News & Views | Pg 04
Understanding The Digital Age: Cybersecurity, Privacy, And Data Protection

Insight | Pg 24
AI & Its Implications On Information Security

ITNEXT

FOR THE NEXT GENERATION OF CIOs

THE YEAR OF AI REVOLUTION

NEXT100 leaders foresee AI seamlessly integrating into the fabric of enterprise ecosystems. Explore what's in store for tech deployments in the year ahead in our special edition.

October-November-December 2023 | ₹100 | Volume 14 | Issue 09 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

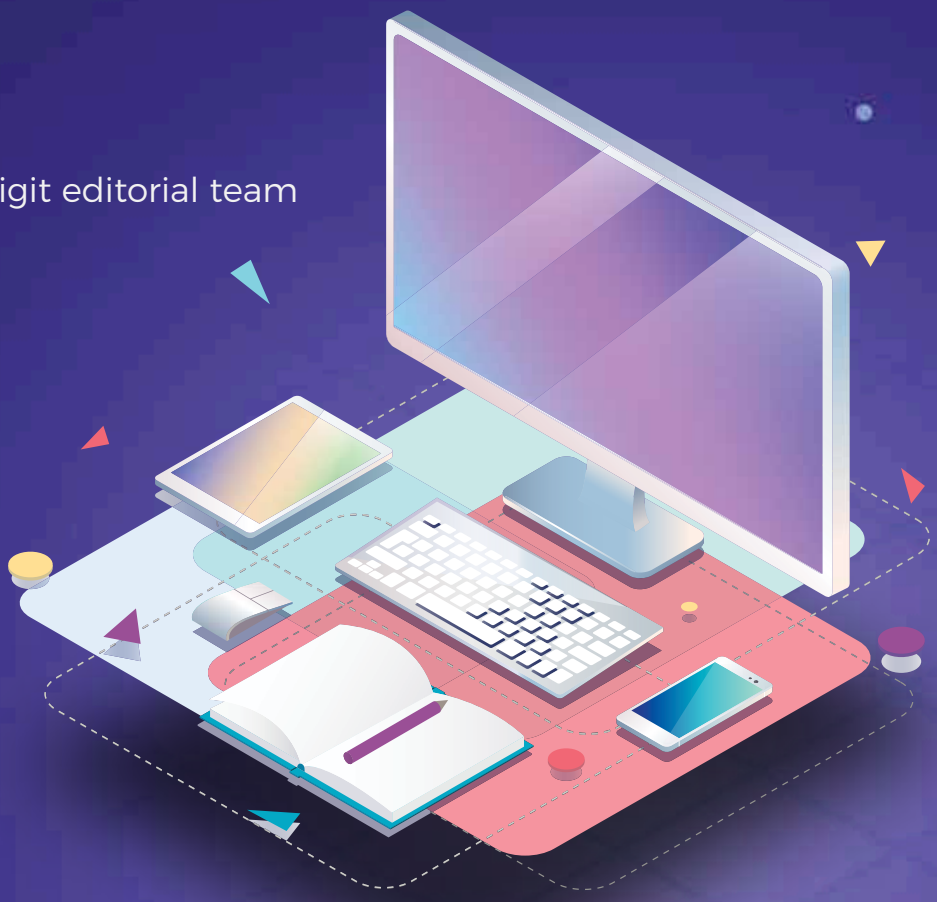
LAUNCHING

digit SQUAD

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

- Launch your own tech channel on Digit.in
- Become a Digit Certified tech influencer
- Engage with digit editorial team
- Make money



Apply now by scanning the QR code

www.digit.in/digit-squad/apply.html

PPP 2.0

India's DPI enhances sectors like health and education, offering mutual benefits for government and private companies in terms of revenue and efficiency.

Shyamanuja Das

No one has seen tomorrow. That doesn't stop analysts and media from forecasting the future occasionally because they give something to work towards.

When it's near-term predictions, usually, practitioners have a better tap because no one knows better than them what they are up to. Yes, in the short term, they influence the future the most.

Various factors influence technology adoption. Some supply-side forces include technology development, the number of technology companies backing a particular technology, their market prowess, etc. The demand side forces have a competitive nature of a business segment, level, nature of regulation, technology maturity in a particular organization, and skill availability.

Of late, environmental factors have become important influencers of technology adoption by businesses. Most prominent among these is the growing consumerization of technology.

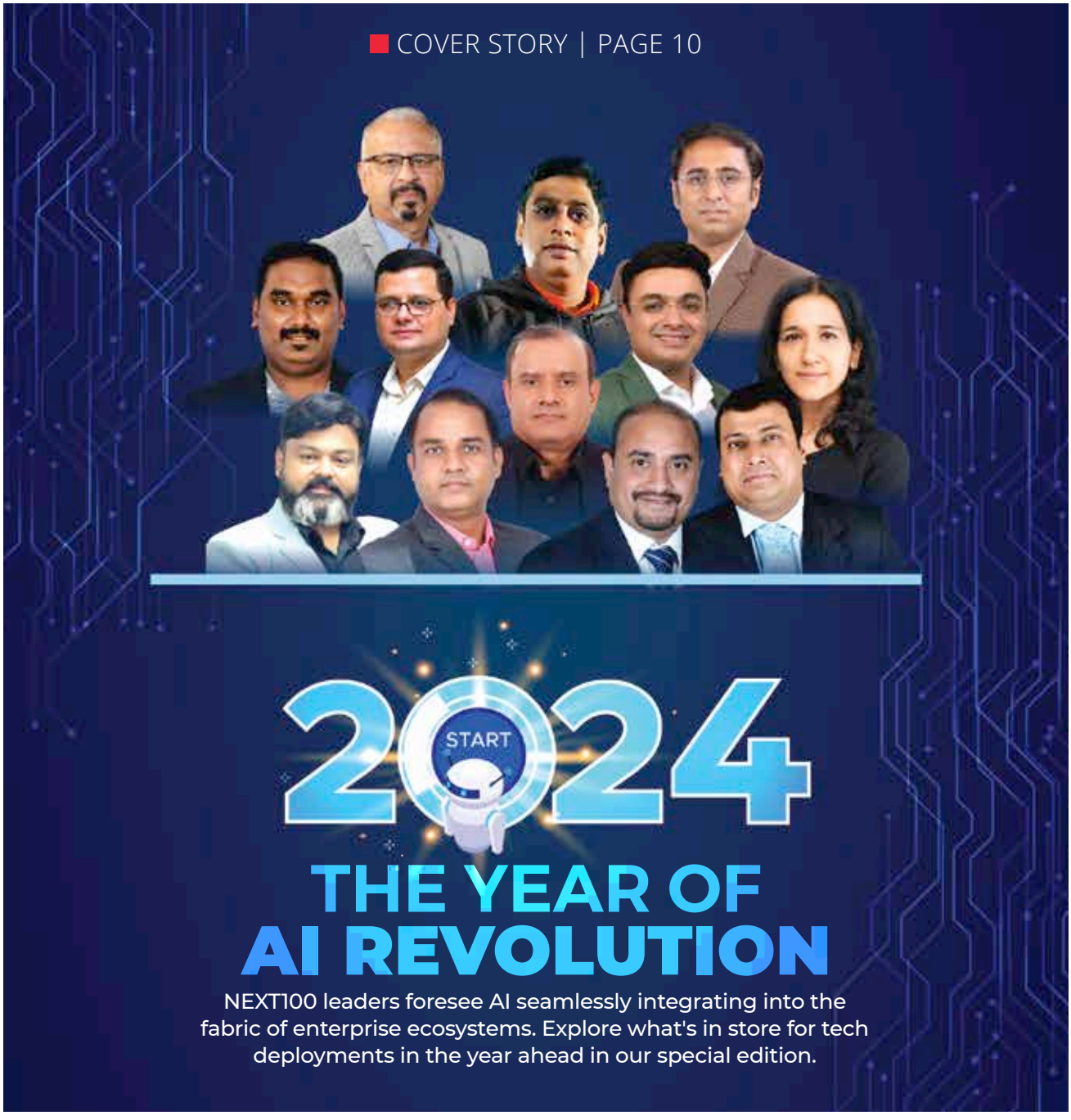
I would like to point out one such rising factor in India: the aggressive digitization of governance and citizen service infrastructure. While that itself is a catalyst of growing consumer digitization and is well-acknowledged, it can drive economic growth for the country and make businesses and the government more efficient by avoiding duplication in technology investment and even making them more effective by dramatically increasing reach. Call it Public Private Partnership (PPP) 2.0. It is something that will happen anyway. The idea is to accelerate it by becoming proactive.

