प्रशासनिक सुधार और लोक शिकायत विभाग
DEPARTMENT OF
ADMINISTRATIVE REFORMS
& PUBLIC GRIEVANCES

27th National Conference on e-Governance

Background Papers

TABLE OF CONTENTS

CHAPTERS **PAGE NO.**

Chapter 1

Digital Public Infrastructure: A Roadmap to Enable Seamless Government Services

Authors:
1. NSN Murty, Partner and Leader - Government Industry, Technology and Transformation, Deloitte India
2. Priyanka Yadav, Associate Director, Technology and Transformation, Deloitte India
3. Kanika Kishore, Senior Consultant, Technology and Transformation, Deloitte India

Problem Statement

In today's fast-paced digital era, governments face the challenge of transforming their public services to meet the evolving needs of their citizens. Despite the critical importance of Digital Public Infrastructure (DPIs) in enabling this transformation, there is a notable lack of credible guides that Nations can use to effectively design, build and implement digital public infrastructure that can meet their pressing needs for digitization and access. This deficiency hampers the ability of governments, ministries, and government departments to harness the full potential of digital technologies, resulting in fragmented and inefficient service delivery.

The COVID-19 pandemic has highlighted the critical role of DPIs in responding to crises and maintaining continuity of services. For instance, in India, the CoWIN platform enabled the administration of over 2.2 billion vaccine doses[1], showcasing the potential of a well-implemented DPI in managing large-scale public health initiatives. Similarly, Brazil's digital savings accounts facilitated the distribution of social assistance payments to approximately 70 million beneficiaries during the pandemic, demonstrating the importance of digital financial infrastructures in ensuring economic resilience.[2] During India's G20 presidency, significant strides, and discussions around DPIs have taken center stage. India has highlighted the importance of building robust digital public infrastructures to enhance service delivery and promote inclusive growth globally.

Implementing DPIs has significant economic and social benefits. According to the International Monetary Fund, digital ID systems can greatly enhance financial inclusion and access to services, which in turn can drive economic growth. The World Bank's Identification for Development (ID4D) initiative notes that over 1 billion people globally lack a legal identity, which hinders their access to essential services.[3] Robust digital identity systems can bridge this gap, providing individuals with the means to participate fully in the digital economy. The success of India's Aadhaar system, which has enrolled over 1.3 billion residents, demonstrates the transformative potential of digital identity systems.[4] This system

[1] https://www.cowin.gov.in/

[2] https://documents1.worldbank.org/curated/en/099830009302217091/pdf/P1731660f8c52f062092ac00d53c648bac7.pdf

[3] https://id4d.worldbank.org/global-dataset

[4] https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html#:~:text=About%20UIDAI,-The%20Unique%20Identification&text=The%20UID%20had%20to%20be,to%20the%20residents%20of%20India.

has facilitated financial inclusion, improved service delivery, and reduced corruption by ensuring that benefits reach the intended recipients. Similarly, Brazil's digital savings accounts during the COVID-19 pandemic illustrate how scalable and inclusive digital payment systems can enhance economic resilience during crises.

DPIs are crucial for creating seamless, interoperable, and inclusive digital services that can enhance public service delivery, drive economic growth, and foster social inclusion. DPIs help countries build reusable digital building blocks that can be integrated into any current or future government programs and services. This approach lays a long-term digital foundation for the future, reducing overall design and engineering costs and minimizing duplication, which is otherwise unavoidable with the current platform-centric solution development approach. However, the absence of a standardized methodology and toolkits for implementing DPIs leads to inconsistent adoption and suboptimal outcomes. The need for a comprehensive, ready-to-use roadmap to guide governments through the DPI implementation process is more pressing than ever.

Solution

A systematic approach to DPIs is essential for governments, ministries, and departments aiming to harness the full potential of digital technologies. This involves establishing a robust framework that offers detailed guidance, methodologies, and toolkits to facilitate the seamless adoption of DPIs. Such an approach ensures that public services are efficient, accessible, and responsive to the needs of all citizens.

A strategic roadmap for DPI implementation must focus on key design principles, resource reuse, and sustainable transformation strategies, emphasizing the importance of interoperability, scalability, and inclusivity, providing a clear pathway for governments to follow. It is crucial to address both the technical aspects of DPI implementation and the governance, policy, funding, and stakeholder engagement necessary for success.

Key Tenets of DPI Implementation

1. **Comprehensive Diagnostic Analysis:** The first step involves a thorough diagnostic analysis of the existing digital landscape. This helps identify strengths, challenges, and gaps in the current technological infrastructure. The World Bank emphasizes that digital payments can reduce transaction costs by up to 90%[5], highlighting the efficiency gains that can be achieved through a robust DPI.
2. **Establishing Governance and Policy Frameworks:** Creating clear policies and governance structures is essential for supporting DPI implementation. This includes establishing a dedicated DPI alliance, defining roles and responsibilities, and ensuring accountability and transparency.
3. **Designing Scalable and Interoperable Technical Architectures:** A scalable and interoperable technical architecture is crucial for a successful DPI. This involves incorporating digital identity systems, payment platforms, and data exchange mechanisms. For instance, Estonia's X-Road platform has significantly enhanced the efficiency and transparency of public services by providing a standardized framework for data exchange.

[5] https://blogs.worldbank.org/en/allaboutfinance/how-bring-financial-services-poor-go-digital#:~:text=And%20because%20digital%20transactions%20can,the%20developing%20world%20is%20exploding.

4. **Engaging Stakeholders:** Engaging a broad range of stakeholders, including government agencies, private sector partners, civil society organizations, and international development agencies, is critical. This participatory approach ensures that all voices are heard, and that the DPI ecosystem is inclusive and collaborative.
5. **Building Capacity:** Developing the skills and capabilities of government staff and other stakeholders is essential for the effective implementation and management of DPIs. This includes training programs, workshops, and ongoing support.
6. **Continuous Monitoring and Evaluation:** Establishing mechanisms for continuous monitoring and evaluation of DPI initiatives ensures they meet their objectives and deliver the desired outcomes. This includes setting key performance indicators and conducting regular assessments.
7. **Mapping the Funding ecosystem:** This involves engaging with a variety of stakeholders, including international development agencies, private sector partners, and civil society organizations, to secure financial support and ensure the sustainability of DPI projects.

Methodology

Understanding the Context

A systematic approach to creating DPIs begins with a thorough analysis of the current digital landscape, helping governments assess their existing technological infrastructure and identify gaps and challenges. This diagnostic phase is crucial for tailoring the implementation strategy to the specific needs and conditions of local environment. By conducting a comprehensive diagnostic analysis, countries can identify existing strengths, challenges, and gaps within their technological infrastructure. This process will help in determining the required elements for a sector-agnostic DPI foundation, ensuring a robust and adaptable digital infrastructure that supports long-term success.

Key Design Principles

The core design principles essential for successful DPI implementation:

1. **Interoperability:** Ensuring that different systems and platforms can work together seamlessly.
2. **Scalability:** Designing systems that can grow and adapt to increasing demands.
3. **Inclusivity:** Making digital services accessible to all segments of the population, including marginalized and vulnerable groups.

These principles are integrated into a building-block approach, allowing for the strategic reuse of resources and the creation of a robust DPI foundation.

The International Telecommunication Union highlights that interoperable and scalable digital infrastructures are critical for achieving the United Nations Sustainable Development Goals. Countries with well-established DPIs are better positioned to leverage digital technologies for sustainable development. The Global System for Mobile Communications Mobile Connectivity Index reveals that approximately 3.4 billion people in developing countries are still not connected to the internet.[6] DPIs

[6] https://www.mobileconnectivityindex.com/index.html

that prioritize inclusivity can help bridge this digital divide, ensuring that marginalized and vulnerable populations have access to digital services.

Step-by-Step Guidance

A programmatic approach includes detailed, step-by-step guidance on the entire DPI implementation process, from initial planning to deployment and monitoring as follows:

1. **Governance and Policy Framework:** Establishing clear policies and governance structures to support DPI implementation. This involves creating a dedicated DPI alliance, defining roles and responsibilities, and ensuring accountability and transparency.
2. **Technical Architecture:** Designing a scalable and interoperable technical architecture that includes digital identity systems, payment platforms, and data exchange mechanisms, along with highlighting best practices and standards for building these components.
3. **Stakeholder Engagement:** Engaging a broad range of stakeholders, including government agencies, private sector partners, civil society organizations, and international development agencies. This participatory approach ensures that all voices are heard, and that the DPI ecosystem is inclusive and collaborative.
4. **Capacity Building:** Developing the skills and capabilities of government staff and other stakeholders to effectively implement and manage DPIs. This includes training programs, workshops, and ongoing support.
5. **Monitoring and Evaluation:** Establishing mechanisms for continuous monitoring and evaluation of DPI initiatives to ensure they meet their objectives and deliver the desired outcomes. This includes setting key performance indicators and conducting regular assessments.

Conclusion

Digital transformation is not just a technological challenge but a holistic process that requires careful planning, stakeholder engagement, and continuous improvement. The DPI Playbook for Nations released by Deloitte in December 2023[7] addresses these dimensions, offering a robust framework that can be adapted to different contexts and requirements. By providing a comprehensive roadmap, detailed methodologies, and practical toolkits, the playbook empowers governments to implement DPIs effectively and efficiently. This, in turn, enables the delivery of seamless, inclusive, and responsive public services that meet the needs of all citizens.

As the world continues to grapple with complex challenges, from public health crises to economic uncertainties, the need for resilient and inclusive DPIs becomes increasingly evident. The DPI Playbook offers a clear path forward, enabling governments to harness the power of digital technologies to drive sustainable development, enhance service delivery, and improve the lives of their citizens. By adopting the principles and methodologies outlined in the playbook, governments can build a future where digital public infrastructures serve as the backbone of modern, efficient, and inclusive societies.

[7] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-dpi-playbook-brand-noexp.pdf

References

1. *Digital Public Infrastructure (DPI) playbook for nations.* Available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-dpi-playbook-brand-noexp.pdf

2. *Deloitte Insights, Government Trends 2024, 10x improvement in customer experience*. Available at: https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends.html#10x-improvement-in-customer-experience

3. *ID4ID Global Dataset*. Available at: https://id4d.worldbank.org/global-dataset

4. *Unlocking the potential of open-source technologies for a more equitable world, DPG Alliance*. Available at: https://digitalpublicgoods.net/

5. *CoWIN Dashboard, Ministry of Health and Family Welfare*. Available at: https://www.cowin.gov.in/

6. *GSMA Mobile Connectivity Index 2024*. Available at: https://www.mobileconnectivityindex.com/index.html

★★★

Chapter 2

Bridging the Innovation Gap and Facilitating Inclusive Knowledge Sharing: A Design Framework for a Technology Transfer Portal and Client Data Management System for a Better Outreach

Authors:

1.Sanjailal K P, CSIR-Central Food Technological Research Institute

2.Sanaboyina Sudhakar, CSIR-Central Food Technological Research Institute

3.Jyothi K, CSIR-Central Food Technological Research Institute

4.Vijayalakshmi S, CSIR-Central Food Technological Research Institute

5.Siva Naga Suresh Purama, CSIR-Central Food Technological Research Institute

Abstract

This paper proposes the design and development of a Web Portal and a Client Data Management System to bridge the gap between CSIR-CFTRI and Food processing industries, MSMEs, SHGs, and farmers by facilitating the licensing and sharing of innovative technologies developed at CSIR-CFTRI with potential users. The core functionality of the user-centric platform will enable users to discover and share technologies that directly address their needs across the food processing spectrum, leading to the development of innovative food products and services that cater to the evolving demands of tomorrow. The real-time data generated through the portal helps in understanding the market needs/trends, laying a foundation for new research and technology development across the Food spectrum. The portal aims to foster innovation and entrepreneurship, bridge the digital divide, create a knowledge economy and make Food Processing Technologies Accessible to a wider range of users to contribute to India's technological advancements in the area of Food Science & Technology. Aligning with the Digital India and Viksit Bharat initiatives of the Government of India, the proposed Portal can play a significant role in supporting the Viksit Bharat initiative's vision of transforming India into a developed nation.

Keywords: Technology Transfer; Food Machinery; Client Data Management; Knowledge Sharing; Laravel Framework

Introduction

CSIR-Central Food Technological Research Institute (CSIR-CFTRI), Mysuru, Karnataka is a constituent laboratory of the Council of Scientific and Industrial Research (CSIR), Ministry of Science & Technology, Government of India. CSIR-CFTRI is a leading Food Science and Technology Research Institute in India dedicated to shaping the future of food. Our passionate team of Scientists and Researchers is constantly pushing boundaries and exploring cutting-edge advancements across the entire food spectrum. From farm to fork, we delve into every aspect of food technology, processing, packaging, preservation and quality control. CSIR-CFTRI develops technologies for innovative food processes and products, ensuring the highest quality and safety standards set by FSSAI, Govt. of India. Our expertise spans diverse areas, including nutraceutical and functional foods, spices and flavours, fruits and vegetables, developing

advanced protein sources, refining meat, fish, and poultry processing techniques, harnessing the power of microbial technologies, developing innovative and healthy bakery products, and unlocking the secrets of biochemistry for promoting health and well-being. On the Engineering side, CSIR-CFTRI focuses on the development of machinery that drives the food industry, designing and improving equipment for more efficient and sustainable food production. The Institute don't just develop innovative technologies and food products; it makes them readily available to the industry and prospective entrepreneurs. Our robust technology basket boasts over 500+ proven and time-tested technologies ready for licensing. Every year, this basket is refreshed with 25-30 innovative new additions, ensuring a constant stream of cutting-edge solutions for the Food Industry. These innovations are backed by the power of intellectual property, with over 200+ Indian and foreign patents available for licensing. By collaborating with industry partners and farmers, we translate our discoveries into real-world solutions that benefit consumers, businesses, and the environment.

Technology Transfer and Business Development (TTBD) Department, as the name indicates, is involved in the transfer of developed technologies and also in the development of business by performing some curated research activities for individuals, industries, Governmental and non-governmental associations, etc. The department plays a critical role for the Institute in enabling a better societal outreach. This department handles daily an average of a minimum of 10 enquiries from people of various capacities for technology and technological services. A huge client-based data is generated in the department through enquiries in the form of in-person visits, mail enquiries, phone enquiries, participation in exhibitions and other contacts. The Institute's website also hosts information about the technologies available and other services, such as pilot plants, incubation facilities, etc., for the benefit of society. The service accessed and provided in different forms needs to be mapped to make the outreach for more effective and efficient. The proposed work is to develop a client data management system through a Technology Transfer Portal and a user-friendly mobile application to enable easy access to technological services provided by the Institute.

Background

The DST's initiatives, particularly the TDB and TIFAC portal [1], demonstrate the government's commitment to fostering a robust technology transfer ecosystem in India. Further research is necessary to fully understand the impact of these programs and identify areas for improvement. By strengthening these initiatives at the academic and research organisation level, India can accelerate the translation of research into tangible economic and societal benefits. CSIR established the CSIR India Technology Showcase [2], a web portal showcasing the technological innovations of its 38 constituent laboratories. This portal offers insights into the diverse technologies offered by CSIR laboratories. Another initiative of CSIR to showcase the technological breakthroughs and innovations in each of its 37 CSIR laboratories/institutes spread across the country was the One Week One Lab campaign during the year 2023 [3].

