लोकहितार्थ सत्यनिष्ठा

Dedicated to Truth in Public Interest

PursuIT

First Half Yearly Issue, 2020

ICISA

International Centre for Information Systems & Audit
of CAG of India

PursuIT

First Half Yearly Issue, 2020

CONTENTS

About the Journal

The e-Journal “PursuIT" is a platform for sharing of experience and inculcating professional excellence in the emerging areas in the domain of Information Technology. The e-Journal aims at having features on emerging areas of Information Technology viz. cybersecurity, Internet of Things, Artificial Intelligence, etc. The e-Journal also looks into the technological developments, future of technology, national policies and standards, as well as articles on IT Audit conducted in various SAIs.

Editorial Board

Submission of Articles

To support this initiative of e-Journal, we welcome you to contribute Electronic submission of articles from emerging areas in the domain of Information Technology. The article should be relevant to the theme of the upcoming e-Journal and should be in the range of 1000 to 3000 words. All submissions should be accompanied by a short profile of the author. The article is to be sent to icisa@cag.gov.in.

Feedback/Suggestions

We strive for constant improvement and encourage our readers to provide their valuable feedback/suggestions to make this endeavour successful. Send us your suggestions, comments, and questions about the e-Journal to icisa@cag.gov.in.

Disclaimer

Facts and opinions in articles of the e-Journal are solely the personal statements of respective authors and they do not in any way represent the official position of Indian Audit and Accounts Department or of iCISA. This e-Journal is for internal circulation within Indian Audit and Accounts Department only. The contents of this e-Journal are meant for information purpose only. iCISA disclaims all liability for actions taken or failed to be taken based on any content of this e-Journal.

DG's MESSAGE

Keeping alive the tradition of bringing the latest developments in Information Technology matters by way of an Online Journal PursuIT, iCISA is presenting the fourth e-Journal in this series, and the first issue of 2020.

There are articles in the e-Journal which talk about the changing face of IAAD when it comes to presenting our reports in the form of interactive Digital Reports ('Case for Digital Audit Reports') and accepting authentic digital data in scenarios where digital signatures are not functioning ('Ink signatures on a digital file'). In this issue, we are also starting three new sections – '*i*CISA Study Papers', 'We The People' and 'Made in IAAD'. *i*CISA has recently collaborated with other organisations working in the field of IT for three studies related to emerging areas in ICT which will also shape our future audits. These studies will be published in an abridged form in the section '*i*CISA Study Papers', starting with one in this issue related to 'Cyber Security of Smart Cities'. We will publish other studies in subsequent issues of PursuIT. 'We The People' is an attempt to share the experience and knowledge of members of IAAD who are not officially a part of IAAD as of now but still very much a part of it at heart. 'Made in IAAD' is a section which will publish the stories of in-house development of some IT related initiatives by the members of IAAD. You are requested to encourage IAAD members in your own office to share their stories in this regard with iCISA.

I hope that this e-Journal will add value to its users. Considerable effort has gone into bringing it in its present form and the efforts of the officers who have contributed to it needs to be appreciated. I will also acknowledge the efforts of members of the Editorial Board who provided timely inputs despite their busy schedule. We look forward to your valuable suggestions to make this e-Journal even better in days to come.

K R Sriram
Chief Technology Officer, IAAD &
Director General (iCISA)

Highlights of IT Audit Reports

Information Technology Audit of e-Aushadhi

Name of the State Audit Office: PAG (Audit), Punjab
Report No 4 of 2019 – Social, General and Economic Sectors Non PSUs
Nature of the Project: Web based supply chain inventory management system

Introduction:

With a view to strengthening and streamlining the supply chain management system for storage and distribution of drugs and consumables in the State of Punjab and to eliminate the prevailing manual system of processes followed in the hospitals where the chances of human errors are significant, a customized Drugs and Vaccine Distribution Management System named 'e-Aushadhi' was implemented (August 2014) in Health and Family Welfare Department. The application was developed using programming language Java, with front-end as Red Hat JBoss 6.1 and Database in PostGRES 9.1 (EDB).

Highlights:

(1) Planning and Management - No milestones set for rollout

In the first phase, the implementing agency decided (October 2014) to implement e-Aushadhi. In 100 (out of 485) institutions and three Regional Drug Warehouses (DWH). The application was implemented in these institutions up to March 2015 but no timelines were fixed for rolling out the system in the remaining health institutions.

Also, out of five modules of e-Aushadhi, one sub-module 'Issue to patient' (end user) under the main module 'Inventory Management' was not functional in any of the health institutions as of March 2018.

(2) Application controls

As many as 4,405 delivery challans were frozen[1] after a delay of up to 531 days. In 1,424 instances, the drugs/consumables were accepted with shorter shelf-life by three Drug Warehouses. The users while verifying the supplies of drugs/consumables ignored the system alert with regard to shorter shelf-life in these cases.

1,324 samples of drugs/ consumables were sent for quality check to Central Quality Control Cell (CQCC) after a delay of up to 412 days.

Test reports of samples of drugs/consumables were received after a delay of up to 315 days (387 batches) from Government laboratory and up to 51 days (686 batches) from empanelled laboratories. Activation of drugs not of standard quality (NOSQ) and their distribution showed that the system

[1] *Freezing of 'Challans' means acceptance, by the drug warehouse, of delivery of stock supplied by the supplier in the system e-Aushadhi.*

was not robust and lack of internal control diluted the quality assurance for testing of drugs/consumables.

(3) Internal Controls

Inadequate logical access controls, application standards, audit trails and non-conducting of internal audit showed weak information system security of e-Aushadhi.

This report has presented the Audit Findings related to Process Controls in the order of work flow of e-Aushadhi. This has been aided by a Flow chart of work flow and Audit Findings referring to steps of this Flow chart, thereby increasing ease of understanding.

Access full report
https://cag.gov.in/content/report-no-4-2019-social-general-and-economic-sectors-non-psus-government-punjab

Planning and Implementation of GST IT Project

Executive Department - Union Government, Department of Revenue (Indirect Taxes – Goods and Services Tax)
Report No. 11 of 2019 (Chapter III)
Nature of the Project: Revenue Collection through GST

Introduction:

GST has envisaged integration of tax administration across the country, which required a robust IT backbone. The Goods and Service Tax Network (GSTN) was formed to provide common and shared IT infrastructure and services to the stakeholders for the implementation of GST.

Highlights:

1. In 16 cases, the key validations / functionalities as existing in the rolled outmodules were not found aligned to the applicable provisions. Of these 16cases, the required validation was not included in the Software RequirementSpecification (SRS) itself in seven cases, the validations were not built-in eventhough SRS was correctly framed in eight cases and the SRS provision includeda condition not prescribed in the Act in one case.

2. System validations were not aligned to the provisions of the GST Acts andRules, leaving the following crucial gaps in GST Registration module such as :

a. System failed to validate and debar ineligible taxpayers from availingComposition Levy Scheme

b. Mandatory fields were found made optional or accepting junk values.

c. TDS registrations were allowed under invalid category.

d. Lack of validation of key fields in Registration (Legal Name, Type of

Business and Corporate Identity Number (CIN) with Central board of Direct Taxes (CBDT) and Ministry of Corporate Affairs (MCA) Databases.

3. The payment module, despite being in operation since 1 July 2017, was fraught with operational deficiencies like :

a. Delay in updating the Electronic Cash Ledger (ECL) even aftersuccessful payment of tax by the taxpayer.

b. Lack of assurance on minimum service requirements prescribed for banks.

c. Issues in reconciliation of GST receipts.

d. Issues such as payment initiated before expiry of Common Portal Identification Number (CPIN) but Challan Identification Number (CIN) generated after expiry of CPIN and incorrect display of messages to taxpayers were not dealt with until pointed out by audit.

e. Facility of payment through Debit / Credit cards could not be made available as Ministry did not decide on how to deal with the financial implications. In a system with automated interface between the IT applications of the banks and GST portal, there should be no scope for errors such as invalid GSTIN and expiry of CPIN leading to non-reconciliation of GST receipts.

4. All the IGST Settlement Ledgers were not being generated due to non-implementation of corresponding GST modules, like imports and appeals. This, coupled with the inaccuracies in the settlement algorithm and limitation of the GSTR-3B return in capturing all the information required for settlement, had a bearing on the settlement of funds to the Centre and various States.

a. The incomplete IGST ledgers were partly responsible forRs2,11,688 crore of IGST balance remaining unsettled during 2017-18.

b. Duplicate records were noticed in 6,748 cases in 5 Settlement ledgers,leading to inaccurate settlement of Rs416.07 crore IGST funds for theperiod from July 2017 to July 2018.

5. Business Continuity Policy was not finalised and only Disaster Recovery Planhad been in place.

6. Lack of a systemic approach to change management, coupled with some ofthe deficiencies pointed by this audit remaining unaddressed even after GSTNreported corrective action, indicated the crucial risks existing in theapplication running on the GST portal.

Access full report
https://cag.gov.in/sites/default/files/audit_report_files/Chapter_3_Planning_and_Implementation_of_GST_IT_Project_of_Report_No_11_of_2019_Compliance_Audit_of_Union_Government_Department_of_Revenue_Indirect_Taxes_Goods_and_Services_Tax.pdf

CASE FOR DIGITAL AUDIT REPORTS

- Ms Shefali S Andaleeb , IAAS

Ms. Shefali S Andaleeb, IAAS, M.A. and M.Phil.(Economics), has worked in various capacities in last 20 years.
Her foreign assignments include:
1. World Health Organization Headquarters Audit Geneva and Kualalumpur
2. She was on deputation as Programme Manager with INTOSAI Development Initiative IDI, Norway from March 2010 to March 2015.

Digital transformation marks a radical rethinking of how an organization uses technology, people and processes to fundamentally change business performance
-George Westerman, in Leading Digital: Turning Technology Into Business Transformation.

The Inter-Parliamentary Union (IPU), a global organization of National Parliaments, in its coverage of the Parliaments in the times of pandemic, posed a pertinent question: Can democracy really be distance friendly? There are no easy answers to the question. However, there is "byteful" of emerging data that strongly indicates that legislators, like anyone else, are increasingly resorting to technology and tools to enable Parliaments to continue to work in the times of global pandemic and lockdown. In fact, the continued operation of the Parliaments is even more crucial at the time of such a crisis to maintain legislative oversight over executive. We may be heading towards what is increasingly being called a "new normal". It may not be too far-fetched to think that the new normal for Parliaments could be an increasing reliance on digital tools which help in making remote working possible. Would digital Audit Reports of the National Auditor become one such tool?

The CAG of India prepares approximately hundred Audit Reports annually to report on its compliance audit of government departments and public sector entities, and performance audits on a wide range of subjects including government budget and expenditure, tax and non-tax revenues, social schemes and economic policies implemented through various government departments , public

sector undertakings and government aided institutions at the Union and the State Level. The auditors collect and analyse a vast spectrum of information and statistical data to gain insights into the implementation issues and draw inferences as basis for audit findings and conclusions. A constant challenge faced in drafting audit reports is to find ways of presenting the audit findings in a succinct and incisive manner without being discursive. In past, users of the audit reports have also expressed a view that audit reports tend to be lengthy and data presented in voluminous and not amenable to further analysis.

The other side of the story is the fact that Audit processes themselves have evolved from being document-based to being data-based as more and more functions of the government have got into digital mode. Whether it is tax assessments and collection, or disbursement of funds through public financial management system (PFMS), or whether it is the geographical dispersion of low cost toilets in the country- all this information is now available in the form of digital data.

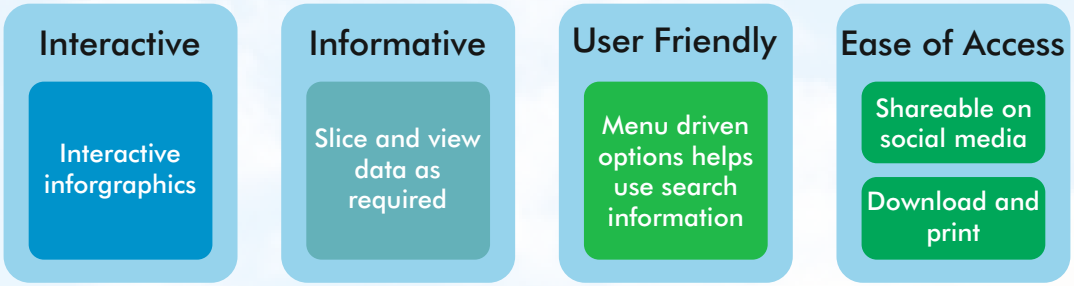
In 2017, the CAG of India decided to commence a pilot project on making the Audit Reports in an interactive digital format, not only to overcome challenges as mentioned above, but also to harness advance data analytic tools that are now available to dig deeper into vast government databases. The Indian Customs Electronic Data Interchange System or ICES is one of the oldest and advanced electronic system of tax assessment and collection in the country. In recent years, the CAG of India has deployed advanced data analytic tools like Tableau and Knime to analyse big data such as Customs revenue database. It was therefore only befitting that the first digital audit report of the CAG of India was based on performance audit of the Customs Department on a very significant subject of inland Container Deports and Container Freight Stations which are a critical link to India's international trade logistics.

