redirect, Insufficient Session Expiration, Path Traversal etc.

Features/Functionalities of ModSecurity

ModSecurity employs a variety of methods to protect websites. Following is a list of the most important usage scenarios for ModSecurity:

Real-time application security monitoring and access control

At its core, ModSecurity gives us access to the HTTP traffic stream in real time, along with the ability to inspect it. This is enough for real-time security monitoring. ModSecurity's persistent

storage mechanism enables users to track system elements over time and perform event correlation. Users can block reliably, if they so wish, because ModSecurity uses full request and response buffering.

Virtual patching

Virtual patching is a concept that addresses vulnerability mitigation in a separate layer, in which you get to fix problems in applications without having to touch the applications themselves. Virtual patching is the quick development and short-term implementation of a security policy meant to prevent an exploit from occurring. The resulting impact of virtual patch is that, while the actual source code of the application itself has not been modified, the exploitation attempt does not succeed. ModSecurity excels at virtual patching because of its reliable blocking capabilities and the flexible rule language that can be adapted to any need. Virtual patching is, by far, the activity ModSecurity offers that requires the least investment, is the easiest to perform, and that most organizations can benefit from straight away.

Full HTTP traffic logging

Web servers traditionally do very little when it comes to logging for security purposes. They log very little by default, and even with a lot of tweaking we can't get all the data that we need. ModSecurity gives us the ability to log everything, including raw transaction data, which is essential for forensics. In addition, we get to choose which transactions are logged, which parts of a transaction are logged, and which parts are sanitized. As a bonus, this type of detailed logging is also helpful for application troubleshooting—not just security.

Web application hardening

One of important uses for ModSecurity is attack surface reduction, in which we can selectively narrow down the HTTP features we're willing to accept (e.g., request methods, request headers, content types, etc.). ModSecurity can assist users in enforcing many similar restrictions, either directly or through collaboration with other web server modules. For example, it's possible to fix many session management issues, as well as cross site request forgery vulnerabilities.

Deployment Options

ModSecurity supports two deployment options: embedded and reverse proxy deployment. Users can pick the most appropriate option based on their goals, requirements, and situation. There are advantages and disadvantages of both options:

Embedded

The embedded option is a great choice for those who already have their architecture laid out and don't want to change it. Embedded deployment is also the preferred option if we need to protect hundreds of web servers. In such situations, it is impractical to build a separate proxy-based security layer. Embedded ModSecurity not only does not introduce new points of failure, but also it scales seamlessly as the underlying web infrastructure scales. The main challenge of embedded deployment is that server resources are shared between the web server and ModSecurity.

Reverse proxy

Reverse proxies are effectively HTTP routers, designed to stand between web servers and their clients. When we install a dedicated reverse proxy web server and add ModSecurity to it, we get a "proper" network web application firewall, which we can use to protect any number of web servers on the same network. This mode gives us complete isolation from the systems (e.g. web servers/applications and databases) we are protecting. On the performance front, a standalone ModSecurity installation will have resources dedicated to it, which means that we will be able to do more (i.e., have more complex rules). The main disadvantage of this approach is the new point of failure, which will need to be addressed with a high-availability setup of two or more reverse proxies.

Transaction Lifecycle

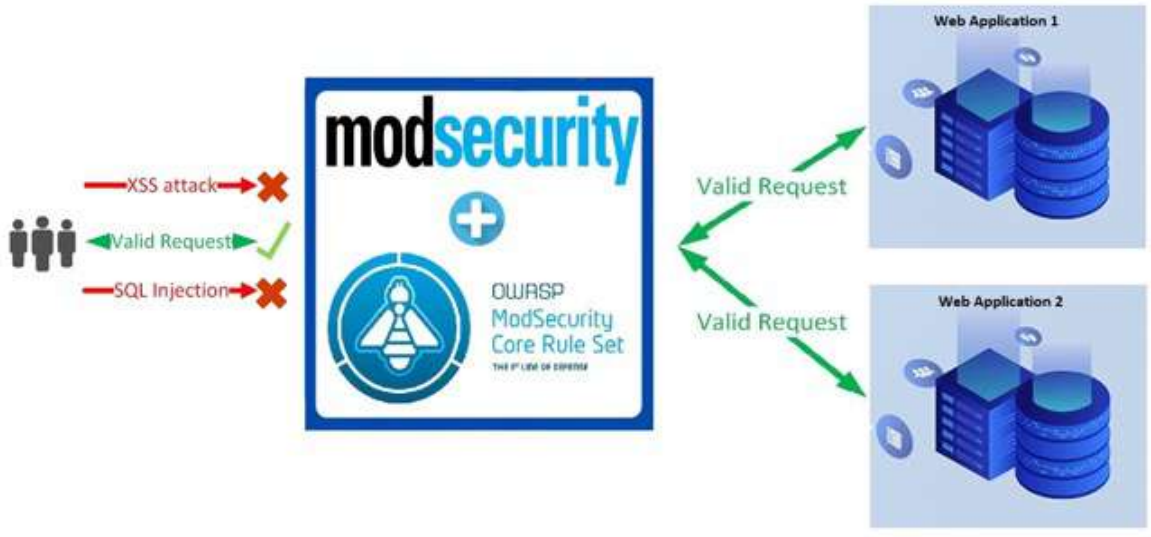
In ModSecurity, every transaction goes through five steps, or phases. In each of the phases, ModSecurity will do some work at the beginning (e.g., parse data that has become available), invoke the rules specified to work in that phase, and perhaps do a thing or two after the phase rules have finished.

Request headers

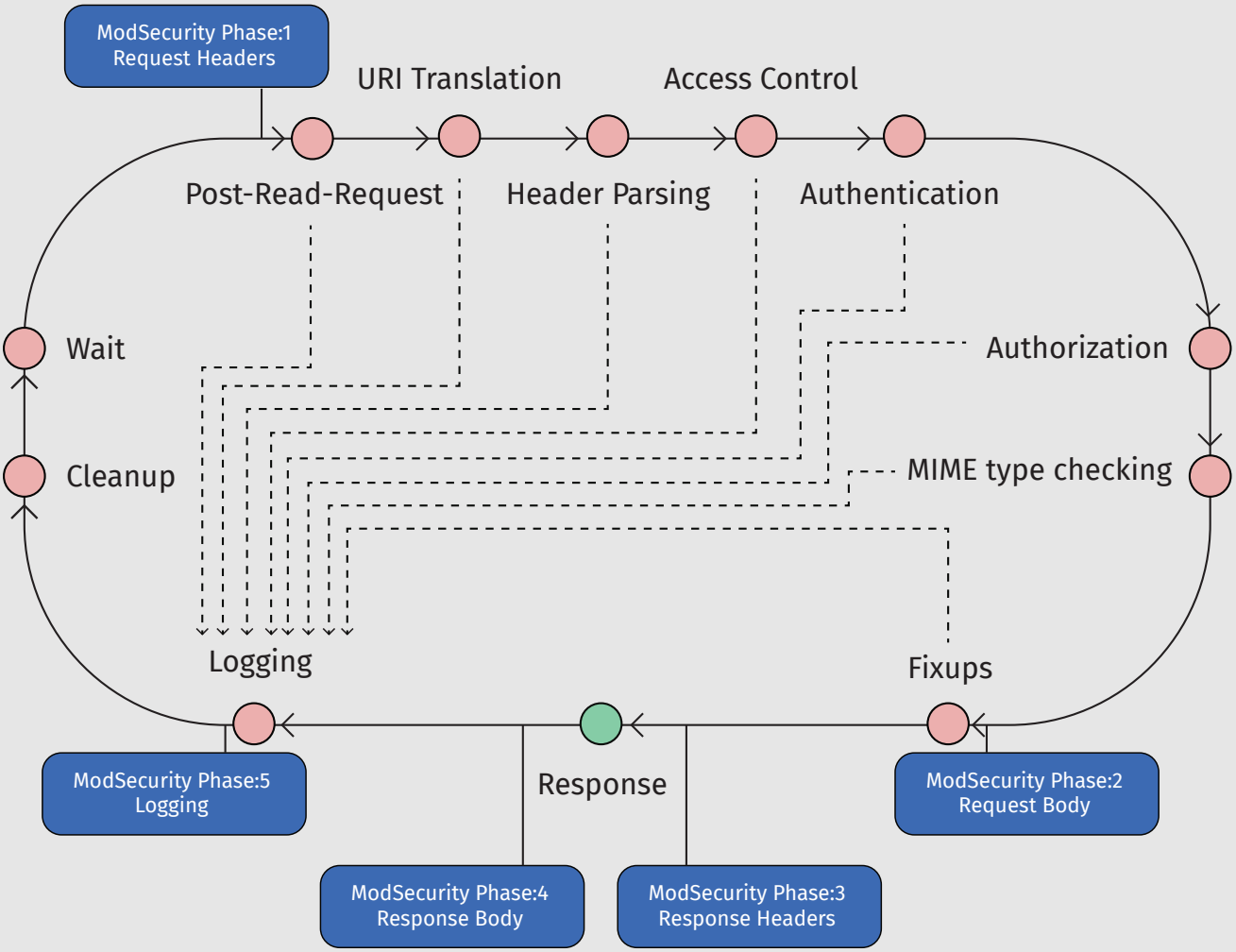
The request headers phase is the first entry point for ModSecurity. The principal purpose of this phase is to allow rule writers to assess a request before the costly request body processing is undertaken. Similarly, there is often a need to influence how ModSecurity will process a request body, and this phase is the place to do it. For example, ModSecurity will not parse an XML request body by default, but we can instruct it do so by placing the appropriate rules into phase 1.

Request body

The request body phase is the main request



▲ ModSecurity



ModSecurity Transaction Phases

analysis phase and takes place immediately after a complete request body has been received and processed. The rules in this phase have all the available request data at their disposal.

Response headers

The response headers phase takes place after response headers become available, but before a response body is read. The rules that need to decide whether to inspect a response body run in this phase.

Response body

The response body phase is the main response analysis phase. By the time this phase begins, the response body will have been read, with all its data available for the rules to make their decisions.

Logging

The logging phase is special in more ways than one. First, it's the only phase from which we cannot block. By the time this phase runs, the transaction will have finished, so there's little we can do but record the fact that it happened. Rules in this phase are run to control how logging is done.

Conclusion

ModSecurity is a very powerful and flexible WAF. It prevents web applications against a number of attacks such as SQL Injection, Cross Site Scripting, Cross Site Request Forgery, Local File Inclusion, Missing HTTPOnly and Secure Flags on Sensitive Cookies, Improper Access Control, Sensitive Data Exposure and many more. Web application administrators can use ModSecurity as a defense against such web application vulnerability exploits. It gives us freedom to decide how to take advantage of the features available in it. This flexibility is a core element of ModSecurity's identity, and complements its open source structure. In fact, users can enjoy complete access to its source code, which empowers them to customize the tool to suit their unique needs.

For further information, please contact:

R. K. Raina
Scientist - F
National Informatics Centre, A-Block
CGO Complex, Lodhi Road
New Delhi - 110003

Email: rk.raina@nic.in, Phone: 011-23405231

Leveraging Big Data & AI-ML for Security Analytics

NIC-CERT's endeavor towards a predictive cyber security approach

NIC has been a prominent target for cyber-attacks. The sheer volume of government applications, websites, services and databases, hosted and managed by NIC makes it a very lucrative targets for cyber threat actors including nation state actors. NIC has been adopting a layered defense approach for mitigating these attacks, with state-of-the-art technology. As modern technology evolved with much more enhanced attack detection and mitigation capabilities, the attackers also evolved and they started chaining multiple exploits, leading to a multi-vector and multi-stage attack.

In a world with technologies powered by AI-ML, the modern threat and attack landscape have undergone a massive change. To tackle this changing landscape, it is imperative to leverage the very same AI-ML to extract crucial insights and analytics, so as to enhance the overall cyber security posture and be better prepared to detect and respond to attacks, as early as possible.

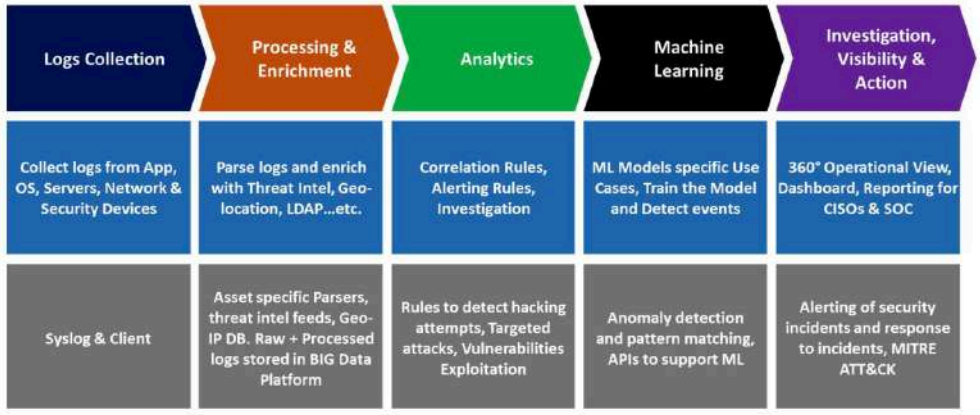
Some of the attacks which involve zero-day vulnerabilities, are even more difficult to detect through conventional security solutions. In order to tackle these changing dynamics in the attacker tactics and techniques, NIC-CERT has embarked on an ambitious initiative for designing and commissioning a robust AI-ML based cyber analytics platform. The platform can be leveraged to spot certain cyber attacks at an early stage and help in improving the security posture of NIC.