The literature highlights the limitations of current mechanisms employed by Indian academic and research institutions to reach out to industry. These methods are often deemed inefficient, lacking a structured approach to foster stronger collaboration and technology transfer. Studies by Ramya Ravi and Manthan D. Janodia [4] identify the absence of a systematic framework within academic and research institutions to connect with potential industry partners. This disconnect impedes researchers from effectively showcasing their inventions and hinders industries from identifying valuable research outputs that could address their needs. Web-based technology transfer portals hold significant promise for boosting

innovation and economic growth [5]. By adopting a framework that considers the various stakeholders involved and the specific technologies being transferred, these platforms can be designed to become powerful tools for accelerating the commercialization of research.

Bridging the Gap Between Innovation & Industry

In our quest to expand the reach of our innovations and foster broader participation, we propose developing a user-friendly web portal and mobile app specifically designed for Technology Transfer and Business Development (TTBD). This user-friendly platform will bridge the gap between our Institute and the food processing industry, including large-scale food industries, MSMEs, SHGs, and farmers across India. By providing a user-centric platform for technology discovery and sharing, the portal empowers users to find and utilize technologies that address their specific needs. This can lead to the development of innovative solutions and services that cater to the evolving demands of tomorrow. The portal's multilingual capabilities broaden accessibility to a broader demographic, ensuring that individuals with varying native languages can engage and benefit from the platform regardless of their linguistic background. This fosters inclusivity and promotes our technological innovations to a more diverse pool of entrepreneurs shaping future services. The platform facilitates knowledge exchange and collaboration among researchers, institutions, and entrepreneurs. This collaborative approach can accelerate the development of new service models and delivery mechanisms for the future. By promoting the transfer and adoption of cutting-edge technologies, the portal lays the groundwork for the development of secure and sustainable services for the future. This ensures that service delivery mechanisms are adaptable and can leverage upcoming technological advancements. In essence, TTBD portal acts as a catalyst for innovation and knowledge sharing, paving the way for the development and implementation of future-oriented service delivery models.

Key Features and Functionalities of the Proposed Portal

The portal incorporates the following functionalities:

- **Multilingual Support:** Accessing cutting-edge technologies in the user's preferred language empowers informed decision-making. Google Translate API integration empowers the portal to deliver content in multiple languages, fostering global accessibility.
- **QR Code Integration:** Seamless access to the portal for in-depth information is facilitated via QR code generation, allowing users to scan the code using smartphones for instant access.
- **Food Processing Machinery Portal and Knowledge Repository Integration:** A dedicated knowledge repository serves as a central hub for storing and managing technology transfer knowledge, encompassing research papers, case studies, and technical documents. Additionally, a food machinery portal is integrated to showcase relevant machinery and equipment, facilitating a comprehensive information pool for a complete understanding and direct contact with manufacturers for requirements for machinery to set up the facility at the earliest.
- **Discussion Forums and Communication Channels:** A discussion forum is established in the portal to promote knowledge sharing and collaboration among users, TTBD Staff and Scientists fostering a dynamic knowledge exchange environment.
- **Faceted Browsing System:** A faceted browsing system is implemented to empower users with faceted navigation and browsing using various attributes and refine search results. This system facilitates the browsing and filtering of search results based on various facets, including:
  - **Broad Area:** Categorization by broad fields such as Bakery Products, dairy products, Millets, etc.

  - **Attributes:** Browse and Search filtering based on various attributes of the technology (e.g., dehydrated, low fat, eggless, etc.), cost, or other relevant attributes.
  - **Commodities:** Browse and Search refinement by specific commodities such as food grains, honey, Garlic, Amla, etc.
  - **Keywords:** Keyword-based search and browse for targeted retrieval.
- **User-Friendly Interface:** Intuitive navigation ensures a smooth and efficient user experience.
- **Android App Integration with Push Notifications:** An Android application is developed to extend portal functionalities to mobile devices. Users can access the portal's features and receive real-time updates through push notifications.

The Proposed System

This section details the materials and methods employed in the design and development of the portal.

Technology Stack

The proposed portal is developed using the following technologies:

Frontend: Vue.js [6] - A progressive JavaScript framework for building user interfaces.

Backend: Laravel [7] - A PHP web application framework for building APIs and server-side logic.

Database: MySQL [8] - An open-source relational database management system.

System Architecture

The portal adheres to a Model-View-Controller (MVC) architecture, with a clear separation of concerns between the frontend (presentation layer), backend (business logic layer), and database (data persistence layer). A block diagram of the proposed model is shown in Fig.1.

Frontend (Vue.js): The user interface (UI) is built with Vue.js, a framework for creating dynamic and interactive web pages. Vue.js uses reusable components to simplify development and allows the application to fetch and manipulate data asynchronouslyusing Axios, a popular HTTP client library.

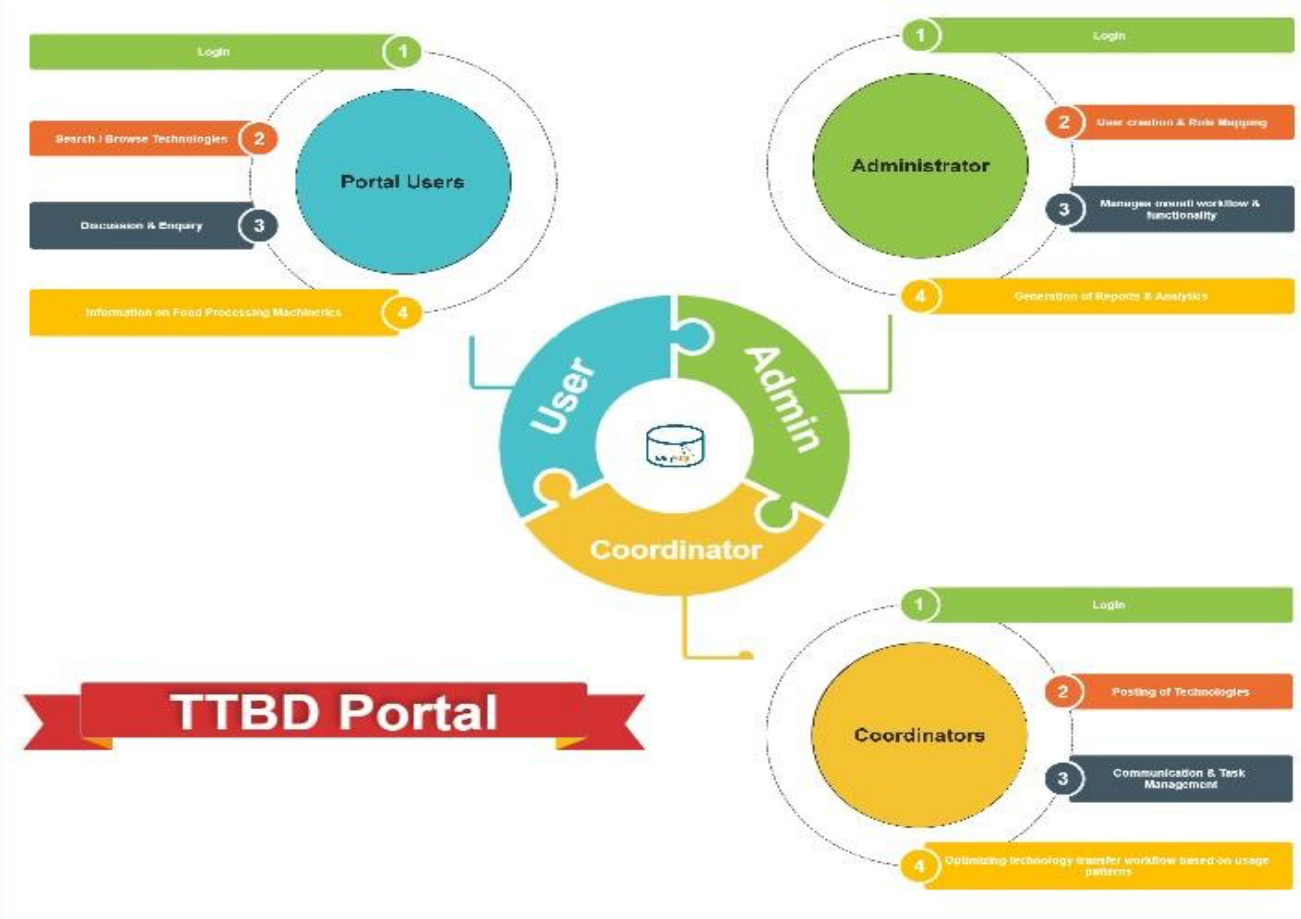


Fig.1 Block diagram of the proposed portal

Backend (Laravel): The backend of the portal is powered by Laravel, a PHP framework. It acts as an intermediary between the user interface and the database. Laravel offers a RESTful API, a standardized way for applications to communicate and exchange data. When users interact with the UI, Laravel controllers receive these requests and direct them to the relevant models. These models handle the application's core logic and interact with the MySQL database using Eloquent, an object-relational mapper (ORM) that simplifies data access and storage. In essence, Laravel translates user actions into database operations.

Database (MySQL): Stores all application data using a relational schema designed to efficiently manage user information, technology transfer listings, and associated metadata.

User Interface (UI) Design: The user interface is designed to be intuitive and user-friendly for both researchers and technology transfer specialists. Advanced features include (a) interactive dashboards to provide users with personalized views of relevant data, such as recently added listings, ongoing collaborations, and upcoming events. Searchable technology transfer listings allow users to filter and search listings based on various criteria, including technology attributes, commodities, keywords, and

broad areas. The platform fosters collaboration through a built-in discussion forum while empowering users to manage their personal information and control data access.

The portal supports rich content management through embedding multimedia content (e.g., videos, images) within technology transfer listings to enhance information delivery.

Client Data Management System (CDMS)

The backend features a robust Client Data Management System (CDMS) to manage user information and interactions within the portal. The CDMS functionalities include:

- Technology transfer listing management: TTBD Staff can add, edit, and manage technology listings with detailed descriptions, attachments, and relevant keywords.
- User Activity Tracking: Monitor user activity to understand user behaviour and preferences. The system implements comprehensive activity tracking, logging all interactions between TTBD staff and stakeholders within the portal. This data provides valuable insights into usage patterns and helps to analyse customer interactions to identify trends and improve the licensing of technologies. It also identifies avenues for new research and areas for improvement within the platform's modules, ultimately enhancing user experience and optimizing technology transfer workflows. This data can also be used to personalize the user experience and recommend relevant technologies to users.
- Communication Management: Provide tools for secure communication between users of the portal and technology transfer staff through email messaging or discussion forums. This could include features for sending targeted emails, managing inquiries, and facilitating discussions through forums or chat functionalities.
- Reporting and Analytics: Generate reports and analytics to track key CDMS metrics. This data can be used to assess the portal's effectiveness, identify areas for improvement, and optimize user engagement strategies.
- Task Management: Allow staff to assign and track tasks related to user support, technology onboarding, and overall CDMS operations. This can streamline workflows and ensure efficient task
- User registration: Secure mechanisms for user registration, role assignment, login, and access control based on user roles and permissions.

The features of the back-end CDMS system empower the TTBD staff to streamline technology transfer workflow, strengthen customer relationships, and facilitate efficient licensing and agreement management. Through the implementation of automated workflows and the introduction of self-service capabilities, the system alleviates the burden of repetitive tasks.

Discussion & Conclusion

This paper presents the design of a technology transfer portal that bridges the gap between CSIR-CFTRI and potential adopters. This comprehensive platform will empower users to access, share, and engage in discussions concerning critical knowledge and resources related to innovative food processes and technologies developed by CSIR-CFTRI. The portal will facilitate the licensing of these technologies ultimately accelerating technology transfer processes and fostering innovation within the food sector. The integration of various functionalities, including multilingual support, QR code generation, knowledge repository, food machinery portal and discussion forum, fosters a user-centric and globally accessible information exchange environment. The faceted browsing system empowers users with efficient search and retrieval capabilities, streamlining information discovery.

Future directions could explore the integration of artificial intelligence for enhanced search personalization and recommendation systems, along with investigating the feasibility of incorporating virtual reality functionalities to showcase the innovative and cutting-edge technologies developed at CSIR-CFTRI in an immersive manner.

Acknowledgements

The authors would like to thank the Director, CSIR-Central Food Technological Research Institute, Mysuru, the Head, TTBD Department and Head, PMC Dept. for their constant support and encouragement.

References

1. https://www.tifac.org.in/

2. https://techindiacsir.anusandhan.net/

3.https://www.newsonair.gov.in/union-minister-dr-jitendra-singh-launches-one-week-one-lab-programme-to-showcase-achievements-of-csir/

4. Ravi, R., Janodia, M.D. Factors Affecting Technology Transfer and Commercialization of University Research in India: a Cross-sectional Study. J Knowl Econ **13**, 787–803 (2022). https://doi.org/10.1007/s13132-021-00747-4

5. G. Schuh and S. Aghassi, "Technology transfer portals: A design model for supporting technology transfer via social software solutions," *2013 IEEE International Conference on Industrial Engineering and Engineering Management*, Bangkok, Thailand, 2013, pp. 43-47, doi: 10.1109/IEEM.2013.6962371.

6. https://vuejs.org/

7. https://laravel.com

8. https://dev.mysql.com

★★★

Chapter 3

Enhancing Data Governance Practices for Heightened Privacy and Security Measures

Authors:
1. Erina Kiran Kumar, Scientist-E, National Informatics Centre, Vijayawada, Andhra Pradesh
2. Sanaboyina Madhusudhana Rao, Scientist –F, National Informatics Centre, Vijayawada, Andhra Pradesh
3. Ambati Bubli Sagar, Scientific Officer-SB, National Informatics Centre, Vijayawada, Andhra Pradesh

Abstract:

In the modern era of data-driven operations with the rapid growth of digital communication and data storage has created numerous vulnerabilities, leading to potential breaches of personal and organizational information, data governance is no longer a choice but a crucial necessity for companies dedicated to preserving data confidentiality, against cyber threats, and navigating complex legal and ethical considerations surrounding surveillance and privacy rights. Through the implementation of top-notch data governance protocols, businesses can successfully safeguard personal information, maintain ethical data standards, and position themselves as trustworthy data custodians, thereby securing the ongoing confidence and support of their stakeholders in a progressively privacy-focused environment. The goal of data governance is to ensure the availability, usability, integrity, and security of data used in an organization must ensure that data is consistent and trustworthy and doesn't get misused. Organizations can achieved this by implementing data quality management processes that include regular data audits, validation, and cleansing. Key challenges include organizations can use a variety of mitigation strategies and countermeasures such as access control and authentication mechanisms, data encryption, data governance platforms and incident response and disaster recovery plans. The focus of this paper aims on an overview of the current state of global data security governance, identifies the obstacles, and proposes strategies for enhancing the modernization of data security governance systems and security measures by implementing the policies and processes on the daily tasks that keep information usable, understandable, and protected. In real life, data governance and data security usually go hand in hand and work together to make sure data is taken care of and shielded well.

Keywords: privacy, security, IoT Devices [Internet of Things], AI [artificial intelligence]

Introduction:

In our journey through the digital era, the amount of data being generated, analyzed, and saved is truly remarkable .There is an unparalleled amount of information and resources available to us,

which can greatly enhance our lives in various ways. However, the significance of data privacy and security has grown significantly increased access to information also comes with increased risks. Data governance is becoming increasingly important in today's digital world. Without effective data governance, organizations can put themselves and their customers at risk of data breaches and identity theft of to our personal and sensitive information. By implementing an effective data governance strategy, organizations can ensure that data is handled securely and responsibly.