This article explores the opportunities and challenges of making digital audit reports by the Supreme Audit Institutions. The article is based on the experience of preparation of the first digital audit report of the CAG of India, in which the writer of this article was closely associated. The digital report was made public in 2019. Though the report is of "pre-COVID" period as one may put it, there are several lessons learned that could be of immense relevance in the times to come.

First Interactive Digital Audit Report of CAG of India

The first interactive Digital Audit Report, digitally signed by the CAG of India, on the Performance Audit of "Working of Inland Container Depots (ICDs) and Container Freight Stations (CFS)" was presented to both the Houses of Parliament on 8 January 2019. Unlike an E-book[2] format, this audit report was designed and prepared as a digital report, using a web-based platform with several interactive features.
See https://cedar.gov.in/AR16-2018-PA-Customs-Union/English.php

Features Of The Interactive Digital Report



The results of data analytics of voluminous customs data performed have been presented as **interactive graphs**, in contrast to two dimensional charts or tables that are usually used in presenting such analysis in a printed format. The advantage of digital medium allowed the report to present the audit findings through visually attractive infographics and the interactive features of the graphs gave readers the **choice of using variety of filters to slice and view data as per their requirement** : for example readers can view imports/exports taking place through various inland container depots (ICD) using filters such as year wise imports/exports, commodity wise imports/exports, commodity and year wise imports/export, and so on. Imports/Exports can be viewed in absolute value terms as well as percentage. The reader can dig deeper into the profile of imports/exports at a selected ICD by filtering data of that particular ICD, for example, the countries through which the imports are coming into the selected ICD and similarly the destination countries of

[2] ***E-book**, in full **electronic book,** is a digital file containing a body of text and images suitable for distributing electronically and displaying on-screen in a manner similar to a printed book- Encyclopaedia Britannica*

exports emanating from the ICD. **Menu-driven options** have been incorporated in the presentation to **enhance the navigation experience.** The **search feature** of the Audit Report helps the user search for specific information and data using key words, which in a printed Report format would have required browsing through the entire report. Thus, the auditee , say the Commissioner of Customs (Import) in an ICD, Tughlakabad in Delhi, will be able to download all the audit findings pertaining to ICD Tughlakabad at a click of a mouse rather than turning hundreds of pages of a printed report.

The users of the Digital Report can share the Report or path of it on social media platforms like Whatsapp, Twitter etc. The report can also be downloaded on individual devices, and if required, can be printed.

STAKEHOLDER RESPONSE

The response to the digital report from the stakeholders – the Parliament, government, and media, hasbeen overwhelmingly positive. In response to the CAG of India's proposal to present his future Audit Reports in a digital format, the Department of Law and Justice of Government of India stated that the Audit Report in digital format is **duly admissible** in lieu of a matter required in writing or in the type written or printed form under the provisions of IT Act 2000. The Ministry of Finance of Government of India has concurred with the CAG's proposal. Most importantly, both the Lok Sabha and the Rajya Sabha have communicated "in principle" approval to accept the audit reports in a digital format stating that it is a **big leap** forward towards digitization of Parliamentary record and reduction in paper. However, they have stated that they need to amend the Rules of Business of both the Houses to accept the Audit Reports as a digital document. Given all of the above, there is no doubt that a good ground has been laid for the CAG's audit reports to go digital.

The initiative of the CAG of India to go digital for presenting audit reports has made the institution of the CAG a front-runner in the community of Supreme Audit Institutions (SAI). The report has been showcased in many fora of the International Organisation of Supreme Audit Institutions (INTOSAI) and has received appreciation of the peers. The EUROSAI IT Audit Working Group has included this report in the list of pioneering examples of work being done in public sector audit[3].

The electronic and print media gave a good coverage to the report once it was made public[4].

[3] *http://egov.nik.gov.pl/g/egov/IN/2017/ICDsCFSs/alg_ICDsCFSs.html*
[4] *https://www.livemint.com/Companies/N448Xxs7no1rB1Pekwevfl/No-policy-framework-for-setting-up-ICDs-CFSs-in-India-CAG.html ; https://economictimes.indiatimes.com/news/politics-and-nation/cag-expresses-concern-over-uncleared-cargo-containing-hazardous-material/article-show/67436843.cms?from=mdr ; https://www.downtoearth.org.in/news/pollution/live-bombs-war-scrap-at-india-s-container-depots-cag-62805 ;*

LESSONS LEARNED

(I) A key lesson which the entire process brought out was that it made us realise that a digital report is not merely an electronic reproduction of printed audit report. A digital report is to be conceptualised as such. In practice this requires a fundamental change in the way we present the audit findings-. Instead of wordy paragraphs, data becomes an integral part of the digital audit report as it allows auditors to narrate the findings through visually attractive, informative and interactive infographics.

On the other hand, if the Audit Report is conceived as a physical document, to be later converted into an electronic document, there is a risk that we transfer the limitations of a physical document into the digital report.

(ii) Another key lesson was the way issues of data ownership and confidentiality of government data were addressed. During the course of preparing the first digital report, one oft-repeated question was regarding data confidentiality of sensitive Customs import /export data that would be put in public domain. Further, if there are errors or inconsistencies of data, who will take the ownership.

The pilot digital report process addressed these issues as follows:

a. All sensitive data – like name of importer/exporter, address , unit prices of imported or exported commodity etc. was masked. Only high level summarised data was put in public domain.

b. While audit took full ownership of the results of data analyses, the basic data remained that of the parent department.

c. Data confidentiality protocols that already exist in the department were complied with.

(iii) Key to a successful digital report is to overcome lagging employee engagement and below-par audit processes. The success of the digital report project was greatly due to a huge buy-in that was created from the very beginning of the project. Thus, what started as initially being seen as a top-driven imposition of a new report format, soon transformed into a collective group effort where both the headquarters' team of CRA wing and the audit teams from field offices worked in close tandem. One important requirement was the way in which audit teams were collecting data and audit evidence- these had to be put together as a database in uniform tabular format rather than as MS word files or scanned documents. The audit teams contributed to the process by putting the data collected in tabular formats created in MS Access. This transformation and buy-in was a key feature to a successful project.

(iv) Going forward, there is a requirement to have an organisation wide policy to address the issues like :

a. Formalising the template of the digital interactive report;

b. Laying down policy for storage and retrieval of digital reports;

c. Working out the modalities with the Ministry of Finance, as a nodal ministry, on the proposed method for obtaining the requisite approval of the President for laying on the report, while also maintaining confidentiality, as well as the procedure to have MoS (F) authentication on the digital Audit Report before it is sent to the Parliament

AUDIT REPORT AS A "DIGITAL DOCUMENT"

Before deliberating on the concept of Audit Report as a digital document, it may be useful to talk about some salient features of what constitutes a document. The International Institute for Intellectual Cooperation[5] defined *"Document" as any source of information, in material form, capable of being used for reference or study or as an authority. Examples: manuscripts, printed matter, illustrations, diagrams, museum specimens, etc.- International Institute for Intellectual Cooperation.*

A digital document is a natural progression in the Information Technology (IT) era where technology has made it possible to express information in various formats.

Over time the notion of document evolved whereby a more functional inference is attached to a document rather than only denoting traditional physical forms of documents. Taking a functional view of what constitutes a document, we should expect documents to take different forms in the contexts of different technologies and so we should expect the range of what could be considered a document to be different in a digital and paper environments[6]. In a digitised environment a **digital document** can be text, image, video, or any combination of these formats.

In short, designing the audit reports in digitally interactive format gives excellent opportunity and a wide canvas for the CAG of India as an organisation to connect with the stakeholders using a variety of mediums such a text, images and videos.

[5] *International Institute of Intellectual Cooperation (1925-1946) established with the aid of the French government and located in Paris, under the Assemble of the League of Nations. It worked on protection of scientific property, library questions, university and school matters, education, youth questions, the future of culture, international collaboration in arts and literature, protection of historical monuments, cooperation between museums and libraries, copyright, etc.*

[6] *Michael Buckland , School of Information Management and Systems, University of California, Berkeley,*

An Audit Report in digital format could be considered as an electronic document which contains text, images and video or a combination of these which communicate the audit findings of the National Auditor, duly approved and digitally signed by the appropriate authority.

DIGITAL AUDIT REPORT AS A LEGAL DOCUMENT

Under Section 4 of Information Technology Act (IT Act) 2000 of the Government of India, legal recognition has been provided to electronic documents, stating that - *Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–*

- *rendered or made available in an electronic form; and*
- *accessible so as to be usable for a subsequent reference*

Section 5 of the IT Act provides for **legal recognition of digital signatures.**

In addition, necessary amendment in the Evidence Act has secured electronic records as 'Evidence' and Parliament has enacted Public Records Act which recognises electronic documents as public documents.

CONCLUSION

Experience of developing the first interactive digital audit report of the CAG of India has clearly proven that presentation of the digital audit reports is viable, it has a high level of acceptance amongst the key stakeholders and users of the report, and the digital audit report qualifies as a legal document.

More so, this initiative of the CAG of India puts the organisaton in the league of a select few Supreme Audit Institutions using the web based interactive format for reporting.

Case for presenting the Audit Reports in a digital format becomes even more stronger in post-COVID scenario as the Indian Parliament and state Legislatures actively consider working in a virtual environment.

Once in public domain, these reports will serve as shareable resource of the Parliament and of citizens.

This section is a new addition to PursuIT. Responding to the fast changing ICT landscape, iCISA took up few studies in collaboration with other organizations working in the field of ICT. Recently three studies were conducted – two in collaboration with the Data Security Council of India (DSCI) and one with the Centre for Development of Advanced Computing (CDAC). The focus of these studies is to come out with audit checklists which the interested Field Offices can then use as an aid whenever auditing an Information System pertaining to these fields. Abridged form of one of such study done in collaboration with DSCI on the theme of 'Smart Cities Cyber Security' aspect is being presented here. The checklists are not being published here as that would have made the article bulky. These can be obtained from iCISA. The other two studies are in the field of 'Data Security in Cloud Environment' (in collaboration with CDAC) and 'Data Privacy in e-Governance Projects' (in collaboration with DSCI). These two studies will be published in subsequent issues of PursuIT.

Smart City Projects: Evolution and Security concerns with reference to Internet of Things (IoT) Technology

Abstract : Across the world governments are conceptualizing smart cities to improve the quality of life of citizens with help of smart technologies. Cities may become smarter, but in absence of a holistic cyber security strategy it may not be a sustainable preposition as with increasing level of digitization, the potential for attack on Information & Communication Technology (ICT) and Operational Technology (OT) components of a city is expected to expand significantly. The emerging risks are rising and becoming advanced like installation of ransomware leading to disruptions, botnet army building a large DDoS against city infra, creating panic and harm to citizens by disabling or sabotaging city infrastructure. The priorities of smart cities is to thwart above attacks and robustly prepare for it. The plan to prepare against complex cyber risks may consist of, strategy, policies, procedures, capabilities and services. It is evident that investment in security would be very productive as the costs of disruption may be quite disproportionate to the investments to be made in cyber security. This paper provides guidance on cyber security of smart cities.

INTRODUCTION

In next two decades more than 600 cities are expected to propel 65 % of global GDP growth and top 100 smart cities may account for 35 % global growth,as per a Mckinsey report. The competition to excel at building smart cities across the world have begun. The objectives are to make future cities vibrant, business friendly, promoting innovation, strengthening infrastructure and enriching living condition of the citizens. Global investments in smart cities are proliferating, no country wants to lag behind, China has currently 300 cities on drawing board, Singapore is planning a smart nation, Taiwan has initiated a USD 625 million IoT fund, Korea is pushing Seoul as model city of the world, Australia is planning 30 minutes smart cities, Denmark is

aiming to become city with zero problems and India is aiming to build 100 smart cities [1][2].

The livability quotient of cities is dripping due to the rapid population influx & urbanization that is straining the city infrastructure, degrading the environment and deteriorating the living conditions. Cities are facing acute pressures of: population growth, economic crisis, higher than normal levels of pollution, increased demands of power and other resources, deteriorating city infrastructure, traffic congestion etc. [6]. It is become a daunting task for the governments and municipalities to even furnish essential public services to the citizens. The only way out of this complex scenario is that the government of a country takes focused and ambitious initiatives to foster sustainable smart cities for resource management and economic growth. For efficient utilization of city resources and other environmental non-renewable resources, there is an urgent need to determine and deploy intelligent & innovative technological solutions for administrating and delivering the city resources [3].