R.S. Mani
Dy. Director General
& HoG
rsm@nic.in

Hari Haran M
Scientist-C
hariharan.m@nic.in

Gaurav Kansal
Scientist-C
gaurav.kansal@nic.in

▼ Security Analytics Platform - Modules



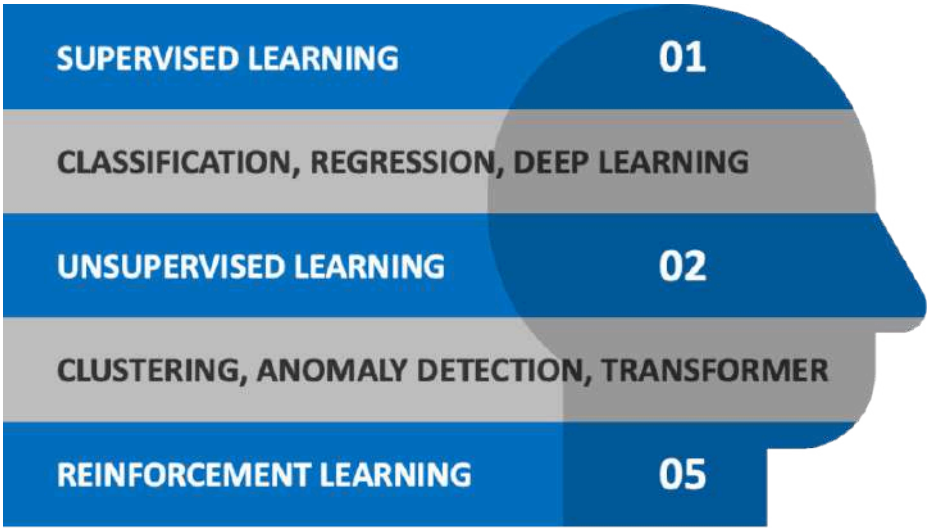
Security Analytics Platform

The security analytics platform is envisioned to handle data in the scale of petabytes and it should be scalable. In this context, Elastic Search and Hadoop can be used as the backend data lake. The elastic search can facilitate the correlation/ alert rules, dashboards and analytics. Whereas, Hadoop can facilitate the machine learning analysis, through additional tools like python, spark. the primary source of data to be ingested into the platform would be the logs generated by various devices, servers, endpoints, applications, websites and services. The logs may be collected from various sources across the Government ICT Infrastructure connected to NICNET and the logs shall be processed and enriched with additional details (like Geo-location, IP/ Domain Reputation, etc). The processed logs will then be analyzed on the analytics platform using various correlation and security rules. In addition to this, a machine learning model will also process the logs and will try to identify various anomalies and suspicious patterns in the logs. Multiple Machine Learning models may be integrated into the security analytics Platform, each ML Model will have AI-ML Models for Security Analytics the capability to train and learn, where by it attains certain level of maturity over a period of time. Once the ML Model attains the maturity level, it can spot much more advanced and complex attacks, which may not be spotted by the traditional rule based SIEM platforms.

AI-ML in Advanced Security Analytics and Threat Detection

AI-ML has become the buzzword in recent times. Most of the new technology products claims to leverage AI-ML in one way or the other. Inspite of all the buzz and being touted as the next big thing in the technology evolution, the journey towards achieving successful results through AI-ML is an arduous task; Especially, when it comes to cyber security and threat/ attack detection, it would require billions of data events to train the model appropriately, so that it can achieve a certain degree of accuracy.

The classification model under supervised learning can be built around knowledge of known classifier objects such as IP addresses, domain names, network object interactions, and other data points, which are extracted from the logs. This can further be used to build various classification models which can be tested and adopted based on classification accuracies and relevance. Unsupervised learning can be leveraged for better grouping of clusters, where various clustering algorithms need to be used to identify and quantify data relationships from data and meta-data extracted from the logs. Deep Learning neural networks can be used for predicting anomalies in the data set gathered from various log sources. One of the key focus areas of the security analytics platform is to transform the security detection from reactive to proactive i.e., aid in predictive analytics.



Features of the Security Analytics Platform

Some of the key features of the platform are as follows:

- Central Aggregated Log Management Platform
- Web and Security Analytics
- Visibility on Attacker Activity
- Detect/ Predict Anomalies or Attacks at an early stage
- Incident Response, Threat Hunting & Threat Intelligence
- Facilitate troubleshooting of website/ application issues
- Dashboard & Reporting

Tactical Insights & Security Posture

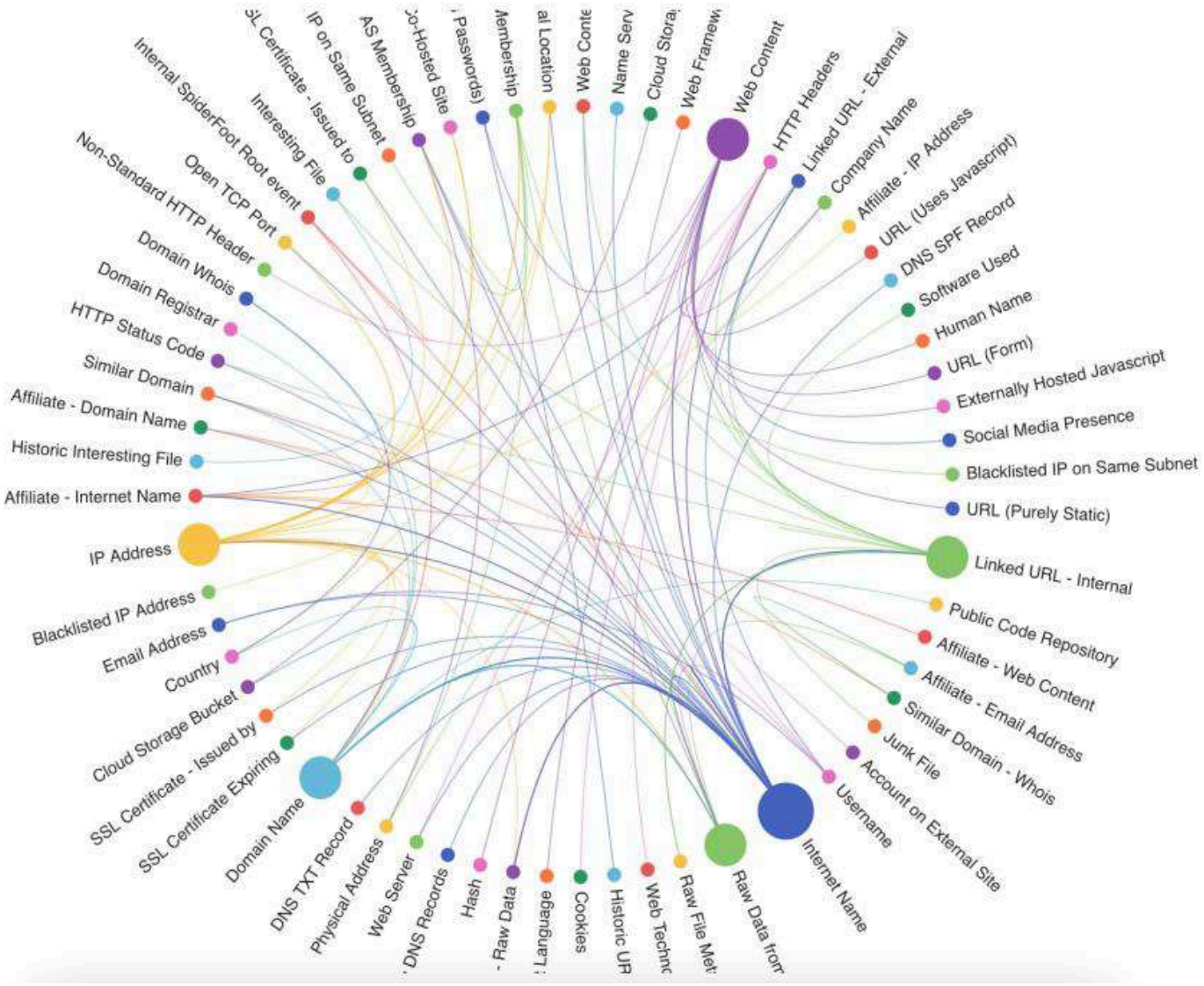
From an ICT perspective, the logs of a system are literally a piece of recorded history of what happened on the system, when it happened, this information can be further inferenced to identify how the specific event happened and why it happened. Considering an organization like NIC, which hosts thousands of websites, applications and not to mention the lakhs of ICT devices spread across the country, collection and aggregation of logs from these devices in itself poses a huge challenge. But if we overcome the challenge and are able to aggregate the data, then the insights that could be derived from the aggregated logs would be invaluable. Since, its practically not possible for a human to physically check and investigate each log event, this is where automated security analytics and machine learning comes into picture; Together, the ML and Security Analytics can quickly sift through billions of log events and filter out those events which could be of interest from a security perspective and it could further extrapolate the relationship between a particular event and a whole plethora of other related data sets, thereby providing tactical insights essential for strengthening our cyber security posture.

The security analytics platform can also provide key web analytics on the site traffic, visitor stats, suspicious hits, etc. The insights generated from one log source can also be correlated with another log source to check for any similarities. For example, an attacker who has attempted to hack into one state government website, was again found to be attempting to hack another central government ministry's website. This is where the analytics platform, will try to inter-relate both the attacks based on various features and attributes, and further the model would try to learn the techniques adopted by the attacker for launching the attack. The learning would then be ingrained into the model and it could train itself for detecting similar such attacks in the future.

Key Benefits of the Security Analytics Platform

The security analytics platform is powered by a massive data lake at the backend, which is essentially a repository of log data collected from various sources. The platform can be leveraged to ask various questions by querying the underlying data to get necessary information. In addition to this, the platform can also offer the following key benefits:

- Huge cost savings in the range of hundreds of crores, which would have been incurred in a corresponding commercial platform
- Security incidents can be identified quickly and action can be taken before any major damage could be done



▲ Extrapolation of Relationships between datasets

- Round the clock visibility can help in identifying which vulnerabilities/ loop holes, are being exploited, this information can aid developers/ administrators to fix them quickly
- Can aid in the troubleshooting of issues in Govt websites/ ICT Infrastructure, the platform can also reduce the time to identify and fix the issue
- As logs from multiple NDCs and States are to be ingested into the security analytics platform, the Machine Learning Models, can get exposed to a vast, varied and more unique data events, which can aid in training the models to achieve a much higher level of accuracy
- Ministry/ State/ Project specific Dashboard and Reporting view, for up-to-date analytics and security posture status

Conclusion

Logs form an important part of an ICT system. All supported ICT systems should be configured to generate and store logs. It is advisable to store the logs in a central logging server, which is independent of the log source. The logs should be configured to capture crucial details like timestamp, source, destination, request, port, protocol, username, etc. The most important aspect is the timestamp, it is essential that all ICT systems within NIC are synchronized with the same time stamp from the central NTP server. If time stamps are not synchronized, then the very purpose of logging may be defeated. Once we collect and aggregate logs from multiple sources, then the AI-ML plays a vital role in fetching key insights from the logs. These insights can further contribute to policy making and other decision support systems. Moreover, it enhances the visibility of what is happening around in the ICT infrastructure and when this visibility combined with the insights, it can become a formidable tool to strengthen the overall security posture of NIC and the government at large.

For further information, please contact:
Hari Haran M
Scientist-C
National Informatics Centre
CGO Complex, Lodhi Road
New Delhi - 110 003
Email: hariharan.m@nic.in, Phone: 011-22907465

Defense in Depth through Layered Security

Importance of Layered Security for Data Defense and Protection

Cyber Security is explained in terms of CIA Triad. The CIA Triad of Confidentiality, Integrity and Availability is considered as the core underpinnings of Information Security. The CIA triad forms the base unto which different approaches to security build upon. All security access controls and vulnerabilities can be viewed in the light of one or more of these key concepts.

Incidents of massive data breaches have become common and the cost of breaches have reached record high levels. The increase in frequency and sophistication of cyber-attacks becomes more relevant as Government Organizations and Enterprises are increasingly relying on networked computing architectures to maintain consistency of services. Breaches and downtime leading to network outage can impact profitability of businesses and availability of government services.

Confidentiality

Confidentiality measures protect information from unauthorized access and misuse. Most information systems house information that has varying degree of sensitivity. Confidential information often has value and systems are therefore under frequent attack as criminals hunt for vulnerabilities to exploit and subsequently gain access to information. Threat vectors include direct attacks such as stealing passwords and capturing network traffic, and more layered attacks such as social engineering and phishing.

Integrity

Integrity related measures protect information from unauthorized alteration. These measures provide assurance about the accuracy and completeness of data. In maintaining integrity, it is not only necessary to control access at the system level, but to further ensure that system users are only able to alter information that they are legitimately authorized to.

Abhishek Sisodia
Scientist - B
abhishek.sisodia@nic.in

Availability

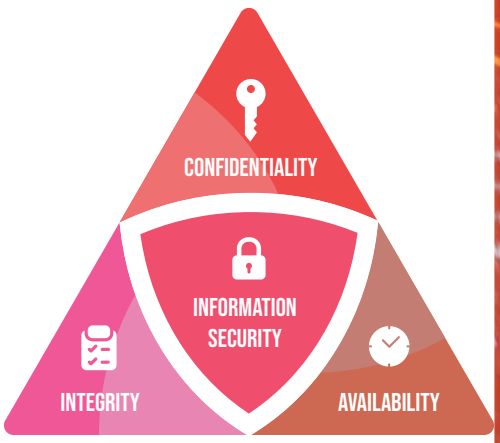
For an information system to be useful it must be available to authorized users. Availability measures provide timely and uninterrupted access to the system. Government, Businesses, Medical, Information and other types of infrastructure are based on the connectivity and availability of resources and services and unavailability can cause chaos and severe damage.

Concept of Layered Security

There are many approaches to deal with the conventional and emerging cyber-threats. Layered approach towards security is one of the most prominent among them.

Layered security is defined as:

Layered security refers to security systems that use multiple components to protect operations on multiple levels and protects the confidentiality, integrity, and availability of the information. The term "layered security" is related to the term "defense in depth", which is based on a slightly broader conception where multiple strategies and resources are used to slow, block, delay, or hinder a threat to subsequently neutralize it.



Layered security is a network security approach that uses several components to protect an organization's operations with multiple levels of security measures. The purpose of layered security approach is to make sure to not leave any single point of failure in the security design. In many scenarios, layered security strategy mitigates the potential weakness of one layer by the strength of corresponding other layers.

Individual layers in a layered security approach focuses threats possessed to Confidentiality, Integrity and Availability. These layers work together to tighten security and by minimizing potential threat surface area for intruders from breaching your network, making it much more robust than relying on a single layer security solution.