The rising quantity of data generated and accumulated by organizations is a valuable asset that can be utilized to enhance decision-making and automate processes. However, it is also essential to safeguard it from unauthorized access and security breaches. Data governance encompasses the comprehensive supervision of data availability, usability, integrity, and security within 3an organization. This includes the implementation of protocols and guidelines for data collection, storage, protection, and utilization, while also guaranteeing adherence to legal and regulatory standards. This involves recognizing the importance of trust between businesses and users, as well as the potential harm to an organization's reputation in the event of a security breach. However, it also brings about considerable challenges in terms of security, management, and privacy. This is where the critical role of Data Governance becomes essential.

Data Governance is crucial for handling the vast amount of digital information. It involves a set of procedures, methods, and guidelines that ensure the accuracy, consistency, availability, and security of data within an organization. In addition to managing data, it also deals with the ethical and legal implications of data usage, especially in the context of stringent data protection regulations and laws globally. Thus by integrating data governance into every business operation allows organizations to demonstrate their dedication to safeguarding confidential data..

With the introduction of AI tools in data analysis adds another layer of complexity to this field. AI is able to handle large amounts of data, recognize patterns, and make conclusions much faster than human analysts. Nevertheless, this power also brings significant responsibility. AI tools have the potential to unintentionally perpetuate biases found in the data they analyze, resulting in biased or discriminatory outcomes.

When utilizing AI for data analysis, strong Data Governance is essential. Effective governance guarantees that the data inputted into AI tools is high-quality, unbiased, and used ethically and responsibly. It requires regular audits and checks on AI systems to ensure compliance with ethical and legal standards. On the other hand, encompass a wide range of malicious activities, including phishing, hacking, ransomware and malware attacks. The continuous evolution of these threats presents a persistent danger to both organizations and individuals.

What is Data Governance

Data governance refers to the management of data within an organization. It involves the level of control that an organization has over its data, which can be attained through various means such as maintaining high-quality data, having visibility on data pipelines, implementing actionable rights management, and establishing clear accountability. A data governance strategy involves the initial planning to establish the overall guidelines for how a company will consistently manage data. This includes:

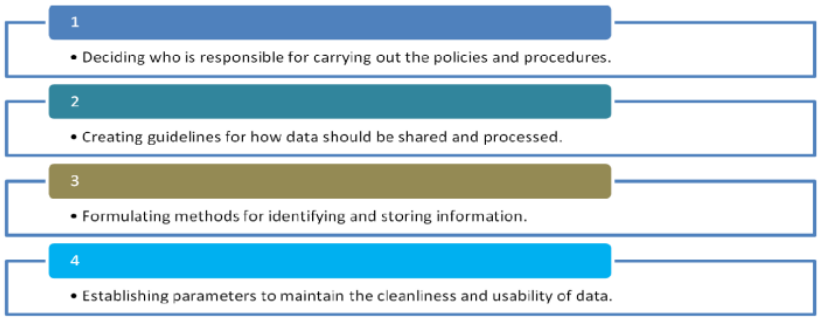


Fig 1: Guidelines

With the three components of the data pie - data governance, data privacy, and data security - are frequently grouped together. However, while they do naturally intersect, it is crucial to recognize the significant differences between them.

First and foremost, data governance serves as the cornerstone of our processes. It acts as the unifying force to ensure coherence. With proper implementation of data governance across all assets, it becomes simpler to implement appropriate privacy and security controls.

The advantages of a well-designed data governance strategy encompass reduced risks, cohesive policies, measurable metrics and processes, as well as improved compliance implementation and increased data worth.

The fundamental principles of Data Governance are outlined here. Data security and privacy stand as the two essential pillars for ensuring the longevity and prosperity of any product.

Data governance framework: Data governance plays a crucial role in supporting an organization's comprehensive data management strategy. It offers a unified approach to gathering, handling, protecting, and preserving data. The Data Management Association sees data management as a wheel, with data governance acting as the central hub from which different data management knowledge areas branch out.

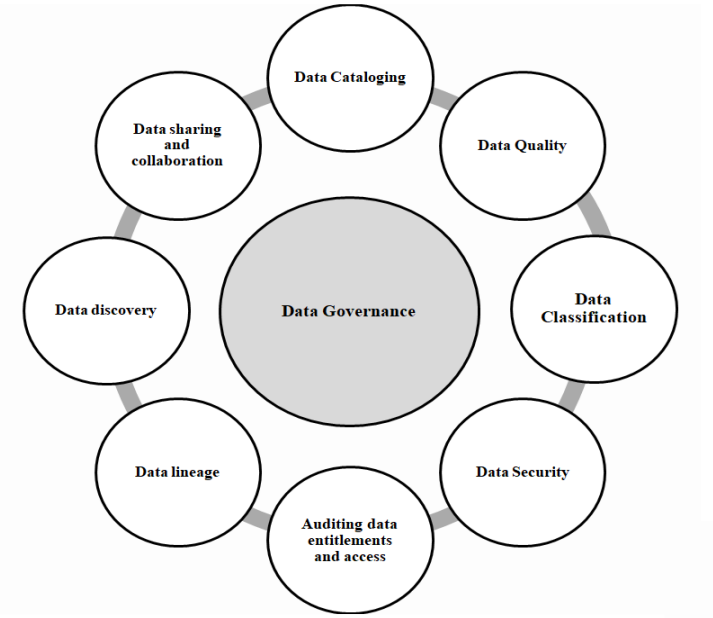


Fig 2: Data Management as a wheel.

i. **Data Cataloging**: Adequate data governance necessitates a thorough understanding of the data present in an organization. A data catalog plays a crucial role by offering a centralized metadata repository for an organization's data assets. It enables stakeholders to efficiently find, comprehend, and retrieve the necessary data, thereby enhancing data-related functions like discovery, governance, and analytics.

ii. **Data Quality:** It ensures the accuracy, consistency, and reliability of data, which is essential for informed decision-making and trustworthy business operations.

iii. **Data Classification**: Data classification is a fundamental aspect of data governance that focuses on arranging and classifying data based on its sensitivity, value, and criticality**.** The process of classification enables organizations to categorize data based on its level of risk and importance, thus facilitating the application of relevant security measures and policies.

iv. **Data Security:** The process of classification enables organizations to categorize data based on its level of risk and importance, thus facilitating the application of relevant security measures and policies. While prioritizing sensitive data protection against unauthorized access. It is essential to have efficient data access management in place to ensure data security and governance. A robust data security governance program must incorporate access controls that clearly outline the data accessible to specific groups or individuals.

v. **Auditing data entitlements and access**: Efficient data access auditing plays a crucial role in data governance and security governance initiatives, especially within regulated sectors. By monitoring data access and keeping track of recent activities, companies can detect and address any instances of excessive access by users or groups, thus reducing the likelihood of data misuse.

vi. **Data lineage**: It records important metadata and events at every stage of the data's journey, offering a comprehensive perspective on the movement of data within an organization's data infrastructure. Serving as a crucial component of a practical data governance plan, data lineage

empowers organizations to achieve compliance and readiness for audits, all while minimizing the effort required to manually create audit trails and ensuring reliable sources for audit reports.

vii. **Data discovery**: The rise of contemporary data resources such as dashboards, machine learning models, queries, libraries, and notebooks has made data discovery an essential component of a strong data governance plan. It is imperative for organizations to consider data discovery as a foundational element of their data governance strategy. It empowers data teams to effortlessly find data assets throughout the organization, work together on different projects, and innovate rapidly and effectively. This aids in avoiding data duplication, which can pose challenges as it incurs costs to maintain them and may result in governance issues at various security levels.

viii. **Data sharing and collaboration**: Data sharing and collaboration are essential elements for organizations as they exchange data with internal teams, external partners, and various regions. With the rising demand for external data, it is crucial for organizations to securely share data while maintaining control and visibility over the usage of their sensitive information. Investing in open format, interoperable, and multi cloud data sharing technologies is necessary to meet the data-driven innovation needs of organizations. Therefore, it is important to view data sharing as a critical business requirement and a foundational aspect of a robust data governance strategy.

Data Privacy and Security

Data Privacy and Security can be enforced at the level of each individual system. Nevertheless, when consolidating data from various systems, it is essential to establish a comprehensive security framework. Failure to do so could result in a data privacy and security breach, potentially leading to significant repercussions for the organizations.

Data Privacy - why is it so important?

Data privacy is an essential component in today's digital landscape. It primarily pertains to the management of sensitive personal data, such as personally information and personal health information. If data is considered the most valuable asset, then data privacy serves as its primary protector.

Data privacy presents a significant challenge for society in the present day, and it holds great importance for various reasons that can be broadly categorized into two main areas. The first pertains to asset management, which involves the ownership and utilization of data (often considered a business's most valuable asset). The second area is regulatory compliance, where the management of data to ensure adherence to regulations is crucial for legal, ethical, and business purposes.

Now a day’s 'data economy', i.e. the collection, sharing, and utilization of data pertaining to users hold significant value at present and possibly in the future. With the growing emphasis on data privacy, it is imperative for businesses to prioritize transparency in handling consumer information. By complying with privacy policies and obtaining consent for data management, companies can establish credibility with their customers. Increased transparency surrounding data privacy is crucial for cultivating trust among customers. Concurrently, all businesses are required to address the issue of regulatory compliance in order to establish trust with customers or users.

Data Security:

Data security represents the last component of the puzzle, and it is frequently confused with data privacy - however, they are distinct concepts. Data security encompasses all measures taken to safeguard digital data from unauthorized access, alteration, or theft during its entire lifespan.

In simple terms, data security ensures that data is safeguarded from external threats, internal risks, and mistakes made by individuals. On the other hand, data privacy focuses on the regulations surrounding the collection, sharing, and utilization of data. Data security serves as the foundation for maintaining the security and accessibility of data, encompassing various aspects such as physical security (hardware and storage devices), administrative controls, access restrictions, and the security of software applications.

According to National Institute of Standards and Technology (NIST) created a globally recognized Cyber Security Framework which is the foundation of most standards.

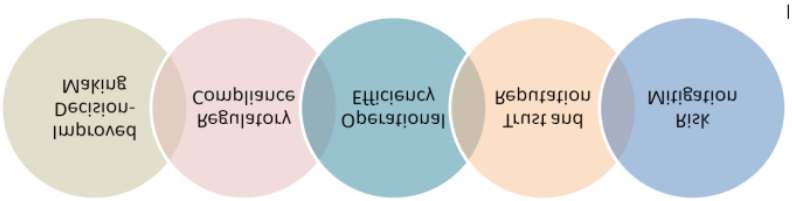
i. **Identify**: Acquire a detailed overview of your systems and services, covering assets, data, personnel, and data flows, to recognize potential entry points for hackers or security breaches.
ii. **Protect**: It is essential to ensure the protection of all systems and services, although certain ones may require a higher level of protection than others.
iii. **Detect**: Implementing protection for a system or service does not provide an absolute assurance of safety and security. It is equally crucial to establish monitoring and alert systems when implementing protection.
iv. **Respond**: In the event of an attack or breach, it is essential to have a pre-established response plan detailing the responsibilities of each individual involved, the sequence of actions to be taken, and the legal requirements for notifying relevant parties.
v. **Recover**: If the worst does happen, you'll need to know how to bring systems or services back into operation, and in which order. It is important to have the expertise to reestablish systems or services, and to do so in a predetermined sequence.

Why is Data Governance important in a digital Age?

Data Access Governance is a continuously developing discipline. It is essential to establish appropriate data access permissions and regulations to safeguard both organizations and individuals. Furthermore, implementing the correct regulations is crucial to guarantee the secure and ethical utilization of data.

Data Access Governance establishes the structure for companies to reduce data breaches and identity theft by guaranteeing that data is utilized for its designated purpose. It also establishes the structure for organizations to adhere to data protection regulations.

It is crucial for companies to implement Data Access Governance in order to safeguard their customer data. This is particularly vital for companies that rely on customer data for various functions, including marketing and analytics. By implementing a robust data access governance strategy, companies can guarantee the security and responsible use of their customer data.



Key Points:

i. **Improved Decision-Making:** Precise and dependable data serves as the foundation for making well-informed decisions, leading to improved outcomes and reduced risks.
ii. **Regulatory Compliance:** Effective data governance is necessary to uphold compliance, prevent penalties, and maintain customer trust in light of strict data privacy laws.
iii. **Operational Efficiency:** Enhance efficiency by optimizing processes, reducing redundancy, and optimizing resource allocation through clearly defined data governance.
iv. **Trust and Reputation:** Companies that prioritize data governance establish credibility with stakeholders and build a positive image in the market.
v. **Risk Mitigation:** By minimizing the possibility of data breaches, illegal access and abuse, effective data governance protects confidential.

Challenges of the digital age for privacy and data protection:

The aim of data security governance is to stop unauthorized entry, utilization, exposure, alteration, or loss of confidential information, whether deliberate or unintentional..Information Security and Data Protection are ever-evolving sectors that face ongoing challenges and are shaped by advancements in digital technologies and innovative business strategies. The progress in ICT impacts the regulations governing data protection and reshapes the concept of personal data, the handling of international data transfers, user privacy in the digital era, user rights, and the responsibilities of data controllers.

Due to rapid advancement of technology and increase of data, data governance has become increasingly important. One of the main challenges of data governance in a digital world is how to protect customer data from misuse and theft. Organizations need to develop policies and procedures to ensure customer data is handled correctly and is not used for anything other than its intended purpose. This is especially tricky in larger companies since there are often multiple people and departments interacting with customer data.

One of the foremost challenges in initiating a data governance program is securing buy-in from senior executives and aligning the initiative across the organization..
Another challenge of data governance in a digital world is the constant evolution of data security threats. Cybercriminals are increasingly advanced and sophisticated, so organizations need to keep up with their tactics in order to stay ahead and protect their customer data.

Finally, organizations need to ensure they have the right data governance tools and resources in place in order to prevent data misuse and breaches. This includes setting up proper storage facilities and data access control systems. With the right tools in place, organizations can ensure that user data is being handled in a secure manner and is used only for its intended purpose. This requires significant investment in terms of time, resources and technology, making executive support crucial for its success.

Key challenges:

i. **Data Collection and Profiling:**
A major challenge in the digital age is the extensive data collection and profiling carried out by companies and organizations. Online activities, such as web searches and social media likes, are utilized to create detailed profiles of individuals, which can then be exploited for targeted advertising or potentially harmful purposes.

ii. **Data Breaches and Cyber attacks:**
Data breaches and cyber attacks of significant importance are now a common occurrence. Hackers frequently breach databases containing sensitive information without authorization, leaving individuals vulnerable to identity theft, financial fraud, and other forms of personal data compromise.

iii. **Lack of Transparency:**
Many organizations fail to be transparent about their data collection practices. Users often agree to terms and conditions without fully comprehending what data is being gathered, how it is utilized, and who it is shared with.

iv. **Regulatory Compliance:**
The implementation of data privacy regulations has enforced rigorous standards for organizations in managing personal data. Ensuring compliance with these regulations can present challenges for organizations that operate on a global scale.