Digital Public Infrastructure (DPI), which India has taken a lead in, can revolutionize its reach. The government has taken several initiatives in health, primary education, higher education, and civil supplies. Private companies can leverage them. The government will benefit from revenue and expertise. Businesses will gain in terms of reach and efficiency. ■

OCTOBER-
NOVEMBER-
DECEMBER 2023
VOLUME 14 | ISSUE 09

Content

COVER STORY | PAGE 10



Cover Design:
VIPIN RAI

ADVERTISER INDEX

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

MANAGEMENT
Managing Director: Dr Pramath Raj Sinha
Printer & Publisher: Vikas Gupta

EDITORIAL
Editorial Director - B2B Tech: Shyamanuja Das
Executive Editor - B2B Tech: Jatinder Singh
Assistant Manager - Content: Dipanjan Mitra
Principal Correspondent: Nisha Sharma

DESIGN
Associate Art Director: Baiju NV
Sr. UI UX Designer: Nikhil Wahal
Sr. Designer: Vipin Rai

SALES & MARKETING
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)
Associate Director - Enterprise Technology:
Vandana Chauhan (+91 99589 84581)
Senior Manager - Community Development:
Neelam Adhangale (+91 98331 68076)

Regional Sales Managers
North: Pratika Barua (+91 99995 10523)
West: Vaibhav Kumar (+91 97176 74460)
South: Brijesh Kumar Singh (+91 98454 15137)
Ad Co-ordination/Scheduling: Kishan Singh

PRODUCTION & LOGISTICS
Manager - Operations: Rakesh Upadhyay
Asst. Manager - Logistics: Vijay Menon
Executive - Logistics: Nilesh Shiravadekar
Senior Manager - Operations:
Mahendra Kumar Singh
Logistics: Mohd. Ansari

Head - Digital & Event Operations: Naveen Kumar
Head - Digital Operations: Atul Kumar Pandey

OFFICE ADDRESS
9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.) 121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published, Printed and Owned by 9.9 Group Pvt. Ltd. (Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.) Published and printed on their behalf by Vikas Gupta. Published at 121, Patparganj, Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091, India. Printed at Tara Art Printers Pvt Ltd., A-46-47, Sector-5, NOIDA (U.P.) 201301.

Editor: Vikas Gupta

9.9 GROUP

Understanding The Digital Age: Cybersecurity, Privacy, And Data Protection

The Data Protection Bill 2023 emphasizes cybersecurity, underscoring the need for organizations to incorporate this focus into their operations.

By Nisha Sharma

The digital age presents both opportunities and challenges in cybersecurity. As connectivity increases, so does the vulnerability of systems, data, and infrastructure. As we observe Cyber Security Awareness Month, it's essential to understand the integral role each individual and organization plays in bolstering cyber defenses. This article delves into insights from industry leaders, highlighting the path IT leaders should consider for a secure digital future.

The widespread impact of personal cybersecurity decisions

Visionet's Vice President & Head of Cloud & Infrastructure Delivery, Bijo Chacko, underscores the essence of this year's theme, 'Cyber Safety Starts With YOU.' He fluently remarks, "In this era of interconnectivity, our online choices shape our personal cybersecurity and have a ripple effect across the digital network, impacting the collective safety of the online world. Empowerment starts with awareness."

Chacko's statement brings to light the streaming effect individual actions have, reinforcing the idea that a single click or a secure password choice can be the difference between a secured and compromised system. His emphasis on simple but crucial practices, like cautious email handling and responsible online behavior, serve as a potent reminder for IT leaders about the importance of fostering a culture of cyber awareness.

Organizational resilience in an inter-connected era

The conversation shifts gears when looking at the broader organizational framework. Samir Kumar Mishra, Director of Security Business at Cisco for India & SAARC, talks about the readiness gap that businesses face today. "A Cisco study indicates that only 24% of organizations in India have the mature level of readiness needed to be resilient against today's modern cybersecurity risks," he states. While the figure is alarming, Mishra's words bring hope. He underscores Cisco's belief that security is, indeed, a collective responsibility. Cisco's vision champions the integration of cutting-edge technologies and expertise to construct resilient security architectures that empower individuals and protect organizations.

The hybrid world we operate in demands a comprehensive understanding of the network's nuances. Mishra rightly says, "If a device is connected, it needs to be protected." For IT leaders, this reiterates the importance of an all-encompassing approach, integrating both point tools and platforms to achieve resilience without complicating the security infrastructure.

Ripu Bajwa, Director and General Manager of Data Protection Solutions at Dell Technologies India, posits, "In this age of connectivity, where the internet has become an integral part of our daily existence, protecting our online privacy is paramount. As a country progressing rapidly towards a digital future, we need to respect and understand the significance of preserving the privacy and security of our personal data."

DPDP Bill 2023

With the introduction of the Data Protection Bill 2023 in India, the emphasis on cybersecurity has peaked, urging organizations and individuals to be more vigilant than ever.

Guardians of cyber trust

Mr. Joy Sekhri, Vice President, Cyber & Intelligence Solutions, South Asia, Mastercard, stresses the non-negotiable essence of cybersecurity and data privacy. He said, "Protecting sensitive information, both customer and internal, is not just a legal requirement but a fundamental trust-building measure." The risks of cyberattacks are multi-dimensional, spanning financial losses, reputational damage, and more. Sekhri emphasizes that protecting data is about maintaining the trust of stakeholders and ensuring the integrity and confidentiality of operations. On the preventative side, investments in encryption, multi-factor authentication, and regular security audits are indispensable. Collaborative approaches, staying abreast of threats, and adhering to industry standards remain pivotal.

On the verge of a cyber-resilient world

Venkatesh Subramaniam, Cybersecurity and Privacy Head at Mindsprint, drives that cybersecurity isn't just an IT issue—it's a brand differentiator and an enabler for businesses. He underlines the importance of adopting a security-by-design mindset in an age where AI, IoT, and Cloud drive innovations. Subramaniam praises the Data Protection Bill 2023, emphasizing that it symbolizes both an opportunity and a collective responsibility. "We must ensure frictionless security and promote cybersecurity education to empower our users."

Navigating the digital defense landscape

Madhusudan Krishnapuram, Vice President of Engineering and Managing Director, India at GoTo, emphasizes shared responsibility for cybersecurity. "It is imperative for businesses to prioritize cybersecurity awareness and invest in technologies such as Zero Trust Network Architecture." He believes in fostering a cybersecurity culture that starts with simplification, arming IT leaders with tools to navigate the intricate world of digital defense.

A clarion call to 'secure the world'

Aladdin Elston, Head – Information Security at Altimetrik, paints a stark picture of the growing cyber threats, with India witnessing an alarming rise in attacks. He sees the Data Protection Bill 2023 as a significant move towards shielding data. Yet, Elston emphasizes that the task isn't solely technological—it's a collective

The dual emphasis on data protection and recovery highlights the importance of having both defensive and responsive measures in place.

endeavor. "The formidable task of thwarting cyber threats can be overcome with a highly skilled team of cybersecurity professionals."

Towards a proactive cybersecurity stance

Balaji Rao, Area Vice President, India & SAARC, at Commvault, comprises the significance of Cyber Security Awareness Month. He speaks to the evolution of cyber threats and highlights the need for a proactive approach. "Enterprises must shift from a reactive to a proactive approach towards cybersecurity." Rao believes in the potential of new-age technologies like AI in early threat detection and emphasizes the value of automation in cybersecurity processes.

Data storage and recoverability

While privacy remains a cornerstone, the dialogue in cybersecurity is rapidly evolving, with an increasing emphasis on data storage and recovery. Mr. Sandeep Bhambure, Managing Director and Vice President for India & SAARC at Veeam Software, reminds us of the gravity of the situation, "Data breaches are not only a threat towards reputation, but attackers can also encrypt data, making it unrecoverable. Businesses should no longer think 'if we get hacked' but rather, 'when we get hacked, what is our recovery plan?'"

Veeam's recent report points to a rising trend in cybersecurity investments across the Asia Pacific. However, mere investment isn't the panacea. As Bhambure aptly points out, bridging communication gaps between IT and senior management, coupled with an emphasis on employee upskilling, is essential to fortifying cybersecurity strategies. Having a proactive business continuity plan, choosing the right backup solutions, and constantly evaluating new technologies will be pivotal in navigating potential cyber threats.