The terms "Defence in depth" and "Layered security" are often used interchangeably, however there is a subtle difference with a lot of overlap. The term "defence in depth" refers to an even more comprehensive security strategy approach than layered security. In fact, one might say that just as a firewall is only one component of a layered security strategy, layered security is only one component of a defence in depth strategy. Défense in depth strategies also include other security preparations which address concerns such as: monitoring, alerting, and emergency response, authorized personnel activity accounting, disaster recovery, criminal activity reporting, forensic analysis etc. But nonetheless, layered security approach is one of most important components of Défense in Depth strategy.

Areas of Cyber Security Threats

Cyber security threats exist at all the OSI/ ISO model layers starting at Layer 7 – the Application Layer because that's the place where users begin by interfacing to the network. For the purposes of creating the most comprehensive Cyber security plan we must actually start BEFORE the Application Layer and address perhaps the biggest vulnerability in the entire network – the user himself. Users are human and are far more subjected to making errors than computers which will perform the same function the same way every time. Threats at each layer of the ISO-OSI model include:

Application Layer Threats

Examples of application layer attacks include distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slow-loris attacks. To combat these and more, most organizations have an arsenal of application layer security protections, such as web application firewalls (WAFs), secure web gateway services, and others. According to the experts "The application layer is the hardest to defend". The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define with an intrusion detection signature. This layer is also the most accessible and the most exposed to the outside world because for the application to function, it must be accessible over Port 80 (HTTP) or Port 443 (HTTPS). Other possible exploits at the Application Layer include viruses, worms, phishing, key loggers, backdoors, program logic flaws, bugs, trojan horses and Ransomware.

Presentation Layer Threats

The most prevalent threats at this layer are malformed SSL requests. Knowing that inspecting SSL encryption packets is resource intensive, attackers use SSL to tunnel HTTP attacks to target the server. Mitigation plans should include options like offloading the SSL and inspecting the encrypted application traffic for the signs of attacks traffic or violations of policy at an applications delivery platform and subsequently encrypting it after the process of inspection is complete.

Session Layer Threat

DDoS-attackers exploit a flaw in a Telnet server running on the networking devices like switches, rendering Telnet services unavailable. Thus, it becomes important that networking hardware is regularly patched for such vulnerabilities, proper access and session restriction policies are configured and firmware is kept up-to-date.

Transport Layer Threats

Transport Layer Security (TLS) is used to secure all communications between their Web servers and browsers regardless of whether sensitive data is being transmitted. TLS is a cryptographic protocol that provides end-to-end communications securely over networks and is widely used for internet communications and online transactions. It is intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail such as Outlook and voice over IP.

Network Layer Threats

Routers make decisions based on layer 3 information, hence the most common network layer threats are generally router-related, including information gathering, sniffing, spoofing, and distributed denial of service (DDoS) attacks in which multiple hosts are enlisted to bombard a target router with requests to the point where it gets overloaded and cannot accept genuine requests.

The most effective protection is achieved by consistently observing best practices for router, firewall and switch configurations. At the router itself it is important to constantly assure that the router operating system is up to date on all security patches, packet filtering is kept enabled and any unused ports are blocked, unused services, and interfaces are disabled. Logging should be enabled, and regular auditing of any unusual activity should be conducted.

Data-Link Layer Threats

The data link layer provides reliable transit of data across a physical link. The data link layer is concerned with physical addressing, network topology, network access, error notification, ordered delivery of frames, and flow control. Frame-level exploits and vulnerabilities include sniffing, spoofing, broadcast storms, and insecure or absent virtual LANs (VLANs, or lack of VLANs). Network interface cards (NICs) that are misconfigured or malfunctioning can cause serious problems on a network segment or the entire network.

Port security is important to tackle Address Resolution Protocol (ARP) spoofing, Media Access Control (MAC) flooding or cloning, Port Stealing, Dynamic Host Configuration Protocol (DHCP) Attacks, layer 2-based broadcasting or Denial of Service Attacks. Switches should be configured to limit the ports that can respond to DHCP requests, static ARP should be implemented and Intrusion Detection Systems (IDS) should be installed.

Physical Layer Threats

The copper & fiber-optic cables that connect everything together create the actual network that everything else uses. Most threats at this layer involve interruption of the electrical signals that travel between network nodes including the physical cutting of cables, natural disasters that bring flood waters which can cause short-circuits, or other human vandalism. Many organizations mitigate these failures by bringing in multiple circuits to the internet.

A superior strategy is the placement of all network core elements such as servers and storage at multiple redundant cloud data centers so that services are available at all the times.

Functional Aspects

An analogy can be drawn between Layered approach to security and physical security at an airport. Just like multiple checkpoints at an airport serve different purpose, different layers of security also prevent different type of cyber threats. What layers of security are used in practice may vary from implementation to implementation, but most common ones are:

Network Perimeter Defense

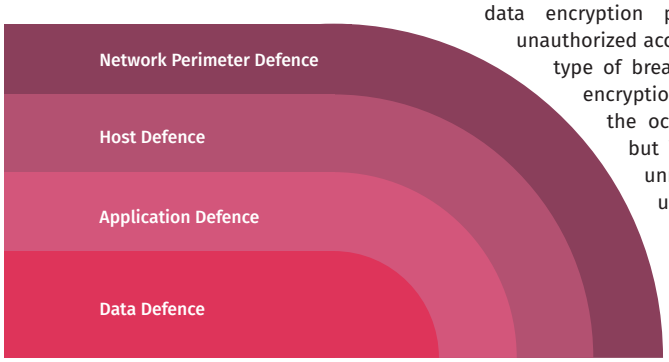
Perimeter defense involves firewalls, intrusion detection and prevention systems, and DMZs. Network Perimeter defence separates an organization's network from External network and prevents unauthorized access to this network. Its components include:

Firewall: Firewall is an essential part of any network security; a firewall stands as the main barrier between the organization's internal secured network and external network. While some firewalls are basic, others can be highly complex and sophisticated like Next Generation Firewalls and Unified Threat Management devices.

Intrusion Detection and Prevention: This system is designed to monitor intrusions and

prevent threats from entering organization's network. The system monitors organization's network continuously and scans the traffic for possible risk to gather more information and administer the proper preventative actions. This system can be used to identify violations against access rules and policies It is also capable of defending against Zero-day attacks.

De-Militarized Zones: The purpose of DMZ is to enable access to resources from the untrusted network while keeping the system or host on an organization's internal private network secure. Resources that are commonly placed within the DMZ are Mail servers, FTP servers, Web servers, DNS servers and VoIP servers.



Host Defence

Host defence comprises of End Points and Anti-malware/ Anti-virus solutions for End User Protection. Whether users use desktop PC's, laptops, iPads, tablets, or any other devices, it is critical to mitigate the risk of attacks which can find their way into an organisation's network by means of the end point/ end user vector. Endpoint security controls protect the connection between devices and the internal network of the organisation. It also protects the user data and resources along with the protecting other hosts from the compromised ones by blocking lateral spread of malware within the organisation's secured network.

Application Defence

Application defence is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification. It involves security measures at the application level that aim to prevent data or code within the app from being stolen, altered or hijacked. It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect apps after they get deployed like Authentication, Authorization, Encryption, Application security testing etc.

Data Defence

Data defence include measures to protect the storage and transfer of data. Different methods include:

Email Filtering: Organisations communicate heavily through email, and cyber attackers make continuous efforts to exploit this dependency. Often, end point/ end user protection is not enough to prevent someone from opening infected emails and attachments. Filtering emails at the gateway can reduce the risk of infections and data breaches.

Email Encryption: Once an email leaves server, it can be intercepted by attackers. If there is any sensitive information within the email, there can be a potential for a breach of data. With email encryption, the email and its data are altered into a non-readable and incomprehensible format.

Data Encryption: Like email encryption, data encryption protects information from unauthorized access even in the event of any type of breach. Using an effective data encryption platform may not prevent the occurrence of a data breach, but it virtually renders the data unreadable (and therefore useless) to anyone trying to access it.

In current times, one more layer of Mobile security has been added to the strategy. Mobile workplaces and virtual offices are becoming the norm, especially due to the growing work-from-home culture in the wake of the COVID pandemic. Mobile devices can increase the risk of security breaches which can lead to disruption of operations, data leaks, compromised information, financial losses, unavailability of services etc. Thus, Mobile Device Management becomes a necessity to ensure the safety and security of the equipment as well as the data and proprietary information for employees working from home and off-site locations. Organisations must make sure that they can encrypt, secure, and remotely remove sensitive data and information that could fall into the wrong hands.

Benefits of Layered Security

The key benefit of layered security strategy is that it provides measures corresponding to Protection, Detection, and Response. Layers are beneficial for many reasons. Each layer provides an additional level of defence so that with each extra layer of security that can be added, it becomes more challenging to find ways to infiltrate the system. While each layer in and of itself is not an adequate defence mechanism, layering them together improves each one's efficiency until the last layer nearly completely blocks out the hacker's ability to gain access. Instead of trying to rely on just one or two levels of defence, like access cards and two-step identification, multiple layers of security will lower the risk of a breach and make it easier to respond to legitimate inquiries and requests.

With a layered defence approach, several things happen. First, threats that are detected early are eliminated so that they won't pose a threat or be able to block authentic attempts to enter the system. The next thing to happen is that if a suspected data packet or email enters the system and is picked up as a threat, but clarification is needed, it is sent to an area where it can be easily verified. This rapid capture and validation process means less downtime and allows organisation to continue to be productive. It also eliminates the need for a security administrator to have to go into the system to sanitize an item. The right defence at the right time within a layered Cyber security program offers an organization a chance to continue to work at full speed while defence mechanisms are in place and taking care of security.

Layered defence approach also reduces false positives that may prevent an organisation from maintaining interaction with legitimate contacts, while at the same time helping improve organisational visibility. By establishing a verified pathway that goes from the network to the server following a defined set of points that lie in between, any type of threat is detected much easier and eliminated without slowing down operations. The layered security concept creates an interwoven network of protection that prevents unwanted intruders from exploiting the existing vulnerabilities (or even lingering for long periods of time) within the system.

Layered approach provides multi-levels of defence that both identifies and eliminates threats on many different levels. With each added layer, it compounds level of protection until a wall of security is created that is almost impenetrable. The increased risk of loss associated with cyber-attacks cannot be denied, so it's vital that a security approach is followed which takes many different types of threats into consideration and deals with each one quickly and efficiently.

Conclusion

Strengthening the cyber-security infrastructure of the country has become imperative with Government of India launching several initiatives for efficient delivery of services to citizens. The country is consistently improving the ranking in Global Cyber Security Index released by International Telecommunication Union (ITU). Continuous efforts are needed to further improve this posture. In a scenario where Governments and corporates are facing frequent data breaches, layered security has become the norm of the day to minimize the conventional as well as the emerging threats.

For further information, please contact:
Abhishek Sisodia
Scientist - B
National Informatics Centre, A-Block
CGO Complex, Lodhi Road
New Delhi - 110003
Email: abhishek.sisodia @nic.in, Phone: 011-24305865

Endpoint: The Start Point of Cyber Security

Enhancing Cyber Security through advanced Endpoint Security

In the realm of cyber security, the term endpoint refers to connected devices on a network such as desktops, laptops, servers, mobile and IoT devices. Endpoints are the interface where human beings who are the weakest link in Cyber Security normally interact. Endpoint security, therefore, is one of the prominent components of cyber security. It involves securing data associated with endpoints from exploitation by threat actors through management of vulnerabilities and patching of software.

Organizations of all types and sizes such as healthcare, finance and defense are at risk from increased volume of organized cybercrime. Being the interface where human beings who are the weakest link in Cyber Security normally interact, these devices are the main targets of malicious actors. Endpoint security has emerged into advanced technology from traditional antivirus solutions for providing faster and comprehensive protection from sophisticated malware and modern zero-day attacks.

Need of endpoint security

Endpoint security is considered as crucial for cybersecurity due to a variety of reasons. The number and variety of endpoints are increasing day-by-day. With the introduction of remote work culture and advancement in the BYOD policies, perimeter security is becoming insufficient to prevent all kinds of malicious activities. The threat landscape is becoming complex due to increased capability of hackers to introduce new ways of accessing the digital assets and manipulate the information. Data being the most prominent asset for an organization in today's environment, the organization can be put at the risk of insolvency through illegal access and theft of that data.

Diwan Hauym Khan
Scientist-F
dhkhan@nic.in

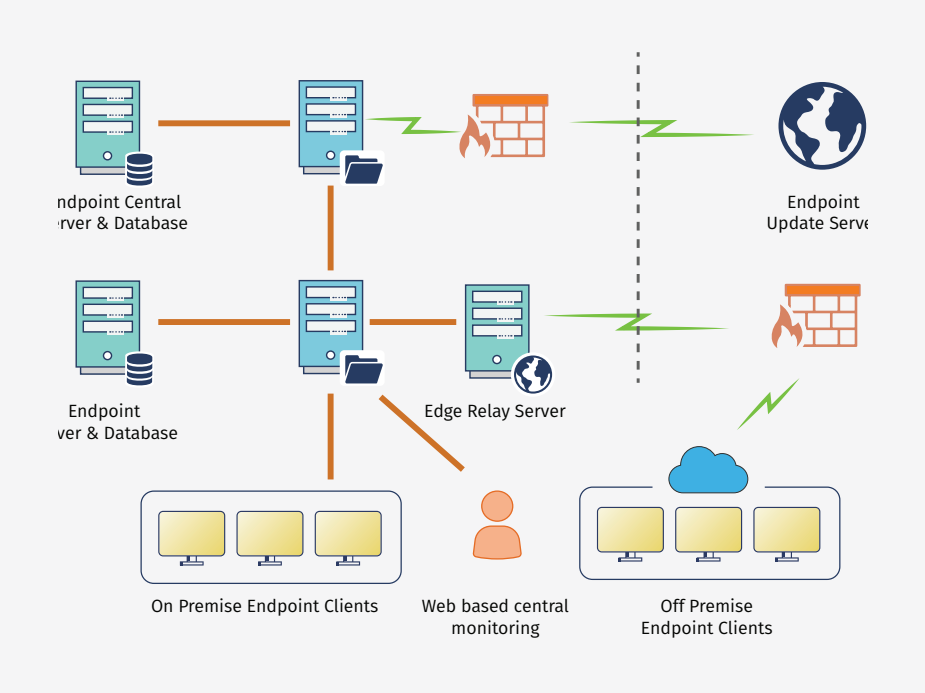
Kirshna Kumar
Scientist-B
kirshna.kumar98@nic.in

Endpoint Security Architecture

The figure illustrates the architecture of a typical endpoint security solution. The prime component in this deployment is the Central Endpoint Server which receives the security updates from the Endpoint Update Server and also functions as a centralized manager. The central server further distributes the updates among a set of Endpoint Servers to which the on premise client systems are connected. Endpoints such as laptops and mobile devices that are outside the organization's intranet are connected to the Endpoint Servers through an Edge Relay Server. The Endpoint Server provides advanced threat protection techniques combined with detection and response through the agent installed in clients. It responds to attacks in real-time and provides immediate and effective protection against zero-day attacks. A web-based central monitoring console is also provided for better visibility to the administrator in managing the endpoint clients.