But what exactly is a Smart City? What makes a city smart and intelligent? Even though there is no unanimously accepted standard definition of what constitutes a smart city, however different consortiums and organization across the world have defined smart cities with different approaches. ITU-T Focus Group on Smart Sustainable Cities defines a smart sustainable city as an "innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects. [3]" BSI Standards Publication elucidates, "Smart cities is a term denoting the effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens [4]". European Cyber Security Organisation (ECSO) explains, "A smart city is an urbanised area where multiple sectors cooperate to achieve sustainable outcomes through analysis of contextual real-time information shared among sector-specific information and operational technology systems [6]. NIST defines, "Smart City is the integration of data and digital technologies data into a strategic approach to sustainability, citizen well-being and economic development. [8]"

The systems and infrastructure either from ICT or OT family which city planners are aiming to digitize and integrate, are vulnerable to cyber-attacks from adversaries. The emerging risks are rising and becoming advanced, e.g. installation of ransomware leading to disruptions, city information

tampered, botnet army building a large DDoS against city infra, leakage of smart city databases, creating panic and harm to citizens by disabling or sabotaging city infrastructure.

The city architectural approaches to intertwine ICT and OT warrants a holistic treatment. From bottom to top, it may consist of layers such as sensors, communication, data and application. Each layer requires protection either unique as per its requirements or security which protects layers interconnected to each other. Each component of city is of prime importance from resilience and protection viewpoint, hence requires special attention from cyber security lens.

The priorities of smart cities is to thwart above attacks and robustly prepare for it. The plan to prepare against complex cyber risks, may consist of, strategy, policies, procedures, capabilities and services. Emerging best practices are, but not limited to, end user awareness, end point protection, segmentation of network traffic, data loss prevention, bi-directional DDoS mitigation etc. The ever-rising attack surface is pushing the city boundaries, hence this is the pertinent time to act and build resilient cities at the earliest.

BUILDING BLOCKS OF SMART CITIES

To make cities smart and sustainable, innovative & affordable technology driven solutions must be designed to address the labyrinth economic, social and environmental needs of the city and its citizens such as: clean air & water, adequate and timely food supplies, safety & security of citizens, disaster

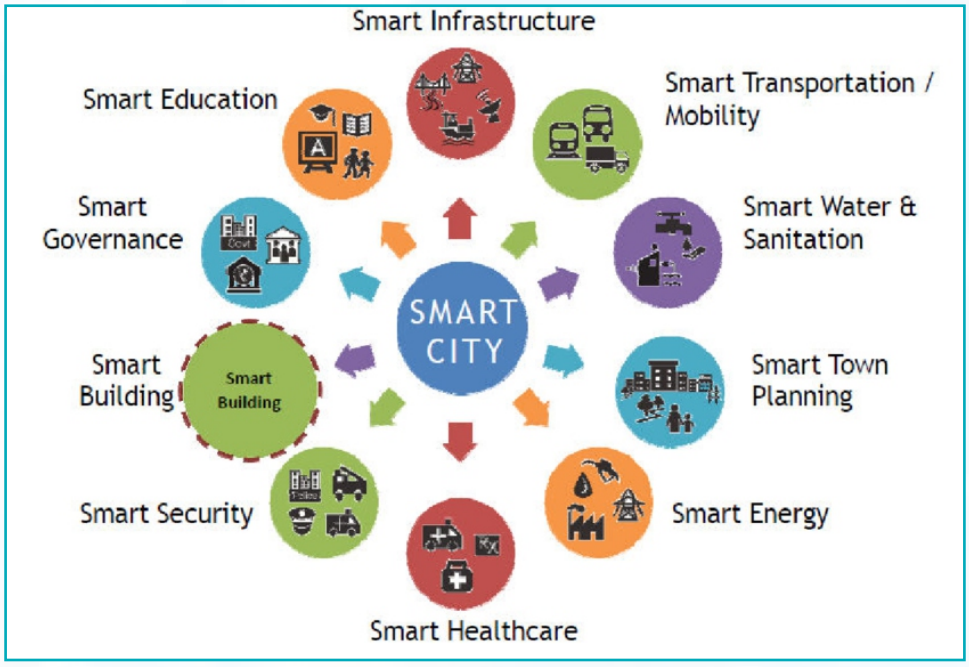


Fig. 1. Building Blocks of Smart Cities [37]

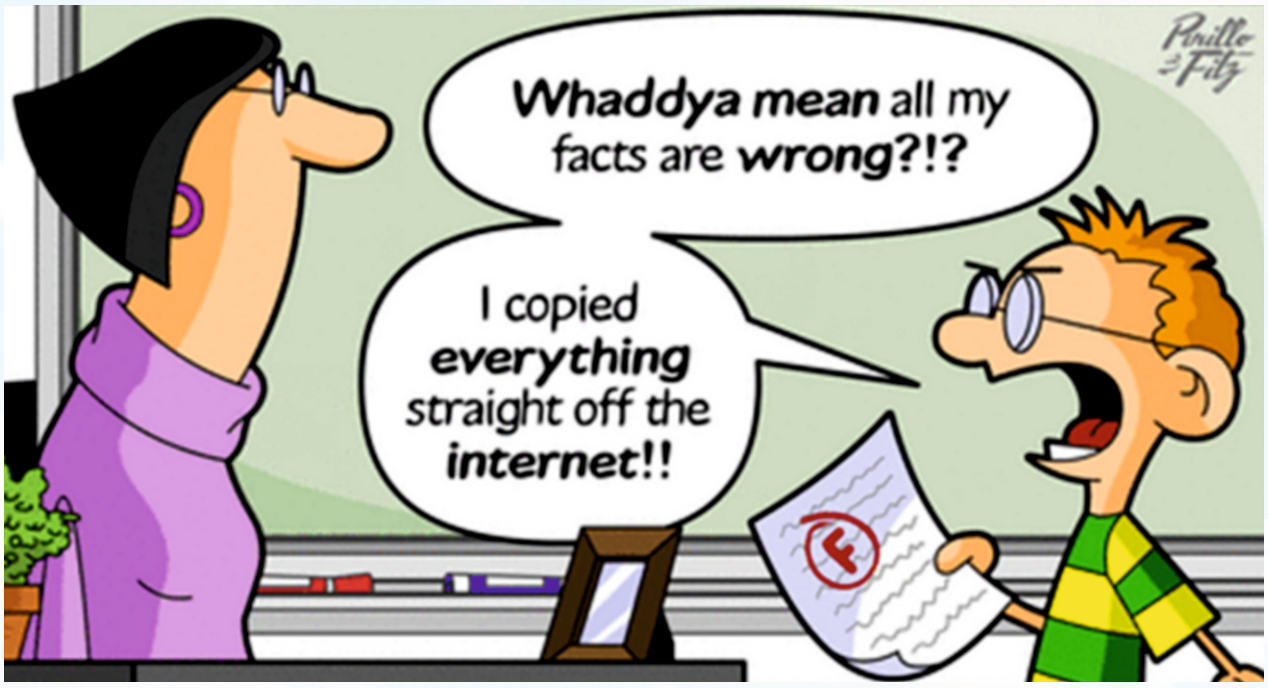
management, ample job and business opportunities, health & wellbeing of citizens and prevention of epidemics, uninterrupted power supply, appropriate waste disposal, convenient means of transportation etc. [4]. These myriad smart city needs are the motivations behind the enlisted building blocks of a smart city as proposed by various consortiums, think-thanks and research organizations. These building blocks and some of their illustrative smart solutions that may be considered are illustrated in figure 1 and table 1. Even though it may not be necessary for a city to roll out all the smart solutions for every building block at its inception stage; an extensible and flexible strategy is recommended while conceptualizing a smart city from scratch. Such a futuristic strategy shall permit fabricating the smart city solutions incrementally. In light of this, it is imperative to have a foresight and interconnect a city's common infrastructure, datasets and technologies[10].

While designing & planning such smart cities the aspirations should be to: (i) enhance the livability conditions in the city which shall in turn improve the quality of life and productivity of the citizens, (ii) contrive and compound the physical or hard infrastructure in the city, (iii) preserve and protect the environmental landscape & natural resources of the city, (iv) boosting the economic growth of the city and fostering circumstances for ease of doing business, (v) ensure equity and social inclusion of citizens from all strata and segments of the city so that every citizen is enabled and empowered to derive benefits from a sustainable smart city; these may become the key performance indicators to evaluate a smart city [9].

A smart city may be planned and developed in three ways depending on city's existing state of affairs and the envisioned smart aspirations from the future city; and Special Purpose Vehicle (SPV) may accordingly strategize the smart projects and initiatives. First one is a retrofitting or improvement-based approach where Brownfield communities are developed by overlaying existing city infrastructure with multiple, smart & innovative ICT based solution and projects. The second strategy is a renewal or redevelopment-based approach where small smart plants such as neighborhoods / blocks / harbors etc. are developed from scratch inside the city or by extending the city. The last strategy is to develop Greenfield cities or New Cities which means to plan and develop the smart city from scratch or ground zero[7][3].

Information and Communication Technologies and Sensor Networks are the underlying backbone of sustainable smart cities. Machine to Machine and Machine to Human communication is what that makes the realization of

smart cities possible. ICT connects and glues together the various building blocks of a smart city for a seamless delivery of services to the end user [5]. The advancements in the Information and Communication Technologies like 4G, LTE, 5G, high speed broadband internet, FTTH, WiFi, Home Area Network like Bluetooth, Zigbee etc. and Wireless Sensor Networks like RFID, NFC, Dash 7 are the propelling fuel for the mission smart cities for countries around the world [12]. It is impossible to foster a smart city without ICT and Wireless Sensor Network (WSN) which form the solid bedrock foundation of every IoET based solution. Some other technological trends and advancements that have accelerated the incubation and blossoming of smart cities are: Big Data Analytics, Cloud Computing, Embedded Systems & IoT, Mobile & Ubiquitous Computing, and Geographic Positioning Systems.



Reference : https://www.rd.com/list/technology-cartoons//

Table 1 : Sample Smart City Solutions For Various Building Blocks

Building Blocks	Smart Solutions
Smart Energy	Smart meters and microgrids to conserve energy based on usage patterns, Energy efficient delivery systems, smart street lighting, Clean energy and low C02 emissions
Smart Mobility	Ride sharing mobile apps, Traffic & congestion management via smart signals, Smart parking, Self driving vehicles, Automated toll and challan tendering, GPS Maps, GPS enabled vehicles and real time navigation support, detailed & accurate public transport schedule
Smart Buildings	Connected & voice controlled home appliances, sensors to monitor and regulate energy consumption, voice support to control devices, smart indoor lighting and temperature control/HVAC, smart home entertainment solutions
Water Management	Smart meters, efficient water distribution networks like electric grids to minimize wastage [11], water quality detectors
Smart Government & Administration	Smart delivery of government services like subsidies & ID documents e.g. renewing DL and vehicle RC, automated tax collection, online delivery of public services via municipalties, GIS linked land usage information for better urban planning [11]
Smart Business & Economy	Civic Hackathons,Online job portals, Improve ease of doing business and streamline tender and procurement processes, Free Public WiFi, boositng e-commerce and delivery channels, video conferencing and alike solutions to improve employee productivity
Smart Tourism	Information booths & kiosks, travel booking help desks & portals, heritage preservation, recreational activities, free hotspots and USB charging sockets [11]
Smart Healthcare	Wearable health monitoring devices, AR/VR based smart solutions for remote health monitoring & diagnosis, Doctor on call like M-Health solutions
Smart Education	Smart classes, AR/VR based virtual learning, E-Learning portals
Smart Security & Surveillance	Face & biometric recognition and use of CCTVs & Drones for live surveillance, Real time video analytics for crime & terrorism prevention
Smart Emergency Services & Risk Management	Real time Social media content monitoring, AR/VR assisted displays for emergency response teams, environment & weather sensors, smart evacuation systems, monitoring air quality, disaster management solutions, fire detectors
Waste Management	Sensors enabled garbage bins, solid waste disposal

Smart City Building Blocks & Threat Landscape

This section maps threats against following five main systems that are essentially required to be in the smart city i.e. Smart Energy, Smart Mobility, Smart Water, and Smart Public Services.

1) Smart Energy [32]

Threats to smart energy categorized into following categories, but not limited to: Network availability, Data Integrity, Information privacy. Some of them are discussed below.

Availability Attacks (DDoS): Open communication infrastructure is embedded into smart grids for data exchange, it makes smart grid vulnerable to attacks such as DDoS. Where it attacks on time constraint and load frequency control of smart grid, creating an adverse impact on delivery of messages and availability of edge devices.