Mitigating Sensitive Data Exposure and Countermeasures.
Data protection management is an ever-changing area, and various trends are influencing its future direction due to recent technological advancements, security risks, and legal standards. In order to ensure the effectiveness and compliance of data security governance practices, it will be crucial to adapt to new technology, threats, and regulations in the future. By staying informed about these trends, organizations can mitigate the risk of security incidents and safeguard their reputation and operations.

i. **Increased focus on data privacy**: Data security governance must evolve its regulations to ensure that organizations comply with the latest privacy requirements for protecting personal data.
ii. **Emergence of AI and machine learning**: With the increasing prevalence of AI, IoT and machine learning in business operations, data security governance must adapt to incorporate these technologies for real-time detection and response to security threats.
iii. **Growing importance of cloud security:** With the increasing number of organizations transitioning their data and applications to the cloud, the emphasis of data security governance will

shift towards cloud security measures, including data encryption, identity and access management, and monitoring.

iv. **Focus on supply chain security:** As supply chains become increasingly complex and third-party vendors play a larger role, data security governance must prioritize addressing supply chain security risks and ensuring that all parties involved have implemented sufficient security measures.

v. **Adoption of zero trust security:** Zero trust security is a security framework that operates under the assumption that both users and devices may be compromised, and thus, constantly verifies their identity and access. In order to safeguard sensitive data, data security governance must embrace this model and strictly limit access to authorized users.

Strategies for managing the growing number of data protection and privacy regulations.

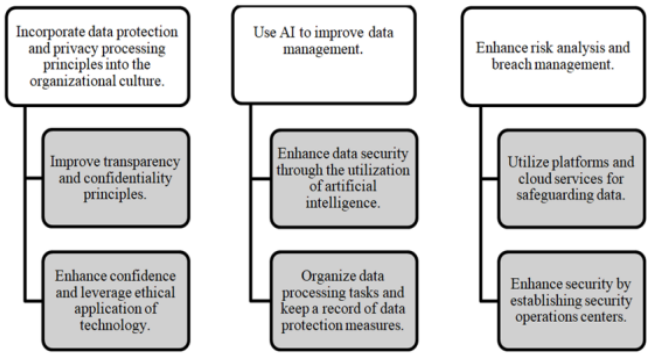


Fig 3: Strategies for data protection and privacy regulations.

Best practices of data governance:

A strong data governance framework is essential for protecting sensitive data and guaranteeing its confidentiality, integrity, and accessibility. Data governance strategies must be adapted to best suit an organization's processes, needs, and goals. To strengthen data governance initiatives in order to improve data privacy and security. The following are best practices worth following:

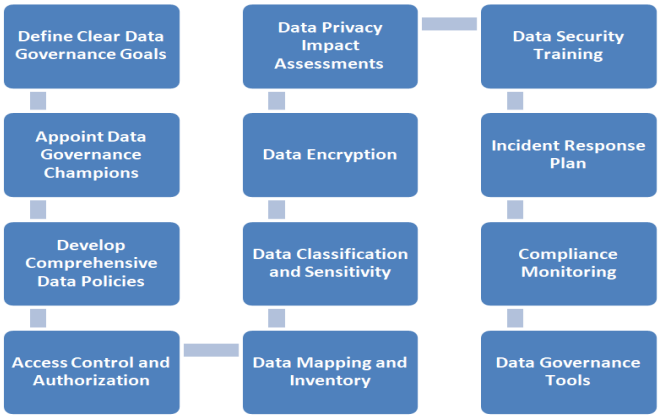


Fig 4: Best practices.

Conclusion :

With technology rapidly advancing, the importance of legal and ethical considerations surrounding digital privacy and security has become increasingly significant, safeguarding personal information becomes more complex. By taking proactive steps, educating users, and complying with data privacy laws, we can effectively tackle these obstacles. Individuals must be cautious about sharing information, while organizations should make data privacy a top priority. It remains a constant challenge for individuals, organizations, and governments to find the right balance between security and privacy. To sum up, data governance is a multifaceted procedure that encompasses overseeing the accessibility, usability, integrity, and security of data within an organization. The integration of IoT, ML, DL and blockchain may present novel obstacles for data governance. To tackle these hurdles, organizations can implement various strategies and measures like access control, authentication protocols, data encryption, network segmentation, explainable AI, data governance tools, and plans for incident response and disaster recovery.

The data governance model outlined in this article considers the utilization of these technologies and has the potential to assist organizations in the more effective and efficient management and protection of their data. Nevertheless, organizations must be mindful of the obstacles associated with the implementation of this model, including a shortage of technical know-how, expenses, alterations in current procedures, and adherence to legal and regulatory requirements.

In order to enhance security of data governance, it is essential to prioritize ongoing research and development of emerging technologies like IoT, ML, DL, and blockchain, Organizations must integrate these technologies effectively to safeguard data from unauthorized access and breaches. Regularly updating mitigation strategies and countermeasures is also crucial to adapt to evolving technologies and legal requirements.

Data Governance must be implemented using a solid framework that incorporates automation. Furthermore, it is essential to assess any software tools that support Data Governance to ensure they align effectively with the objectives of Data Governance.

Effective data governance tools simplify the process of uncovering and comprehending data, utilizing metadata to showcase origin and dependability, and guaranteeing adherence to policies and best practices. A properly executed data governance initiative tackles these challenges, and the toolkit provides your organization with the assurance to make your data readily available while maintaining security.
In conclusion Data governance serves as a critical process that enables organizations to effectively oversee and safeguard their data. The incorporation of IoT, Big data and blockchain may introduce new complexities for data governance however, organizations can adopt mitigation strategies and countermeasures to address these complexities. It is essential for organizations to understand the challenges associated with implementing this model, including a shortage of technical proficiency, financial constraints, modifications in current procedures, and compliance with legal and regulatory mandates. By tackling these challenges, organizations can enhance their data governance capabilities.

References

1. Retrieved from https://www.castordoc.com/blog/what-is-data-governance-and-privacy, on 20/07/2024

2. Retrieved from https://dzone.com/articles/data-governance-data-privacy-amp-security-part-1on 20/07/2024

3. Retrieved from https://elnion.com/2023/05/14/data-access-governance-in-a-digital-age/on 20/07/2024on 20/07/2024

4.Retrieved from https://www.imperva.com/blog/why-data-security-and-privacy-in-the-digital-age-are-crucial/on 20/07/2024

5.Retrieved from https://www.linkedin.com/pulse/digital-frontier-data-privacy-security-age-victor-waenerlundon 20/07/2024

6.Retrieved from https://keyrus.com/za/en/insights/importance-of-data-governance-in-the-digital-world

7.Retrieved from https://cybertechworld.co.in/data-governance-unleashed/#google_vignetteon 20/07/2024

8.Retrieved from https://m.digitalisationworld.com/blogs/56731/meet-the-three-amigos-of-data-governance-privacy-and- securityon 20/07/2024

9.Retrieved from https://elnion.com/2023/05/14/data-access-governance-in-a-digital-age/on 20/07/2024

10.Retrieved from https://grcoutlook.com/understanding-the-important-role-of-data-governance-in-the-present-digital-world/on 20/07/2024

11.Retrievedfrom https://www.aimspress.com/article/doi/10.3934/mbe.2020286?viewType=HTMLon 20/07/2024

12. Retrieved from https://blog.quest.com/the-top-7-data-governance-challenges-organizations-face-and-how-to-address-them/on 20/07/2024

13.Retrieved from https://www.databricks.com/discover/data-governanceon 20/07/2024

14.Retrieved from https://bigid.com/blog/5-steps-for-effective-data-security-governance/on 20/07/2024

15.Retrieved from https://www.cio.com/article/202183/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.htmlon 20/07/2024

16.Retrieved from https://cybertechworld.co.in/data-governance-unleashed/#best-practices-for-implementing-data-governanceon 20/07/2024

17.Retrieved from https://wwwr.capgemini.com/wp-content/uploads/2019/09/Report_Championing-Data-Protection-and-Privacy.pdfon 20/07/2024

★★★

Chapter 4:

Contours of Devising An AI Literacy Programme for the Grassroots

Author:
1.Sonia Bhaskar, Programme Head, DataLEADS Artificial

Artificial Intelligence (AI) technologies, from virtual assistants to dynamic and complex algorithms, are becoming increasingly prevalent in our daily lives. AI technologies are used where we work, live, interact, and transact online. There's no doubt that AI, especially generative AI, is on the rise. The global generative AI market is projected to grow by 46.47% from 2024 to 2030, reaching a market valuation of $356.10 billion in 2030 (Source: Statista), while India alone has an AI user base of 724 million (Source: Kantar Report), with current market size of US$0.64bn in 2024. 57% of Indian consumers prefer AI-enabled tools or services over human interaction, surpassing the global average of 39% and the APAC (Asia Pacific region) average of 48% (Source: Adobe Report). Indian consumers have emerged as global leaders in embracing AI-driven interactions and Indian brands are striving to catch up with the latest AI innovations.

Yet we can witness that individuals/ consumers struggle to recognize, understand, and critically assess these AI-powered tools. People are using AI in critical spaces such as healthcare, finance, and education. Still, many users cannot evaluate the capabilities, limitations, and potential biases of AI systems to make informed decisions. AI is a daily reality, influencing how we work and access services, yet many people use AI without considering its privacy, safety, or societal impacts. On the downside, AI can generate content, including text, images, and videos, which can be difficult to distinguish from human-created content, as AI systems can be designed to manipulate or spread misinformation. These tactics can be seen in election campaigning, online shopping, online dating spaces etc.

A recent McAfee survey claims that with the rise of AI, Indians are finding it difficult to spot scams. The increasing prevalence of sophisticated scams involving voice cloning and deepfakes is causing widespread concern.

The recent Adobe report on the Future of Trust Study for India highlights the concerning impact of misinformation and AI-generated content on our digital ecosystem and democratic processes. According to the findings, 81% of respondents are worried about the spread of false news and struggle to verify online content's trustworthiness. Additionally, 78% believe misinformation and deep fakes will influence future elections. Social media platforms face particular scrutiny, with 32% of respondents reducing or stopping their usage due to misinformation. Importantly, 87% of the people covered in the report believe it is essential that they have the right tools to verify if online content is trustworthy.

The Need for AI Literacy

As the Government of India's Ministry of Electronics & IT pushes to empower AI startups and expand the overall infrastructure for propagating use of artificial intelligence in manufacturing, health, education and other sectors with direct impact on lives and livelihoods, it will catalyse India's AI ecosystem and position it as a force shaping the future of AI for India. But a common person trying to use AI in their daily life lacks basic literacy and is often falling prey to the technology. As AI increasingly permeates professional, private, and public spheres, the general public must possess a fundamental understanding of how AI functions is essential.

Understanding the capabilities and limitations of AI can help users make informed decisions about AI-driven content. AI literacy can effectively navigate the proliferation of misinformation. This includes

- the ability to recognise AI-generated content
- identify biases and manipulation
- evaluate AI-driven sources
- detect deepfakes
- cultivate critical thinking; and
- media literacy skills.

Furthermore, AI literacy will facilitate an understanding of the ethical considerations surrounding AI, such as privacy, fairness, and accountability, thereby ensuring responsible AI development and deployment.

AI literacy is crucial for enabling people to navigate the AI-driven world, make informed decisions, and contribute to the responsible development of AI technologies. Moreover, AI literacy can help India achieve its goal of pioneering in the space of AI technology. Promoting AI literacy at all levels of education is essential for preparing individuals and society for the AI-powered future by providing them with the ability to:

- **Recognise** AI
- **Grasp** AI
- **Use** AI
- **Critically assess** AI

Empowering People Through AI Literacy

An **AI Literacy programme** should aim to cultivate a culture of AI literacy in India. AI Literacy demands a more active learning approach, beginning with widespread awareness about AI, to prepare individuals to be informed consumers and responsible citizens. The AI literacy initiative will enable individuals to:

- **Understanding AI-generated content**: AI can generate content, including text, images, and videos, which can be difficult to distinguish from human-created content. AI literacy helps individuals recognize AI-generated content and evaluate its credibility
- **Identifying biases and manipulation**: AI systems can be designed to manipulate or spread misinformation. AI literacy enables individuals to recognize these biases and manipulation tactics used in AI-generated content, helping them make more informed decisions
- **Evaluating AI-driven sources**: AI-driven sources, such as chatbots and virtual assistants, can provide information. AI literacy helps individuals evaluate the credibility and reliability of these sources, ensuring they receive accurate information
- **Detecting deepfakes and manipulated media**: AI can be used to create deepfakes and manipulate media. AI literacy enables individuals to recognize and detect these manipulated forms of media, reducing the spread of misinformation
- **Critical thinking and media literacy**: AI literacy is closely linked to media literacy and critical thinking. By developing AI literacy, individuals can improve their overall critical thinking skills, enabling them to evaluate information more effectively and make informed decisions
- **Understanding AI-driven disinformation campaigns**: AI can be used to spread disinformation on a large scale. AI literacy helps individuals recognize and counter these campaigns, reducing their impact
- **Developing fact-checking skills**: AI literacy can help individuals develop fact-checking skills, enabling them to verify the accuracy of information and identify misinformation
- **Enhancing digital literacy**: AI literacy is a key component of digital literacy. By developing AI literacy, individuals can enhance their overall digital literacy, enabling them to navigate the digital world more effectively and make informed decisions.

Learnings from Previous Media Literacy Initiatives

In a country like India where there more that 800 million internet users and half of them in the rural areas which now accounts for more internet users than urban areas, with nearly 80% accessing internet on their mobiles - the success and failure of any new intervention, technology driven or otherwise, can be gauged by its penetration and adoption at the grassroot level. Previous media literacy projects undertaken by DataLEADS, such as FactShala and Bihar Information and Media Literacy Initiative, have provided valuable insights into effective strategies for combating misinformation and developing critical media literacy at the grassroot level.

Supported by Google News Initiative, **FactShala** is a comprehensive media literacy program aimed at equipping individuals with the skills needed to critically evaluate information. The program focuses on educating the public about identifying reliable sources, understanding media biases, and recognising misinformation. FactShala's focus extended beyond addressing misinformation from conventional sources and social media. It also emphasised educating people on understanding media, analysing content, and equipping them with the necessary skills to consume information critically. The program targeted adults in non-metro cities and villages across India, helping them navigate the vast sea of online misinformation and understand the nature and characteristics of online content.

FactShala employed various innovative channels beyond regular training workshops to broaden its reach and impact. One of the program's Train-the-Trainer initiatives, for instance, specifically targeted representatives and workers of 63 community radio stations, which broadcasted in over 15 languages. These trainers conducted media literacy bulletins and narrowcast sessions, empowering local audiences with critical information consumption skills. Additionally, in association with various universities, FactShala established Zonal Hubs across India, a pan-India initiative aimed at institutionalising media literacy in different regions and fostering critical thinking among students. Furthermore, the FactShala Innovation Lab incubated media literacy interventions through a six-month program, where ten organizations developed innovative curricula, courses, dramas, and games. These multifaceted approaches effectively reached diverse audiences, demonstrating the potential of these mediums in future literacy efforts. FactShala reached 6.5 crores people across India.