Evolution of endpoint security

The business of endpoint security started in late 1980s with the introduction of antivirus solution which is a signature based malware recognition system. With the increased popularity of e-commerce and internet, detection of malicious activities has become more complex and can no longer rely on signatures. Traditional endpoint solutions have become incapable to handle sophisticated and emerging threats like file-less malware and zero day attacks. Therefore, advancement is required in end point security solutions with the proposition of more integrated, multistage defense system to handle the outsmart attackers. Advanced endpoint security requires detection and correction of hidden threats in seconds, in place of months. This is possible only with the automation of sharing threat intelligence among connected components for detection and correction of threats while teaming up of humans



with machines. Traditional endpoint security solutions such as firewall, antivirus, reputation, and heuristics are integrated with machine learning and artificial intelligence to detect and prevent advanced threats with nearly same speed as of threats.

Traditional Antivirus

Antivirus is an endpoint solution developed for the detection, prevention and elimination of malicious actors such as viruses, worms, and Trojans on end point devices based on large database of malware signatures. The antivirus solutions detect malware with the scan of files and directories based on patterns that matches the malware signatures on file. Antivirus software is provided by a number of vendors, with the versions developed for small businesses, personal use and large enterprises. The antivirus software has the capability to scan the system on-demand as well as at scheduled intervals. They also warn the user before visiting the malicious sites by virtue of its safety features. Further, they have the capability to identify different types of threats that are attacking the endpoint device. The major limitation of these solutions is that they are able to recognize only known threats and need to update signature database for new threats.

Advanced Endpoint Security

Cyber world requires advanced endpoint security solution as applicability of traditional solutions is limited only to known threats. Advanced endpoint security integrates features of traditional solutions such as firewall, antivirus, reputation, and heuristics with Behavioral Analysis, Machine Learning and containment. Besides, Endpoint Detection and Response (EDR) is also integrated to detect and prevent file-less, zero-day and script based threats like ransomware. The key capabilities of advanced endpoint security solutions are explained below.

Security Analytics: In security analytics, data related to endpoints is aggregated and analysed using security analytics tools for the detection of potential attacks. Malicious activities and associated harmful effects are identified and mitigated to avoid the damage caused by them.

Machine Learning: Machine learning is one of the prominent components of artificial intelligence (AI), through which enormous data is analyzed for behavioral learning of endpoints. Based on behavioral learning, malicious activities are identified and automatic security processes such as quarantining the endpoint and/or issuing of alerts are triggered. In present working environment, Machine Learning has become one of the important techniques for the detection of advanced threats at endpoints such as novel and zero day attacks.

Real-Time Threat Intelligence: Real-time threat intelligence provides updates from external security agencies about novel security threats such as zero-days, file-less malware and other trending malware in the cyber world. It expedites threat analysis, detection and prevention in the real-world scenario.

Internet of Things (IoT) security: With the advent of smart everything (like smart cities, smart industry, smart healthcare) IoT has incredible impact and proliferation in every domain of life. According to surveys, the count of IoT devices connected worldwide will cross a trillion towards the end of this decade. These devices are highly vulnerable to cyber threats due to their limitation in computation, network capacity and storage, and ubiquitous nature. Therefore, IoT security requires self-healing and automated mechanism for detection of threats, avoidance of data compromisation and reduction of response and downtime.

Endpoint Detection and Response (EDR): EDR integrates rule-based automated analysis and response capabilities with the endpoint data gathering and real-time persistent monitoring. The main focus of EDR is on identification and investigation of suspicious activities at endpoints along with automation for faster detection and response. Threat intelligence feed from various sources enhances the efficiency of EDR solution for the identification of advanced exploits such as zero day and multi-layered threats. Some EDR solutions utilize Artificial Intelligence and machine learning for the automotive investigation and analysis about potential threats.

Endpoint Encryption: Encryption is the technique to encode data on endpoint devices in unreadable format to make it unusable for unauthorized actors. For authorized users the data would be decrypted with the associated decryption key to make it accessible. Sensitive information of critical applications such as healthcare, banking, defense etc. is protected from unauthorized access using endpoint encryption. Using this technique, the operating system can be protected from "Evil Maid" threats which install corrupt boot files and key logger.

Extended Detection and Response (XDR): XDR is an enhanced form of EDR with improved detection and response capabilities using real-time data. It is a SaaS-based technique that collects data across multiple components and correlates it by utilizing behavioral analysis, threat intelligence and data science techniques. XDR has the ability to optimize response with increased visibility and advanced context while reducing the scope and severity of attack.

Conclusion

Attackers usually target endpoints devices as the start points for malicious entity. Advanced security solutions are required for quick detection, analysis, blocking, and containing of threats. For this purpose, the endpoint security technologies need to collaborate with each other and share threat intelligence.

For further information, please contact:
Diwan Hauym Khan
Scientist-F
National Informatics Centre, A-Block, CGO Complex
Lodhi Road,
New Delhi - 110003
Email: dhkhan@nic.in, Phone: 011-2430 5608

DevSecOps

Producing high quality, secure software at pace

Enterprises across the world are demanding software release at high speed to meet business requirements. when software is developed at such speed, security should not be left behind which can only happen if security is built in to SDLC. Such requirements gave birth to technologies like Agile development, DevOps and DevSecOps.In this paper we describe the DevOps technology that enables Development team and Operation team to collaborate with each other on day to day basis such that operational issues and customer problems reduce to a larger extent. We also explain DevSecOp technology that allows security to be built in to the application through automation, cultural shift, application security programs etc. In the end we describe what technologies and tools NIC is providing to the developers to implement DevSecOp across organisation.

We must always meet customer's requirement. Be it any role in the software industry - developer, tester, security auditor or manager, our job is to support the business so that it wins in the marketplace. Now, there is tough competition among the business players in every field to woo the customers. So, they demand product innovation and delivery at a rapid pace. Three or four product releases in a year is no longer a norm, business demands the release every week or every month with new features or to support the customer requirements. These paradigm shifts happening in the industry gave birth to technologies like Agile Software Development practices, DevOps, DevSecOp etc.

Why DevOps?

If Development and Operation work in silos, then when a developer writes code, builds it, tests it and deploys it into the operation, it normally fails. Whatever the failure may be- deployment failure, operation failure or crashes, the customer faces the problem in running the business. Normally, in such cases, the blame game begins, people from development say that there are operational issues and people from operations blame it on development issues and a lot of time is lost in the process. This usually happens because development and operation are not in sync with the software stack, tools and versions. Moreover, as discussed earlier, it is today's requirement to push the code to deployment/operation at a rapid pace, certain deployment each day. DevOps was created to address all these issues.

DevOps best practices can be narrowed down to three basic principles called the three ways :

Anil Kumar Jha
Sr. Technical Director
(Application Security Group)
aniljha@nic.in

First way

The first principle says we need to accelerate the work from development to operation, and then to the customer. This can be achieved by limiting work in progress and through automation.

Second way

The second way enables constant flow of feedback from operation to development. This can be achieved through continuous integration, build and deployment process working together with a fast, automated suite of tests.

Third way

The third way is about creating a culture of continual experimentation and learning.

While DevOps culture brought a lot of innovation to the software development process, security was either not considered or not able to keep pace with the rate at which software was being built and released. DevSecOp is an attempt to inject security into the DevOps process and make sure that software delivery rate is not disturbed due to this injection.

DevSecOp is short for Development, Security and Operation. This technology dictates that security is not the job of one group, rather everyone including development, security, operation quality is responsible for security. If any issue comes in production, all the teams should work together to resolve the issue therefore all the teams should learn security. Security should not be an afterthought, rather it should be built into the application. Security should be discussed and practiced during all the phases of Software Development life cycle during requirement analysis, architecture, design, development, testing and in operation.

Hence, to deliver software at high speed and make it secure as well, security needs to be built into the application development workflow and process. The earlier we introduce security into SDLC, the sooner we will be able to identify and fix vulnerabilities in the software, rather than waiting till the end for security assessment reports or run time issues in the operation. Organizations can introduce security into existing continuous integration and continuous delivery (CI/CD) pipelines. Just like after a build failure, software is not eligible for deployments in the production, a policy may be defined by the organization, if a security issue is caught in the CI/CD pipeline, the application should not reach production until the vulnerabilities are taken care of.

To implement DevSecOp, organizations need to integrate application security tools into CI/CD pipeline.

Some of the tools are:

- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)
- Dynamic Application Security Testing (DAST)

SAST

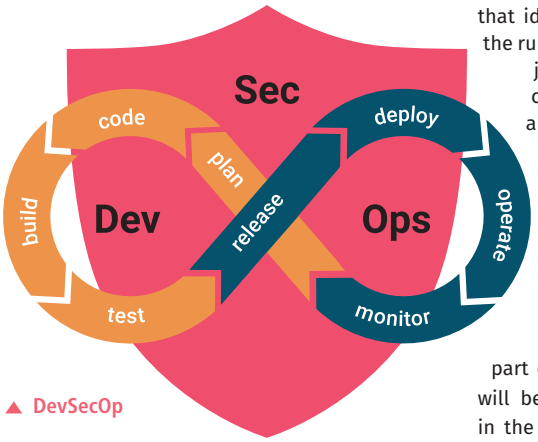
SAST tools scan the source code of the application and identify security vulnerabilities that may be exploited by the hacker while in production. These tools pinpoint the code location where security issues exist. This tool is used by the developer while the developer is writing the application and so the advantage of this tool is that the developer may fix all the security issues reported by the tool during the development phase of SDLC.

SCA

SCA tools scan the source code and binaries to identify vulnerabilities in open source libraries included in the application. These tools not only uncover the security issues but also highlights the licensing risks due to open source software components.

DAST

DAST is an automated black box testing technology that attacks our web applications/ APIs just like hackers would do. DAST tools do not require access to source code to perform the scan on web applications/APIs. Since these tools attack the application in real time just like a hacker and provide proof for each of the reported issues, it has a low number of false positives.



▲ DevSecOp

In NIC, the Application Security Group is providing the following tools to developers to enforce security in the CI/CD pipeline through automation:

HCL Appscan Source for Development

This tool provides a plugin to integrate in Developer IDE like Eclipse, Microsoft Visual Studio etc. This allows developers to scan the code, find vulnerabilities and fix it during the development phase of SDLC. This tool also provides recommendations for the issues reported by it.

HCL Appscan Enterprise

This tool is a black box security testing tool that identifies the security threats by attacking the running web applications/APIs/ web services just like hackers. It does not require source code of the application and can scan the applications developed in any language. It also provides proof of the reported issues of what parameter tampering/ manipulations/fuzzing were done and its effect on the target application.

With traditional software development strategies, it is not possible to deliver secure software at high velocity. DevSecOps is the philosophy of incorporating security practices within the DevOps using automation and security tools, and thus enabling secure software delivery through the seamless and transparent integration of security into the CI/CD pipeline.

RATNABOLI GHORAI DINDA
Dy. Director General, NIC

Conclusion

If we utilize these tools regularly as a part of our design and development work, we will be able to eradicate security issues early in the SDLC. Moreover, the developers acquire a lot of security knowledge in the process and will apply these learnings in the other projects they work up on. All these things will certainly make a cultural shift in the organization and will ultimately make the software much more secure, robust and resilient.

For further information, please contact:
Anil Kumar Jha
Sr. Technical Director
Application Security Audits & Assessment Division
National Informatics Centre, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003
Email: aniljha@nic.in, Phone: 011-24305140

Preventing Cyber Crisis

‘Must haves’ for all organizations to secure against cyber crisis

A secure cyber space is crucial for development of any country in economic, political and social spheres. Increased adoption of digital technologies has redefined the cyber security landscape. Cyber crisis is no more a luxury that any progressive state can afford. A set of baseline requirements are suggested that all organizations must have to prevent cyber crisis.

Dependence on Information Technology to make our day-to-day tasks easier has increased with computers playing key roles in all spheres of life such as governance, transportation, health care, and banking. Cyber security is vital for protecting all of these functions as any crisis in the cyberspace will endanger one’s life and property, in letter as well as spirit. The wide spectrum of hackers, criminals, terrorists, and state actors are constantly engaged in cyber space with malevolent activities ranging from stealing money and classified information to damaging important data and denying the availability of vital services. Since the cyber warfare is a never ending one, all stakeholders involved in providing IT enabled services should be prepared to manage any crisis that emerge in their cyber domain.

Evolution of a Cyber Crisis

As in the real world, the cyber space also is filled with innumerable events happening on a regular basis. An event refers to any observable occurrence in a system or network. Browsing a webpage, logging into a system, sending a mail and sharing a file are all examples of Events. The number of events taking place in a network is usually so high so that they are often counted in terms of Lac of Events per Second (EPS). While most of the events are harmless and result in a positive outcome, there are certain adverse events that can have negative consequences and even lead to disruption of service. Adverse events that pose a threat to the security of the computer or the network are called security incidents. In other words, security incidents are adverse events that breach the information security triad of Confidentiality, Integrity and Availability (CIA). Happenings like unauthorized access to a system and misuse of resources to virus attacks and violation of security policy of the organization are common examples of cyber security incident. These incidents may threaten lives, economy, national security, and erode public confidence if they are not properly attended in a timely manner, resulting in what is termed as Cyber Crisis.