Conclusion

In assessing the perspectives provided by industry leaders, it's evident that the cybersecurity landscape in the digital age is multifaceted, requiring attention at both the individual and organizational levels. Individual actions in the digital space have cascading effects on broader systems, emphasizing the importance of personal cybersecurity awareness. Organizations, on the other hand, face a readiness gap, with many not adequately prepared for modern cyber threats. The introduction of the Data Protection Bill 2023 highlights the legislative emphasis on cybersecurity, but it's equally crucial for organizations to internalize this emphasis and integrate it into their operations. The dual focus on data protection and recovery underscores the importance of having both defensive and responsive measures in place. Collaboration, a shift from reactive to proactive strategies, and continuous education and upskilling are all integral components of a robust cybersecurity approach. The insights provided reaffirm that while technology plays a pivotal role in cybersecurity, the human element remains at the core of building a secure digital future. ■

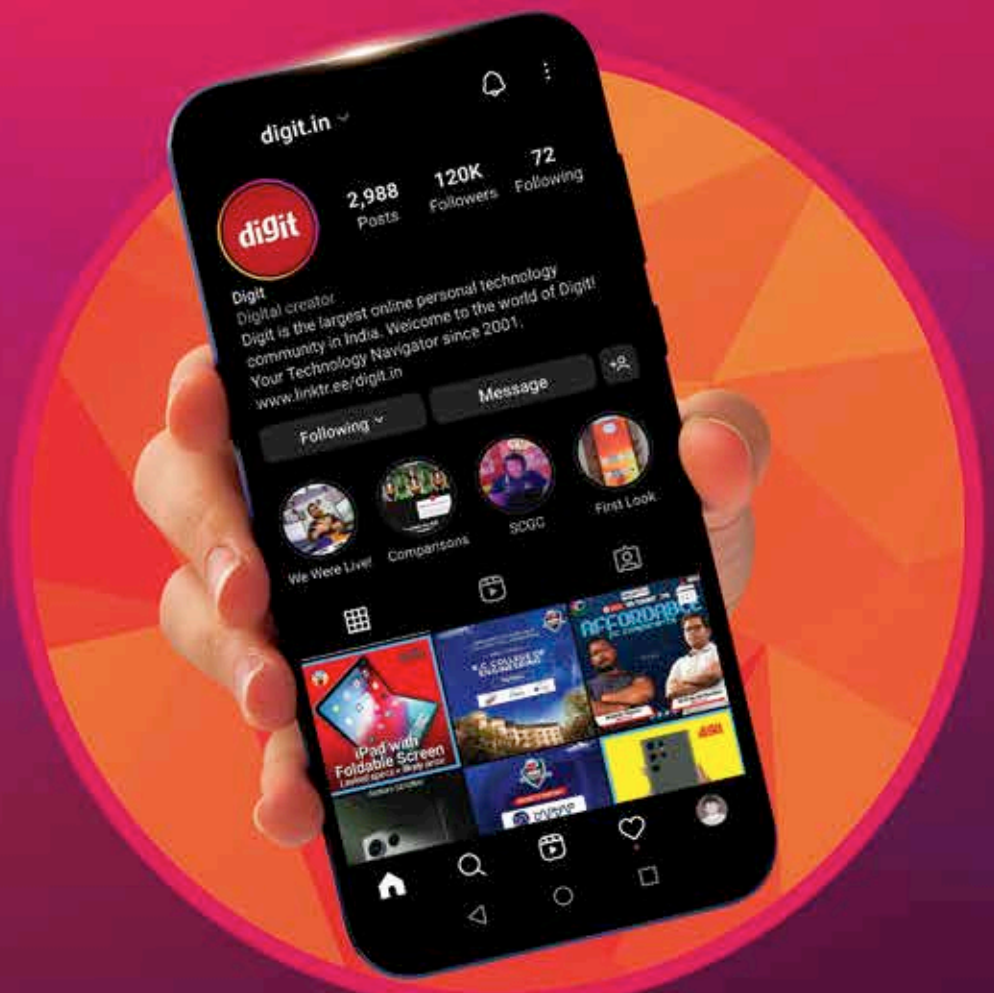
@DIGIT.IN

FOLLOW US ON

Instagram

FOR THE LATEST UPDATES IN TECH

digit.in



Trend: Generative AI ++

The IT Departments should stop selling themselves short and work with business functions to exploit this easy and economical tool.

By Akash Jain

We launched the Navigator MasterClass on Emerging Trends a couple of months back with a discussion on Generative AI (Gen-AI). It generated some discussion that was interesting; this author also talked on the subject with consulting clients, prospects, peers, friends and family. An interesting common perception emerged: "Gen-AI is all and only about text and image generation." ChatGPT and DALL-E created enough sensation to become the sole "spokespersons" for Gen-AI. This is akin to catching a tiger by its tail so we will look at the REAL business value of Gen-AI we will look at real-life use cases that are either already live or are WIP and what impact they have made on the core business.

Before looking at use cases, let us try to understand Gen-AI. If we were to look at traditional IT jargon, Gen-AI is Decision Tree, Recursive Loop, and Data Management on steroids, and then SOME MORE. The point being made is that there is potential for business applications.

In fact, Gen-AI is built around the concept of CREATIVITY; neurologically speaking, 'creativity' is the process of making connections that are not obvious and may even appear weird. The difference between human creativity and Gen-AI is that the latter is Explainable.

Two more points are worth noting before we look at the live examples. Firstly, Private datasets are the way to go; even if one uses public data (in addition to internally generated data), it should be brought (copied) into the private dataset. The negative stories of the NY Times Food Reporter's Thanksgiving Di.nner Menu or the Washington Post reporter being told of mankind's destruction methodology were based on public domain data. This data is full of errors, omissions, fraud, and bias, so the result will not be reliable for businesses.

Which brings us to the second key point. Gen-AI's full power is exploited alongside another technology that generates relevant and specific data. Let us now look at a few use cases.

GE Aviation started with the objective of reducing unplanned downtime for its jet engines. It installed IoT sensors on jet engines, and Gen-AI uses this data to predict the need for maintenance. This has allowed GE to schedule the maintenance activity proactively. GE Aviation has been able to reduce its unplanned downtime by 20%.

Maersk wanted to make its shipping operations more efficient. So, it created Digital Twins of its ships and supply chains. Gen-AI simulated the performance under different conditions, including weather, traffic, demand, etc. By predicting the problems before they occur, Maersk has improved its on-time delivery rate by 3%.

Nvidia used Gen-AI to power autonomous vehicles. Edge computing collects data from vehicle sensors like cameras, radar, light detection, ranging, etc. Gen-AI uses this data to make decisions about vehicle control, and the edge devices make these decisions in real-time, right at the spot they are to be implemented. Nvidia also uses Gen-AI in another unrelated application. It uses Gen-AI to train and deploy new AI models for spatial computing. Developers use its Omniverse platform to train and test new spatial computing models.

In 2024, despite challenges, the successful implementation of genAI will necessitate firms aligning their AI strategy with data and cloud strategies.

Magic Leap is another company using Gen-AI with spatial computing. By integrating these into its Augmented Reality platform, it is adding realistic 3D objects and environments for real experiences. This platform is still under development, though initial versions are already available and deployed for many uses, including spatial audio and a brush to draw across multiple devices from multiple locations.

Stratasys was searching for newer ways to manufacture aerospace parts. It uses Gen-AI algorithms to generate new aerospace parts designs (that are optimized for weight and strength). The designs are then sent to the Additive Manufacturing system for prototyping and manufacturing. The new parts are lighter, stronger and cost less.

These are just six of the dozens (if not hundreds) of real-life examples. All these beg the question: is simple text generation an underutilization of Gen-AI? Not really. This author is currently working on a purely text-based consulting assignment, which will be on a private dataset. This system will allow a team of just ten customer service executives to answer 150,000 questions on operating 1500 variations (brand, size, model, etc.) of all household appliances. It will ALSO allow an on-site service technician to learn about the installation or repair of these appliances, all in real-time. These technicians will mainly be in over 500 Tier 2, 3, and 4 cities nationwide. Just to give the readers a perspective, this company, Serviz, currently finds a service technician in these 500+ cities who knows the particular brand of the appliance to be serviced; the new system will make the service technician brand-neutral.

The conclusion from all these examples is that the IT Departments should stop selling themselves short and work with business functions to exploit this easy and economical tool. ■

THE YEAR OF AI REVOLUTION

NEXT100 leaders foresee AI seamlessly integrating into the fabric of enterprise ecosystems. Explore what's in store for tech deployments in the year ahead in our special edition.

Happy New Year, IT Leaders! As we bid farewell to 2023, we're stepping into a technological era dominated by advancements in AI, including Generative AI and the ever-evolving field of cybersecurity. This transition is especially critical for enterprises adapting to AI's expanding influence across manufacturing, BFSI, and automotive sectors.

In this special edition, we've invited Next100 winners to share their perspectives on the tech trends they foresee dominating in 2024. Their invaluable insights provide a glimpse into how technologies like Generative AI transform supply chains and manufacturing operational efficiencies, especially in areas like predictive maintenance and real-time decision-making.

Furthermore, this edition highlights the integration of AI, RPA, and Generative AI, which is forging powerful data processing and analysis platforms, thus enhancing business processes across various sectors. It also sheds light on the role of digital transformation, leveraging Generative AI and semantic models in industries like agriculture, leading to increased precision and efficiency. The dual role of AI in cybersecurity, as both a defensive tool and a potential threat, is also explored, emphasizing the need for predictive analysis and insider threat detection.

These articles delve into the transformative impact of AI in the BFSI sector, highlighting the role of intelligent processes in advanced fraud detection, customer service automation, and predictive analytics. Ethical AI and robust governance are also discussed to mitigate risks and ensure responsible AI use.

The influence of Gen AI in automotive manufacturing, leading to improved production outcomes, and the revolutionary changes brought about by AI and ML in IT operations, necessitating new data management and security strategies, are also key topics.