Rogue/Infected devices: Malware propagation in smart grid devices exploits common hardware vulnerabilities. All smart systems are interconnected, due to which distribution occurs at an expedited rate within devices and there is a possibility of its escalation to other architecture layers.

2) Smart Mobility [32]

Threats to smart mobility are categorized into the following categories, but not limited to: Physical Threats, Threats to Communication Channels, Cloud Data Protection.

Fault Injection: Fault/ malicious content injection into vehicle networking components – an attack on ECU module or software controller leads to engine operation failure in smart vehicles and can defeat central managing system.

Man in the Middle: MITM attacks- an interception attack, is executed through various attack mechanisms such as sessions or cookies hijack, wireless network eavesdropping. Man in the middle on communication channel between component of smart cars (for e.g. ECU) and cloud storage results in exposing sensitive information to attacker.

3) Smart Water[33]

Cyber threats to smart city water system are classified into following categories, but not limited to: Threats on Sensing Devices, Sub Component Communication, End User Applications.

Data Tampering: Data being deliberately altered, edited during its transmission from sensors to central storage could allow attacker change water usage readings.

Jamming: Adversaries continuously monitor wireless network to determine frequency of data transferred between two nodes. Attacker could send malicious data packets communication to hinder the reception of data at the receiver end. In water system it could

result in unavailability.

4) Smart Public Services [34]

Emerging technologies and innovation in the traditional urban landscape also brings new threats and risks, which may directly impact residents, city administration and businesses. Cyber security threats applicable to smart traffic control systems, smart lighting systems, surveillance & overall smart city administration are discussed below.

Traffic control system has three major components: 1) Micro Control: Road network strategy, 2) Macro Control: Demand prediction control at every intersection, 3) Information Transmission: Information detector. Compromise of any one of the above components may impact adversely on entire traffic control system. Interception attacks (i.e. MITM) due to vulnerabilities in communication channel would also allow attacker to read information from sensors and manipulate the signals. Traffic and surveillance cameras are the eyes of the city; Vulnerability in DVR and OSD controller or cameras, accidently accessing open internet could make city blind. City authority may not be able to access cameras when required. DDoS is most common attack on smart surveillance.

Smart city administration is responsible for governance and all other management activities within smart cities. Lack of firm cyber security strategy and plans, user access management and security testing would give attacker humongous opportunities to cause harm.

Smart City Architecture Layers & Threat Landscape

In this sub-section we try to analyze possible threats to a smart city as per its different architectural layers.

1) Sensor/Device Layer [35]

In smart city architecture, Internet of things sensor layer incorporates large number of distinct and heterogeneous devices. Radiofrequency Identification (RFID) tags are implemented in the various sensor-based components/devices of smart cities and prone to many cyber-attacks that we discuss here. Communication between RFID tags and reader is achieved via unique product code (EPC). RFID tags are prone to unauthorized access by illegal users causing data theft.

Tag Killing: Tags can be made useless with help of techniques such as application delete or kill command by the attacker. Due to this reader may be unable to read or identify the tags.

Tag Cloning: Tag cloning to gain data from original tag and makes unauthorized copy of the captured data on a new tag.

Spoofing: Spoofing attack, tag data is duplicated and communicated to reader. Spoofing attack exploit vulnerability in protocol used in RFID

communication.

2) Communication Layer [35]

This layer comprises of 4G/5G networks, Network layer and messaging platforms, Internet, WLAN and GPS. Devices/sensors communicate with data layer through cellular / wireless network. Attacks are mainly categorized into four categories and are captured in below representation: Attacks against Authentication, Attacks against Integrity, Attacks against Privacy, Attacks against Availability.

3) Data Layer

The data generated in a smart city from each of the components is expected to be of exponential scale in terms of storage, volume, velocity and veracity. Securely storing the data is one of the major challenge in smart city infrastructure. Threats to data layer discussed below but not limited to following:

Insecure API Communication: Most software and application connected to the Cloud infrastructure use APIs to interact with Cloud services andAPIs usage might get exposed to broken authentication attacks and access control bypass.

Data Leakage at rest - Insecure Encryption, SQL Injection: Data hosted in a multitenant environment, it can be potentially accessed by adversaries or even third-party providers, due to insecure encryption, loose access control policies and SQL injection attacks.

Data in Motion - Sensitive data leak, Availability: Side channel and DDoS scenarios create severe bottleneck hence secure transmission of data flow, automated detection and response are essential part of data protection strategy

4) Application Layer [35]

Application Layer threats are divided into following three categories: Threats to Smartphones / Web Applications, Application Layer Protocols, Operating System Level Threats. Some examples of each are described here.

Buffer over Flow Attack: Web application vulnerability deals with memory allocations and buffers, usually exploited when given low level read and write access to memory. Buffer over flow vulnerability in smart city administration web application would expose sensitive data to the attackers.

SQL Injection: Malicious SQL query injection leads to unauthorized access to the databases vulnerability can exploit the web app by injecting malicious client side script into webpages.

The smart city foundational approaches and architectures differs with respect to objectives a city aspires to achieve. Preceding sections illustrated the basic building blocks of smart cities as proposed by various global consortiums or envisaged by the countries for their cities including India. Next endeavor is to understand smart city architectural distinctions which can be achieved with exploration of architectural approaches and its interconnection with cyber security constituents. It is imperative to learn potpourri of architectural choices as defined by different institutions, to select a hybrid approach based on a city needs, objectives and goals to ensure security, safety and resiliency.

Think tank institutions such as National Institute of Standard & Technology, US (NIST), European Union Agency of Cyber Security (ENISA), and Cloud Server Alliance (CSA) have taken a lead globally to define standard cyber security architectures for smart city implementations. At the same time regulators and capability providers have also defined approaches to secure smart cities globally. This section entails study of cyber security architectures as proposed by various institutions to derive a best practices model for envisioning secure smart cities. In this section we first discuss the Global Architectures proposed and implemented by consortiums and countries, and then we deliberate on India approach to securing smart cities as envisaged by its Ministry of Housing and Urban Affairs Cyber Security Guidelines. Each architectural approach is studied with a framework consisting of following elements i.e. capture the philosophy for broader understanding, nuances of cyber security considerations and key learnings from cyber security perspective while conceptualizing a smart city.

A. NIST [13][14]

Philosophy: Smart city blocks and architecture consist of separate cyber security functions which warrants distinct Treatments.

1) Cyber Security Approaches

- Functions to be considered for cyber security consideration are, but not limited to, asset management, business environment, risk management, identity management, data protection, continuous monitoring, response & recover, incident management, protection processes, awareness & trainings
- For each cyber security function, requirement mapping is warranted

2) Key Learnings

- City needs to build application and device inventory
- Business environment mission, objectives, dependencies needs

alignment with cyber security goals of cities

- Cyber security policy with defined RACI matrix and mapped to compliance landscape
- A separate risk management function consisting of processes, threat maps and mitigation strategies
- Identity and access management encompasses authentication, credential management, remote access, role based access, Network integrity and device management
- Data protection at rest and in motion
- Detection of anomalies and its correlation augmented with robust security monitoring
- Strategy and plans for response and recovery in case of cyber incidents
- Defined protection processes for areas such as secure development, security change management, BCP/DR
- Awareness & Trainings for all stakeholders

B. ENISA[15]

Philosophy: Smart city architectural components require integrated cyber security strategy and ICT and OT cyber requirements intertwines for a safe smart city.

1) Cyber Security Approaches

- Cyber requirements defined for different layers from bottom to top which are field components, data transmission network, data processing, data aggregation & connectivity, smart processing
- Threats mapping as per different architectural layers

2) Key Learnings

- To protect field components hardware and software diagnostics processes and capabilities are a must, other areas include legacy infra refresh, device hardening and building resiliency
- Hardware redundancy strategy and shutdown procedures are to be defined for protecting components pertaining to field which is to be augmented with M2M and network security
- For data processing key elements are encryption, monitoring, debugging, log capturing and monitoring and role of response teams
- Smart processing is to be protected with KPI monitoring, design specifications, InfoSec policy of a city, incident reporting system, web services protection and access control

Guidelines as per other frameworks such as those from Cloud Security Alliance (CSA), France Telecom Authority etc are also part of the detailed study and may be referred to from the full study paper.

RISK ANALYSIS, SCENARIOS AND MITIGATIONS

Many attacks have been reported on smart cities all over the world. A few of them are discussed in Table 2 and what could have been done to prevent such attacks.

Table 2 : ATTACKS ON SMART CITIES

Scenarios	Risk	Mitigation
Oct 2017, one of the major metropolitan city affected badly due to organized distributed Denial of service (DDoS) attack and resulting into crashing entire transport system. Threat's impact on Security Triad: Availability	Transport administration system in one of the European country affected by distributed denial service, larger impact of attack on train traffic management. Train arrival/ departure services had to be managed manually.	Early detection: monitor and analyze network traffic continuously Set up bandwidth limit on network Deploy DDoS protection Solution
In March 2018, Interception attack on smart water treatment plant in undisclosed city in Europe. Threat's impact on Security Triad: Confidentiality	In Water treatment plant, using interception attack mechanisms such as MITM, attacker tried to change the level of chemicals used for water purification. Such attack scenarios could directly harm many lives, posing risks to citizen health safety.	Traffic filtering based on strong rules/ signature and behaviour Employ robust encryption mechanisms Obtain TLS/SSL certification for web applications
Malware attack on air traffic control systems in Nov 2016. Threat's impact on security triad: Confidentiality and Integrity	Malware attack on air traffic control system in one of European country, affected several airports, preventing air traffic controllers from having aircraft information screen.	Secure wireless communication IAM – Authentication/ Authorization Network protection

SMART CITY PUBLIC POLICIES

Globally, countries are working towards thwarting cyber threats against smart cities and are invested in ramping up the security and privacy strategies to protect infrastructure and data. Few countries including India have set a precedent by leapfrogging in taking significant steps on regulations, standards and framework to fortify cyber security for smart cities environment [36]. In this section, we discuss the key learnings from public policy perspective for different countries around the world.

A. United States of America

- The USA government released the Internet of Things Cyber Security Improvement Act, 2017, to establish minimum cyber security standards for IoT devices.
- Multiple cyber security capability firms collaborated to launch a not-for-profit forum 'Securing Smart Cities', which released 'Cyber Security Guidelines for Smart City Technology Adoption.
- NYC Secure is an initiative for citizens of New York City. It includes a free city-sponsored smartphone protection application that will issue warnings to users when suspicious activity is detected on their phones, as well as new protection for the city's public Wi-Fi networks.
- Los Angeles launched a City-Based Cyber Lab to strengthen cyber security for its businesses and residents. The lab is a public-private partnership that will disseminate information and intelligence based on analysis of more than one billion security-related events and over four million attempted intrusions into city networks per day.

B. India

- Ministry of Housing and Urban Affairs (MoHUA) Guidelines: MoHUA, the Government of India, released a model framework for cyber security in smart cities on 20 May, 2016. It covers the security of smart cities across different layers, namely sensor layer, communication layer, data layer and application layer.
- Draft Personal Data Protection Bill: The Personal Data Protection Bill includes provisions to protect personal data as an essential facet of information privacy. The bill provides guidelines on the data processing grounds, rights of the data principal, penalties and exemptions, amongst other areas. The bill aims to protect the autonomy of individuals from data privacy violations by the state and private entities. Once enforced, the bill will impact how the smart city information systems store and process personal/sensitive data.
- The IoT Draft Policy of India discusses the focused pillars of IoT, namely: Demonstration Centres, Capacity Building & Incubation, Standards, R & D and Innovation,

Incentives & Engagements, Human Resource Development, Governance Structure. Many security principals from an IoT perspective e.g. to protect cloud and applications, Safety standards for sensor and device usage etc. are suggested in this draft report.

The Smart City Policies from some other countries may be referred to from the full Study Paper.

WAY FORWARD

As India is on a journey of envisaging 100 smart cities by 2022, we studied issues of cyber security and data privacy emanating from global implementations and analyzed a representative sample of RFPs of Indian cities, twelve in total out of forty published so far by various states, covering categories such as matured, average, below average proposals and RFPs from different parts of India. Enlisted below are some of the key learnings from the research study on Indian RFPs, that must be taken into account while conceptualizing any smart city [21-31].

- Security of field equipment and protection of industrial software systems must be considered and focus should not be only on protecting IT infrastructure while implementing smart city solutions.
- Existing security architectures must be benchmarked against best international standards.
- Clear guidelines that the smart city must follow w.r.t. cyber security and data privacy must be laid down.
- In environments where high information security is required e.g. nuclear power plants, electric power generation etc., data flow must be restricted to uni-directional using data diodes.
- Onus for designing and planning cyber security & privacy requirements of a smart city, must not lie only with system integrators. Cyber security requirements of a smart city must be planned holistically in consultation with all stakeholders. Also a SLA must also be defined for cyber security requirements.
- All applications must be tested for performance & security.
- Continuous monitoring should be done in real time and logs be maintained and analyzed for thwarting cyber attacks.