Prevention better than cure

The preliminary step in managing any kind of crisis is prevention of its occurrence, and this is more true in case of cyber crisis. Organizations of all sizes should build cyber security capabilities to safeguard its assets from cyber-attacks. Since cyber security is a continuously evolving process (and not an off-the-shelf product), organizations should inculcate a culture of cyber security

C.J. Antony
Dy. Director General &
HoG (Network Security)
antony@nic.in

in all spheres of their functioning through appropriate policies, processes and protocols. To begin with, the following baseline requirements are recommended as 'must haves' for all organizations to secure against cyber crises.

Inventory of hardware and software assets

Maintaining an accurate and up-to-date inventory of hardware and software assets related to the organization is the first and foremost step for ensuring protection against cyber-attacks. A latest inventory is very essential to control the access for these solutions, besides detecting the unauthorized ones and hardening the vulnerable ones. Keeping such a record of assets deserves importance because, as the saying goes, we cannot protect what we do not know. An automated asset management system may be deployed for this purpose as newer solutions are being added and obsolete and faulty ones are getting removed on a daily basis, especially in large organizations. Obtaining a one-time-approval should be made mandatory before connecting new systems in the corporate network. A stringent Bring Your Own Device (BYOD) policy which also includes employee exit strategy may be put in place.

Secured configuration of Hardware and Software

The configurations with which the hardware and software solutions are released by the OEMs are meant for easy and quick installation in a network. The default settings ranging from the user accounts and passwords till open ports and protocols are made to enable plug-and-play deployment of the solution with less security. It is often found that these configurations are seldom modified for lack of time, expertise and even fear of malfunctioning, leaving wider attack surfaces for the attackers. Therefore, each hardware and software component should be put in use only after proper hardening and secured configuration following the principle of zero-trust. Subsequent modifications in the settings should be done only after following a proper change management process. All the solutions should be periodically subjected to security audit to ascertain any deviation from the established security norms.

Vulnerability Assessment and Patch Management

Vulnerabilities in operating systems, development frameworks, browsers, etc. are entry points for cyber-criminals to leash out attacks. An un-patched system gives attackers an easy avenue to penetrate the network and compromise the cyber infrastructure of the organization. With novel vulnerabilities and exposures getting reported every day, organizations should make conscious efforts for vulnerability and patch management based on cyber security alerts being raised by the concerned agencies. A pro-active mechanism to identify, mitigate and patch the vulnerabilities should be established and linked with the inventory management system mentioned earlier. Client users should be encouraged to regularly avail the updates from OEMs by enabling the auto-update feature of the system and application software.

Controlled use of Admin privileges

Misused Admin privileges are a common cause of security breach in any network. Admin privileges must be restricted in the system and application software as well as network and security appliances. Practice and propagate the principle of least privilege, as running computer in administrator role leaves it vulnerable to security risks and exploits. Access to any system should be provided only on a Need to Know basis. Additional user accounts created on need basis should be deleted or deactivated once the requirement is over. Any temporary escalation of user privileges should be undone immediately after the proposed task is accomplished. Activities that require admin privileges should be performed by the designated system administrator only and the admin should use due diligence while using the system and privileges. Actions performed by privileged users should be constantly logged and regularly monitored to detect any adverse events.

Endpoint protection

Endpoint of the information technology network consisting of desktops, laptops and hand-held devices are often turn-out to be the start point of a cyber crisis. Endpoints need special attention and protection to avoid any incident that may turn out to be a crisis as they are the interface where human beings usually interact. Malware is the most common attack vector that targets the endpoints. They are malicious software intentionally designed to disrupt, damage and gain unauthorized access to computer systems and networks. Security solutions that prevent the malware from entering, executing, accessing sensitive data, and infiltrating the data, should be deployed to safeguard the endpoints. As newer mutants of malware are getting generated rapidly, traditional antivirus solutions are seldom effective to counter this nuisance. Next generation solutions based on Artificial Intelligence, Machine Learning and Behavior Analysis are need to detect and mitigate fresh variants of malware.

User Awareness and Capacity Building

Many organizations tend to neglect the most important layer of defense against cyber-attacks - the end users. Human Beings being the weakest link in Cyber Security paradigm, continuous efforts need to be made to keep them aware and alert of the latest Tactics, Techniques and Procedures (TTPs) of cyber-criminals. New vulnerabilities are emerging every day and a proper understanding of the prevention, detection and mitigation techniques is very essential to remain protected. Security awareness empowers people connected with business to perform their roles by protecting the organization from potential security threats. Any investment in cyber capacity building will enhance the success rate of other policy initiatives in long-run. Thus, awareness creation is a marathon process, not a sprint race that can be accomplished in a short period of time.

Conclusion

Cyber space is an intrinsic part in the development of any country. Attacks on critical information infrastructure are continuously being leashed-out by state and non-state actors, posing threat to national security. The identity and capability of the attackers are seldom known and this often gives them an edge over the victims. With cyber-crime growing into a multi-billion-dollar industry, cyber-criminals are increasingly getting empowered and creative day-by-day. Organizations must have a strong and agile security posture to deal with these headwinds and ensure reliable and responsible service to their users.

For further information, please contact:

C.J. Antony
Dy. Director General & HoG
Network Security Group
National Informatics Centre, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003

Email: antony@nic.in, Phone: 011-24305166

Automated Vulnerability Analysis & Reporting Tool

Detecting most common vulnerabilities efficiently

Web applications are frequent targets of cyber-attacks. To defend against such attacks, it is imperative to patch vulnerabilities present in a web application and hence vulnerability analysis is an important part of web application security. Manually analyzing a medium to large-sized web application is a time-consuming and error-prone process due to the presence of many components. A tool that can automatically analyze and report vulnerabilities in a web application can reduce the effort needed for vulnerability analysis, thereby enabling web application owners to fix and patch the vulnerabilities before they can be exploited. AVART (Automated Vulnerability Analysis and Reporting Tool) is such a tool that comprises automated vulnerability analysis of web applications and a dashboard for reporting. AVART can detect most common web application issues in a fast and efficient manner.

AVART (Automated Vulnerability Analysis and Reporting Tool) is a DAST (Dynamic Analysis and Security Testing) Tool developed to automate the process of vulnerability assessment and analysis of large number of web applications and thereby reduce the time and manual effort required. An easy to use web based interface along with a dashboard was a primary requirement of the tool to make it possible for users with all minimal knowledge of application security to use the application. The user interface of the application is shown in figure 1 through 3.

Features of the application

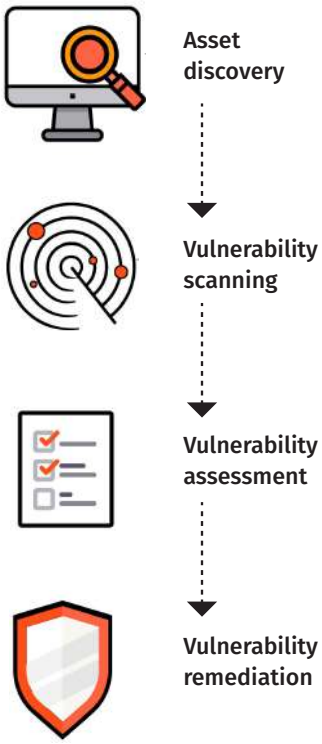
The application was designed for vulnerability analysis of production web applications. To prevent damage to production web applications, the application does not perform high risk vulnerability analysis including injection attacks. The application provides the following features for testing common web applications vulnerabilities.

Dashboard

Tasiruddin Ahmed
Scientist-F
asm-tasir@nic.in

Bronjon Gogoi
Scientist-C
asm-bronjon@nic.in

- Analyse web applications for SSL issues
- Analyse web applications for security misconfiguration like missing HTTP security headers, vulnerable HTTP methods
- Analyse web applications for usage of known vulnerable components
- Analyse web applications for sensitive information disclosure vulnerabilities
- Analyse web servers and discovery of open ports



- Scheduled batch analysis of web applications to collectively scan a large number of web applications simultaneously
- Dashboard with reporting feature for easy reporting of vulnerabilities discovered along with mitigation measures

User Classes and Characteristics

- Security Auditors: Security auditors can use the AVART tool to analyse websites for security issues without having to scan each website one by one and let the tool do the scanning automatically for all the websites in the domain of the security auditor.
- Project Coordinators: Project coordinators can use the tool periodically on their websites and applications to discover vulnerabilities on their own and fix them based on the solutions provided in the reports.
- Developers: Developers can use the tool to discover and subsequently fix vulnerabilities before submitting the application for audit.
- Any Other Stake Holder: The application is user friendly and easy to use and hence should be usable by any user with some knowledge about application security.

Benefits of the application

- Quick and easy analysis of web applications for discovery of common web application vulnerabilities without minimal knowledge of application security.
- Easy reporting via dashboard.
- No licensing restrictions and hence can be used simultaneously by many users.
- Automated scan allows for simultaneous scanning of a large number of web applications thereby reducing the manual effort required for discovery and reporting of vulnerabilities.
- Solutions for mitigation enable quick resolution of security issues.

Technology used

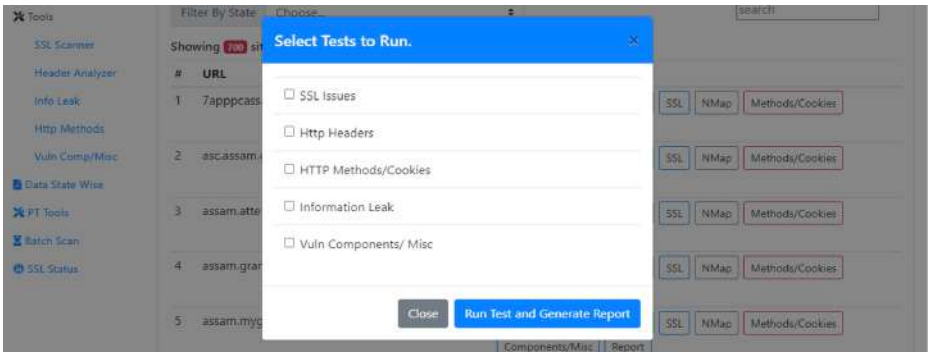
The tool is developed as a web based application and the backend is developed in the form of an API to enable integration with other systems in the future. Following technologies were used for development of the application

- **Frontend:**
  Angular JS
  Bootstrap
  jQuery for the front end
- **Backend:**
  NodeJs
  PHP
  OpenSSL
  MySQL database

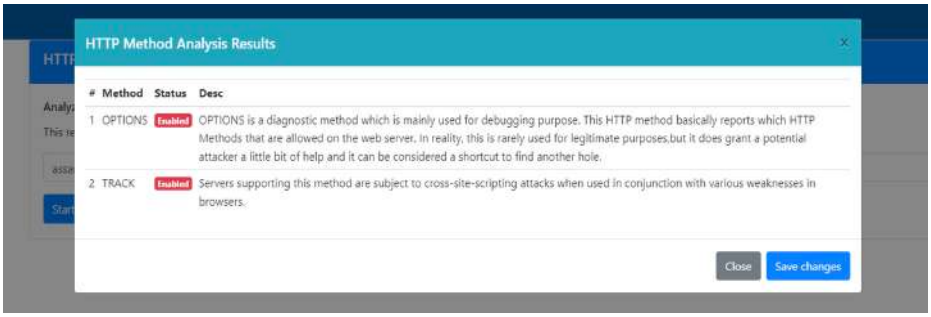
Future Road Map

To develop a full fledged DAST tool for security analysis and penetration testing of web and mobile applications that can be used for easy, efficient and effective management of various parameters of application security.

Penetration Testing Tools



Sample Penetration Testing Result



Comprehensive Security Assessment

A proactive granular approach for enhancing security

Comprehensive security assessment follows a layered approach, wherein it covers the assessment of all the in-line infrastructure components (network devices, security devices, Server environments and Mobile/web applications/APIs) to ensure that all areas of threats, vulnerabilities and risks are identified and reported.

Comprehensive Security Assessment (CSA) Audit is to carry out in depth analysis of existing Application, Web Infrastructure threats and check for the existing built-in security controls in the running Project portal. The CSA further aims to trace hidden security issues, check for strong access controls, assessment to prevent Data breaches and recommends strong measures for Data Security.

Comprehensive security assessment follows a layered approach, wherein it covers the assessment of all the in-line infrastructure components (network devices, security devices, Server environments and Mobile/web applications/APIs) to ensure that all areas of threats, vulnerabilities and risks are identified and reported.

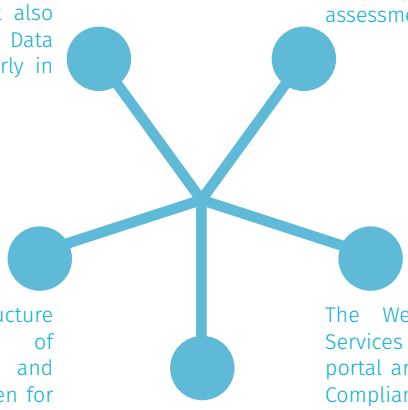
The CSA approach includes five key verticals that should be executed to assess the respective Project portal strengths and weakness.

The outline scope for Security Compliance testing process should be properly documented with steps clearly laid out in the test plan. It should also include layered deliverables with deliverables in each assessment step. The Components included in CSA scope are:

All the below processes are taken up continuously in iterative mode till all the raised vulnerable issues are not mitigated. The CSA process provides granular Security compliance assessment mechanism that would help us to build a viable and fool-proof security posture.

The Business logic Process Compliance check mainly involves Access Control checks (as per ISO 27001:2013), Checks for Out-of-bound processes Being used (like OTPs/password changes etc.), API and Data Security Controls (Data Privacy, Sensitive Data Handling etc.),Audit Logs Check of complete process workflow. This test also focuses to ensure that Data Security controls are properly in place or not.

The External facing Infrastructure Assessment covers Configuration/ Firewall Rules and Vulnerability Assessment of in line Perimeter/ Security Devices being in use by respective Project portal. The Public IP Addresses/URLs are also taken up of Security Compliance assessment



The Internal Infrastructure Vulnerability Assessment of internal Servers, Security and network devices is also taken for Security Compliance testing.