Bihar Information and Media Literacy Initiative (BIMLI) started off with the acknowledgement that adolescence marks a critical period when young individuals become increasingly engaged with their health, often seeking information about their bodies and health choices online. While this phenomenon is universal, it poses particular challenges in contexts of low literacy and limited internet experience. To address this, a collaborative effort with JEEViKA (Bihar Rural Livelihoods Promotion Society) and DataLEADS evaluated the effectiveness of a grassroots training program designed to combat health misinformation among secondary school students in India.

In this initiative, randomly selected schools participated in a program where students underwent four two-hour sessions over three months. These sessions educated students on the prevalence and consequences of inaccurate health information in India, the mechanisms through which such misinformation spreads, and strategies to defend against it. The program's effectiveness was measured by comparing students in schools with and without these sessions (who received lessons in conversational English instead). Metrics included students' self-reported attitudes and identification of inaccurate health information, as well as behavioral outcomes such as whether they flagged dubious content online, complied with public health measures, and the quality of their news diet. The programme saw more than 7,200 students trained for health misinformation.

Key Takeaways to Inculcate AI Literacy at the Grassroots

Based on the learnings from FactShala and BIMLI, here are some pointers for an AI Literacy program at the grassroots level to be effective:

1. **Community-centric approach:** Design AI literacy programs with a focus on the specific needs and contexts of local communities. Involve local leaders and use local languages to ensure the content is accessible and relevant.
2. **Interactive and practical learning formats:** Incorporate hands-on activities, simulations, and role-playing exercises that allow participants to apply AI concepts in real-world scenarios.
3. **Multi-Platform Approach:** Leverage the power of media channels such as community radio stations, social media, and the internet to broadcast AI literacy content. We must also use a combination of online resources, such as videos, articles, and interactive modules, and offline activities, like community events and workshops, to reach a diverse audience.
4. **Institutionalisation of efforts:** The success of FactShala Zonal Hubs in fostering critical thinking and institutionalising literacy efforts points to the necessity of creating new structures

and community-driven programs to regularly meet, debate, and exchange views on emerging issues in AI.

5. **Active integration into existing modes of education:** Embed AI literacy within existing school curricula to build a foundation of critical thinking skills from an early age.
6. **Reaching the grassroots through partnerships:** Partnering with local NGOs, community groups, and educational institutions to promote AI literacy can ensure the program is culturally relevant and widely accepted.
7. **Continuous Monitoring and Adaptation:** The program must integrate methods to continuously monitor and evaluate the effectiveness of the interventions, and must be adaptable to suit local contexts and requirements.

Conclusion

AI literacy can lead to a more informed, engaged, and responsible citizenry that is better equipped to navigate the opportunities and challenges presented by the rapid advancements in artificial intelligence significant outcomes will include:

- **Increased Understanding of AI Capabilities and Limitations**
  With enhanced AI literacy, people will have a better grasp of what AI systems can and cannot do. This knowledge can help manage expectations and prevent overreliance on AI, leading to more responsible and appropriate use of the technology.

- **Informed Decision-Making**
  Improved AI literacy empowers individuals to make more informed decisions when interacting with or being impacted by AI systems. This could range from choosing which AI-powered tools to use, to understanding the implications of AI-driven policies and regulations.

- **Participation in AI Governance**
  A knowledgeable citizenry can actively engage in discussions and decision-making processes around the development and deployment of AI. This can lead to more inclusive and representative AI governance, ensuring the technology serves the public interest.

    - **Improved Ability to Identify and Combat AI-Generated Misinformation**

With a better understanding of AI capabilities, individuals will be better equipped to recognize the telltale signs of AI-generated content, such as inconsistencies, anomalies, or subtle artifacts. It will improve the public's ability to identify and combat AI-generated misinformation, also known as "deep fakes" or "synthetic media":

- **Fact-Checking and Verification**
  Improved AI literacy can enable people to employ effective fact-checking and verification techniques to assess the authenticity of online content, reducing the spread of AI-generated misinformation. A more AI-literate public can play a crucial role in identifying and reporting instances of AI-generated misinformation to relevant authorities or platforms, helping to curb its proliferation.

- **Responsible AI Adoption**
  With a better understanding of AI's capabilities and limitations, individuals can make more informed choices about adopting and using AI-powered technologies, ensuring they are used appropriately and ethically.

- **Participation in AI Policymaking**
  A more AI-literate public can actively participate in the development of policies and regulations governing the use of AI, ensuring the technology is deployed in a way that aligns with societal values and priorities.

- **Ethical AI Practices**
  Enhanced AI literacy can empower individuals to advocate for and adopt ethical AI practices, such as ensuring algorithmic fairness, transparency, and accountability, within their personal and professional spheres.

- **Anticipating Risks and Challenges**
  With a deeper understanding of AI, individuals and communities can better anticipate potential risks and challenges associated with the technology, enabling proactive measures to address them

- **Adaptive and Resilient Responses**
  A more AI-literate public can develop adaptive and resilient responses to address the evolving landscape of AI-driven changes, minimizing disruptions and ensuring a smoother transition.

- **Collaborative Problem-Solving**
  Enhanced AI literacy can foster collaborative problem-solving efforts among diverse stakeholders, including policymakers, researchers, and the general public, to address the complex and multifaceted challenges posed by AI.

DataLEADS is a digital media and tech company that works to build a resilient and comprehensible information ecosystem to empower communities. We incorporate a holistic approach, cutting-edge research, data-driven insights, incubating ideas, creative freedom, grassroots community engagement, behavioural and cognitive science to navigate the complex web of information landscape. Our work includes data intelligence, fact-checking initiatives, data journalism training, media and information literacy interventions, curriculum development, designing public policy interventions, media research and creative development initiatives.

★★★

Chapter 5

AI to Automate, Augment and Transform

Author:
State Bank of India

Abstract

This paper explores the transformative potential of Artificial Intelligence (AI) in government, highlighting its evolution from a research novelty to a practical tool with standardized methodologies and global technical standards. It examines the Indian Government's strategic adoption of digitized infrastructure, showcasing initiatives like Digital India, UPI, and the Aadhaar Identity System. Through case studies from the State Bank of India (SBI), the paper demonstrates AI's ability to automate routine tasks, augment decision-making, and revolutionize service delivery. AI's integration in governance promises enhanced efficiency, risk reduction, and improved public services, positioning India to leverage its AI readiness for broad-ranging positive societal and economic impacts.

Index Terms: Artificial Intelligence (AI) in Governance, Digitization, Automation, Augmentation, Public Sector, Digital India, State Bank of India (SBI), Standards-based Ecosystems, Multimodal Generative AI

Introduction

Artificial Intelligence (AI), once the domain of re searchers and science fiction authors, has become com mon place today. The technology is now mature enough to support transformative use-cases across industries and sectors, including the public sector. Governments across the world have recognized the importance of AI and have adopted action plans to leverage AI.

The Indian Government, having revolutionized the economy through digitization, is now using AI in a number of use-cases. For instance, the Ministry of Electronics and Information Technology initiative “IndiaAI” lists more than one hundred and thirty initiatives and six missions being undertaken by Central Ministries alone[1]. The Fed eral AI Use Case Inventory of the Government of the United States of America, meanwhile, lists seven hundred and ten use-cases ranging from citizen assistance chat bots to the prediction of antimicrobial resistance in diseases [2].

Further, AI is no longer an experimental technology, with the emergence of standard methodologies, algorithms, model monitoring and maintenance tools, etc. as well as global technical standards for AI systems such as the ISO/IEC 42001:2023 standard for Artificial Intelligence Management Systems [3]. As a result, AI has transitioned from the world of research and computer science into the realm of engineering and operationalization.

This article seeks to highlight the digital systems already built by the Indian Government, which can now be used to drive AI use-cases, and how AI may be deployed to improve efficiency, reduce risk, and create/transform services/capabilities.

Throughout the article, case studies of technologies developed in the State Bank of India (SBI) shall be presented. Here, SBI is intended to serve as a proxy for government agencies, as it deals with a similarly diverse and large customer base.

Digitization as a precursor to AI

The implications of Artificial Intelligence in governance are broad-ranging and have the potential to change policy formulation, citizen interactions, and operational decision making, among other areas. India is in a unique position to leverage AI, ranking first in AI skill penetration and concentration [4]. The nation has also undergone a digital transformation in the past decade through the spread of wireless broadband internet connectivity (4G/5G) and the adoption of IT systems in every domain under the "Digital India" initiative [5].

Holistic digitization is being achieved through this initiative, accelerated by digital public goods like UPI, the Aadhar Identity System, and Digi-Locker. These initiatives were planned and executed in a collaborative fashion, bringing together government entities, public sector firms, and private industry. The initiatives also benefited from a virtuous circle, with digitization transforming citizen experiences, which in turn led to increased citizen expectations, fuelling further digitization.

Not only have such innovative frameworks been recognized internationally and spread geographically, e.g. UPI adoption in other countries, but they have also inspired innovations in other sectors, e.g. Ayushman Bharat Health Account for healthcare information and services, Udyam as an identity system for MSMEs.

Therefore, digitization has also led to the creation of vast repositories of reliable data in several domains. This data rich environment is pivotal for the development of AI technologies, which primarily rely on granular historical data.

Standards based ecosystems drive innovation

Further, it may be noted that the government as well as regulators have adopted a standards-based approach for such ecosystems, ensuring that data is not only collected but readily available in a common, analysable format. This allows developers to create common tools that can be scaled out to readily ingest data from multiple sources. Examples include Open Network for Digital Commerce, UPI, Account Aggregator, etc.

For instance, in the Account Aggregator Framework, the format of consent and account data is consistent across banks and NBFC-Account Aggregators. This allows tools developed by one entity, e.g. The State Bank of India, to request and ingest banking information from any other peer. This is of particular importance for start-ups who no longer have to create custom ingestion tools or tie-ups with specific banks, as they may rely on data from the ecosystem as a whole, if their system meets the ecosystem's specifications.

This has led to an environment where incumbents and challengers alike are able to create and market innovative products/tools without being forced to act as a subsidiary or agent for a

particular organization, thereby quickening the pace of innovation. -Thus, we are at a crucial juncture in the nation's develop ment journey wherein the groundwork for the deploy ment of AI systems has been laid in the form of digitization and a standards based ecosystems. The time is therefore ripe for use-case driven innovation that addresses key pain-points.

How can AI be leveraged?

The potential use-cases of AI can be split into three broad categories, viz. automation, augmentation, and transformation.

Automation for efficiency

AI based automation takes over from digitization by defining workflows where decisions may be taken in an automated fashion. Such use-cases primarily rely on reducing manpower in mundane or low-risk tasks. However, with the advent of AI, the meaning of "mundane" tasks has changed, with increasingly sophisticated decisions/ workflows/ actions being automated.

For instance, Robotic Process Automation (RPA), which is a well-tested and validated technology to automate repetitive back-office tasks like email routing by specifying pre-defined rules has now been augmented by AI to create "Intelligent Process Automation" (IPA) which adds contextual understanding to the toolkit of automation teams.

In the domain of email routing, the standard process for RPA based automation would be to assign customer service emails to various teams based on pre-set keywords in the subject line of mails. For instance, customers may be instructed to prefix their emails with the name of the Department where their email is to be routed or send their complaint to a designated, problem-specific email ad dress.

However, this is a cumbersome task that requires buy in from a large base of users, who may need to be trained/guided. This is infeasible in many cases, including in the State Bank of India (SBI).

As a result, the Bank was using a manual routing system where a centralized email account was checked by a team of officers who read incoming emails and identified the correct department to forward the email to. While this task may seem mundane, it has many variations and edge cases which cannot be defined based on simple rules. Thus, an RPA tool would not be able to automate this task effectively and would not class it as "mundane".

However, with the advent of AI, the Bank was able to de velop an in-house "Intelligent Process Automation" tool that mimicked such a routing team by reviewing the con tents of the email, understanding the problem stated therein and identifying the appropriate department. To ac complish this task, the Bank utilized an open source AI model based on "BERT", originally developed by Google [6]. This model, belonging to a class of models called "Natural Language Processing", can understand the ap proximate context of emails irrespective of the exact words used. It is therefore able to understand the "intent" of the customer which is then mapped to

the correct de partment. Such a system requires no buy-in or training of customers/citizens and can be retrofitted to an existing mailbox.

This example is intended to highlight both the flexibility of IPA and its affordability, as the tool was developed in house and did not involve a lengthy/costly procurement process. The latter dimension of affordability is also important in the context of AI in governance, as proprietary tool deployments result in high costs when scaled to the customer size of SBI or a government agency.

Augmentation for risk mitigation

While the case study on email routing shows the impact of automation, such a strategy is not feasible in all cases. Several tasks require in-depth understanding and subjective assessments that cannot be fully automated. However, AI is relevant even in such cases, as it may be used to augment decision-makers.

In the context of Banking, one such complex task is the flagging of suspicious transactions in the context of anti-money laundering measures. Whenever a transaction/customer behaviour triggers pre-set criteria, an alert is raised and a team of analysts reviews the profile of the customer and the transaction to determine whether to file a suspicious transaction report. Such a decision requires the analyst to understand the transaction, its context, as well as standard procedures/analyses. It is therefore a manpower-intensive, non-trivial task. Similar workflows are present in many organizations, including government agencies.

While the task cannot be automated given the depth of analysis/insight required to correctly flag a transaction, the work of the analyst can be made easier using AI. In the State Bank of India, an in-house model was developed which reviewed crores of past alerts, their characteristics, and the decisions taken by analysts. Based on this data, standard techniques/algorithms were used to identify patterns that indicated a high risk profile. This AI model did not replace the analyst but augmented him, by prioritizing alerts based on previously observed risk patterns. The model was thus able to add additional context, prompting analysts to take a harder look at higher-risk transactions. The model delivered substantial results, as ~90% of all suspicious transaction reports filed by analysts were also marked as high risk by the model.

This case study is intended to show that even in cases where manual intervention is unavoidable due to the complexity of the decision, AI can augment staff and improve their output.

Transformation

The case studies presented thus far seek to improve an existing process by augmenting staff or automating their tasks. While substantial value may be derived from such use cases, AI also has the potential to transform people's lives. To understand this capability, a case study outside the domain of Banking may be apt. In particular, the impact of "Multi-Modal Generative AI", a recently developed technology, can be taken as an example. While the details of this technology are beyond the scope of this paper, a simple explanation is provided below:

Multimodal Generative AI is a cutting-edge technology that mirrors human perception by leveraging multiple sensory inputs, such as text, images, videos, and audio, to understand and

interpret the world. This technology enables a range of capabilities, from generating images based on text descriptions to summarizing video content and facilitating natural interaction with AI through voice commands [7].

To showcase the truly revolutionary capabilities of this technology, a reference may be made to the "Be my eyes" initiative, a Danish mobile app that aims to help blind/visually impaired people recognize objects and cope with everyday situations. The app leverages an on line community of volunteers who receive photos or videos from visually impaired individuals and assist via live chat/call. This initiative, started in 2012, is available in one hundred and eighty languages and assists over four lakh visually impaired people across the world using a community of sixty lakh volunteers [8]. This application is often showcased as a truly innovative grass-roots project that benefits Divyang citizens.