We end our study of cyber security concerns with respect to smart city projects around the world, by proposing the following layer wise best practices that we segregate under two categories: Minimum, that must be adhered to while envisioning & planning a smart city; and Advanced, which are good to have and may be followed as per budget and time constrains. We also discuss the governance best practices for smart city security issues.

A. Application Layer

1) Minimum

Security Incident and Event Management: Analyse log and event data in real time to provide threat monitoring, event correlation and incident response.

Identity and Access Management: The capability to manage the complete lifecycle of a user and devices. It may have capabilities of federated identity and role-based access control that automatically matches job roles, business unit identifiers and locations to their relevant privilege levels.

Encryption: The message exchange between various applications in the smart city is to be encrypted and authenticated.

2) Advanced

API Management: Applications outside the Data Centre (DC) may talk to the applications hosted in the datacentre through only predefined APIs with planning, design, implementation, testing, publication, operation, consumption, maintenance, versioning and retirement of APIs.

Web Application Firewall: WAF to protect web applications and APIs against external and internal attacks, monitor and control access to web applications, and collect access logs for compliance/auditing and analytics.

B. Data Layer

1) Minimum

Framework of Data Exchange: Data exchange between various sensors and their management applications may happen via this layer, thus making it one true source of data abstraction, normalization, correlation and enable further analysis on the same. Adequate security should be deployed to protect data layer from data confidentiality breach and unauthorized access.

2) Advanced

Data Loss Prevention: DLP solution may require capabilities to secure data both at rest and in motion. To discover sensitive data within an organization and mitigate the risk of its loss at the endpoints, in storage and over the network.

It may have centralized management console, support for advanced policy definition, event management workflow and reporting.

C. Communication Layer

1) Minimum

Gateway Protection: The connectivity provisioning via gateways needs to include elements such as authentication with identifiers and its traffic to be encrypted. The gateway traffic is recommended to be monitored for anomalous behaviour as per city infrastructure functioning.

Demilitarized Zones: The internet facing part of the data centre should have a demilitarized zone where all the customer application servers would be located that are customer facing.

2) Advanced

Network Segmentation/Zoning: The data centre is to be segmented into multiple network zones with each zone having a dedicated functionality e.g. all sensors for one operational domain may connect to the data centre in different dedicated zones, and the internet facing side of the data centre is recommended to be in another zone. All the sensors in the Smart city should connect to a completely separate network. Wireless layer of the Smart City Network may be segmented for public and utility networks by using Virtual Private Networks (VPNS) or separate networks in the wired core, so that any traffic from the internet users is not routed into the sensor networks and vice-versa.

Network Flow Visibility: From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. Wireless broadband plan and architecture for the specific city may be prepared.

D. Sensor Layer

1) Minimum

Discovery Capability: Asset discovery capability for operational technology environment is a software-only product (native Windows or Docker container) that discovers city network topology, device identity, hardware and software configuration, and data flow. It is to capture configuration data that passive scanning may not be able to deliver.

Authentication: The process of introducing and on boarding devices into an IT/OT environment must be securely controlled while meeting the specific requirements of different OT environments. Capability may provide several environment alternatives for device registration models, including automated device registration which enables secure, without manual intervention, physical control, or system access to target devices.

2) Advanced

Sensor Network Security: Isolated networks is to be marked with identifiable boundaries. A program of boundary scanning will help to identify leaks with ease. Map the consequences of violating the network separation, if violations occur, clear significances should be established. All sensors deployed as part of IT and OT based systems in the smart cities may communicate with only authorized wireless network, and do not connect to the rogue networks. All traffic from the sensors in the smart city to the application servers is recommended to be encrypted with SSL and authenticated prior to sending any information. The data at rest and in transit must be encrypted.

E. Security Governance

1) Minimum

Security Governance: The entire Information Technology (IT) infrastructure deployed as part of Smart city should follow standards, policies, frameworks like below and as applicable and appropriate.

- Data Privacy and Information Security Policy
- Information Security Management: ISO 27001
- Business Continuity Management: ISO 22301
- Sustainable Cities and Communities: ISO 37120
- Security Controls for Cloud Security: ISO 27017
- Cloud Privacy Protection: ISO 27018
- Smart City Standards: BSI PAS 180, BSI PAS 181, BSI PAS 182
- Wi-Fi access - PEAP (Protected Extensible Authentication Protocol), 3rd Generation Partnership Project (3GPP)
- DSCI Privacy and Security Framework

The reference architecture of Information Technology (IT) infrastructure in Smart city suggested by National Institute of Standards and Technology (NIST) serves as a common starting point for system planning while promoting interoperable functional building blocks, which are required in a smart city.

Cyber Incident Management: Cyber Incident Management teams need to be set up to manage and mitigate the cyber incidents and risks for the smart city. All the information on incidents be shared regularly with the respective Computer Emergency Response Team (CERT) of the country and designated cyber security incidence response teams of the smart city and take help to mitigate and recover from the incidents.

Processes and Procedures for Secure Disposal: Consisting of elements such as secure device disposal, inventory removal, data purging, data archival and records management etc.

2) Advanced

Security Testing: All applications, ICT and sensing layer including sensors should undergo vulnerability assessment and penetration testing before deployment and prior to every version change/upgrade. In case of no changes, a yearly vulnerability assessment and penetration should be conducted.

This is abridged version of Way Forward. Complete recommendations may be referred to from the full Study Paper.

References :
[1] Stories tagged 'Smart Cities'", Nextcity.org, 2018. [Online]. Available: https://nextcity.org/daily/tags/tag/smart%20cities. [Accessed: 28- Nov- 2018].
[2] The most insightful stories about Smart Cities", Medium.com, 2018. [Online]. Available: https://medium.com/tag/smart-cities. [Accessed: 28- Nov- 2018].
[3] ITU-T Focus Group on Smart Sustainable Cities, "Setting the framework for an ICT architecture of a smart sustainable city", ITU-T, 2015.
[4] The British Standards Institution, "Smart cities – Vocabulary", BSI Standards Limited, 2014.
[5] P. Budde, "Smart Cities of Tomorrow", in Cities for Smart Environmental and Energy Future: Impacts on Architecture and Technology, S. Rassia and
P. Pardalos (Eds.), Ed. Springer, 2014, pp. 9-21.
[6] European Cyber Security Organisation (ECSO), "Smart Cities and Smart Buildings Sector Report: Cyber security for the smart cities sector", 2018.
[7] CISCI, CNBC TV18, moneycontrol, "Digitizing India Smart Cities."
[8] NIST and its partners, "A Consensus Framework for Smart City Architectures (IES-City Framework)", 2018.
[9] Deloitte, "Smart Cities: The importance of a smart ICT infrastructure for smart cities", 2017.
[10] GSM Association, "Keys to the Smart City", 2016.
[11] National Institute of Urban Affairs, m2mpaper.com, "Smart Cities in India - the role of m2m + iot."
[12] S. Talari, M. Shafie-khah, P. Siano, V. Loia, A. Tommasetti and J. Catalão, "A Review of Smart Cities Based on the Internet of Things Concept",
Energies — Open Access Journal of Energy Research, Engineering and Policy (Published Online by MDPI), vol. 10, no. 4, 2017.
[13] NIST, "NIST Smart City Framework", 2016.
[14] NIST, "Cyber Security Framework", 2016.
[15] ENISA, "ENISA Smart City Cyber Security", 2017.
[16] Cloud Security Alliance, "Securing Smart Cities", 2017.
[17] I. Al Mallouhi and R. Daluwakgoda, "Securing Smart City Platforms IoT, M2M, Cloud and Big Data", in RSA Conference, Abu Dhabi, 2015.
[18] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris and D. Barthel, "Security and Privacy in your Smart City", in Barcelona Smart
Cities Congress, Barcelona, 2011.
[19] Trend Micro Forward-Looking Threat Research (FTR) Team, "Securing Smart Cities: Moving Toward Utopia with Security in Mind", Trend Micro, 2017.
[20] CISCO, "Cisco Kinetic Security Technical Paper", 2018.
[21] Ahmedabad Smart City, "RFP I", 2018.
[22] Pune Smart City, "RFP II", 2018.
[23] Bhopal Smart City, "RFP IV", 2018.
[24] Agra Smart City, "RFP V", 2017.
[25] Rajkot Smart City, "RFP VI", 2018.
[26] Gandhinagar Smart City, "RFP VII", 2018.
[27] Varanasi Smart City, "RFP VIII", 2018.
[28] Ranchi Smart City, "RFP IX", 2017.
[29] Cochin Smart City, "RFP X", 2017.
[30] Shirdi Smart City, "RFP XI", 2018.
[31] Faridabad Smart City, "RFP XII", 2018.
[32] Z. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed and M. Peacock,
"Future challenges for smart cities: Cyber-security and digital forensics", Digital Investigation, vol. 22, pp. 3-13, 2017.
[33] S. Ijaz, M. Shah, A. Khan and M. Ahmed, "Smart Cities: A Survey on Security Concerns", International Journal of Advanced Computer Science
and Applications, vol. 7, no. 2, 2016.
[34] I. Barara, "Technology Evangelist", Technology Evangelist. [Online]. Available: https://technologyevaneglist.wordpress.com. [Accessed: 28- Nov- 2018].
[35] A. AlDairi and L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies", Procedia Computer Science, vol. 109,
pp. 1086-1091, 2017.
[36] DSCI and PwC, "Creating Cyber Secure Smart Cities", 2018.
[37] https://www.researchgate.net/profile/Aniruddha_Uniyal/publication/283291632/figure/fig2/AS:391459372060696@14703425-95360/Smart-City-Components-After-Murthy-2015.png

This section is a new addition to PursuIT. IAAD Family is spread far and wide across this globe through current and former members of the Department. Celebrating the spirit of 'Vasudhaiv Kutumbkam - The World Is a Family', this section aims at sharing the knowledge and experience of former members of IAAD.

CLOUD COMPUTING – SECURITY FRAMEWORK

- Sh Alok Ojha

Sh Alok Ojha is currently working as Chief Audit Executive in the World Meteorological Organization. He is experienced as a civil servant in Indian Audit & Accounts Service and international civil servant in the United Nations system. His areas of expertise are auditing, risk management, financial information analysis and controls in IT environment.

The International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) define cloud computing as "a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand". In its general sense describes the provision of computing services through a network from a distant source.

It has issued a security framework for cloud computing which is briefly described here. Interested readers could refer to the ITU publication X.1601 for details.

Cloud computing can be categorized according to deployment and service models, each of these having security implications.

Cloud Deployment Models

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (such as business units). It may be owned, managed and operated by the organization, a third party or some combination of them, and it may exist on or off premises.

The private cloud might be based on resources and infrastructure already present in an organization's on-premises data center or on new, separate infrastructure, which is provided by a third-party organization. In some cases, the single-tenant environment is enabled solely using virtualization software. In any case, the private cloud and its resources are dedicated to a single user or tenant.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Service Models

There are three basic service models, which define the boundaries and responsibilities of the cloud service provider and the client with respect to the use of the hardware infrastructure, associated middleware and software applications:

Infrastructure as a Service (IaaS)

IaaS replaces the client's computing and networking hardware with raw computing resources delivered online, from the cloud (distant data centres), via the Internet;

Platform as a Service (PaaS)

PaaS replaces the hardware, as well as some layers of middleware and software, providing a client with a ready-made application development platform from the cloud where the client can develop, test and run its own applications;

Software as a Service (SaaS)

SaaS delivers complete functionality of applications from the cloud, where all the layers (hardware, networking and software) are managed by the provider. The client mainly uses the applications developed and serviced by the provider.

Benefits

The reasons and benefits for the move towards cloud computing are diverse in nature – technical, financial and functional – but these divisions are not watertight. Technical advantages often enable other benefits, such as collaboration or agility.

Service continuity

"Business continuity", is one of the most appreciated properties of cloud computing for organizations and is often a major reason for moving their operations to the cloud. Whether an organization is experiencing a natural disaster, power failure or other crisis, having critical data stored in the cloud isolates them from adverse conditions at the organization's location

Cost benefits

Cost-efficiency is one of the main promises of cloud computing technology. Cloud suppliers justify this

claim based on the fact that computing resources are shared among clients, and the economies of scale resulting from large data centres while each client is billed for their actual use of resources. Additionally, using public cloud services eliminates the capital investments required to purchase computing hardware, software and associated networking infrastructure.

Flexibility and agility

Most cloud products are preconfigured, tested and designed to be quick and easy to deploy. Clients can normally select the products and operating parameters online through a user-friendly interface, and the service is available for use almost instantly. This is in stark contrast to the lengthy deployment of conventional computing resources and it is rightly perceived as adding significant agility to an ICT environment. The downside of this approach is an apparent lack of flexibility and customization scope in standardized, ready-made cloud products.