The Web/Mobile App/API/Web Services being used by the Project portal are also taken for Security Compliance testing

The Network and Deployment Architecture is reviewed for any security gaps

Rajesh Mishra
Scientist-F
mrajesh@nic.in

Web Shells

Comprises Data Security, Application and Web Infrastructure Audit

Web Sites/ Information ssystems are frequently exposed to code originating from various, possibly unknown/ un-trusted sources. This may include but not limited to hackers uploading malicious contents such as web shells on vulnerable sites.

About Webshell

Typically, web shell is a sophisticated piece of code or program capable of traversing areas of File system of host server, gathering information thru reading code and critical information, Spying on Event Logs, open ports, processes etc. The shell gives the creator/user the ability to create, edit, delete or download any file of choice, to gain root access to server. The following is a snapshot of such webshells.

Affected server are exploited where script owners try to access information saved on this systems. Webshells are scripts written in the supported language of a target web server including PHP, Python, ASP.Net and Unix Shell Script etc.

Web server are subjected to reconnaissance for identification of vulnerabilities that can be exploited leading to installation of the shell script. These are usually possible through public file upload pages and applications vulnerable to remote File inclusion/ Local File Include (LFI).

Impact of webshells

Depending on the sensitivity of the digital assets/services, their presence on the info/ transaction server, may mar the business image as the contents would be of doubtful origin.

Detecting Web Shells

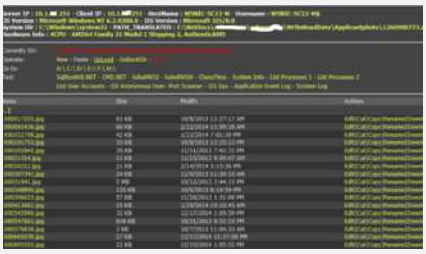
Site owners/admin can detect the presence of shell on their host web server system either by noticing of unusual timestamps, presence of suspicious files in internet available locations. The following snapshot shows the presence of webshells in a file uploads directory. These may go undetected as the names are as per the accepted pattern.

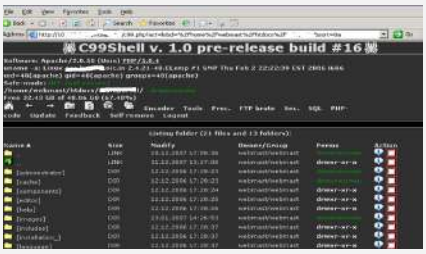
Block Web Shell

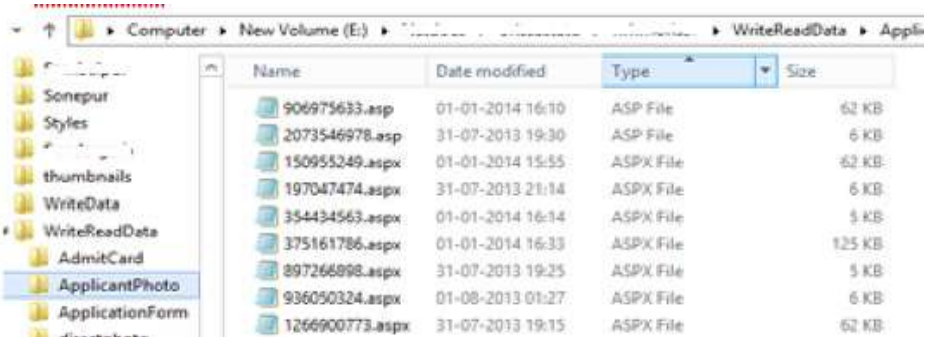
Protection against web shells include, mitigation of web application vulnerabilities. Securing Web server configuration weaknesses including for ex: in case of php, disabling functions such as exec (), shell_exec (), eval () in php.ini makes it hard to execute php based webshell. Web Applications with file upload features should be thoroughly tested.

Conclusion:

It then is the responsibility of all stakeholders to avoid such occasions by proactively contributing to information assurance by complying with security policies and procedures, and periodic monitoring and reporting any suspicious activity or content such as webshells in their respective digital assets and frontiers (web sites/applications).



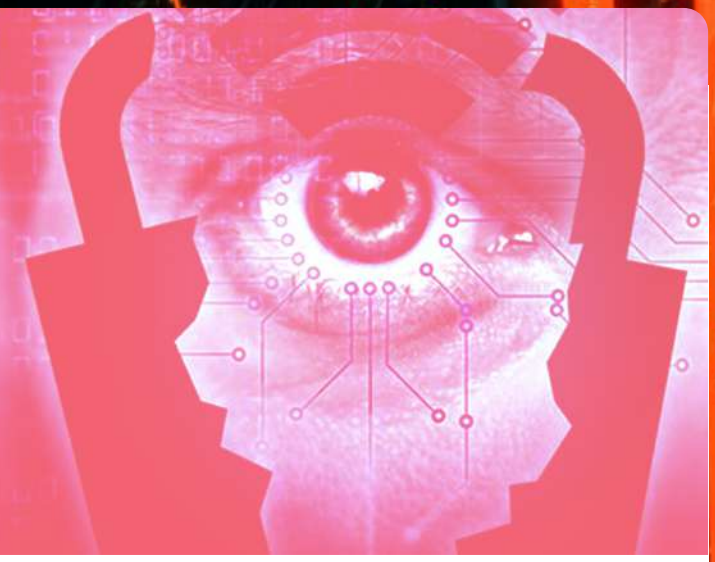




Snigdha Acharya
Scientist-F
snigdha.acharya@nic.in

Detecting Web Infra Vulnerabilities

The imperative facet to secure a software



Web infrastructure consists of Server infrastructure and Application code. If the Web-infrastructure is vulnerable, application also becomes vulnerable to attackers, even if application is audited/ hardened. As time progresses Penetration Testers find vulnerabilities in web infrastructure components (Software components include Operating system, Content Management System (CMS), Plugins, Vendor specific software etc.). These vulnerabilities are published/ reported in security forums. These vulnerabilities are called known Component vulnerabilities in software.

Software vulnerabilities publishing is still process for disclosing vulnerabilities publicly. National vulnerability database (NVD) is one such database which publishes Common vulnerability enumeration (CVE) for vulnerabilities including web infrastructure, CMS etc.

Old version software contains vulnerabilities, which need to be patched or updated to latest versions/patches. Metadata information of Webservers, CMS and errors gives web infrastructure information. Attackers perform identification of web-infrastructure information from website using fingerprinting tools from different metadata (headers, default installation file comments, and configuration files) handlers. Vulnerable Scanners have database of all CVE and privileged (undisclosed vulnerabilities) for different platforms. Insecure libraries and plugins are continuously published in security forums. All these leads to high attack success for attackers. Malicious users continuously scan internet for vulnerable applications to deface/leak critical data/ phishing etc.

Malicious users also perform supply chain attack on software before release to make them use by production systems, example of one such release is php8.1.0.-dev [zerodium vulnerability].

Third party libraries are extensively in application usage due to ease of use. These libraries usage, testing and maintaining is very difficult for production environments because of sole dependency of third party groups.

Software vendors/publishers component security releases are common if software is prone to security issues. Popular web CMS Drupal, Joomla and WordPress had multiple security releases in the past. Identifying these CMS components were very easy to identify as the structure and display of these systems/live Websites are publicly available.

Tools to detect lower version

Opensource Scanners (such as whatweb and wappalyzer) allow filtering of Web-Infrastructure details by scraping the headers, default installations. Open source Scanners , specific to CMS tries to identify vulnerable themes and Plugins. Examples of such scanners are wpscan, droopescan. Open source scanners altogether gives full initial assessment of web applications. These Scanners after modifying the source codes can also be used as full-fledged fuzzing tools for particular vulnerabilities. Enterprise scanners provide full security scan of applications including CMS and other applications. These scanners have also support from respective vendors

Patching Web infrastructure

- Server hardening is one such process to stop disclosing server technical metadata for finger printers/ scrappers. It may not stop fully, if attacker uses automated exploits on applications.
- Patches should be incorporated for Critical Security updates of software releases on regular basis. Minor patches applying to software is less difficult when compared to major version(s), in the production systems, as any downtime in production environment, may not be feasible.
- Organizations should know patch requirement applications based on asset collection for updating/ upgrading/virtual patching (through Web Application Firewall-WAF).Virtual patching can be applied by putting the website behind WAF.
- Applying updates and configuration changes are required throughout the application lifetime to make it free from vulnerabilities.

Kasi Viswanath Kethineni
Scientist-C
kasiviswanath.k@nic.in

Cyber Security Awareness

Quotes & Tips

Coffee and passwords are best when they are strong.

The most efficient cyber defenders: Anticipation, Education, Detection, Reaction & Resilience.

Cyber Criminals need to be right only once. We need to be right always.

Those who do not archive the past are condemned to retype it!

A good programmer always looks both ways before crossing a one-way street.

Cyber Security is a shared responsibility; hold everyone accountable.

Security is a Process; NOT a Product.

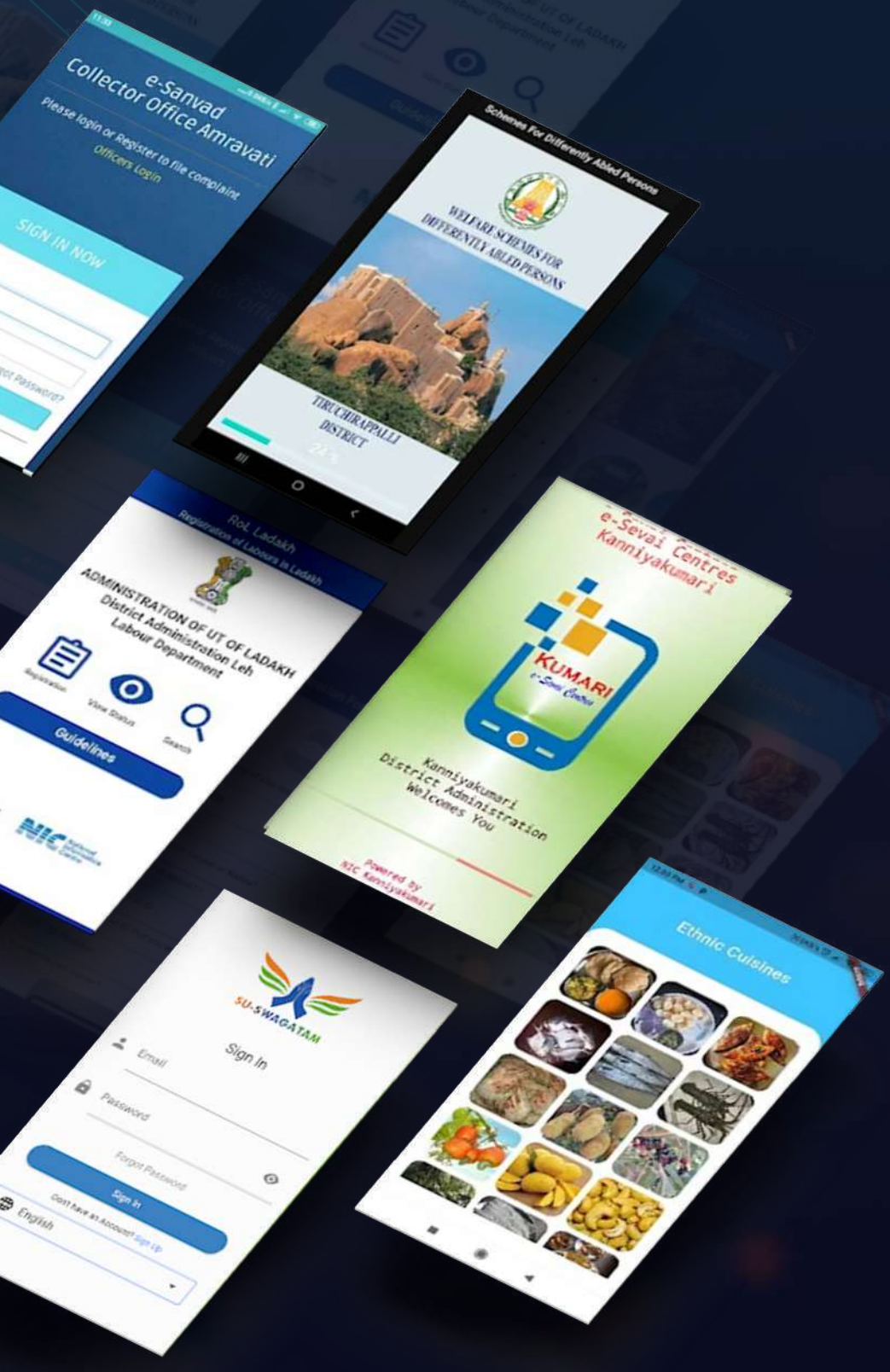
Be suspicious of email attachments, even if they appear to be from a known person.

Security may cause inconvenience sometimes, but is a necessity at all times.

Security is only as Good as your weakest link

Appscape

Showcasing latest mobile apps developed by National Informatics Centre



Welfare Schemes for Differently Abled Person (WS-DAP)

NIC Tiruchirappalli, Tamil Nadu developed 'Welfare Schemes for Differently Abled Person (WS-DAP) Person' Mobile App acts as a citizen charter for differently-abled persons & provides details of welfare schemes implemented by State & Central Govt. Departments.

The government of Tamil Nadu is committed to the all-around development of differently-abled persons. Towards achieving this goal, the State Government created a separate department for differently-abled persons during 1993. As a pioneering step, the Government also formulated a comprehensive welfare policy during 1994. The State Government's endeavor is to create an inclusive society by integrating the differently-abled persons in the mainstream by eliminating all kinds of issues raised by the community. The Government also provides a number of comprehensive welfare measures to different categories of the differently-abled person barriers causing hurdles in their overall development. Several innovative schemes have been introduced to prevent and control the occurrence of disabilities and their after-effect. Many steps have been taken to access the rehabilitation services through recognized and registered Non-Governmental Organizations. The app provides information service on various welfare schemes for the differentially abled.