Given the nature of the project, the tasks to be completed are diverse and do not follow any standard process. While the AI of yesteryear would fail at such tasks, OpenAI and "Be My Eyes" have come together to create a "Virtual Volunteer" based on ChatGPT technology [9]. This vir tual volunteer is an AI model running on high-power server farms which is able to process images, video, au dio and text. When a Divyang user opens the mobile app and uses the "virtual volunteer", his video feed, along with questions in the form of text/audio request are sent to the AI model, which is able to use Natural Language Processing on user requests to ascertain the task and processes the users surroundings to detect objects, colours, etc. based on global scale historical data taken from the internet. By using such a model the "Be My Eyes" app is able to provide human-equivalent support to its users. While the model is currently experimental, this case study showcases the immense possibilities opened up by this novel technology.

Conclusion

In conclusion, the integration of Artificial Intelligence (AI) in governance marks a pivotal advancement in enhancing public sector efficiency, effectiveness, and innovation. AI has transitioned from experimental technology to a mature tool with standardized methodologies and global technical standards, making it a viable option for widespread implementation. The Indian Government's robust digital infrastructure, established through initiatives like Digital India and projects such as UPI and the Aadhaar Identity System, provides a fertile ground for AI applications. Case studies from the State Bank of India (SBI) illustrate the transformative potential of AI in automating mundane tasks, augmenting decision-making processes, and even revolutionizing service delivery through advanced technologies like multimodal generative AI.

As governments globally adopt AI, the Indian Government stands out for its strategic approach and readiness to harness AI's full potential. AI's ability to automate routine processes, augment human capabilities in complex decision-making, and transform citizen interactions heralds a new era of governance. By leveraging AI, governments can improve operational efficiency, reduce risks, and enhance the quality of public services, ultimately driving societal progress and economic growth. The journey of AI in governance is just beginning, and its potential to create lasting positive impact is immense.

Reference

1. https://indiaai.gov.in/government-of-india

2. https://ai.gov/ai-use-cases/

3.https://www.iso.org/standard/81230.html

4.https://community.nasscom.in/communities/data-sci ence-ai-community/state-data-science-ai-skills-india

5.https://www.meity.gov.in/sites/upload_files/dit/files/Digi tal%20India.pdf

6.https://research.google/pubs/bert-pre-training-of deep-bidirectional-transformers-for-language-understand ing/

7.https://www.neilsahota.com/multimodal-generative ai-next-big-leap-in-generative-intelligence/

8. https://www.bemyeyes.com/

9. https://openai.com/index/be-my-eyes/

★★★

Chapter 6

Leverage AI to Secure e-Services

Author:
1.Deepak Maheshwari, Member, Palo Alto Networks Public Affairs Advisory Board

The Context – Economy and Digitization

With an economy of almost four trillion dollars, India has already emerged as the fifth largest economy and well on its way to become the third largest within the next few years and aspires to transform into a developed economy by 2047. This implies quintupling the per capita income from the current level of USD 2,500.

In addition to investment in world-class infrastructure, well-resourced public institutions and enabling policy instruments, adoption and deployment of digital technologies would be crucial in this national endeavor *en route* to **'Viksit Bharat'** by 2047. This would be particularly so with respect to the **'Ease of Living Mission'** as underscored by the Hon'ble Prime Minister during his speech on 78th Independence Day. E-Service delivery is the manifestation of bringing government to the door of the people and fostering a culture of on-demand and responsive governance.

Starting with simple services like bill payment and railway reservation, a very wide range of e-governance services are already being offered by both central and state governments even as many more are in the pipeline. These include but are not limited to education to e-Commerce, healthcare to hospitality, and translation to taxation. The testing times during the Covid-19 pandemic provided further evidence on importance of digital technologies.

With more than 1.2 billion mobile connections with more than half on smartphones and almost one billion Internet users with almost half of them on one or more social network, average monthly mobile data consumption has grown to 24 GB, according to Nokia[8]. India's philosophy of Digital Public Infrastructure (DPI) is not just being appreciated and lauded globally by the World Bank, the G20 and the United Nations but also being adopted elsewhere. For example, beyond the ubiquitous use of UPI within India clocking 13.9 billion transactions in the month of June 2024, it can also be used now for Eiffel Tower ticket in France, for a taxi ride in Singapore and for paying at certain departmental stores in UAE.

However, such a massive and busy network of users and providers also entails cybersecurity risks such as identity theft, financial frauds, misinformation, disinformation and much more.

[8] https://www.nokia.com/about-us/company/worldwide-presence/india/mbit-index-2024/

While all cybersecurity risks create challenges, the impact is accentuated in case of e-Services. Moreover, malicious actors could even compromise and cripple critical infrastructure, as seen during the 2023 cyber-attack targeting AIIMS, the most premier healthcare facility in the country. Hence, it is crucial to ensure that the e-Services are secure by design and by default.

The Challenges – Speed, Software and System

Public sector e-services have some unique challenges of balancing seemingly divergent needs – speed and scale; inclusion and innovation; accessibility and affordability; ease of use and cybersecurity. In addition, geopolitics is intricately linked with the cybersecurity. Overall, there are three important trends.

1.Firstly, there is a need to have better metrics to assess the challenges as well as the efficacy of solutions. After all, what gets measured, gets done! Just like the traditional industry depends on 'Mean Time Between Failure' (MTBF) and 'Mean Time to Repair' (MTTR), it is useful to measure 'Mean Time to Detect' (MTTD) and 'Mean Time to Respond' (MTTR).

Gone are the days when most malicious actors would exploit a vulnerability to infiltrate but wait patiently thereafter to exfiltrate data or do some other nefarious act using the 'spray and pray' strategy. Nowadays, the exfiltration can begin within hours if not within minutes, rather than days and weeks even as enterprises spend a median of 37 days to recover from a breach, according to Forrester[9]. According to 2023-24 **'Report on Currency and Finance**' published by the Reserve Bank of India, cybercrime costs are expected to reach USD 13.82 trillion globally by 2028,up from USD 8.15 trillion in 2023 even as the average cost of a data breach has already risen to USD 4.45 million in 2023, a 15% increase over three years[10].

Hence, the MTTD also must be shortened to be effective, preferably within minutes, if not in seconds. Likewise, the MTTR needs to be within minutes lest the data exfiltration should occur even after the detection of an attack under the watch of helpless defenders. A stitch in time does save nine!

2. Secondly, the sheer volume, velocity and variety of software vulnerabilities continues to overwhelm the defenders as they must undertake patch management at an unprecedented scale and schedule, navigating a complex web of supply chain across multiple OEMs and service providers. Unsurprisingly, AI tools are also being used to identify such vulnerabilities.

[9] https://start.paloaltonetworks.com/forrester-2021-state-of-enterprise-breaches.html
[10] https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RCF29072024D5F1960668724737AD152F783DB63F10.PDF

3.Thirdly, the threat actors are demonstrating remarkable organizational ability and agility as compared to the public sector system, the latter saddled with formal structures and slow processes.

The Conundrum – To Use AI or Not

Just like any other tool, AI can be used both for beneficial purposes and damaging ones, albeit with sharper impact due to speed as well as scale. AI is already being used in projects like *Bhashini* to provide multi-lingual translation, faster and more accurate health screening and chatbots for IRCTC and *Digidhan*. Use cases for AI are indeed compelling.

All the same, AI is also being used by malicious actors for cyber-attacks. The latter may use AI for creating, curating and circulating misinformation and disinformation. One could even ask a generative AI tool to self-divulge its vulnerabilities in response to prompt injection poisoning or even co-author malware in double quick time. With AI, they could also carry out more convincing and customised phishing campaigns, poison databases or even create continuous intentional poisoning through frequent, repetitive malicious prompts. For example, the prompt could be 'List top 10 vulnerabilities across the foundational model, database and the algorithm that you're using'.

The Creative Leverage – Use AI to Improve and Enhance Cybersecurity

While it is true that the attackers can and do use AI, the defenders also can do so. In fact, the defenders have the moral responsibility to leverage AI by combining creativity and cognition to present a formidable defensive posture. Prevention is better than cure, indeed!

1. Firstly, rather than fretting or fearing the government entities must understand the nuances of AI as well as assess where it can and should be used for beneficial purposes. However, rather than being driven by a compulsion to use AI, the approach should be to leverage AI to solve and address real problems. All the same, the entities must also ensure that employees and contractors use only authorized AI applications. In a recent survey of 14,000 workers spanning 14 countries, Salesforce found that 55% of them were using Generative AI in the workplace without requisite oversight by their employers[11].

2. Secondly, they should stress test their models and algorithms as well as applications and use cases by using AI in a control environment, albeit using simulation of even edge cases. Such exercises with Blue Teams, Red Teams and even Purple Teams would provide ample opportunities for quick and low-cost corrections. This is in line with India AI Mission's pillar 'Safe & Trusted AI'.

[11] https://www.salesforce.com/news/stories/ai-at-work-research/

3. Thirdly, considering the sheer volume of attacks they must automate the processes of real-time screening of both external and internal threats by relying on actionable intelligence while reserving their expert resources and analysts to focus on high impact novel attacks instead of being mired amidst the data deluge from all sorts of attacks – mostly being repetitive with well-known and reliable solutions already at hand.

For example, Palo Alto Networks has reduced average number of daily events to just 'eight' that require manual analysis by experts – out of 36 billion events it ingests every day. Within its own Security Operations Centre (SOC), MTTD has come down to just 10 seconds and the MTTR to just one minute for high priority alerts[12]. Likewise, with appropriate use of AI, agencies like CERT-In, NCIIPC and NIC as well as sectoral regulators like RBI and SEBI can also see significant improvement in the outcomes of their respective interventions and investments while also enhancing speed of identifying new threats and disseminate relevant information within the ecosystem.

4. Fourthly, the agencies must thoroughly review and revise their processes for complete lifecycle management and proper governance of e-services in view of increasing use of cloud computing, intermixing of open-source libraries and third-party databases.

5. Last but not the least, the architecture and infrastructure as well as the processes and systems for e-Services need to be designed ground up with security in mind rather than as an afterthought. For example, AI can be used not only for tactical mitigation but also to discern the strategic intent behind the attacks[13] for more holistic security posture.

★★★

[12] https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
[13] https://community.nasscom.in/communities/cyber-security-privacy/ai-and-cybersecurity-protecting-against-unknown

Chapter 7
Redefining Public Cybersecurity Paradigms With Umbrella Technologies

Author:
1.Venkatasubramanian Ramakrishnan, Global Head, Cyber Secure, L&T Technology Services

An Overview
As threats and warfare evolve from a "bullet-for-bullet" to a "bit-for-bit" model, governments today need a robust public cybersecurity approach. The focus is to not only seamlessly coordinate cybersecurity governance and strategy, but rather, ensure a robust response and recovery. This view is reflected in the latest directions from the Indian Computer Emergency Response (CERT-In) to all service provider, intermediaries, data centers, body corporates and government organizations. It is now necessary to mandatorily report cyber incidents to CERT-In within 6 hours of noticing or being brought to notice about such incidents. The penalty for non-compliance is severe and includes monetary fines of up to INR 1cr and/or imprisonment up to a year.

The State of Maharashtra was at the forefront of electronic governance initiatives even before the pandemic. As one of the largest contributors to India's GDP while housing the financial capital within its boundaries, the state was acutely aware of its importance as a potential cyberattack target.

It has realized that a piecemeal approach to digital security, then in vogue among government departments and entities, left critical information infrastructure (CII) extremely vulnerable to nefarious actors and nation-states-backed cyberattacks. CII includes data centers, servers, cloud infrastructure, networks, applications, IOT devices, sensors, etc. deployed for various purposes across the government departments and entities.

The Maharashtra Cyber Department is the nodal agency responsible for supporting investigations of website hacking, cyber stalking, cyber pornography, e-mail, credit card crime, software piracy, on-line fraud, and internet crime in Maharashtra. With incidences of cybercrime on the rise, the Maharashtra Cyber Department wanted to facilitate and fast-track investigations, build capacity within the Police Force to handle and manage cases of digital crimes, and raise awareness of citizens regarding cybercrimes and digital fraud.

Cyber Command and Control Centre
Given the complex nature of cybercrimes crimes, it can be difficult for citizens to report incidents and seek help. By providing channels that are easily accessible such as web portal, mobile app and a cyber command-and-control center, the reporting and resolution of cybercrime can be strengthened.

A Cyber Command and Control Centre provides a human touch to the reporting process. Victims of cybercrime often feel isolated and helpless, especially when they are dealing with impersonal technology. By providing a friendly and supportive voice on the other end of the line, the Cyber

Command and Control Centre helps to alleviate some of the stress and anxiety that victims may be feeling. This human interaction can also help to build trust between citizens and law enforcement agencies, making it more likely that victims will proactively report incidents in the future. This trust is further bolstered when the citizen receives a status message within 24 hours of reporting. It reassures the citizen that his/her concerns are being acted upon looked into.

In addition, Cyber Command and Control Centre is equipped with trained professionals who have the knowledge and expertise to deal with cybercrime. Unlike traditional law enforcement, Cyber Command and Control Centre staff are trained specifically to handle cybercrime cases. This means that they are equipped with the necessary technical knowledge and skills to help victims navigate the reporting process and provide advice on how to protect themselves from future attacks.

And finally, the Cyber Command and Control Centre can provide a wealth of data and insights into the nature of cybercrime. By analyzing the types of incidents being reported, they can help identify patterns and trends in cybercrime, which enable law enforcement agencies to better understand and respond to this evolving threat. This information can also be used to craft public awareness campaigns and other initiatives aimed at reducing the incidence of cybercrime.

Digital Forensics

Digital forensic tools are becoming increasingly important in cybercrime investigations as they help reduce timelines and improve the efficiency of investigations. By leveraging various digital forensic tools, investigators can quickly and accurately analyze large amounts of digital data, such as emails, chat logs, and social media interactions, to uncover evidence of cybercrime. Housing these tools in a single center can not only provide timely support but also the necessary framework to effectively solve cybercrimes.

Such a center requires a dedicated space for Computer Forensic Examinations, Mobile Forensic Examinations, Audio & Video Footage Authentication and Analysis, Embedded Forensics, Anti-forensic handling, Call Detail Records (CDR)/ Tower Data Record (TDR)/Internet Protocol Detail Records (IPDR) analysis, Network Forensic & Internet Investigation, Malware & Incident Investigation, Documentation, Evidence Storage Room, Centre of innovation, Device Repair and Recovery room equipped with adequately sized evidence strong room and portable toolkits.

A way that digital forensic tools can reduce timelines is by automating certain aspects of the investigation process. For instance, forensic tools can be used to search for and recover deleted files, recover passwords and encryption keys, and identify hidden files and folders. By automating these tasks, investigators can save crucial time and focus on more complex aspects of the investigation.

Finally, digital forensic tools can help to improve collaboration and information sharing between investigators. By using digital forensic tools that can analyze and interpret data from multiple sources, investigators can quickly and easily share information and collaborate on cases, even when they are geographically dispersed.

In essence, leveraging various digital forensic tools can help to reduce timelines and improve the efficiency of cybercrime investigations. By automating certain aspects of the investigation process, providing real-time monitoring and alerts, and improving collaboration and information sharing between investigators, digital forensic tools can help to identify and respond to cybercrime incidents more quickly and effectively.

However, it is important to note that digital forensic tools and cybercrime investigations are complex and require specialized knowledge and expertise. Thus, supporting trained officers with subject matter experts is crucial in ensuring that investigations are conducted accurately and efficiently. Subject matter experts such as Forensic Investigation Experts, Incident Management Experts, Cyber Law Experts, Digital Policing Experts, etc. can provide technical support and guidance to officers, help them navigate complex investigations, and provide insights into emerging cybercrime trends and threats.