Lastly, the edition addresses the environmental challenges faced by cloud computing, underscoring the need for innovations in renewable energy and eco-friendly practices to achieve sustainable solutions.

We highly value your feedback and encourage you to share your thoughts. If you have any comments, suggestions, or feedback regarding the content or any aspect of IT Next, please feel free to reach out to the Executive Editor, IT Next, Jatinder Singh, at Jatinder.singh@9dot9.in or Principal Correspondent, Nisha Sharma, at nisha.sharma@9dot9.in. Your input is crucial for our continuous improvement and ensuring our content resonates with our readers. We appreciate your support and look forward to your thoughts and suggestions. ■

Generative AI In Smart Manufacturing

A change management strategy is essential to assure that AI-driven plans are successfully executed across the company.

By Gyan Prakash

In Smart Manufacturing, IT leaders are critical in driving supply chain optimization through Generative AI. Smart Manufacturing uses Generative AI to optimize supply chain processes, enhancing productivity and adaptability. Generative AI systems also optimize logistical routes, resulting in lower costs and faster delivery times by using dynamic capacity utilization integrated with capable to promise features to the sales team. Furthermore, generative AI systems can optimize logistical routes by considering variables like traffic, weather, and fuel economy, resulting in lower costs and faster delivery times. The following are some ways that generative AI might support supply chain optimization in the present smart manufacturing environment:

- **Demand forecasting:** Generative AI can produce more precise demand projections by analyzing

past demand data. By doing this, manufacturing organizations can minimize stockouts and reduce excess inventory by better matching their production plans and inventory levels with actual consumer demand.

- **Production planning and scheduling:** By taking into account a number of variables, including machine availability, resource limitations, and order priority, generative AI can help optimize production schedules. It can create schedules that optimize resource use, cut lead times, and minimize downtime.
- **Inventory management:** AI algorithms can produce prediction models considering lead times, demand variations, and seasonality. This enables businesses to keep their inventory levels at ideal levels, lowering carrying costs and guaranteeing product availability.
- **Supplier relationship management:** Generative AI has the potential to assist manufacturers in assessing and refining their supplier relationships. Based on past data and current information, it may negotiate contracts, evaluate supplier performance, and recommend adjustments to sourcing strategy.
- **Quality control:** AI may create algorithms that leverage IoT sensors and visual systems to monitor product quality continuously. Only high-quality products can pass through the supply chain by setting off warnings and remedial actions in response to any violations of quality criteria.
- **Predictive maintenance:** Manufacturing equipment predictive maintenance schedules can be produced by generative AI models. Anticipating when equipment requires servicing helps lower maintenance costs and unscheduled downtime.
- **ChatGPT for service & maintenance** – ChatGPT is a useful industry maintenance and service tool. Its natural language processing powers can help with various jobs, from giving advice and information to fixing technological problems. Ensuring data security, integrating it with pertinent systems, and regularly training and updating the model to adjust to particular industry requirements are all crucial. Additionally, technicians and shop-floor workers may find it simpler to communicate using ChatGPT efficiently if they use a well-designed user interface.

IDC forecasts that combined investments by manufacturers will account for 16.6% of $154 billion in 2023 global AI sales.

- **Supply chain network architecture:** Generative AI can optimize supply chain network architecture. This involves figuring out where distribution centers and warehouses should be located in relation to lead times, transportation costs, and demand trends.
- **Cost optimization:** Models for cost optimization that take into account a variety of cost elements, including production, transportation, and inventory carrying costs, can be developed using generative AI. These models can pinpoint supply chain management tactics that are economical.
- **Real-time decision:** Generative AI can produce real-time decision support tools that consider the dynamic conditions of the supply chain. This allows producers to make well-informed judgments at any moment.
- **Continuous improvement:** By evaluating previous performance data, producing insights, and proposing process improvements, generative AI can help find areas for continuous improvement.

IT leaders can use the following steps and methods to optimize the advantages of generative AI in smart manufacturing for efficient supply chains.

- **Recognize smart manufacturing principles:** IT professionals should be well-versed in integrating IoT devices, data analytics, AI/ML, and generative AI technology into the manufacturing process. Gaining this knowledge is essential to using generative AI efficiently.
- **Data strategy and integration:** Ensure that information is gathered, processed, and merged into a centralized data platform from various sources, such as IoT sensors, manufacturing systems, and ERP. Accessibility, security, and data quality are crucial. Data governance and ensuring that data is prepared for AI applications are the responsibilities of IT leaders.
- **Generative AI talent and skill development:** Assemble or appoint a group of people with machine learning and AI experience. It's crucial to train and upskill current employees in AI technology. IT directors should encourage an innovative and always learning culture within the company.
- **Choosing the best Generative AI tools:** Assess and choose generative AI platforms or tools based on what works best for your manufacturing processes. Consider elements like scalability, compatibility with current systems, and simplicity of integration.
- **Best use case identification organization:** Work closely with corporate executives to determine the precise applications of generative AI in supply chain optimization. Examples include demand forecasting, production scheduling, quality assurance, and inventory management. Sort use cases based on how much room they provide for improvement.

IT leaders may successfully use Generative AI to drive supply chain optimization in Smart Manufacturing, helping businesses in achieving increased productivity, lower costs, and increased competitiveness.

- **Proof of Concept (PoC) development:** Implement PoCs to illustrate the benefits of generative AI for the use cases that have been discovered. IT directors should supervise the development and execution of these proofs of concept, ensuring they complement the organization's strategic objectives.
- **Data modeling and training:** Manage the creation and instruction of generative AI models. Preprocessing data, feature engineering, choosing a model, and adjusting hyperparameters are all involved in this. Ensure the models can handle real-time data and are reliable, accurate, and robust.
- **Integration with current IT infrastructure:** Work with IT teams to synchronize generative AI models with current IT infrastructure, such as SCADA, MES, and ERP systems. Ensure seamless data transfer between these platforms and the AI models.
- **Security and compliance:** To address cybersecurity concerns and safeguard critical industrial data by putting strong security measures in place. It is imperative to adhere to industry norms and data privacy legislation.
- **Monitoring and maintenance:** Use monitoring tools to monitor how generative AI models perform in real-time. IT directors should supervise routine model upgrades, maintenance, and retraining to guarantee that the models remain valuable over time.
- **Change management:** Work on change management tactics to ensure the company is prepared to use AI-driven solutions. This could entail educating staff members, outlining the advantages of AI, and resolving any change-aversion.
- **Cooperation with stakeholders:** Encourage cooperation among supply chain managers, corporate executives, and other stakeholders. Ensure the company's strategic goals align with generative AI solutions.
- **Follow the agile principle:** IT executives ought to encourage a culture of innovation and constant development. Invite end users to provide input, then consider their ideas while optimizing.
- **Scalability:** Consider how scalable generative AI technologies will be. IT leaders should ensure that generative AI capabilities can adjust to shifting requirements and growing data volumes as smart manufacturing develops.

With the support of the aforementioned actions, IT leaders may successfully use Generative AI to drive supply chain optimization in the context of Smart Manufacturing, assisting the company in achieving increased productivity, lower costs, and increased competitiveness. They also need integration with current systems (like Manufacturing Execution Systems or Enterprise Resource Planning) and the know-how to create and manage AI models to apply generative AI in supply chain optimization for smart manufacturing. A change management strategy is also essential to guaranteeing that AI-driven plans are successfully implemented across the company. ■

Gyan Prakash is a Senior Consultant at Cognizant MLEU Consulting.

Unified Strategy For AI, RPA, And Generative AI Deployments

An RPA solution automates data handling and analysis, integrating AI/ML for predictive insights and content creation.

By Amit Bansal

With the latest technological advancements to solve large complex business problems, organizations are looking at building and deploying Intelligent Automation solutions packaged all in one to inherit capabilities of BPM, RPA, AI/ML, and GenAI to give them an enhanced CX experience.

A typical architecture designed toward these solutions is essentially encapsulated around these critical components:

- **Data processing layer:** This layer encompasses a range of tasks, such as gathering data from various sources in multiple formats, cleaning and normalizing the data, performing preliminary processing, and subsequently storing it in databases.
- **Cloud SaaS:** Cloud is the most common platform, which not only provides ease of storage and access to data but also provides enhanced security at an optimized cost.
- **Extraction models:** Various data analytic models are used for unstructured data.
- **AI/ML models:** These are advanced algorithms designed using deep learning algorithms to generate business insights by bringing in predictive and prescriptive analytics.
- **GenAI model layer:** This generates new content using advanced LLM models, providing on-the-fly solutions for business problems.
- **Integration layer:** All the different solutions are integrated through an integrated solution (like MuleSoft, Informatica, etc.), depending upon the enterprise tech stack spread.

Take a typical business use case – the end client shares data in different formats. An RPA solution is deployed to not only collate/validate data, extract and transform it into a consumable for-

mat, but also to apply data analytics to generate meaningful insights through predictive AI/ML models along with enabling GenAI using LLM models to generate content for ready usage.