B V Sivaraman, DIO (dio-trc@nic.in)

Kumari e-Sevai Centres

The e-Sevai Maiyam scheme was formulated under the National eGovernance Plan. The e-Sevai Maiyams located are the front-end delivery channels to provide various Tamil Nadu Government e-services. As per Government guidelines one e-Sevai Maiyam has to be established for 6 Village Panchayats. As 277 Common Service Centres are running successfully in Kanniyakumari

District, the ratio of one e-Sevai centre for one Village Panchayat is established by District Administration, through Public-Private Partnership (PPP) model. In Kanniyakumari District, the PPP model is implemented through various service agencies namely Primary Agriculture Cooperative Credit Society (PACCS), M/s TACTV Ltd., Pudhu Vaazhvu Project (VPRCs) aided by Village Poverty Reduction Committees of the World Bank, Village Level Entrepreneurs (VLEs), International Fund for Agricultural Development (IFAD), Fisheries Department (FSHD) who shall establish and operate e-Sevai Centres which are to be the front end e-service delivery points of various schemes of Tamil Nadu Government. Any common public who wants to avail an e-service, has to always approach the nearest e-Sevai Maiyams to his locality. The IT-enabled Government Services should be accessible to the common man in his / her village, through efficient, transparent, reliable, and affordable means.

G A Shaik Muhamed, DIO (dio-kny@nic.in)

e-Sanvad -Grievance Redressal

NIC has developed e-Sanvad Mobile app to address the grievances of the citizens of Amravati District, Maharashtra. Through this app, Citizens can submit their grievances/complaints with photos & locations, and the Redressal officers can monitor the same for necessary actions. e-Sanvad Mobile app for Grievances Redressal for the citizens of Amravati District. In Mobile based e-Sanvad system citizens can register their Grievances using a Mobile App and the Disposal of grievances and Monitoring is also done by means of a Mobile App. In Government Offices daily no. of Complaints are receiving from Citizens from different ways i.e. Manual, Dispatch, email, Portal, etc. As the no of Complaints and types of complaints are received, Grievance Redressal is the main challenge today's District Administration is facing. Grievance Redressal primarily covers the receipt and processing of complaints from citizens. It includes actions taken on complaints raised by Citizens to avail the Government services more effectively.

- Citizen Registration- App-Citizen can launch their grievances through citizen e-Sanvad Mobile app if he wishes to add photo and location of grievances for the event and location details
- Officers Redressal App- Officers can view citizen's grievances on their mobile app and take the necessary action on the basis of photo and location
- Collector Monitoring- Overall activities are monitoring by Collector and Administration done by Admin Module

B V Sivaraman, DIO (dio-trc@nic.in)

SU-SWAGATAM

The 'Su-Swagatam' Mobile App was launched by the Ministry of Home Affairs, Government of India, and developed by NIC. This app has been designed with a holistic view of serving the visitors at various stages and facilitates foreign nationals intending to visit India, to obtain Visa related services. The main objective of the app is to facilitate Visitors seeking Indian Visa abroad and obtaining visa-related services within India while their stay.

The app will ease out the Indian Visa-related information dissemination to target users. App has been designed with the holistic view of facilitating Visitors at each touchpoint, from getting an Indian Visa to exploring Indian Culture, Heritage, Business Prospects, Medical treatment, Education, emergency services, and Yoga/ Spirituality in India. The App has been enabled with the following informative and facilitative features:

Online Visa Application - e-Visa - Visitors may avail Indian e-Visa through an online application. **Regular Visa** (From Indian Mission / Consulate) - Visitors may fill regular Indian Visa for and submit to the concerned Indian Mission/Consulate. **Visa on Arrival** - Nationals of (Japan, South Korea, UAE) may fill online visa forms prior to landing on designated Indian ports. **Visa & FRRO Status** - Visitors may check the status of their online Visa application & FRRO services.

Anand Swarup Srivastava (anands@nic.in)

RoL Ladakh

NIC Leh, UT of Ladakh developed 'RoL Ladakh' Mobile App facilitates registration and verification of migrant & native labours in Leh & Kargil Districts. This app also builds up a database of labours for assessment of the availability of workers in the districts. RoL Mobile Application is an initiative by District Administration, Leh towards facilitating simple registration of migrant and native labours, verification of the authenticity of particulars for issuance of labour cards, buildup a database of labours for assessment of the availability of workers for various developmental and agricultural works in the district. The objectives of this Mobile application are:

1. To give a platform for the workers to register themselves with the concerned labour department for labour cards from anywhere anytime 2. The labour department to verify the authenticity of workers based on which labour card is to issued. 3. Build up a database of migrant and native workers needed for assessment of the availability of labours for developmental projects and agricultural works. 4. One point data source to facilitate/ enable the citizens in obtaining labour to engage for their domestic and agricultural works as per their requirement. 5. The information collected will be helpful for the assessment of planning, development, and executing of projects. Further, the citizens will also be benefitted from this app as they may search for labours/ workers from anywhere at any time without going here and there for the search of workers to engage in their domestic or agricultural works.

Punchok Paldan, DIO (dio-lld@nic.in)

Sindhudurg District Tourism

The 'Sindhudurg District Tourism' app facilitates the travellers to explore the Tour Circuits of the District with a navigation facility and image gallery of sightseeing places. NIC Sindhudurg developed mobile app aids to discover tourist attractions, accommodations and important contact details of Sindhudurg, Maharashtra. In response to the theme "District Governance through Mobile App," we have attended the six-day training program conducted by NIC Training Division. Work Station is prepared for Mobile App development. IDE is Android Studio and Framework is Flutter. the proposed APP is static in nature and provides information about the tourist destinations in the district and travel plans. The menu items provided in the App is as below :

1. Tour Guide 2. Even Calendar 3. Hotels/ Resorts/ Home Stay details 4. Tourist places 5. Image Gallery 6. Contact details 7. Emergency contacts. The tourist places are categorized into three 1) Beaches 2) Temples and 3) Hill Stations.

The app also provides information on Tour Circuits like one-day and two-day tours. Image Gallery as high-quality photos/ images of major tourist destinations in the district. A navigation facility is provided in the App for easy traverse App. NIC has developed an e-Sanvad Mobile app to address the grievances of the citizens of Amravati District, Maharashtra. Through this app, Citizens can submit their grievances /complaints with photos & locations, and the Redressal officers can monitor the same for necessary actions.

Antony Thomas A, DIO (dio-sin@nic.in)

For NIC apps related query, please contact

Android
Sandeep Sood
Email: sood.sandeep@nic.in | Phone: 0177-2880890

iOS
Andrews Varghese
Email: kerkan@nic.in | Phone: 0497-2700761

Visit the Mobile App Store at
https://egovmobileapps.nic.in

Hon'ble Prime Minister interacted with Covid Vaccine Beneficiaries and Officials of HP through NIC Video Conferencing Services

Hon'ble Prime Minister of India, Shri Narendra Modi interacting with the beneficiaries and health officials of Himachal Pradesh

Hon'ble Prime Minister of India, Shri Narendra Modi, interacted with the beneficiaries and Health officials of Himachal Pradesh on 6th September 2021 on achieving the hundred percent target of Covid19 vaccine vaccination. He appreciated the fact the Himachal Pradesh reached this milestone ahead of all other States despite the difficult geographical and weather conditions. Vaccine beneficiaries from Hamirpur, Lahaul, and Spiti, and Mandi districts interacted with the Hon'ble Prime Minister. Health officer, Asha worker, and Anganwadi worker from Kullu, Shimla, and Una interacted. Hon'ble Prime Minister congratulated the HP on becoming the first State to complete the 100 percent vaccination target.

Shri Jai Ram Thakur, Hon'ble Chief Minister of Himachal Pradesh welcomed Hon'ble Prime Minister and thanked him for providing sufficient quantities of Covid19 vaccine to the State so that all eligible persons could be administered the first dose in a record time. This has been possible due to the production of Covid19 vaccines in the country.

- Ajay Singh Chahal, Himachal Pradesh

Launch of Online Portal of New Central Sector Scheme for Industrial Development of J&K by Shri Amit Shah, Hon'ble Union Minister of Home Affairs

Hon'ble Home Minister & Cooperation Minister Shri Amit Shah launching online Portal for registration under the new Central Sector Scheme for Industrial Development of J&K

Online Portal for registration under the new Central Sector Scheme for Industrial Development of J&K at https://jknis.dpiit.gov.in was launched by Hon'ble Home Minister & Cooperation Minister Shri Amit Shah on 31st August 2021. Union Commerce & Industry, Food & Public Distribution and Textiles Minister Shri Piyush Goyal, Limited Governor of Jammu & Kashmir, Shri Manoj Sinha, Dr. Jitendra Singh, Union Minister of State (I/c) of Science & Technology and Earth Sciences, Minister of State for Home, Shri Nityanand Rai, Ministers of State for Commerce & Industry, Shri Som Prakash, Smt. Anupriya Patel and senior officials of the Government of India were also present on this occasion. Refer Press release at https://pib.gov.in.

This online portal has been designed and developed for effective implementation of the scheme in a transparent manner and with the objective of ease of doing business. The entire process under the scheme i.e. applying for registration, submitting claims and their processing within the Department is through the portal deliberately done to avoid human interface.

- DPIIT Informatics Division, NIC

Hon'ble Union Minister Shri Ashwini Vaishnaw, and Hon'ble Chief Minister of Meghalaya, Shri Conrad Kongkal Sangma jointly launched the MeghEA Project via NIC Video Conferencing Services

The MeghEA initiative is spread across 6 pillars which are Governance, Human Resources, Entrepreneurship, Primary Sector, Infrastructure and Environment. It is envisioned to make Meghalaya a high-income State by 2030. The project aims to improve service delivery and governance for the people using power of digital technologies.

- Informatics News Desk , NIC-HQ

Shri Rajeev Chandrasekhar, Hon'ble Minister of State reviewed the progress of ICT projects at Budgam District, Jammu & Kashmir

The Hon'ble Minister of State for Ministry of Skill Development & Entrepreneurship and Electronics & Information Technology, Shri Rajeev Chandrasekhar recently chaired a meeting with the officials of Budgam District, Jammu & Kashmir to monitor the progress of ongoing and planned projects. He lauded the role played by NIC in driving the country towards inclusive Digital Transformation.

To streamline the delivery of citizen based services residing in far flung areas by leveraging Information and technology, NIC in association with District Administration, had designed Mobile Apps namely 'AurZuv'- providing information on Geo tagged healthcare centers and health e-services, 'Meri-Awaaz' : an Online water bodies grievance redressal portal for protection and restoration of water bodies of District Budgam, 'COVID Care': to monitor patient care at Block level and an App providing online Government services.

-Jit Raj, Jammu and Kashmir

Inauguration of Online Payment Services on Vahan and Sarathi under Transport Department in Mizoram

Hon'ble Transport Minister of State Shri T. J. Lalnuntluanga inaugurated Online Payment Services in Vahan and Sarathi on August 31st, 2021 at Secretariat Conference Hall, MINECO, in Aizawl. The inauguration program was chaired by Commissioner & Secretary, Transport Department Shri K. T. Beicho, IRAS in the presence of selected officials from the Transport Department, SBI, and NIC Mizoram.

Delivering his inaugural speech, the Hon'ble Minister expressed his gratitude towards the State Transport Department, NIC, and SBI for launching online payment services in Mizoram and shared his appreciation for the team involved in achieving the milestone. He also mentioned that the Transport Department, Government of Mizoram had signed a Memorandum of Understanding (MoU) with the State Bank of India for integrating SBIePay in Vahan and Sarathi on June 5th, 2020 however the COVID-19 pandemic and subsequent lockdown caused a delay in the implementation of the system. He then highlighted that the good coordination between NIC and SBI with the Transport Department has been fruitful which made it possible to successfully roll out the project for the benefit of the general public.

Hon'ble Transport Minister of State Shri T. J. Lalnuntluanga inaugurated Online Payment Services in Vahan and Sarathi

Apart from the Transport Minister, Transport Director Shri R. Lalrammawia as well as Transport Project Coordinator, NIC Mizoram, Smt C. Lalmuanawmi and Deputy Manager of SBI Shri J M Dawnga Chhangte also give short speeches.

The inaugural function ended with a Vote of Thanks by Shri Zothangzuala Chhangte, Joint Director (Hqrs), Transport Department, Mizoram.

- Lalhmachhuani, Mizoram

Hon'ble Chief Justice J&K and Ladakh High Court Inaugurated Virtual Traffic Courts

Hon'ble Chief Justice J&K and Ladakh High Court Shri Pankaj Mithal inaugurated two Virtual Traffic Courts at Srinagar and Jammu in an impressive ceremony held at District Court Complex Mominabad Srinagar on 26th of August, 2021. The Virtual Traffic Court at Srinagar was inaugurated physically while, in Jammu through the Virtual mode in presence of the Judges of the High Court of Jammu & Kashmir and Ladakh. Justice Ali Mohammad Magrey, who is also Chairperson of IT Committee, Justice Dhiraj Singh Thakur, Justice Vinod Chatterji Koul, and Justice Sanjay Dhar attended the ceremony at Srinagar whereas, Justice Tashi Rabstan, Justice Sanjeev Kumar, Justice Sindhu Sharma, Justice Rajnesh Oswal, Justice Puneet Gupta and Justice Javed Iqbal Wani attended the ceremony virtually from Jammu wing of High Court.

Hon'ble Chief Justice J&K and Ladakh High Court Shri Pankaj Mithal inaugurating Virtual Traffic Courts at Srinagar

- Jit Raj, Jammu & Kashmir

Inauguration of 'Revenue eServices & Mobile App' by Hon'ble CM of Kerala, Shri Pinarayi Vijayan

Hon'ble Chief Minister of Kerala, Shri Pinarayi Vijayan, inaugurated various Revenue eServices, revamped Revenue Land Information System (ReLIS) Portal, Revenue ePayment Portal, and Mobile Application for Revenue eServices on 9th September 2021 in the presence of Shri K. Rajan, Hon'ble Minister of Revenue, Shri Antony Raju, Hon'ble Minister of Transport, Shri G R Anil, Hon'ble Minister of Food & Civil Supplies, Shri Roshy Augustine, Hon'ble Minister of Water Resources, Shri P Prasad, Hon'ble Minister of Agriculture, Shri Ahammad Devarkovil, Hon'ble Minister of Ports, Shri K. Krishnankutty, Hon'ble Minister of Electricity (through VC), Team NIC (through VC), Shri Biju K, Land Revenue Commissioner, Secretaries, and Officials from Revenue Department. Revenue eServices Mobile App are designed and developed by NIC Palakkad District Centre for the Land Revenue Department, Government of Kerala.