Facilitation of innovation

Due to their ability to dedicate significant resources to research and development, large cloud providers are typically able to use and offer recent and innovative products and technology, at a pace that would be difficult to follow for ICT departments of individual organizations. Smaller, specialized providers are also able to offer innovative services in their niche markets.

Modernization of information and communications technology

Cloud technologies may offer a solution for the replacement of obsolete ICT systems. While this benefit may be difficult to quantify, cloud computing can play an important motivational role and be a factor of productive consolidation of organizational ICT.

Handling of Spike Demand

The cloud usage has the ability to cater to temporary or periodic spikes in computing and associated requirements e.g. if there is a heavy load on IT infrastructure on the last few days of the month/ quarter/ year due to filing of forms / returns etc., such a periodic spike is more easily handled through cloud computing rather than creating permanent increase in infrastructure to handle this temporary peak load/ spike.

Cloud computing Security

A growing reliance on cloud computing is prompting concerns over security, privacy and ownership of user data. The challenges associated with cloud computing are also related to confidentiality issues about sensitive or private data. It should be noted that risks can be mitigated, or some aspects of risk can be transferred partially to the

cloud service provider, by ensuring clear contractual safeguards, but there will always be a residual risk.

Some of the risks associated with cloud computing are the same as those inherent to traditional ICT systems that use remote and distributed processing, with data and information travelling through broadband networks and/or the Internet, as well as those associated with outsourced service provisioning, whereby one or several third-party actors intervene, requiring additional security precautions.

Some of the risks in the cloud computing are qualitatively new and emanate from distributed and shared nature of cloud computing. They include issues related to data confidentiality.

Issued in 2015, recommendation ITU-T X.1601 (10/2015) contains a security framework for cloud computing, in which security threats and challenges in the cloud computing environment are analysed and a framework methodology provided for determining which security capabilities require mitigating security threats and addressing security challenges.

Threats and Challenges

Threats have the potential to harm assets such as information, processes and systems and therefore organizations. Threats may be of a natural or human origin and could be accidental or deliberate. A threat may arise from within or from outside the organization. Threats can be classified as accidental or intentional and may be active or passive. The specific threats encountered are highly dependent on the chosen specific cloud service. For example, for a public cloud, threats can arise from the split responsibilities between the Cloud Service Consumer (CSC) and Cloud Service Provider (CSP): complexities of specifying jurisdiction over data and processes, consistency and adequacy of data protection, and maintenance of confidentiality, etc. However, for a private cloud, in general the threats are simpler to address because the CSC controls all the tenants hosted by the CSP. Security Challenges are difficulties other than security threats due to nature and operating environment of cloud services including "indirect threats". An indirect threat is where threat to one participant of a cloud service may have adverse consequences for others. Challenges when not properly addressed may leave door open to threats,

Data loss and leakage This threat emanates from multi-tenancy nature of cloud environment. It is safeguarded by encryption and access management controls. Nonetheless, the possibility of loss of confidentiality exists including leakage and unauthorized processing of personally identifiable information.

Insecure service Access The system

administrator credentials are more vulnerable in a cloud computing environment because it is difficult to use location data to reinforce identity controls.

Insider threats Insider threats have the same sources as those in a traditional ICT environment, however their impact is amplified in a cloud environment.

Ambiguity in responsibility Lack of clarity in responsibilities of the service provider and service customer can result in conceptual and operational conflicts. What might be "data controller" role by one side could be seen as "data processor" role from the other. The ambiguity can be accentuated by international role.

Loss of Trust Cloud services often operate as a black box for the customer. There is no means for the customer to directly evaluate the security implementation levels.

Loss of Governance For customers there is almost always a loss of governance of IT systems, specially in public cloud model. The access levels of the administrator determined by the provider may not be in consonance with that of the customer.

Security Capability

Trust Model

A common trust model between the different providers is necessary to ensure a trustworthy service. There are several trust models out there and one which is most relevant and suitable should be implemented.

Identity and Access Management (IAM)

IAM contributes to confidentiality, integrity and availability of service and resources and becomes essential in cloud computing environment.

Physical Security

Physical security – including access control to service provider's premises and equipment needs to be achieved at a level which is commensurate to the value of the data and systems.

Interfaces Security

The communication between service providers and customers happens through interfaces which are secured by mechanisms like authentication, encryptions, digital signatures etc.

Virtualization Security

This refers to the security of the virtualized environment. The hypervisors (the host machine for virtual machines), implement security protocols to protect the guests from attacks.

Network Security

Networks are secured by both physical and virtual isolations and securing communications. They include border access controls and traffic segregation systems.

Data isolation, protection and confidentiality protection

Isolating data of different tenants, protecting them for changes and in accordance with the law is important. Mechanisms to Ensure privacy confidentiality of data based on agreed upon protocols is an important security capability feature.

Security Coordination

Security controls are implemented differently and capability to coordinate between them and ensure that the conflicts are eliminated is a capability to look for in the cloud service provider.

Operational Security

Security policy definitions and related activities such as configuration management, security management, disaster recovery and incident response mechanisms of the provider.

Security Framework

Security framework for cloud computing means understanding the threats and challenges exist and then mapping them against the capabilities of the provider to identify gaps and determine controls that need to be in place.

(1) Identifying Security threats and security implementations of the challenges in the cloud computing service.

(2) Identify the needed high-level security capability based on identified threats and challenges which could mitigate security threats and address security challenges.

(3) Derive security controls, policies and procedures which could provide the security abilities that are needed.

The security framework will thus take a form of a matrix with threats and challenges on one side and capabilities required on the other. Adapting them to the specific environments and threats enables deriving the required security framework. The framework needs to be under continuous review for emerging threats/risks and changes in the security capabilities triggered by changes in cloud service provision network.

INK SIGNATURES ON A DIGITAL FILE

- Sh J J S Anand, Sr AO

Sh J J S Anand is working as a Senior Audit Officer, Data Analytics Group in O/o. PAG (Audit-1), Karnataka. He was the EDP Faculty in RTC Bangalore from 2003 to 2013 and handled EDP Courses in RTC Bangalore. From 2014 to 2017 as an Audit Officer, O/o. Pr.AG (G&SSA), Karnataka, he conducted IT Audits, Transaction and Certification Audits. He is experienced in setting up and connecting to Oracle, MS Sql Server and MySQL databases and querying the data using SQL and other CAATs.

Pervasiveness of digital resources

In this age of pervasive computing almost every audit is an audit in the IT environment. Data in digital format is often the raw material as well as means of doing the audit and the data so used constitutes the main audit evidence too.

Chain of custody issues in audit evidence

Obtaining relevant data presents challenges by way of hesitation of the auditee in sharing the data and delays. Hence, ink signed authenticated requests for data are documented to aid follow up. Whenever the volume of data involved is small enough to support email transmission, official email communications with attachments can be used to collect data and can help support the assertions regarding the integrity of the content of the attachment and the sender as regards non repudiation of the content and the communication as **audit evidence.**

However, more often than not, the data involved is voluminous and run into gigabytes. Hence the auditee institutions copy the data to external hard disks or such other media and hand deliver the media with a covering letter stating that data is provided in the accompanying media, possibly adding the name of the file/files stored therein. While this is sufficient to support the fact that there is an accompanying storage media containing the data, it does not place on record and provide a means to verify what data was sent and whether the data received was the same. This can result in communication gaps and erroneous conclusions, especially when the files transferred are prone to inadvertent editing and saving as can happen with excel and text files. A similar situation in a paper document transfer scenario is taken care of by appropriate page numbering and ink signed initials on each page by the sender. In the case of the transmission of digital files over digital media, there is need to irrefutably bind the covering letter to the digital file/s being transmitted.

Solution

The following process was used to solve the problem when it was encountered in an IT Audit and the auditee was issued a request setting out the process which is outlined below.

How to compute MD5 or SHA256 hash in Windows environment.

1. Open Command Prompt
2. certutil -hashfile<name_of_the_data_file> the above command outputs the SHA256 hash
3. certutil -hashfile<name_of_the_data_file>md5
4. the above command outputs the MD5 hash

For each digital file that is conveyed, the auditee was requested to compute the Md5 hash (128 bits long represented by 32 character long alphanumeric string result irrespective of the size and type of file, including an empty file) and include it in the ink signed reply accompanying the storage media. The receiver (Audit) would recompute the hash and verify that the recomputed hash matches with the hash result mentioned in the ink signed letter. Even small change in the content of the file will result in great change in the hash digest and can be noticed during the matching of the hashes(due to mismatch).

The use of the hash to implicitly apply an irrefutable ink signature on the digital file being transferred was explained and demonstrated to the auditee. The data dump was obtained following this process and validated before using in Audit.

The process was very simple and easy to deploy. Standard built in tools were available in windows and Linux / Unix systems to generate the hashes. The method could be used whether the files were received over emails or on physical storage media.

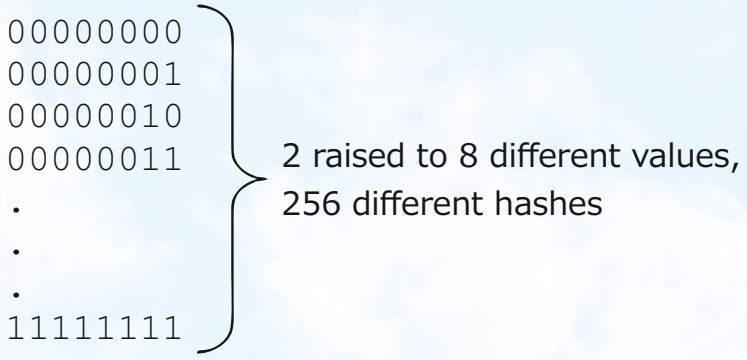
Understanding Hashing

Hashing is a one way process to generate a fixed length output of bits from a digital file of any arbitrary length including an empty file. This output called hash digest or hash serves as a small digital fingerprint of the input which can be arbitrarily large. As long as the input is the same the process results in the same output. This implies that if the stream of bytes constituting a file is not changed in any way, the hash digest of the file will remain the same. The process is so designed that it is computationally impossible to discover (reverse engineer) the specific input which generated the hash digest.

Strength of Hashing Algorithms

There are several Hashing Algorithms such as MD2, MD5, SHA-1, SHA-2, SHA-256, etc. and more will be developed as the processing power of computers increases over time. Sufficiency of

cryptographic strength of a Hashing Algorithm to be employed is decided based on the sensitivity of the data in question. Hence, in the instant case MD5 was used for securing the Auditee to Auditor data transmission though there are stronger Hashing Algorithms[7]. In reality, the hashing process maps the infinite number of digital files possible in the world (each being streams of bytes of varying length and sequence) to the finite number of hash digest values that can exist for any Hashing Algorithm. This can be seen from the following explanation. MD5 outputs a 128 bit hash. For the sake of brevity and ease of understanding if we assume that it is an 8 bit hash, the entire universe of hashes looks like the list below:



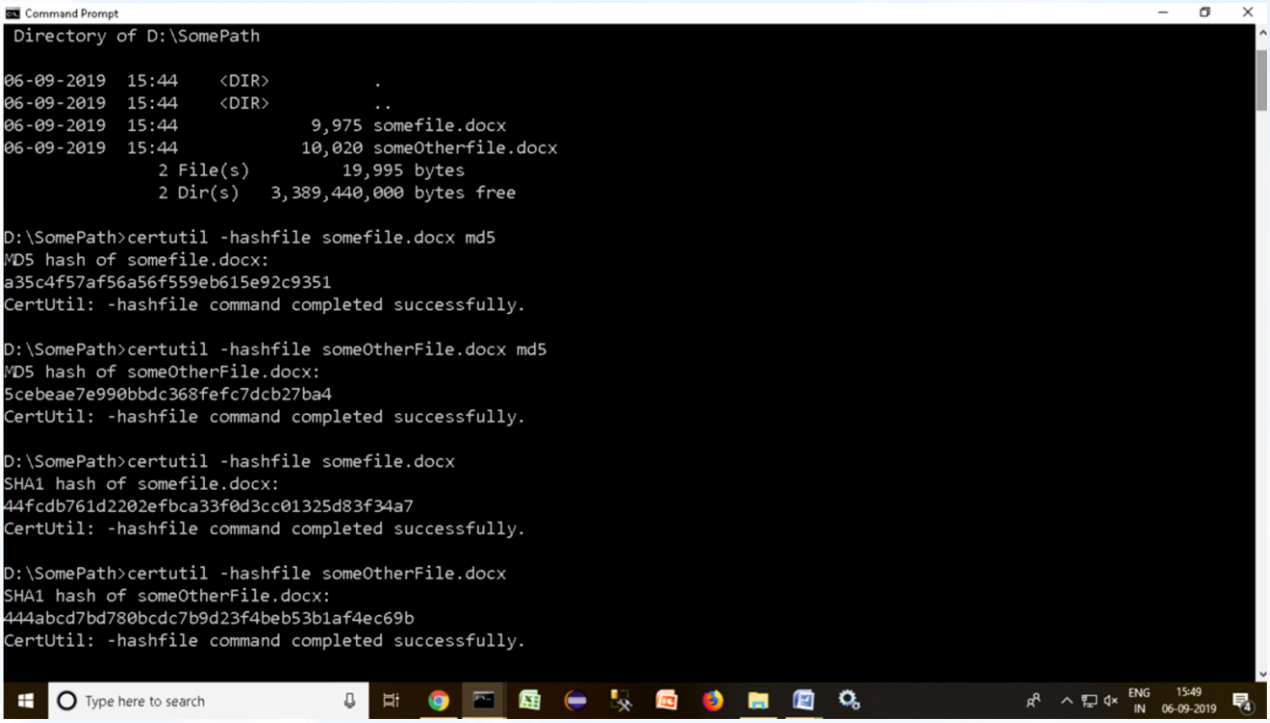
This means there are 256 different hashes if the hash length is 8 bits. Thus if one collected 257 different files (brute force) and calculated hashes, atleast one hash collision is guaranteed. For a 128 bit long hash, there are 2^128 different unique hash results. If 2^128 + 1 different files were collected and hashed, atleast one collision is guaranteed. These are bruteforce methods to discover collisions. Thus for any hash digest value there exists several different input files each of which share (hash collision) the same hash digest. However, as the hash length increases, the above computation effort to identify collisions becomes expensive. Thus, for a given input X and thus its hash digest D, it becomes computationally expensive and hence practically impossible to find another stream of bytes Y whose hash digest is also D when an appropriate Hashing Algorithm is employed.