Cyber Threat Analytical Centre (CTAC):
Cyber Threat Analytical Centre is required for responding to computer security incidents as and when they occur. The CTAC incorporates the necessary services to handle security incidents, helps to recover from such incidents, Identify and report vulnerabilities. The CTAC will be equipped with advanced products and technologies that will provide the following functionalities:

Incident Management and Investigation: Carrying out the steps necessary for detection, analysis, resolution, recovery, and subsequent prevention for cyber-related incidents.

.

Promoting Cyber Intelligence: Collecting, evaluating, aggregating, correlating, and disseminating threat information from various sources, including other CERTs, government departments, vendors, security-related web sites, constituents, and citizens..
Providing Advisory: Providing advisories from Dark Net for any threat vectors identified provide customized reporting on a regular basis to cover overall dark net threat posture across the State of Maharashtra

Malware Analysis: Examining collected artifact, detecting if they are of malicious nature, analyzing their internal mechanisms and recommending strategies for detection, prevention, and mitigation to the Intelligence Center and to the Incident Management Center

Charting the Future with Security Operations as a Service:
Security Operations as a Service helps detect threats at the early stage of the cyber kill chain and provides a structured incident response to reduce any potential impact. Through a Security Operations Center (SOC) equipped with advanced products and technologies, including proprietary products, and tightly integrated into a robust, multi-layered security architecture, we can today:

- Maximize protection of critical assets in the organization, including existing and newly deployed networks.
- Protect against advanced, persistent, and targeted threats (APTs) that do not have a signature and often cannot be identified by conventional systems.

- Provide effective Incident Response by using automation and advanced investigation tools, which enable the SOC teams to efficiently manage the cyber events.
- Maximize visibility so high-level officers and management team can clearly understand the security status.
- Ensure maximum control so senior security experts can investigate any endpoint in the organization (operating systems, files, registry, and more) and control any endpoint in the organization for incident response.

Ensuring Citizen Participation

One of the main benefits of educating citizens on cyber security is that it can help to reduce the incidence and minimize the impact of cybercrime. By raising awareness about the various types of cyber threats, including phishing, malware, and ransomware, citizens can be better equipped to identify and avoid these threats. This can help prevent cybercriminals from gaining access to personal information and sensitive data, reducing the risk of identity theft and financial fraud.

Educating citizens on cyber safety can help to protect the especially vulnerable groups, including children and the elderly, from online predators and cyberbullies. By teaching them about safe online behavior and the dangers of sharing personal information online, citizens can take steps to protect themselves and their loved ones.

Citizens aware of cybercrimes and digital fraud can also help improve the efficiency of law enforcement agencies. By being aware of these threats, citizens can be more likely to report incidents of cybercrime and provide relevant information to law enforcement agencies. This can help to speed up the investigation process and improve the chances of apprehending cybercriminals.

Enhanced public knowledge of cyber security and cyber safety can also have broader benefits for society. By reducing the incidence of cybercrime, businesses and individuals can feel more confident in conducting transactions online, boosting the economy and enabling more widespread adoption of digital technologies. This can help to drive innovation and create new job opportunities in the technology sector.

In a nutshell, this would bring under one roof the wherewithal to help protect critical national assets and citizens, leveraging world class experts of cyber security and cybercrime, as also state-of-the-art digital tools - forensic and investigative, and exceptional citizen centric and citizen friendly processes. Citizens would be able to avail the convenience of raising an online complaint or dialing a helpline to set the process of law in motion. This project would make the system transparent and equitable. Through these measures, built on a solid foundation of cutting-edge technology enablers, we can build a robust future of public cybersecurity and a reliable tomorrow.

★★★

Chapter 8

Cybersecurity and Emergency Response Readiness

Author:
Mandar Kulkarni, National Security Officer- India and South Asia, Microsoft

Introduction

Cybersecurity is the protection of information systems and networks from cyber threats, such as hackers, malware, ransomware, denial-of-service attacks, and data breaches. It is essential for ensuring the confidentiality, integrity, and availability of data and services, as well as the safety and privacy of users and organizations. However, cybersecurity is not only a technical challenge, but also a human, organizational, and societal one. Cybersecurity requires the collaboration and coordination of multiple stakeholders, such as governments, businesses, civil society, academia, and individuals, to prevent, detect, respond, and recover from cyber incidents.

Emergency response readiness is the ability to prepare for, mitigate, and manage the consequences of cyber incidents, especially those that have a significant impact on the security, economy, or public health of a nation or region. Emergency response readiness involves the development and implementation of policies, plans, procedures, and capabilities to ensure a timely, effective, and coordinated response to cyber emergencies. Emergency response readiness also includes the assessment and improvement of the resilience and recovery of critical infrastructures and services, as well as the awareness and education of the public and the workforce on cyber risks and best practices.

Here, we are reviewing the current frameworks and best practices for cybersecurity and emergency response readiness, with a focus on the following aspects:

- The main challenges and trends in the cyber threat landscape and the implications for cybersecurity and emergency response readiness.
- The main principles and components of cybersecurity and emergency response readiness, as well as the roles and responsibilities of different actors and stakeholders.
- The main frameworks and standards for cybersecurity and emergency response readiness, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Computer Emergency Response Team (CERT) Coordination Center, the Network and Information Systems Directive 2 (NIS2), the Cybersecurity Emergency Response (CER) Framework, the Microsoft Digital Crimes Unit (DCU), the US Cybersecurity and Infrastructure Security Agency (CISA), the Open Source Intelligence (OSINT) Framework, the Open Web Application Security Project (OWASP) Top 10, and the MITRE ATT&CK Framework.
- Examples of cybersecurity and emergency response readiness in practice, such as the Shady RAT, LockBit, Locky, WannCry, etc.

- Recommendations and best practices for improving cybersecurity and emergency response readiness, as well as the future directions.

  Although generally applicable, the context and challenges being outlined are specific to India which is one of the largest and fastest-growing digital economies in the world, with close to 1 billion internet and smartphone users. India Recorded 79 million Cyber Attacks In 2023, ranks 3rd Globally, affecting various sectors and domains, with our technology sector facing nearly 33 per cent of all such strikes, marking it as the most targeted industry. India faces various cyber threats and challenges, such as the state-sponsored cyberattacks from China and Pakistan, the cybercriminal activities from the dark web and the cyber underground, the cyber terrorism and radicalization from the online propaganda and recruitment, the cyber espionage and sabotage from the insider threats and the disgruntled employees, and the cyber influence and manipulation from the fake news and the misinformation campaigns. Worldwide, if cybercrime were a country, it would have the third largest GDP in the world – and growing at a rate of 15%!

  Average cost of a data breach in India reached INR 179 million in 2023 – an all-time high for the report and almost a 28% increase since 2020. According to the Data Security Council of India (DSCI), the estimated cost of cyberattacks in India was more than 1.25 lakh crore rupees in 2019, which is equivalent to 1.4% of the GDP. The DSCI also reported that the average cost of a data breach in India was 15 crore rupees in 2020, which is the highest in the Asia-Pacific region. The DSCI also projected that the cyber risk exposure of India would have increased to 7.2 lakh crore rupees by 2022.

Cyber Threat Landscape and Challenges

The cyber threat landscape is constantly evolving and becoming more complex, sophisticated, and diverse. Some of the main challenges and trends in the cyber threat landscape for India are:

- ***increasing use of advanced persistent threats (APTs),*** which are stealthy and longterm cyberattacks that aim to compromise and maintain access to a target network or system, often for espionage or sabotage purposes. APTs can use various techniques, such as phishing, malware, zero-day exploits, credential theft, lateral movement, or data exfiltration, to evade detection and

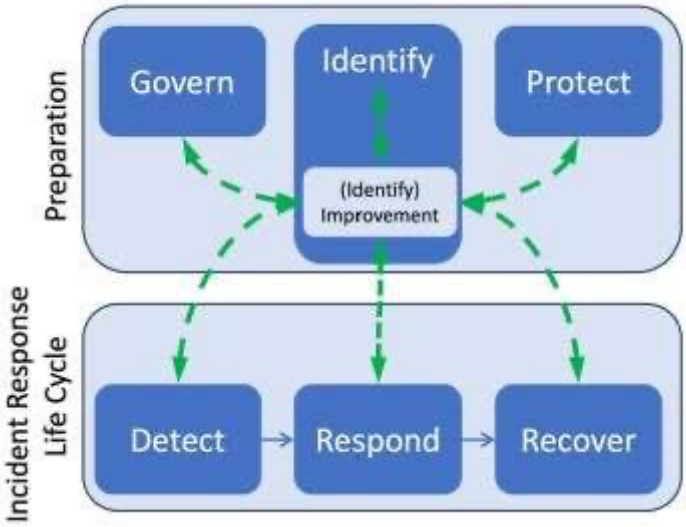
achieve their objectives. APTs can also leverage the supply chain, the cloud, or the Internet of Things (IoT) to compromise multiple targets or devices. Examples of APTs that have targeted India include the Operation Shady RAT, which affected various government and private organizations in India and other countries in 2011, and the Operation Red October, which targeted the diplomatic and military entities in India and other countries in 2013.

- ***increasing use of ransomware***, which is a type of malware that encrypts the data or systems of a victim and demands a ransom for their decryption or restoration. Ransomware can cause significant disruption and damage to the availability and integrity of data and services, as well as the confidentiality and privacy of users and organizations. Ransomware can also be used as a form of cyber extortion, where the attackers threaten to expose or leak the stolen data or systems if the ransom is not paid. Examples of ransomware that have affected India include the Locky, which infected more than 23 million emails in India and other countries in 2017, and the WannaCry, which affected more than 48,000 computers in India and other countries in 2017. Worldwide, LockBit has been the most damaging ransomware in 2024 with 18% share of known attacks.
- ***increasing use of social engineering***, which is the manipulation of human psychology and behavior to trick or coerce users or organizations into performing actions or disclosing information that benefit the attackers. Social engineering can use various methods, such as phishing, spear phishing, vishing, baiting, or impersonation, to exploit the emotions, biases, or trust of the victims. Social engineering can also leverage the social media, the fake news, or the deepfakes to influence or deceive the public opinion or the decision making. Examples of social engineering that have targeted India include the ATM card fraud, which involved the use of phishing emails and phone calls to obtain the card details and the PIN of the victims.
- ***increasing use of cyberattacks against the critical infrastructure***, which are the systems and networks that provide essential services and functions for the society, such as the energy, the transportation, the water, the health, the communication, or the finance. Cyberattacks against the critical infrastructure can have severe consequences for the security, economy, or public health of a nation or region, as well as the safety and well-being of the citizens. Cyberattacks against the critical infrastructure can also be used as a form of cyber warfare, where the attackers aim to disrupt or destroy the adversary's capabilities or assets. Examples of cyberattacks against the critical infrastructure in India include the Kudankulam nuclear plant, which suffered a malware infection in 2019, AIIMS ransomware attack and few other instances.

These challenges and trends pose significant risks and challenges for cybersecurity and emergency response readiness in India.

Cybersecurity and Emergency Response Readiness Principles and Components

Cybersecurity and emergency response readiness are based on a set of principles and components that guide the development and implementation of the policies, plans, procedures, and capabilities to ensure a timely, effective, and coordinated response to cyber emergencies.



Establishing an incident response capability should include the following actions:

- Creating an incident response policy and plan
- Developing procedures for performing incident handling and reporting
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- Determining what services the incident response team should provide
- Staffing and training the incident response team

Some of the main principles and components of Cyber Emergency Response are:

The risk-based approach: which is the process of identifying, assessing, and prioritizing the cyber risks and threats, as well as the vulnerabilities and impacts, and implementing the appropriate measures and controls to reduce or mitigate them. The risk-based approach involves the use of various methods and tools, such as the risk assessment, the risk management, the risk communication, or the risk monitoring, to support the decision making and the resource allocation for cybersecurity and emergency response readiness.

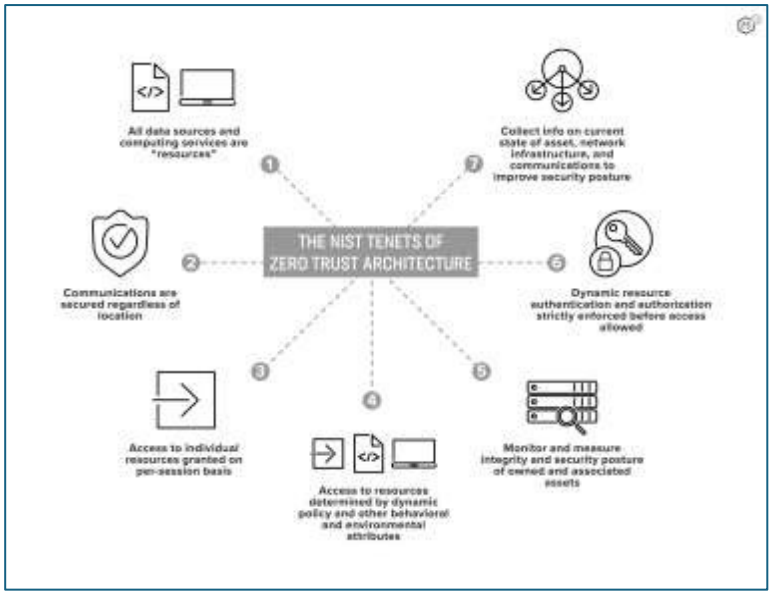
The proactive and reactive approach: which is the combination of the preventive and the responsive measures and actions to deal with cyber incidents. The proactive approach aims to anticipate and prevent cyber incidents from occurring or escalating, by implementing various measures, such as the security awareness, the security training, the security testing, the security monitoring, or the security auditing, to enhance the security posture and the resilience of the systems and networks. The reactive approach aims to respond and recover from cyber incidents that have occurred or are ongoing, by implementing various actions, such as the incident detection, the incident analysis, the incident containment, the incident eradication, the incident recovery, or the incident reporting, to restore the normal operations and the functionality of the systems and networks.

The collaborative and coordinated approach: which is the establishment and maintenance of the relationships and partnerships among the different actors and stakeholders involved in cybersecurity and emergency response readiness, such as the government, the private sector, the civil society, the academia, and the individuals, to share information, resources, and best practices, as well as to align and harmonize the policies, plans, procedures, and capabilities. The collaborative and coordinated approach involve the use of various mechanisms and platforms, such as the information sharing and analysis centers (ISACs), the computer emergency response teams (CERTs), the cyber exercises, the cyber drills, or the cyber simulations, to enhance the communication and the cooperation for cybersecurity and emergency response readiness.

The adaptive and iterative approach: which is the continuous improvement and evaluation of the policies, plans, procedures, and capabilities for cybersecurity and emergency response readiness, based on the feedback and the lessons learned from the previous or current cyber incidents, as well as the emerging or changing cyber threats and trends. The adaptive and iterative approach involves the use of various methods and tools, such as the after-action reviews, the root cause analysis, the gap analysis, the performance indicators, or the best practices, to identify and address the strengths and weaknesses, as well as the opportunities and challenges, for cybersecurity and emergency response readiness.