Inaugural address by Hon'ble Chief Minister of Kerala Shri Pinarayi Vijayan during the function

- Asha Varma, Kerala

Hon'ble CM Haryana, Shri Manohar Lal launched the Auto Appeal System (AAS) Portal

Hon'ble Chief Minister Haryana, Shri Manohar Lal launched the Auto Appeal System (AAS) portal (https://aas.saral-haryana.nic.in) on 1st September 2021, a first of its kind of system in India, to ensure the timely delivery of the service to the citizens. This software has been developed for Right to Service Commission Haryana to implement the Right to Service Act 2014 in letter and spirit. During the launch, Shri Deepak Bansal, DDG & SIO made a detailed presentation of all aspects of AAS Portal.

The app will automatically bubble up from Designated officer to Grievance Officer-I, Grievance Officer–II, and the Right to Service Commission.

Hon'ble Chief Minister Haryana, Shri Manohar Lal launching the AAS Portal

- Deepak Sawant, Haryana, Chandigarh

Hon'ble Union Minister of Housing and Urban Affairs, Shri Hardeep Singh Puri, launched NCR Geo-Portal (PARIMAN)

NCR Geo-Portal (PARIMAN) is a unique geo-referenced data repository of about 289 layers for the NCR Planning Board (NCRPB). It is developed by Geo-Spatial Technology & Services Division, NIC on Bharatmaps platform lead by Shri J. K. Mishra Scientist-E under the guidance of Shri Amit Bhargava, Scientist-F and HoD, and Shri Vishnu Chandra, DDG and HoG with the data from NIC, NCRPB, NCR participating States and concerned Ministries / Departments.

It is accessed through log-in credentials and all stakeholders of NCR are given the log-in credentials for this. This is Version-1 and further improvements are planned to make it a robust system to facilitate better sub-regional and local planning. It is launched by Shri Hardeep Singh Puri, Hon'ble Union Minister of Housing and Urban Affairs on 31st August 2021 in the presence of Hon'ble Chief Minister of Haryana, Cabinet Ministers of Govts. of Delhi, Uttar Pradesh, and Rajasthan, Secretary, Ministry of Housing and Urban Affairs, DG, NIC and other senior officers of the Ministry and NIC.

Hon'ble Union Minister of Housing and Urban Affairs, Shri Hardeep Singh Puri, launching NCR Geo-Portal (PARIMAN)

- Geo-Spatial Technology & Services division

Union Minister for Panchayati Raj and Rural Development Hon'ble Shri Giriraj Singh inaugurated the revamped SVAMITVA Dashboard

SVAMITVA (Survey of Villages Abadi and Mapping with Improvised Technology in Village Areas) Scheme is a Central Sector scheme launched by Hon'ble Prime Minister of India on National Panchayat Day i.e 24 April 2020 to be implemented in nine states.

The Ministry of Panchayati Raj (MoPR) is the Nodal Ministry for the implementation of the scheme. The aim of the scheme is to conduct a drone-based survey in Aabadi areas and create Georeferenced household records. In the States, the Revenue Department / Land Records Department will be the Nodal Department and shall carry out the scheme with the support of the State Panchayati Raj Department. Survey of India is the technology partner for the implementation of the survey. The scheme was nationwide launched by the Hon'ble Prime Minister on National Panchayati Raj Day, 24th April 2021.

It is developed by the Geo-Spatial Technology & Services Division, NIC under the guidance of Shri Vishnu Chandra, DDG, NIC. The teams consist of Shri V. Udaya Kumar, DDG, NIC, Shri J. K. Mishra, Scientist-E, and Shri Dhrubajyoti Sarma, Scientist-D Detailed presentation on SVAMITVA Dashboard was made by Shri Udaya Kumar, DDG, NIC during the National Meet.

Hon'ble Union Minister for Panchayati Raj and Rural Development, Shri Giriraj Singh inaugurating the revamped SVAMITVA Dashboard

- Nittal Srinivas, Delhi

Hon'ble Chief Minister, Uttar Pradesh inaugurated the appointment letters distribution ceremony

Hon'ble Chief Minister of Uttar Pradesh, Shri Yogi Adityanath has inaugurated the appointment letters distribution ceremony for 2846 newly selected Lecturers & Assistant Teachers through UPPSC under the Secondary Education Department, GoUP at Lok Bhawan, Lucknow on 12th August 2021 in a mega event.

Allotment of colleges for the newly recruited candidates qualified for Lecturers and Assistant Teachers was done through an online portal by NIC UP eCounseling team. On this special event, the Hon'ble Chief Minister distributed the appointment letters to 11 selected candidates of Lucknow Division and Hon'ble Ministers in charge, and public representatives of all 75 districts were also distributed the appointment letters in the respective district.

Hon'ble Chief Minister, Shri Yogi Adityanath Uttar Pradesh inaugurated the appointment letters distribution ceremony

Dr. Dinesh Sharma, Hon'ble Dy. Chief Minister, UP praised the effort of NIC Uttar Pradesh in the IT-enabled projects successfully implemented in the education sector.

Dr. Satish Chandra Dwivedi, Hon'ble Basic Education Minister, GoUP also highlighted the contribution of NIC UP in various selection processes of teachers.

- Vandhana Singh, Uttar Pradesh

Hon'ble Chief Minister of Meghalaya, Shri Conrad K Sangma Launches, the Mobile App ' The Pensioners' Life Certificate Verification'

On the 15th July 2021, Hon'ble Chief Minister Shri Conrad K Sangma launched the 'Pensioners' Life Certificate Verification' Mobile App, in the presence of Cabinet Minister of Information Technology, Shri Hamletson Dohling, the Chief Secretary, Shri M. S Rao, Addl. Chief Secretary, Smti. R. V. Suchiang IAS, State Informatics Officer & DDG NIC, Shri Timothy Dkhar, Secretary, Finance, Shri P. K. Agrahari, and pensioners who joined the launch via video conferencing.

The mobile app uses Face Recognition as a means of life certification, eliminating the need for a Pensioner of the state government, from having to appear before a Treasury Officer to prove that he is still alive to receive the pension.

Hon'ble Chief Minister Shri Conrd K Sangma, inaugurating the Mobile App 'The Pensioner's Life Certificate Verification'

- Lalhmachhuani, Meghalaya

Hon'ble Chief Minister of Assam launches mVahan & Learner License from Home applications

Hon'ble Chief Minister of Assam Shri Himanta Biswa Sarma today launched two online citizen-centric applications in the Transport Sector – the Learner License from Home Application and the mVahan fitness testing the mobile app in Guwahati, September 03, 2021. The Hon'ble Transport Minister Shri Chandra Mohan Patowary was present in the inauguration.

The mVahan app enables fitness testing of vehicles in any District Transport Office of the State. The App makes it mandatory for the Motor Vehicle Inspector to upload photographs of the vehicles along with the Registration Plate so that fitness testing cannot be done without the presence of the vehicle. mVahan also uses geofencing technology to restrict the fitness testing within 500 m from any designated testing spot. The Learner License from Home marks Assam's foray into Aadhaar-Authenticated contactless services.

Hon'ble CM Assam launches mVahan & Learner License from Home Applications

The Chief Minister has taken the initiative to implement a bunch of about 20 such contactless services in the Transport Sector through NIC in the course of the next six months.

- Kavita Barkakoty, Assam

Inauguration of "DBT on e-Need Based input" Web portal and Input Odisha Mobile App

Hon'ble Minister of Agriculture and Farmers' Empowerment, Govt. of Odisha, Dr. Arun Kumar Sahoo, inaugurated the web portal "DBT on e-need based input" and Input Odisha Mobile App https://dbtinputodisha.nic.in on 2nd August 2021 at Krushi Bhawan, Odisha in the presence of Shri R K Sharma, IAS, Agriculture Production Commissioner, Smt. Kabita Roy Das, DDG and SIO, Odisha, Smt. Anu Garg, IAS, Principal Secretary of Water resource, Shri S K Vashishth, IAS, Commissioner-cum-Secretary, Agriculture and FE, Dr. M Muthu Kumar, IAS, Director Agriculture & FP, Shri R Raghu Prasad, IFS, Commissioner-cum-Secretary Animal Husbandry, Vice-Chancellor, OUAT, Shri Rohit Kumar Lenka, IFS, Director Horticulture, and Director Soil Conservation Shri H K Panda.

Hon'ble Minister of Agriculture and Farmers' Empowerment, Dr. Arun Kumar Sahoo, Government of Odisha inaugurating the web portal "DBT"

Pesticides & insecticides play a vital role in the management of insects, diseases & weeds of different crops. Enforcement of quality use of pesticides is governed by the State government.

- Hara prasad Das, Odisha

Hon'ble Chief Minister of Sikkim Shri Prem Singh Tamang Inaugurated new NIC Building & NKN Operation Centre at Gangtok

New NIC Sikkim Building and NKN Operation Centre were inaugurated by the Hon'ble Chief Minister of Sikkim Shri Prem Singh Tamang on 22nd September 2021 at Gangtok. The function was attended by Hon'ble Cabinet Ministers Shri Kunga Nima Lepcha and Shri Sanjeet Kharel, Advisor Information Technology Shri G.T. Lamtha, Chairman Information Technology Nawraj Gurung, and many senior bureaucrats of the Government of Sikkim.

From NIC, Director General Dr. Neeta Verma participated in the function virtually whereas Deputy Director Generals, D.C. Mishra, R.S. Mani, Dr. Seema Khanna, Seemantenee Sengupta, Manie Khaneja, and a few others from NIC HQ. were physically present at the inauguration function.

Hon'ble Chief Minister of Sikkim Shri Prem Singh Tamang inaugurated the building by cutting ribbons and unveiling the plague

On arrival at NIC premises, Hon'ble Chief Minister was given warm welcome by Hon'ble Ministers Shri Kunga Nima Lepcha and Shri Sanjit Kharel along with Shri D.C. Misra DDG and Shri Birendra Chettri SIO Sikkim.

-Laxmi Prasad Sharma, Sikkim

Launch of a booklet on NIC Telangana State Unit by Hon'ble Minister ITE&C, Industries, and Urban Affairs, Government of Telangana

Shri KT Rama Rao, Hon'ble Cabinet Minister for IT E&C, MA&UD and Industries & Commerce Departments, Government of Telangana has launched the Booklet on NIC Telangana State Unit on 8th September 2021 in the presence of Shri Jayesh Ranjan, Principal Secretary of the Industries & Commerce (I&C), Information Technology (IT) Departments Shri K. Rajasekhar, DDG & State Informatics Officer & NIC Officers.

-Telangana State Centre, Hyderabad

Shri K T Rama Rao, Hon'ble Minister ITE&C (2nd from left) along with Shri Jayesh Ranjan, Principal Secretary of Information Technology (IT) (leftmost), and Shri K. Rajasekhar, DDG & State Informatics Officer (3rd from left) launching the NIC Telangana State Unit Booklet.

Hon'ble Minister, Shri Ram Surat Kumar releases the new look and feel Biharbhumi, and the Online DCLR Court Case Management System of Bihar

The new look and feel Biharbhumi and the Online DCLR Court Case Management System have been officially released by Shri Ram Surat Kumar, the Hon'ble Minister of Revenue, Bihar at the Minister Chamber. The redesigned Biharbhumi was released on 31st July, 2021 and the Online DCLR Court Case Management System was launched on the 1st of August 2021.

Speaking to the Media on the occasion, the Hon'ble Minister mentioned that these two user-friendly citizen centric services with enhanced features have been rolled out to extend better online services to citizen. The citizen has to register self at the portal to avail the Biharbhumi online services.

Release of Biharbhumi, the online mutation portal with new look and feel by the Hon'ble Minister of Revenue, Shri Ram Surat Kumar at the Minister Chamber

- Rajiv Ranjan, Bihar

Hon'ble Chief Minister of Delhi, Shri Arvind Kejriwal launches the Faceless Transport Services

Hon'ble Chief Minister of Delhi, Shri Arvind Kejriwal, launched Faceless Transport Services - a landmark initiative for the citizens of Delhi on the 11th of August 2021. A total of 33 major services - 17 related to vehicles and 14 related to driving licenses have been covered under this initiative. Now, except for two services - Driving Test and Vehicle Fitness Inspection, there is no need for citizens to visit the Transport Office for any requirement and the complete process is online and automated.

As a technical partner to the Delhi Transport Department, NIC has played a major role in this citizen-centric initiative. These services are based on the Vahan and Sarathi platform, which have been extensively customized as per the requirement of the State Government. It may be mentioned that the processes of transport departments are executed through two flagship systems namely Vahan and Sarathi, currently implemented in 1300 RTOs across 34 States / UTs.

- Informatics News Desk , NIC-HQ

NIC wins the Special Award for Aarogya Setu App as a 'COVID-19 Response Solution' at IHW Digital Health Summit

NIC wins the Special Award for Aarogya Setu App, under the category of 'COVID-19 Response Solution', at IHW Digital Health Summit & Award 2021. Shri R. S. Mani, DDG, and Dr. Seema Khanna, DDG, NIC received the award in a virtual event, organized by IHW Council.

Recognizing that the pandemic has digital health delivery 'directly' to the people, Dr. Neeta Verma, Director General, National Informatics Centre has said that privacy issues were addressed during the development of Aarogya Setu. Speaking at the IHW Digital Health Summit and Awards 2021, organized by the leading health awareness institution Integrated Health & Wellbeing (IHW) Council, Dr. Verma along with other leading public health experts and innovators underscored digital platforms as an integral part of the Indian healthcare ecosystem and emphasized on ensuring access for all. At the award ceremony, Dr. Neeta Verma was conferred with the award for Digital Transformer while the National Informatics Centre received the special award for developing COVID-19 Response Solution.