[7] *IT (Certifying Authorities) Rules, 2000 as of its 2009 amendment has deprecated the use of MD5 in favour of SHA-1 and SHA-2 in the context of digital signature certificates.*

A word about the way forward

This process of including the hash digest as part of communications conveying digital data can be implemented to strengthen the data acquisition process in all audits where digital data is acquired, particularly when adoption of digital signatures and the corresponding verification processes have not matured enough in the auditee and auditor.

Sample output of md5 / SHA256 hash generation screens



"What we really need in IT
is someone who has super powers."

Reference : https://www.rd.com/list/technology-cartoons//

This section is a new addition to PursuIT. It aims at highlighting the efforts of members of IAAD in developing in-house applications in the field of ICT for achieving certain goal in official functioning thereby easing out the current manual process. iCISA does not personally endorse these applications, yet it appreciates the scientific temper shown by the members of IAAD in developing these.

Automated Module for Quarterly Tour Program Generation

- Sh Abhay Singh, IAAS

Sh Abhay Singh, IAAS is currently posted as Director (Research / IT Audit), iCISA. Since childhood he has been fascinated by how stuff works and that took him to field of Engineering. He did his B.Tech. in Electronics & Communication Engineering. With time he fell in awe of the most intricate machine - the human brain. This has taken him to field of Psychology and he is currently pursuing Masters in Psychology. As a developer in his previous job as Research Engineer in Department of Telecom, he feels that Technology can create a lot of transparency, at the same time it can cause a lot of opacity too. He believes that its the job of an Auditor to make sure that Technology remains a slave and doesn't become a master.

Introduction

In the State Audit Offices of Indian Audit and Accounts Department, audit planning is done on an annual basis wherein the units to be audited in a year are picked up from the universe of all the auditable units keeping in mind the risk profiling and resources (human and time etc.) at hand. Once the annual plan is prepared, this is put into action by way of Quarterly tour programmes. The quarterly tour programme is made separately for each functional Sector/Wing (General / Social / Revenue/ Economic etc as per erstwhile nomenclature) within an office wherein the units chosen to be audited in that quarter by the Sector/Wing are allotted to the audit teams available in that quarter with the Sector/Wing.

In the Office of the Principal Accountant General (Audit), Punjab, Chandigarh (henceforth called Office), an automated module was developed in-house to help the different Sectors/Wings in generating the Quarterly tour programme. This article talks about the salient features of this application.

Need for Automation

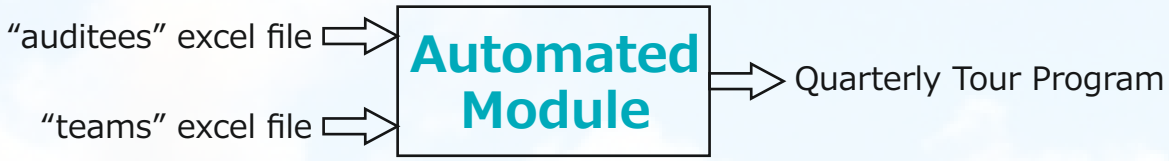
While preparing this Quarterly tour programme a number of checks are applied by the Headquarter section of each Sector/Wing as per the extant departmental/office specific guidelines. Some of these checks are not to repeat the team members who have audited a unit in previous audit; in case an audit of

financial statements for a PSU is ongoing, the compliance audit of such a unit, in case it's due, is to be handed over to the same team; total number of days allotted to a team must not exceed the working days in a Quarter and so forth. Other than this, there is an important human angle to this issue. Some audit assignments are seen easier compared to others due to logistics involved. For example, an audit in Chandigarh is seen much easier than an audit in a border district of Gurdaspur due to traveling hassle and also the lesser amenities present in a remote area. Mostly these so thought easier assignments are limited in number and hence not all audit teams get these. The teams that are not able to get these assignment tend to blame the HQ Section for bias against them even when there might be no such biases at play. Such issues can surface up in any such scenario where human discretion is at play.

Technology can be a saviour for both the above challenges – taking care of the procedural checks as mentioned above, and also ruling out the unwanted human discretion. Leveraging these benefits of technology an application was developed in 'C' language using Dev C++ as the platform, to generate the Quarterly tour programme.

The Automated Module

Since second quarter of 2015 (starting 1st July 2015) the Central Coordination Cell (CCC) of the Office generates the quarterly tour program after taking inputs from the six functional Sectors/Wings in form of two excel sheets named "auditees" and "teams", and then inputting these two files into the automated module which outputs the tour program for each sector individually.



The excel file "teams" has information about all the field teams which will be operating in coming quarter and getting the auditees allotted from "auditees" excel file. It has following format (with one example) –

Sr. No.	Team Id.	Team Members Name	Team Members Salary Code
1	T1	SH. MD. HASIM (Senior Audit Officer), SH. A. K. SRIVASTVA (Assistant Audit Officer), SH. SUMIT (Auditor)	1635, 1984, 2526

ILLUSTRATION 1

Salient points about excel sheet "teams" are :

• "Team Id" is unique field amongst different teams. This "Team Id" will be used in the auditees file in case of any default teams. What is a default team is discussed later in the article.

• "Team members name" field contains all the team members of a team along with their designations.

• "Team members Salary code" field contains the unique codes assigned to the team members of a team. In this Office, the salary codes were used. They can be any other codes either to uniquely identify all the Team members of a Sector.

• "Team members Salary code" field is used to avoid any team getting an audit if any of the team members was present in the last audit of that unit. Here names are not used as many a times Sectors may contain officers with same name. Also there can be slight mis-spelling in names which is not present in case of codes.

The excel file "auditees" has information about all the auditee units which will be audited in coming quarter by a Sector/Wing and has following format (with one example)

Sr. No.	Name of the Unit	Category	Previous Team Members Names	Total Days	Team allotted This Quarter	Address 1	Address 2	Address 3	Previous Team Members Codes	Local Days
1	SUPERINTENDENT, CENTRAL JAIL, KAPURTHALA	A	MANHAR PREET SINGH	10	NA	SUPERIN-TENDENT,	CENTRAL JAIL,	KAPUR-THALA	1152	0

ILLUSTRATION 2

Salient points about excel sheet "auditees" are :

• "Category" defines the risk level – A/B/C – A being highest risk and C being lowest risk.

• "Previous Team Members Names" – as the name suggests, it contains the names of officers who conducted the last audit of this unit.

• "Previous Team Members Codes" – field contains the unique codes assigned to the team members of the team which did the previous audit of this unit. In this Office, the salary codes were used. They can be any other codes either to uniquely identify all the Team members of a Sector. Now "Previous Team Members Codes" of 'auditees' sheet are matched against "Team members Salary code" of 'teams' spread sheet to avoid a unit being allotted to officers who have audited it last time.

• "Total Days" provides the total number of days that are provided to this unit's audit. "Local Days" defines the number of days during the audit that a team will be stationed at Chandigarh. Here it needs to be understood that these "Local Days" are mostly same as

"Total Days" but not always. Especially in long drawn audit assignments such as Performance Audit where a team might need to visit the field units along with the HQ at Chandigarh.

• "Team Allotted This Quarter" is to be mentioned as NA as this field will be auto-filled by the automated module by allocating one of the Team IDs of the team which will audit this unit in coming quarter.

• "Address 1", "Address 2" and "Address 3" are Address of the Auditee.

PROGRAMME LOGIC

These two files are fed into the automated module. The module then allots the Audit teams to all the auditees by taking into consideration these four harmonizing parameters (in that order of precedence) –

1. Audit days need to be evenly distributed between teams of a sector. Here evenly distributed means an allotment where all the teams get total number of audit days within a narrow margin of Standard deviation, e.g. if total audit days in a quarter are 200 and are to be distributed amongst 4 teams, then an example of even distribution is 4 teams getting 47,53,48 and 52 days of audits in that quarter. An example of uneven distribution will be 4 teams getting total 200 days divided as 37, 39, 61 and 63 days of audit in a quarter. Here total days in both distributions (47,48,52,53) and (37,39,61,63) are 200.

2. Local audit days need to be evenly distributed between teams of a sector. This means keeping Audit days evenly distributed, going for an even distribution of local days at Chandigarh amongst the teams by allotting the units having the local days within a narrow margin of Standard deviation.

3. Count of different types of units as per their category (A/B/C) need to be evenly distributed between teams of a sector. After having kept the audit days and local days at Chandigarh within a narrow zone of standard deviation, the count of a particular category of units (A/B or C) will be evenly distributed amongst all teams.

4. Total days of different types of units as per their category (A/B/C) need to be evenly distributed between teams of a sector. After having distributed the above three parameters evenly, choosing a distribution where the audit days for a particular category (A/B or C) are also evenly distributed amongst the teams.

Based on this harmonizing principles, the Automated module generates a text file which has following format (with one example) –

S.No.	Name of Unit	Method of Allotment	Cate-gory	Audit Days	Start Date	End Date	Allotted Team_ID	Allotted Team	Previous Audit Team	Address 1	Address 2	Address 3
1	MD, PSWC, CHAN-DIGARH	COMPUTER GENERATED	A	26			T07	SH. SANJEEV KUMAR (AUDIT OFFICER), SH.DILIP SINGH (ASSISTANT AUDIT OFFICER)	SH. GURTEJ SINGH (SR.AO), SH. DARSHAN SINGH (AAO)	MD	PUNJAB STATE WARE-HOUSING CORP LIMITED	CHAND-IGARH

ILLUSTRATION 3

This text file is then sent to respective Sectors/Wings by the Central Coordination Cell for getting it approved by the Competent Authority. Once approved, this sheet is broken Team wise and audits for a Quarter are handed over to all the teams. Sectors may propose changes in the output generated by Automated Module but all such changes need to be approved by the competent authority.

As it can be seen in Illustration 3, that two columns of "Start Date" and "End Date" of allotment file are empty and are not filled by the automated module. These will be filled by the respective sectors keeping in mind the chronology of audit units taken up by a particular team.

Integrity of Allotment Process

The module also generates a log file having all the steps of allotment for a Sector / Wing. If there is any alteration in the output file, it can be checked against the log file. This log file may be referred to understand the process of allotment and also provides an audit trail.

Gradual Evolution of the Module

Initially entire allotment by the automated module was done on a random basis keeping the broad principles of harmonization intact, as explained above. This means that all teams had equal probability of being chosen for a unit (unless they had one or more team members who have done the same audit last time, in which case this team will not be considered for this unit).

Gradually a demand from Sectors/Wings came that a particular audit assignment such as Performance Audits /Thematic Audits needs to allotted to a pre-decided team. Subsequently, a functionality was provided in the module to meet this demand. For all such units where a Sector felt that the module should not do a random allocation and instead chose a team as decided by the Sector, the HQ section simply needs to mention that Team ID in the column "Team allotted This Quarter" of 'auditees' spread sheet (as shown in Illustration 2 above). The module will not change this default team.