A thoughtful deployment strategy revolves around the following:

- Data injection by the client and posted on cloud/client-server. It has files in different formats, which have plain text as well as handwritten images.
- A gateway is required to connect the client and your ecosystem.
- UI is created to bring about an enhanced UI/UX experience.

There is a typical need to manage different work items and assign them to the team to ensure timely action to help with the same:

- Data is ingested into a UI (BPM workflow) tool to manage workflow effectively.
- RPA is used to extract, move, and compare data across multiple systems.

A database schema is designed for storing:

- Structured data directly fed from client systems.
- Unstructured data can be converted into a structured format using various text processing algorithms, such as AWS Textract.

For seamless exchange of information across systems, APIs are leveraged.

- The output of this data is consumed through APIs and streamed into queue systems (CI/CD) [or] AWS Queue (if you are using AWS as an underlying cloud solution)
- Parallelly, data is stored in a data lake (e.g., AWS S3 bucket).
- Likewise, ChatGPT is used as a GenAI platform for building customized solutions and helping solve different business use cases.
- These are being pushed into the Application queue, and downstream automation can post the validated data to UI for client consumption.
- Secure Shell (SSH) connection is established for deployment from one environment to another. At times, private/public keys are used to create secure connections.
- Varied Integration solutions provide seamless integration of various applications to make it a coherent solution.

Below is a sample of deployment steps:

Setting up front-end:
The Front-end web interface is designed using Python libraries to create interactive web applications with minimal code to help with easy integration:

- By calling the RPA code package.
- Using AI/ML models.
- Generative AI service-based application.

Deployment automation:
The entire deployment of the application can be automated using Terraform, an infrastructure as a code tool

RPA package creation:

- The package is created with the designed RPA bots.
- Queues are established.
- DB schema is developed along with folder creation
- Orchestrator is set up to capture Transaction count, SMTP server, TMHP portal, and credentials.

Setup code repositories:

- AWS Codecommit hosts the private GIT repositories.
- Use the code-commit repo link and encryption parameters are set up for HTTPS.
- The AWS Code pipeline automatically deploys code from the AWS Repository into the EC2 instance.

Setup CI/CD pipeline:
Use this CI/CD pipeline moving forward and execute the below steps:

- Establish Python dependencies by running install_dependencies.sh, followed by the configuration of files.
- Private and Public SSL keys are generated along with SSL ciphers to enhance the security of the SSH channel.
- The server starts, and the CI/CD pipeline pushes an update restart_ service command.

Optimizing data structures:
Repeated read requests from DB to AI/ML model can be avoided using in-memory data structures [Redis (Remote Dictionary Server), compatible with multi-threading].

Backup setup:
Daily backups occur inside the Amazon Sagemaker notebook via 'cron,' using "crontab -e," which automatically opens the "vi" editor.

Generative AI solution deployment:

- Configure parameters in a .tf file, which can be used by Terraform script to create necessary AWS resources.
- Amazon Bedrock and ECS Faregate cloud services are used to deploy the GenAI solution.
- Initialize the Terraform plan through the terminal and deploy the application.
- The idea is to have a secured environment with encryption enabled so that all the systems can synchronize through an integrated platform from data injection with RPA to extraction, implementing data analytics through AI/ML coupled with GenAI content generation deployed on the cloud with a seamless automated deployment pipeline. ■

The author is a Sr. AVP with EXL is driving Digital Transformation initiatives for Fortune 500 clients through GenAI, AI/ML & HyperAutomation solutions.

Digital Transformation With Generative AI And Semantic Models

More than 90% of the data generated in the manufacturing processes is enormous and largely unstructured.

By Ajay Malgaonkar

"Today, technology allows farmers to create more with fewer resources," the CEO of John Deere, a global agri-solutions manufacturing company, said in CES 2023 Keynote.

Since 2019, the organization has been building solutions that use technology like computer vision and advanced sensing, machine learning, and data analytics, embracing smart industrial strategy based on Industry 4.0 to drive the transformation journey.

One of the ways that John Deere helps the farmers with technology solutions is through its Operations Center platf orm. This platform provides farmers with access to data and insights from their equipment, which can help them make better

decisions about their operations. A "See & Spray" innovation exemplifies the successful collaboration of technology, enterprise, and consumers. See & Spray is a precision spraying technology that uses cameras, computer vision, and machine learning to identify weeds and only spray them, leaving crops unharmed. This can help farmers reduce their herbicide use by up to 77% and save millions of gallons of water usage.

This is not the only example of innovative use of the latest technology trends. Many organizations, particularly in manufacturing, are putting severe efforts into embracing new technologies to benefit end consumers.

Many of these use cases, which were never thought possible before, are becoming a reality due to accelerated technological development and affordability.

The transformation model

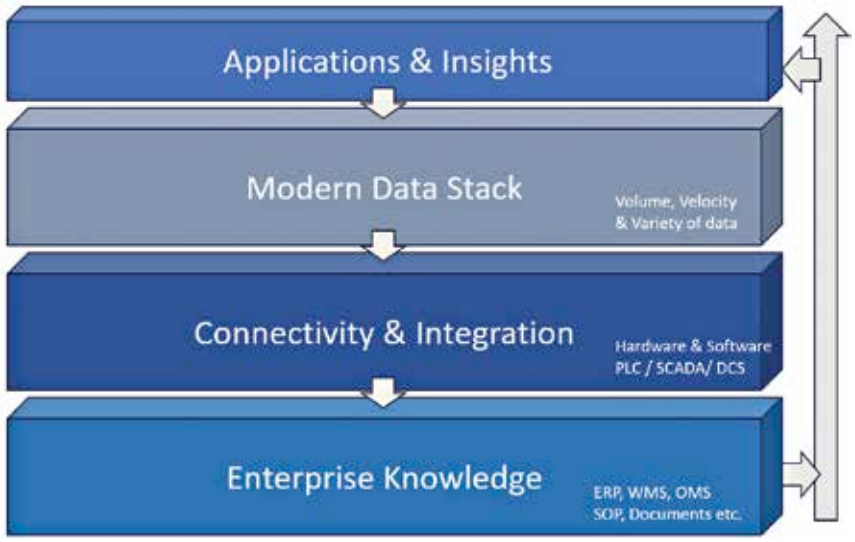
The applications and insights drive the top layer to generate autonomy for consumers. The top layer relies heavily on the enterprise data housed in a modern data stack, which could be in any form: structured, unstructured, historical, real-time, etc.

The third layer forms the connectivity between the enterprise's various hardware, machinery, equipment, sensors, processes, and software and harnesses the enormous data generated by multiple functions in the modern data stack.

The foundation layer is the enterprise knowledge generated from ERP software, warehouse management, order fulfillment, consumer usage & behaviors, and differentiation created through standard operating procedures, best manufacturing practices, quality control processes, and various documents.

The gap (Information Technology + Operational Technology)

While enterprises strive to digitalize and automate every aspect of shop-floor entities, operational technology is undergoing a huge transformation.



At every step, the real-time data emitted by the sensors and processes can generate crucial insights to boost productivity. More than 90% of the data generated in the manufacturing processes is enormous and largely unstructured.

Over the last few decades, enterprises have matured in digitalizing business applications through information technology.

However, there is a strong need in the market to bring information technology and operational technologies together to generate better insights.

Enters Generative AI

A recent manifestation of generative AI by chatGPT, Bard, Dall-E, etc., has triggered the 'Art of Possible' in generating insights from unstructured data. With the help of large language models (LLMs), enterprises can harness the knowledge layer to form critical business decisions. Through summarization, Q&A, findability, etc., enterprises can augment their expertise with the help of machines.

Retrieval-Augmented Generation

Retrieval-augmented generation (RAG) is a technique in natural lan-

guage processing (NLP) that combines the strengths of retrieval-based models and generative models to improve the quality and relevance of generated text.

Retrieval-based models find relevant information from large datasets, while generative models are good at creating new text. RAG uses a retrieval-based model to find relevant information from a dataset. This information is then used as input to a generative model, which creates new text based on the retrieved information.

RAG is effective for various NLP tasks, including question-answering, summarization, and machine translation. For example, in question answering, RAG can generate more comprehensive and informative answers by providing the generative model with access to relevant information within the enterprise or from the web.

The use case

Imagine a troubleshooting scenario for an injection molding machine that otherwise requires a company expert to visit the site and diagnose.

What if the expert is not available at the time? How about a support engineer taking the help of generative AI and carrying out the following steps:

- Uses Computer Vision to identify the machine's 'make' and 'model'.
- Accesses the product catalog and retrieves the troubleshooting manual.
- Follows the steps suggested by the app to carry out inspection and diagnosis.
- Uses troubleshooting videos retrieved from the knowledge database using the AR/VR tool on the site.
- Accesses service history and known error database to arrive at concise root causes to fix the issue.

This is just a sample; the use cases of generative AI would be numerous and vary from industry to industry. We have just started scratching the surface of this new innovative tool, which is still graduating.