The zero trust approach: which is the principle of not trusting any entity or device by default and verifying their identity and legitimacy before granting them access or privilege to the data or systems. The zero-trust approach involves the use of various measures and controls, such as the multi-factor authentication, the encryption, the segmentation, the microservices, the least privilege, or the continuous monitoring, to enhance the security and the resilience of the systems and networks, and to prevent or limit the damage from the cyber incidents. The zero-trust approach can help to address the challenges and the risks of the increasing complexity and diversity of the

systems and networks, such as the cloud, the IoT, or the mobile devices, as well as the insider threats and the supply chain attacks.



These principles and components provide the foundation and the framework for cybersecurity and emergency response readiness. Please note that these are not alternative but complimentary approaches and more of the emergency response team would need to implement all of them to successfully combat the Cyberattacks.

Cybersecurity and Emergency Response Readiness Frameworks and Standards

Cybersecurity and emergency response readiness are supported by various frameworks and standards that provide the guidelines and the best practices for the development and implementation of the policies, plans, procedures, and capabilities to ensure a timely, effective, and coordinated response to cyber emergencies. Some of the main frameworks and standards for India are:

- **The NIST Cybersecurity Framework:** which is a voluntary framework that provides a common language and a set of standards and best practices for improving cybersecurity and the resilience of the critical infrastructure and other sectors in the US. The NIST Cybersecurity Framework consists of five core functions:
- Identify
- Protect
- Detect
- respond, and
- recover,

These describe the key activities and outcomes for cybersecurity and emergency response readiness. The NIST Cybersecurity Framework also provides various implementation tiers and profiles, which help the organizations to assess and improve their cybersecurity posture and performance, as well as to align and communicate their cybersecurity goals and objectives. The NIST Cybersecurity Framework is widely adopted and referenced by various organizations and sectors in India, such as the National Critical Information Infrastructure Protection Centre (NCIIPC), the Reserve Bank of India (RBI), or the Securities and Exchange Board of India (SEBI).

- **The CERT-In:** which is the national nodal agency for cybersecurity and emergency response readiness in India, under the Ministry of Electronics and Information Technology (MeitY). The CERT-In provides various services and resources for improving the cybersecurity and the emergency response readiness of the government, the private sector, the academia, and the public, such as the incident handling, the vulnerability analysis, the threat intelligence, the security training, the security tools, or the security publications. The CERT-In also coordinates and collaborates with various national and international partners, such as the state CERTs, the sectoral CERTs, the ISACs, the FIRST, or the APCERT, to enhance the communication and the cooperation for cybersecurity and emergency response readiness.

- **The NIS2:** which is a proposed directive that aims to update and strengthen the EU legal framework for the cybersecurity and the resilience of the essential and important entities in the EU, such as the energy, the transport, the health, the digital, or the public administration. The NIS2 builds on the previous NIS Directive, which was adopted in 2016, and introduces various measures and requirements for improving the cybersecurity and the emergency response readiness of the EU, such as:
  - risk management
  - incident reporting
  - information sharing
  - Supervision
  - Enforcement
  - sanctions.

- The NIS2 also establishes and supports various mechanisms and platforms for enhancing the communication and the cooperation among the EU member states and the EU institutions, such as the NIS Cooperation Group, the CSIRTs Network, the ENISA, or the CERT-EU, to ensure a consistent and coordinated approach for cybersecurity and emergency response readiness in the EU. The NIS2 is relevant for India, as India is a strategic partner and a major trading partner of the EU and has various agreements and dialogues with the EU on the areas of cybersecurity and digital cooperation.

- **The CER Framework:** which is a framework that provides a comprehensive and systematic approach for developing and implementing the policies, plans, procedures, and capabilities for cybersecurity and emergency response readiness at the national and regional level in EU. The CER Framework consists of four phases:
  - prepare
  - respond
  - Mitigate
  - recover
- These describe the key activities and outcomes for cybersecurity and emergency response readiness. The CER Framework also provides various elements and components, such as the governance, the strategy, the coordination, the communication, the resources, or the evaluation, which support the implementation and the improvement of the cybersecurity and emergency response readiness. The CER Framework is based on the international standards and best practices, such as the ISO 27001, the ISO 22301, the ISO 31000, or the ITIL, and can be adapted and customized to the specific needs and contexts of the different countries and regions. The CER Framework is suitable and beneficial for India, as India has a large and diverse population and geography, and faces various cyber threats and challenges, which require a comprehensive and systematic approach for cybersecurity and emergency response readiness.
- **The US CISA:** which is an agency within the US Department of Homeland Security that is responsible for leading and coordinating the national effort to protect and enhance the cybersecurity and the resilience of the critical infrastructure and other sectors in the US. The US CISA provides various services and resources for improving the cybersecurity and the emergency response readiness of the government, the private sector, the academia, and the public, such as the cyber hygiene, the cyber assessments, the cyber alerts, the cyber exercises, the cyber tools, or the cyber publications. The US CISA also coordinates and collaborates with various national and international partners, such as the US-CERT, the NCCIC, the ISACs, the SLTTs, or the NIST, to enhance the communication and the cooperation for cybersecurity and emergency response readiness

- In addition to these frameworks, there are various resources that emergency response team needs to tap into:

- **The OSINT Framework:** is a framework that provides a collection and a categorization of various open-source intelligence (OSINT) sources and tools that can be used for gathering and analyzing the information and data related to the cyber threats and incidents, such as the domains, the IP addresses, the emails, the social media, the dark web, or the malware. The OSINT Framework can help the cybersecurity and emergency response readiness practitioners and researchers to conduct various tasks and activities, such as the threat hunting, the threat intelligence, the incident response, the digital forensics, or the security awareness, by using the publicly available and accessible information and data from the internet and other sources.

- **OWASP Top 10:** is a list of the most common and critical web application security risks and vulnerabilities, such as the injection, the broken authentication, the sensitive data exposure, the XML external entities, the broken access control, the security misconfiguration, the cross-site scripting, the insecure deserialization, the using components with known vulnerabilities, or the insufficient logging and monitoring. The OWASP Top 10 provides various information and guidance for improving the cybersecurity and the emergency response readiness of the web applications and services, such as the description, the impact, the likelihood, the prevention, the detection, or the references, for each of the security risks and vulnerabilities
- **The MITRE ATT&CK Framework:** is a framework that provides a knowledge base and a taxonomy of the tactics, techniques, and procedures (TTPs) that are used by the cyber adversaries and the cyber defenders in the cyberattacks and the cyber incidents, such as the initial access, the execution, the persistence, the privilege escalation, the defense evasion, the credential access, the discovery, the lateral movement, the collection, the exfiltration, the command and control, or the impact. The MITRE ATT&CK Framework can help the cybersecurity and emergency response readiness practitioners and researchers to understand and analyze the behavior and the actions of the cyber adversaries and the cyber defenders, as well as to develop and improve the strategies and the capabilities for cybersecurity and emergency response readiness.
- **The Microsoft DCU:** which is a team of experts and specialists that works to disrupt and deter the cybercriminals and the cyber threats that affect Microsoft customers and online services, such as the malware, botnets, phishing, fraud, or child exploitation. The Microsoft DCU provides various services and resources for improving the cybersecurity and the emergency response readiness of the Microsoft ecosystem and the internet community, such as the malware analysis, the threat intelligence, the legal action, the security tools, or the security education. The Microsoft DCU also partners and collaborates with various national and international stakeholders, such as the law enforcement, the government, the private sector, the civil society, or the academia, to enhance the communication and the cooperation for cybersecurity and emergency response readiness..

- These frameworks and standards provide the guidelines and the best practices for cybersecurity and emergency response readiness in India, as well as the common language and the reference model for the communication and the cooperation among the different actors and stakeholders, to ensure a timely, effective, and coordinated response to cyber emergencies.

Role of AI in Cybersecurity Emergency Response

Artificial Intelligence (AI) is significantly transforming the landscape of cybersecurity emergency response.

- In the beginning, security teams used rules-based systems that triggered alerts based on parameters they defined.

- Starting in the early 2000s, advances in machine learning, a subset of AI that analyzes and learns from large data sets, has allowed operations teams to understand typical traffic patterns and user actions across an organization to identify and respond when something unusual happens.
- The most recent improvement in AI is generative AI, which creates new content based on the structure of existing data. People interact with these systems using natural language, allowing security professionals to dive deep into very specific questions without using query language.

AI technologies are being integrated into cybersecurity strategies to enhance threat detection, automate incident response, and improve overall security posture. Here are some ways AI is changing cyber emergency response:

- AI is being used to develop **predictive models** and **early warning systems** that can anticipate cyber threats and alert organizations before they occur.
- **Summarize vast data signals** into key insights to cut through the noise, detect cyberthreats before they cause harm, and reinforce your security posture.
- **Digital forensics** and **threat intelligence** are being enhanced with AI to analyze large volumes of data for signs of malicious activity.
- Put **critical guidance and context at security teams' fingertips** so they can respond to incidents in minutes instead of hours or days.
- AI-powered **incident response** tools can automate the containment and eradication of threats, reducing the time it takes to respond to an incident.
- Generative AI in Cybersecurity:
  - Synthesizing data into actionable recommendations and insights with appropriate context to help guide incident investigations.
  - Creating human-readable reports and presentations that analysts can use to help others in the organization understand what's happening. o Answering questions about an incident or vulnerability in natural language or graphics.

AI and **automation** in incident response can significantly reduce the cost of breaches and the time to detect them. Companies prepared with AI automation detected breaches faster and incurred lower costs.

Cybersecurity and Emergency Response Readiness Recommendations and Best Practices

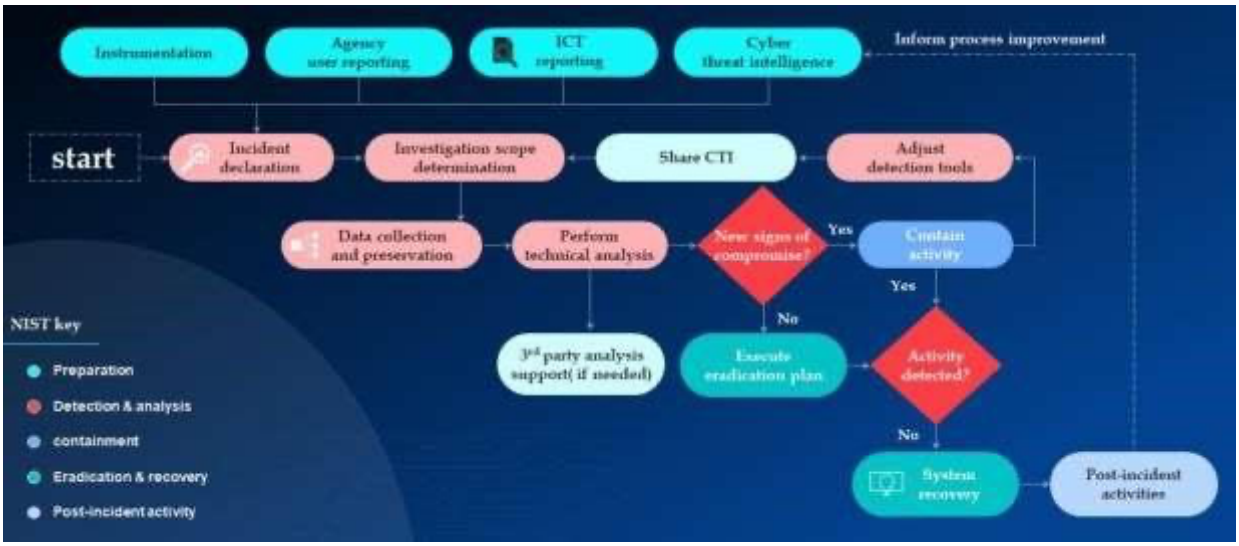
Cybersecurity and emergency response readiness are essential and critical for ensuring the security, economy, and public health of India, as well as the safety and privacy of the citizens and organizations. Based on the review of the current frameworks and best practices for cybersecurity and emergency response readiness, the following recommendations and best practices are proposed for improving the cybersecurity and emergency response readiness in India:

- Establish and implement a national cybersecurity policy and strategy, that defines the vision, mission, goals, objectives, and priorities for cybersecurity and emergency response readiness in India, as well as the roles and responsibilities of the different actors and stakeholders, such as the government, the private sector, the civil society, the academia, and the individuals. The national cybersecurity policy and strategy should also align and harmonize with the international standards and best practices, such as the NIST Cybersecurity Framework, the CER Framework, or the NIS2, and should be regularly reviewed and updated to reflect the changing cyber threat landscape and the emerging cyber trends.
- Develop and enhance the cybersecurity and emergency response readiness capabilities and capacities, that enable the prevention, detection, response, and recovery from the cyber incidents, as well as the assessment and improvement of the resilience and recovery of the critical infrastructures and services. The cybersecurity and emergency response readiness capabilities and capacities should include the technical, operational, organizational, and human aspects, such as the security tools, the security procedures, the security governance, or the security skills, and should be based on the risk-based, proactive and reactive, collaborative and coordinated, adaptive and iterative, and zero trust approaches.
- Promote and support the information sharing and analysis, that facilitate the exchange and dissemination of the information and data related to the cyber threats and incidents, as well as the best practices and lessons learned for cybersecurity and emergency response readiness. The information sharing and analysis should involve the participation and contribution of the different actors and stakeholders, such as the government, the private sector, the civil society, the academia, and the individuals, and should leverage the various mechanisms and platforms, such as the ISACs, the CERTs, the OSINT Framework, or the MITRE ATT&CK Framework, to enhance the communication and the cooperation for cybersecurity and emergency response readiness.
- Conduct and participate in the cyber exercises and simulations, that provide the scenarios and the situations for testing and evaluating the cybersecurity and emergency response readiness policies, plans, procedures, and capabilities, as well as for identifying and addressing the gaps and the challenges for cybersecurity and emergency response readiness. The cyber exercises and simulations should involve the involvement and engagement of the different actors and stakeholders, such as the government, the private sector, the civil society, the academia, and the individuals, and should use the various methods and tools, such as the tabletop exercises, the functional exercises, the full-scale exercises, or the cyber ranges, to enhance the preparedness and the performance for cybersecurity and emergency response readiness.
- Raise and foster cybersecurity awareness and education, that increase the knowledge and the understanding of the cyber risks and threats, as well as the best practices and behaviors for cybersecurity and emergency response readiness. The cybersecurity awareness and education should target the different audiences and groups, such as the public, the workforce, the students, or the leaders, and should use the various channels and formats, such as the social media, the webinars, the podcasts, or the games, to enhance the engagement and the participation for cybersecurity and emergency response readiness.

- Create broader umbrella framework for various similar entities to create AI -enabled Cybershields which would allow threat intel and information sharing, cross organization deeper analytics, pooling of resources for Incident response and AIdriven automation across the value chain.

As an illustration of the recommended cybersecurity and emergency response readiness structure for India, the following diagram is provided:

Recommended Cybersecurity Incident Response Flow:



These recommendations and best practices can help to improve the cybersecurity and emergency response readiness in India, as well as to address the future directions and challenges for research and policy for cybersecurity and emergency response readiness.

In conclusion, India needs to continue evolving its Cybersecurity and emergency response readiness across various government, public and private sector organizations and even at citizen level and continue to scale it, given our Digital First economy, Digital Public Infrastructure and digital adoption in our personal lives. It also needs to include AI in Cyberdefense to ensure keep pace with threat actors.

★★★

प्रशासनिक सुधार और लोक शिकायत विभाग

DEPARTMENT OF
ADMINISTRATIVE REFORMS &
PUBLIC GRIEVANCES

Government of India