After few Quarters, it was further desired that in some cases, it's not a single field team but a set of few teams which are competent to carry out a certain type of audit, e.g. in Revenue Sector out of 17 teams, 4 teams are considered competent enough to do VAT audits (Value Added Tax was present at that time). This demand was also coded into the module. In such cases the Sector simply needed to mention the multiple Team IDs, eg T1/T2/T4 , in the column "Team allotted This Quarter" of 'auditees' spread sheet (as shown in Illustration 2 above). The module would then consider only these three teams for allotting this unit, keeping the broad principles of harmonization as discussed earlier.

It was also suggested to Sectors that the default teams provided by Sectors should be kept to a minimum else the purpose of this automated module is not achieved to its optimum.

All such default allotments are also

brought to the notice of competent authority to rule out any vested human discretion. This is done by mentioning the "Method of Allotment" in the output file (Illustration 3). "Method of Allotment" column has one of the three values –

• COMPUTER GENERATED – if allotment is purely done by the module

• MULTIPLE DEFAULT TEAMS PROVIDED BY SECTOR - if sector has provided multiple eligible teams out of which one has been allotted by the module by harmonization

• PRE-ALLOTTED TO SINGLE TEAM BY SECTOR - if sector has provided single default team, in that case module doesn't make any changes and simply accepts this allotment.

There were few minor changes too which were suggested by the Sectors with passage of time such as including Mohali along with Chandigarh for audits having local days aspect. Also considering multiples names of same place was also coded into module, eg Mohali got rechristened as Sahibzada Ajit Singh Nagar or SAS Nagar, so these strings to also qualify for local audit days.

One more change that was brought in the module was more of an ease of business issue than related to allotment logic. Earlier Central Coordination Cell (CCC) would collect the auditees and teams files for all 6 Sectors/Wings and would centrally run the automated module. Before doing the actual allotment, the module first checked the entries in these files and suggested errors in data entry, or codes etc. CCC would then get these errors corrected by the concerned Sector and then re-run the allotment module. Often this sanitization process (error cleaning process) would be iterative in nature thereby burdening CCC. On their request, the application was broken down into two parts – Sanitization module and Allotment module. This Sanitization module was distributed to all the Sectors / Wings. Now all the Sectors were supposed to prepare the two spread sheets and run the Sanitization Module on their own till such time that both the files contained no errors. Subsequently, these files were sent to the CCC which would then run the allotment module in one go thereby reducing considerable workload at their end.

Benefits of the Module

The automated module perfectly met the needs of automation as mentioned at the beginning. The procedural checks could be performed with cent per cent accuracy. It also took away the unwanted human intervention in audit allotment exercise. At the same time, there were some other benefits too such as generation of Audit Intimation letters to all the auditees at a single click (using Mail Merge feature) which were earlier being generated manually. This reduced a lot of human effort for all the Sectors and also errors which resulted during manual preparation of these letters.

Way Forward

No machine can match human intelligence. The module doesn't try that either. It takes away and at the same time allows for human discretion in the form of Default Teams, as asked by the Sectors. There are several improvement points that the module can still move towards. One of such betterment point is picking up the unique codes of employees directly from a centralised data base rather than asking the Sectors to fill these in spread sheets, as this process is time consuming as well as can cause errors.

With coming of pan-Department audit process automation system – One IAAD One System (OIOS), may be this information will be available in a much easier manner to the Module through OIOS. Maybe the audit program generation itself will become a part of OIOS someday and the Module will cease to function. These issues will only be answered in times to come. As of now, the automated module is trying to optimally combine the wisdom of human experience with neutrality of a machine.

Reference : https://www.rd.com/list/technology-cartoons//

MANI App

"Mobile Aided Note Identifier (MANI)", a mobile application for aiding visually impaired persons to identify the denomination of Indian Banknotes.

Indian banknotes contain several features which enable the visually impaired (colour blind, partially sighted and blind people) to identify them, viz., intaglio printing and tactile mark, variable banknote size, large numerals, variable colour, monochromatic hues and patterns. Technological progress has opened up new opportunities for making Indian banknotes more accessible for the visually impaired, thereby facilitating their day to day transactions, MANI, has following features:

a) Capable of identifying the denominations of Mahatma Gandhi Series and Mahatma Gandhi (New) series banknote by checking front or reverse side/part of the note including half folded notes at various holding angles and broad range of light conditions (normal light/day light/low light/ etc.).
b) Ability to identify the denomination through audio notification in Hindi/English and non-sonic mode such as vibration (suitable for those with vision and hearing impairment).
c) After installation, the mobile application does not require internet and works in offline mode.
d) Ability to navigate the mobile application via voice controls for accessing the application features wherever the underlying device & operating system combination supports voice enabled controls.
e) The application is free and can be downloaded from the Android Play Store and iOS App Store without any charges/payment.
f) This mobile application does not authenticate a note as being either genuine or counterfeit.

Reference:
https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=49022
https://play.google.com/store/apps/details?id=com.rbi.mani&hl=en_IN

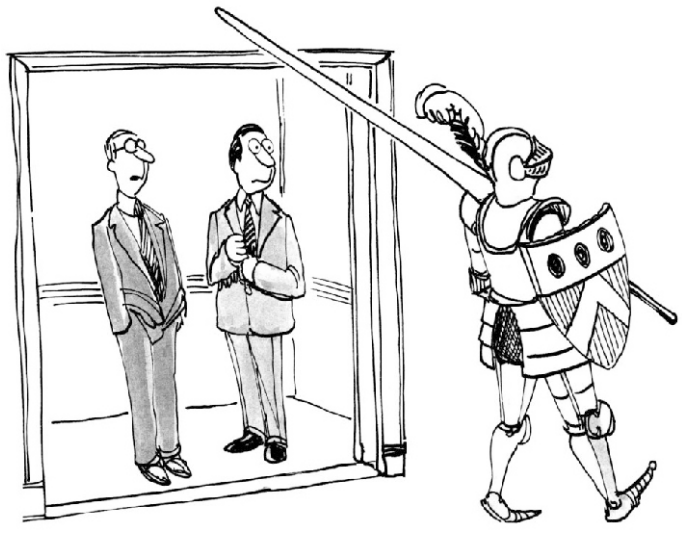
Aarogya Setu App

Aarogya Setu is a mobile application developed by the Government of India to connect essential health services with the people of India in our combined fight against COVID-19. The App is aimed at augmenting the initiatives of the Government of India, particularly the Department of Health, in proactively reaching out to and informing the users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19. User has to keep open the Bluetooth of the device to keep on line.

Aarogya Setu

मैं सुरक्षित | हम सुरक्षित | भारत सुरक्षित

Reference:
https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en_IN



"He really takes IT Security seriously."

Reference : https://www.rd.com/list/technology-cartoons//

1. Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra)

The Cyber Swachhta Kendra is a part of the Government of India's Digital India initiative to create a secure cyber space by detecting botnet infections and to notify, enable cleaning and securing systems of end users. It is a set up for creating a secure cyber eco system in the country in accordance with the objectives of the "National Cyber Security Policy". This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

certin
enhancing cyber security in India

2. e-Aksharayan

e-Aksharayan is an outcome of effort of consortium members sponsored by Ministry of Electronics and Information Technology for converting scanned printed Indian Language documents into a electronically accessible format of - Hindi, Bangla, Malayalam, Gurmukhi, Tamil, Kannada & Assamese. A A4 size Gray level and black 'n' white images up to 3500 × 3500 pixels (BMP,TIFF & PNG) at 300 dpi can be converted into editable text with upto 90-95% recognition accuracy at character level & 85-90% at word level in 45-60 seconds.

It Works on Windows Operating System and also features with Unicode typing tool for typing in Indian Language with Sakal Bharati font (11 Indian Language scripts in a Single font).

Source:-
https://www.cyberswachhtakendra.gov.in/
https://tdil-dc.in/eocr/index.html#features

3. WireGuard: Next Generation Kernel Network Tunnel

WireGuard is the result of an academic research paper which clearly defines the protocol and the intense considerations that resulted in a communication protocol that implements virtual private network (VPN) techniques to create secure point-to-point connections. It aims for better performance than the IPsec and OpenVPN tunnelling protocols using a codebase of around 4000 lines for Linux and may be reviewed by single person.

Cryptographic primitives and the fact that WireGuard lives inside the Linux kernel ensures high speed secure networking.

It is also suitable for both small embedded devices like smartphones and fully loaded backbone routers.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Source:-
Technical whitepaper of WireGuard,
https://en.wikipedia.org/wiki/WireGuard

Reference : https://www.rd.com/list/technology-cartoons//

Quiz Time

1. Which of the following is a cyber security body in India?

a. ISO 27001:2013
b. NASSCOM
c. CERT
d. NeGP

2. An activity of getting information by listening in on telephone, extension line, wiretap or cubical wall while the victim gives credit card or other personal information to a legitimate agent is called:

a. Dumpster diving
b. Shoulder surfing
c. Snagging
d. None of the above

3. What do you mean by CIA triad?

a. Computer Information Assurance
b. Confidentiality, Information, Assurance
c. Confidentiality, Integrity and Availability
d. Confidential Information Acquisition

4. This not only serves as acknowledgement but also helps to validate both sender and receiver is genuine.

a. Email
b. Digital Certificate
c. Private Key
d. Chat

5. In context of computer security, which of the following cannot be termed as threat?

a. Burglar
b. Virus
c. Earthquake
d. Software bugs

6. This is very low- tech approach. A thieve can go through garbage cans or trash bins to obtain cancelled checks, credit card statements or bank account information that someone has carelessly thrown out.

a. Dumpster diving
b. Snagging
c. Spoofing
d. None of the above.

7. What do you mean by DoS attack?

a. Disk Operating System Attack
b. Die of Software attack
c. Dozens of Shoulders attack
d. None of the above

8. _____ refers to finding a user's password.

a. Sniffing
b. Snagging
c. Social Engineering
d. Spoofing

9. Which of the following is not true in context of authorization and authentication?

a. Authentication validates your right to access and possibly change something.
b. Authentication is usually done by a username and password.
c. In authentication, the system determines whether you are what you say you are using your credentials.
d. Authorization refers to rules that determine who is allowed to do what.
e. All of the above are true.

10. The program that act like something useful but do the things that are quite damaging. The programs of this kind are called _____.

a. Virus
b. Worm
c. Trojan
d. Malware

11. Which of the following acronyms refers to a software distribution model in which a cloud provider manages and hosts an app that users access via the internet?

a. IaaS
b. PaaS
c. SaaS
d. None of the above.

12. What is a public cloud?

a. A cloud formation that can be seen across the globe
b. A cloud service that can only be accessed from a publicly shared computer
c. A multi-tenant cloud environment accessed over the internet
d. A cloud environment owned, operated and controlled by a public company

13. ..... is to protect data and passwords.

a. Encryption
b. Authentication
c. Authorization
d. Non-repudiation

14. Open source refers to

a. Free download software
b. Free software
c. Freedom to access source code
d. Source code is inaccessible

15. Which State has become the first state in India to launch free email address in Hindi for its resident

a. Uttar Pradesh
b. Rajasthan
c. Himachal Pradesh
d. Haryana

16. Which is not among the key principles of e-Kranti

a. Mobile First
b. Cloud by default
c. Fast track approval
d. No Language Localization

17. Which is the largest world's largest rural broadband connectivity project using optical fibre

a. Bharat Net
b. India Net
c. One India Net
d. None of these

18. Which one is not a web browser

a. Google chrome
b. Python
c. Internet Explorer
d. Mozilla Firefox

Answers to the Quiz published in previous issue of Journal (2019 Second issue)

QUIZ

Q. NO	ANSWERS	Q. NO	ANSWERS
1	C	10	B
2	A	11	C
3	B	12	B
4	B	13	B
5	D	14	D
6	D	15	C
7	A	16	C
8	C	17	D
9	D	18	D

Disclaimer

This Journal is conceived, designed and presented by International Centre for Information Systems and Audit (iCISA) which is a field Office of SAI, India, i.e. CAG of India, for internal circulation within Indian Audit and Accounts Department only.

This Journal aims to share with readers the latest developments in the field of Information Technology and shall be used for information ONLY. Though all efforts have been made to ensure the accuracy of the facts and figures, the same shall not be construed as statement of law or used for any legal purposes. In case of any ambiguity or doubts users are advised to check it with the authors and officers of iCISA before taking any decision based on information contained therein. The contents of this journal are meant for informational purposes only. iCISA disclaims all liability for actions taken or failed to be taken based on any content of this journal.

This Journal has provided web links to various outside websites also for information ONLY and hence does not assume any responsibility for the contents included therein.

Compiled & Designed By:

Abhay Singh, Director (R&I), *i*CISA
Manish Kumar, AAO (R&I), *i*CISA
Vijay Kumar, Sr. Auditor (R&I), *i*CISA

2020 First Half Yearly Issue