Bring method to madness!

Every enterprise has realized the potential of generative AI. Technology is more than just hype since it makes everyone think differently about the same problems not solved earlier by using contemporary technologies.

When traditional AI (Predictive AI) started gaining a foothold in enterprises, it was highly limited to the IT department and Data Analytics within IT. The Enterprise Data Management group defined the AI strategy, created the common infrastructure, and generated data lakes to harness and deploy AI models for usage. The applications largely depended on the structured data, which was in the custody of data analytics units and required to be governed to avoid redundancies.

Generative AI has pierced every aspect of the enterprise, not only data management teams but also app development, integration, DevOps, customer experience, infrastructure units and CRM, Customer Support, Marketing, etc., in the hands of business. This means every unit is bubbling with innovative ideas to apply generative AI for their respective use cases and participate in the transformation journey. The results will be tangible and directly impact the business outcomes; hence, everyone is queuing up.

Very shortly, this will lead to a chaotic situation if not handled with maturity. While the generative AI matures, enterprises are still experimenting with different proprietary and open-source GPTs, unaware of which to use. Redundancy in creating data products and fetching unstructured information, which is pre-validated, are some of the challenges surfacing.

There is paramount pressure on IT departments to be hyper-agile and build governance models with design patterns, reusability, and service discovery capabilities … all within the gamut of uncompromised information security within and outside and the ease of provisioning. The euphoria and parallelism in building the products to bridge this gap is taking its toll on the enterprise software products & platform providers as no single tool or platform can satisfy every enterprise's aspirations.

Enterprise strategy to build Gen AI platform

There is no magic wand that will solve the challenges in this space. However, the good news is technology is fast evolving towards maturity.

Enterprises need the following capabilities in their enterprise AI platforms:

- Model repository & configuration management
- Automation in Model training/ retraining and deployment
- Model observability for drift
- Model Security and explainability/ audibility
- Composable apps/ services
- Workflow / Chaining

The top-tier players in this space have complemented their Gen AI platforms with most of the capabilities listed above. Bedrock from Amazon, WatsonX from IBM, Microsoft Fabric, and OpenAI service on Azure and Google Vertex AI are some of the key platforms to help build and manage generative AI apps at the enterprise level. Frameworks like Langchain are gaining popularity as they aid in building templatized AI applications.

Enterprises must embrace the fundamental principles of digital product engineering-

- Solve business problems with a productized approach.
- Build solutions like digital products that can be extended beyond the current use case, within and outside the organization.
- The solution must be built using scalable, modular, cloud-native, microservices-based, event-driven architecture and serverless capabilities.
- The architecture must support multi-tenancy.
- Follow agile methodology equipped with DevOps/ CICD and Automated testing for scaling purposes.

The challenges of generative AI and how to overcome

The concept is very fresh and constantly evolving. It's no surprise to know its caveats.

- **Hallucination** – occasionally, the model may throw irrelevant or even synthetic responses that appear true but not.
- **Generic/ Bookish knowledge** – The insights generated from a large but finite data set that is generic.
- **No Guard Rails** – Enterprise wants to apply guard rails with respect to who accesses what information, what to dispose of, and what not to.
- **Does not understand the context** – Generative AI works on largely unstructured data, which lacks context. The next thing the enterprise would be looking for is how to narrow down the response with concise knowledge provided through context.

The RRR of the New Frontier

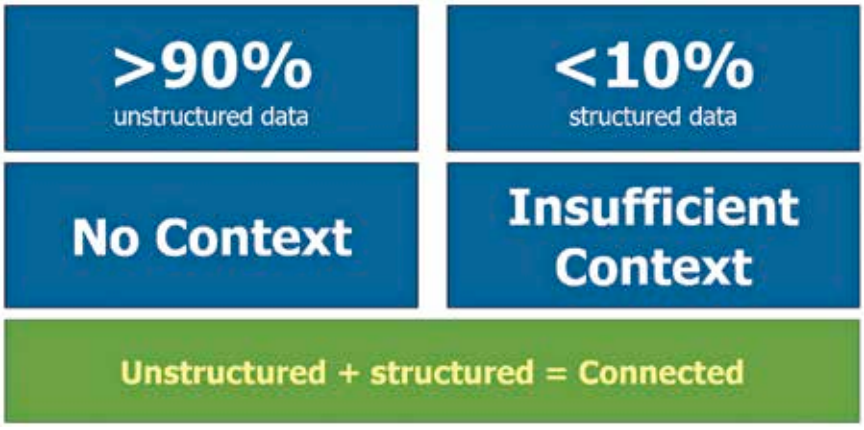
As enterprises mature in experimenting and implementing generative AI solutions, there are 3 R's that every enterprise would benefit from

- **Relevance** – The new solution architectures will combine the structured data with insights generated from unstructured data to be fed to generative AI models for "relevant" output rather than generic.
- **Reasoning** – Most use cases around unstructured knowledge are to understand the entities and concepts, their attributes, and the complex relationships amongst them. The semantic model, which would help build the complex network of each entity's relevance in the enterprise, will lead to understanding the "Reasoning" of certain events, defects, faults, failures, results, and achievements and help take corrective actions before they occur.
- **Recommendation** – Once the enterprise brings the unstructured and structured data together, the new frontiers will build the AI models using machine learning to forecast the following link in the relationship, whether structured or unstructured, and generate fairly accurate recommendations.

Importance of Semantic models

Using generative AI for insights from unstructured data will be like looking for a needle in a haystack. Enterprises must start building semantic models for their business and data.

The next crucial step is to converge generative AI-driven insights from unstructured data with the structured relationship between business entities and enterprise data.



Relevant structured data will provide the much-needed "context" to the problem statement and allow the enterprise to generate intelligent insights through in-context learning.

The ultimate path will lead to a unified analytics platform using LLMs and Semantic Models to achieve hyper-personalization. ■

Ajay Malgaonkar is a Next100 2023 awardee and heads the engineering for Prolifics.

Artificial Intelligence's Role And Strategy In Cybersecurity

AI unique abilities help security professionals to stay one step ahead of cybercriminals by automating tasks, analyzing massive datasets, and making real-time decisions.

By Bhabani Chatterjee

In the age of digital transformation, where data is the lifeblood of businesses and individuals alike, the importance of cybersecurity cannot be overstated. The ever-evolving threat landscape demands innovative approaches to safeguarding digital assets. Now, they are also turning to it to shore up their defenses against the crime that inevitably follows. We wanted to learn more about how they are doing this and, more importantly, how they can do it better.

Artificial Intelligence (AI) has emerged as a powerful ally in the fight against cyber threats, offering the promise of enhanced defense strategies and proactive threat mitigation. This article explores the pivotal role AI plays in cybersecurity and outlines key strategies for its implementation.

The power of AI in cybersecurity

Artificial Intelligence has revolutionized the way we approach cybersecurity. Its unique capabilities empower security professionals to stay one step ahead of attackers by automating tasks, analyzing massive datasets, and making real-time decisions.

Here are some of the key ways AI enhances cybersecurity:

Threat detection

AI-powered systems excel at identifying and recognizing patterns that may indicate a cyber threat. They can swiftly detect anomalies, unusual

behavior, and potential vulnerabilities across a network.

Behavioral analysis

AI algorithms can analyze user and network behavior to establish baselines and detect deviations promptly. This helps identify insider threats and advanced persistent threats (APTs).

Predictive analytics

AI's ability to analyze historical data and predict future threats is a game-changer. It enables organizations to defend against potential cyberattacks and vulnerabilities proactively.

Automated response

AI can not only detect threats but also respond to them in real-time. Automated incident response can isolate compromised systems, stop malicious processes, and mitigate the impact of an attack.

Security training

AI-driven tools can simulate cyberattacks and provide security teams with hands-on training, helping them prepare for evolving threats.

At Capgemini, through our comprehensive analysis of various AI use cases in cybersecurity spanning across many domains, several significant findings have come to light:

A heightened necessity for AI in cybersecurity: Most organizations have recognized the need to reinforce their cybersecurity measures by incorporating AI. Nearly two-thirds of these entities now believe that identifying critical threats without the assistance of AI is an increasingly challenging task.

Accelerated adoption of AI in cybersecurity: The pace of AI integration into cybersecurity is rising. Approximately three-quarters of organizations are actively exploring and experimenting with AI in various cybersecurity use cases, reflecting a growing momentum in its adoption.

Strong business justification for AI: An overwhelming three out of five organizations have established a robust business case for implementing AI in their cybersecurity strategies. They have observed that the utilization of AI significantly enhances the accuracy and efficiency of cyber analysts, underscoring the tangible benefits derived from AI integration in this context. Numerous companies have already incorporated AI into their cybersecurity efforts or have imminent plans to do so. To achieve optimal results, they should develop a strategic roadmap for AI integration within the cybersecurity domain. This entails tasks such as pinpointing essential data sources and establishing robust data platforms to effectively leverage AI, selecting the most pertinent use cases to expedite and optimize advantages, fostering external collaborations to bolster threat intelligence, implementing security orchestration, automation, and response (SOAR) mechanisms to enhance security management, providing training for cyber analysts to work with AI proficiently, and instituting governance protocols for AI in cybersecurity to ensure sustained enhancements over the long term.

Approximately three-quarters of enterprises are actively exploring and experimenting with AI in various cybersecurity use cases, reflecting a growing momentum in its adoption.

Strategies for AI implementation in cybersecurity

To harness the full potential of AI in cybersecurity, organizations must adopt comprehensive strategies that align with their security goals. Here are some key strategies:

Data collection and analysis

Gather and store extensive data from various sources, including logs, network traffic, and user behavior. AI systems require robust datasets for training and continuous improvement.

Machine learning models

Develop machine learning models to analyze the data and recognize patterns, anomalies, and threats. Con-

tinuous model training and fine-tuning are crucial for optimal performance.

User and Entity Behavior Analytics (UEBA)

UEBA systems leverage AI to analyze the behavior of users and entities. Implementing UEBA can help identify insider threats and compromised accounts.

Threat intelligence integration

Integrate threat intelligence feeds with AI systems to update them with the latest threats and attack techniques.

Automation and orchestration

Use AI for automating repetitive tasks and orchestrating incident response. This speeds up reaction time and reduces human error.

Collaboration and information sharing

Encourage collaboration among security professionals and organizations. Sharing information about emerging threats and vulnerabilities is critical in a connected world.

Continuous monitoring and assessment

AI should be continuously monitoring the network and systems for new threats. Regular security assessments and audits ensure the AI systems are effective and aligned with the organization's evolving needs.

Challenges and ethical considerations

AI possesses the potential to reshape the landscape of cybersecurity, yet it also ushers in a host of challenges and ethical considerations. These include concerns related to privacy, the potential for biases within AI models, and the crucial necessity for human oversight.

The discourse concerning the ethical ramifications of incorporating AI into business processes is legitimate and paramount. We have all experienced AI's advantages and unforeseen consequences in our daily lives. Contemplating the utilization of this formidable technology in safeguarding personal and corporate data naturally gives rise to contemplation.

Organizations processing AI-driven strategies can better safeguard their digital assets in an increasingly complex and interconnected cyber landscape.

Nonetheless, cybersecurity is a clear and compelling case for AI's widespread and accelerated adoption, extending its reach to encompass enterprises and their Security Operations Centers (SOCs). The rationale is strikingly evident: malevolent actors are devoid of ethical restraint, harnessing AI to conceive and launch innovative attacks. In the absence of AI-driven defenses, their intrusions become significantly more potent. This paper delves into why companies must embrace AI as their primary defense and why such adoption is ethical and morally imperative.

The defining capability AI furnishes cybercriminals with is speed. It empowers them to inflict more significant harm in shorter durations and swiftly adapt to evolving security responses by applying machine intelligence to their operations. Conversely, AI equips security teams with the swiftness required to counter and outperform these attackers. By harnessing AI and automation, SOCs can expand to cope with the escalating volume, complexity, and diversity of AI-based cyberattacks.

AI empowers computers to acquire, analyze, and disseminate information at a pace far surpassing human security analysts. Consequently, AI enhances the efficiency of SOCs by reducing manual analysis, streamlining evidence collection, and correlating threat intelligence, resulting in quicker, more consistent, and more precise responses.

Conclusion

AI has become an indispensable tool in the realm of cybersecurity. Its capacity to analyze vast amounts of data, predict threats, and automate responses offers a formidable defense against the ever-evolving cyber threat landscape. Also, Artificial intelligence (AI) is no longer a futuristic concept but a crucial component of modern cybersecurity. Real-world examples and case studies demonstrate how AI enhances threat detection, automates responses, and improves security.

Organizations implementing AI-driven strategies can better safeguard their digital assets in an increasingly complex and interconnected cyber landscape. While the benefits are evident, it's important to address ethical considerations, such as privacy and bias, to ensure AI's responsible and effective use in cybersecurity. Organizations can bolster their cybersecurity posture by implementing AI strategies and staying vigilant, safeguarding their digital assets in an increasingly interconnected world. However, it's essential to address AI's ethical and operational challenges, ensuring that it serves as a responsible and effective guardian of digital security. ■

Bhabani Chatterjee is a NEXT100 winner and engagement leader at Capgemini.

AI & Its Implications On Information Security

While AI has the potential to enhance security measures through threat detection, anomaly identification, and rapid response, it simultaneously presents new challenges.

By Samrat Bhatt

Artificial intelligence, often abbreviated as AI, represents the forefront of technology's quest to replicate human-like thinking in machines. It aims to imbue computers and systems with the capacity to perform tasks that we commonly associate with humans, like intelligence and decision-making.

AI, the 'X' factor behind security researchers and attackers, will pave a unique future for InfoSec researchers/practitioners and malicious actors. The cyber threat landscape is expected to be significantly impacted by the proliferation of AI. While AI has the potential to enhance security measures through threat detection, anomaly identification, and rapid response, it simultaneously presents new challenges. AI is a weapon; would it be used to guard or rob us depending on who's using it, a security professional or an attacker?

Cybercriminals are increasingly leveraging AI to create sophisticated and evasive attacks. These AI-driven threats can autonomously adapt, discover vulnerabilities, and exploit them unprecedentedly.

As a result, the battle between AI-driven security and AI-driven cyber threats is poised to intensify, ushering in an era of constant technological evolution and vigilance in the cybersecurity domain.

Let's focus on some of the top potential tactics that attackers may employ in 2024 utilizing AI; it is essential to note that cybersecurity professionals and organizations are actively working to counter these threats. Here are some scenarios to consider:

- **AI-enhanced attack automation:** Attackers can leverage AI to automate various stages of attacks, from reconnaissance and vulnerability scanning to exploitation. AI-driven bots can continuously scan the internet for vulnerable targets and launch attacks autonomously, significantly increasing the scale and frequency of attacks.
- **Advanced phishing and social engineering:** AI-powered spear phishing attacks become more sophisticated and convincing. Attackers can create highly personalized messages and mimic trusted contacts or authority figures, making it challenging for targets to discern the deception.
- **AI-generated malware:** Malware authors may use AI to generate polymorphic malware that constantly changes its code to evade traditional signature-based antivirus solutions. AI can also be employed to improve the delivery and execution of malware, making it more effective and challenging to detect.
- **Deepfake impersonations:** Attackers could create deepfake audio and video content to impersonate key figures or executives within organizations. Such deepfakes could be used in social engineering attacks, insider threats, or extortion attempts.
- **AI-powered reconnaissance:** AI can be employed for more efficient surveillance. Attackers may use AI to mine open-source intelligence, social media, and publicly available data to gather information about potential targets and identify vulnerabilities.
- **Exploiting AI-based security tools:** Attackers may target AI-based security solutions, attempting to deceive or bypass them. For instance, they could use adversarial attacks to fool AI-driven anomaly detection systems.
- **AI for evasion and camouflage:** AI can help attackers evade detection by identifying security patterns and finding weaknesses in security measures. Attackers can use AI to camouflage their malicious activities as legitimate traffic or behaviors.
- **Quantum computing threats:** While not AI-specific, attackers may exploit emerging quantum computing capabilities to crack existing encryption methods and undermine data security.

AI can be a powerful tool for attackers and defenders, but proactive defense and threat detection can help mitigate the risks associated with the changing cyberthreat landscape. AI will be pivotal in enhancing security measures and combating emerging threats. Here are some scenarios to consider:

- **Advanced threat detection and response:** AI-driven security solutions will provide real-time threat detection and response. Machine learning algorithms will continuously analyze network traffic, identifying and mitigating anomalies and threats more effectively than traditional methods.
- **AI-powered security analytics:** Security analysts will rely on AI-driven analytics to rapidly process vast amounts of data. This will help identify patterns and anomalies, enabling proactive threat hunting and faster incident response.
- **Autonomous security systems:** Security systems will become more autonomous with AI. They will automatically respond to threats, isolate compromised systems, and initiate recovery procedures, reducing the required response time and human intervention.
- **Threat prediction and prevention:** AI will be used for predictive analysis, enabling security professionals to anticipate potential threats and vulnerabilities. By analyzing historical data and emerging trends, AI can help organizations bolster their defenses before attacks occur.
- **AI for insider threat detection:** AI will assist in identifying insider threats by analyzing employee behavior and identifying unusual patterns. This will help in detecting malicious or inadvertent insider activities.
- **Quantum-safe cryptography:** As the advent of quantum computing threatens current encryption methods, AI will aid in the development and implementation of quantum-safe cryptography to protect sensitive data.
- **AI-enhanced phishing detection:** AI-powered solutions will provide more robust protection against attacks. They can analyze email content, sender behavior, and other factors to identify phishing attempts more accurately.
- **Advanced access control:** AI will improve access control systems, providing more dynamic and adaptive authorization based on user behavior and context, enhancing security while maintaining user experience.

Artificial Intelligence (AI) represents a transformative force in information processing, enabling the unprecedented handling of vast data sets. Yet, this power also can magnify the spread of misinformation when not adequately controlled. The solution lies in harnessing AI's capabilities to counter its vulnerabilities. As our reliance on AI deepens, it is paramount to grasp the intricacies of misinformation dissemination, employ AI-driven strategies to combat it effectively, and uphold transparency and human-centric values in applying this influential technology. In this ever-evolving landscape, adapting our approaches to tackle misinformation is essential, ensuring responsible AI usage and fostering a trusted digital environment. ■

Samrat Bhatt is a Sr. Director of Information Security at MatchMove India.

Navigating Cybersecurity: Challenges & Strategies For 2024's Landscape

Cyberattacks are becoming more sophisticated and adaptive, demanding a proactive and dynamic approach to security.

By Kamal Sharma

As the digital environment advances rapidly, cybersecurity is a pivotal element of global information security. Entering 2024, the intricacies and challenges in safeguarding digital assets for individuals, corporations, and governments are scaling new heights. This article aims to explore critical cybersecurity challenges anticipated in 2024, examining their implications and dissecting effective strategies for mitigating these risks.

Cybersecurity challenges in 2024

AI-powered attacks: In 2024, we can anticipate a surge in AI-powered cyberattacks. Cybercriminals are increasingly leveraging artificial intelligence and machine learning to enhance the sophistication of their attacks. These AI-driven attacks can adapt and evolve in real-time, making them formidable adversaries for traditional security measures.

Ransomware escalation: Ransomware attacks will continue to be a significant concern in 2024. What's particularly alarming is the shift towards double-extortion attacks. Cybercriminals not only encrypt victim data but also threaten to release sensitive information, creating a potent weapon for extortion.

Supply chain vulnerabilities: With the globalization of supply chains, businesses are increasingly interconnected, creating opportunities for malicious actors to exploit vulnerabilities. In 2024, we expect more attacks targeting supply chains to disrupt operations and compromise security.

IoT vulnerabilities: The proliferation of Internet of Things (IoT) devices is a double-edged sword. While they bring convenience, they also introduce new vulnerabilities. Unsecured IoT devices are an attractive entry point for cybercriminals, creating potential gateways into larger systems.

Quantum computing threats: Quantum computing, although not fully matured, threatens current encryption methods. As quantum computing capabilities advance, traditional encryption algorithms may become obsolete, necessitating a shift to quantum-resistant encryption.

Through a precise understanding of these evolving threats and adopting strategic defenses, stakeholders can strengthen their cybersecurity posture in an increasingly interconnected world.

Effective strategies for the evolving landscape

Adopting zero-trust architecture: Zero Trust is a security model that assumes no one, whether inside or outside an organization, can be trusted. This approach verifies every user and device, ensuring only authorized entities can access sensitive data or systems. In 2024, implementing a zero-trust architecture will become crucial.

AI and machine learning for defense: Just as cybercriminals utilize AI for offense, organizations can harness the power of artificial intelligence and machine learning for defense. These technologies can detect anomalies, predict threats, and respond to attacks in real-time.

Ransomware resilience: Organizations must develop comprehensive ransomware resilience plans. Regularly backup data, educate employees about phishing and social engineering tactics, and have incident response strategies in place. It's essential to be prepared for a ransomware attack and reduce the likelihood of paying a ransom.

Third-party risk management: To address supply chain vulnerabilities, robust third-party risk management is essential. Assess and continuously monitor the security posture of your suppliers and partners. Require them to meet specific security standards and employ secure practices.

IoT security best practices: Implement strict security measures for IoT devices, including strong authentication, encryption, and regular software updates. Ensure that IoT devices are isolated from critical networks to contain potential breaches.

Preparing for quantum computing: While quantum-resistant encryption is still in development, organizations should prepare for the eventual adoption of quantum computing by staying informed about advancements in post-quantum cryptography and planning to transition to more secure encryption methods.

Conclusion

As we enter 2024, the cybersecurity landscape continues to evolve, presenting new and complex challenges. Cyberattacks are becoming more sophisticated and adaptive, demanding a proactive and dynamic approach to security. By adopting these effective strategies and staying ahead of emerging threats, individuals, businesses, and governments can navigate the digital frontier and protect their assets in the face of ever-present cyber threats. In this dynamic environment, preparedness and adaptability are the keys to a secure future. ■

Kamal Sharma is a GM IT at Encore ARC Pvt Ltd.

Importance Of Digital Certificate Management & Cyber Hygiene

The future of security is passwordless authentication only for the majority of the IT Enterprise landscape.

By Nitan Gulati

As the enterprise IT landscape has emerged in hybrid and distributed models across the globe, managing digital certificates across the cloud, firewalls, and applications, be it internal or external; data centers have become increasingly complex. Manual certificate processes and legacy management are further intensifying the problem, resulting in frequent application outages and increased vulnerabilities that, in turn, impact the security scorecard of an organization and disrupt CIA triads.

With an industry experience of more than two decades, I can say aloud and request leaders to avoid fundamental pitfalls that often hamper organizations from achieving the level of digital trust required to safeguard sensitive information and maintain a secure, hygienic environment. Few of them noticeably are-

- Digital certificates are managed within spreadsheets and notepads.

-Say a big No to the manual process.
- The same certificate and key are used across multiple use cases. – If a single key is compromised, it can provide unauthorized access to multiple systems, causing a high risk of security breach.
- No certificate expiry notifications – This can result in unexpected outages more than we realize.
- Critical storage practices are poor – The tendency for most of us to place private keys in insecure locations causes potential unauthorized access. Robust key storage locations such as FIPS 140-2 Compliant HSM should be practiced.

Ninety days of SSL/TLS Validity is coming our way…?

The number of Digital certificates that were there during the last two decades versus today's fast-growing technology world has skyrocketed & since then, we have witnessed the life span of certificates trend shrinking from 7 years to 5 years followed by three years and literally one year now & most likely in times to come it might be just 90 days only (it's not a typo error, smiles) if Certification Authority Browser (CA/B) Forum proposal passes. However, this trend makes it harder for attackers to exploit fraudulent certificates. Still, the cost of operational and service downtime and recent incidents involving industry biggies have highlighted the significance of managing digital certificates in an automated way, which guardians of secure digital communications often overlook; these incidents raise the red alarm that no entity, regardless of whatever annual turnover it may have is immune to consequences of expired certificates.

Pay attention to NIST – it's time to focus on visibility!

In 2020, the National Institute of Standards and Technology (NIST) published Special Publication 1800-16: Securing Web Transactions, TLS Server Certificate Management; this framework emphasizes that organizations need to carry out fundamental certificate life cycle management tasks, such as

- Finding flaws in cryptographic methods or software libraries.
- Identifying expiring certificates and replacing them.
- A single central inventory is recommended, as it minimizes the possibility of overlooking critical TLS server certificates.

A single central inventory is recommended, as it minimizes the possibility of overlooking critical TLS server certificates.

Using the power of automation in Handling Certificates makes IT professionals better

The need to issue, renew, and revoke certificates makes automated Certificate Life cycle management (CLM) necessary. Modern CLM tools are essentials nowadays, and in times to come, they will be a must-to-have rather than a good-to-have from a budgeting forecast perspective and with apparent reasons for enabling the IT workforce to put their expertise on elsewhere productive things like business process automation, etc., rather than spending massive time on manual processes. Accepting automation can feel like a leap of faith for a few organizations, but as certificate numbers continue to grow, the risks associated with manual work will become evident.

Cyber security hygiene and etiquette are in our genes – No choice moving forward

We all have witnessed an increase in numerous outages, service downtime, and exfiltration happening majorly across all different industries and sectors during the last few years, and I would not talk about various IT tools, be it SIEM, PAM, ZTNA, MDR, EDR, XDR, etc. which is of-course essential depending on business information sensitivity; however, fundamentally, it is our right to follow simple benchmark guidelines & should adhere to security etiquettes in our genes such as hardening systems, zero trust, conditional access, having only required licensed software, permitting only OEM recommended browsers which should have auto-update enabled, turning windows firewall to always ON, be it on any endpoints or servers, encrypting devices, allowing only role-based access control with just in time access / denying privilege account to login on odd-hours. Bring in two-tier access control and strict no domain admin eco system, no internet on servers unless recommended. Let us embrace this as it would provide sound sleep for techies guys.

Interestingly, the future of security is passwordless authentication only for the majority of the IT Enterprise landscape (Millennials would love not to use the traditional approach of complex passwords) and enforcing Data classification at whatever channels we can, thereby protecting and safeguarding humongous tera bytes from exfiltration; this would reduce attack surface & will maintain CIA triads.

Let us confidently navigate and browse the online world and keep customers happy and secure. Signing off as of now and continue to excel in automation and keep things around us safe, digitally or otherwise. ■

Nitan Gulati is an Associate Director at Evalueserve.com Pvt Ltd.

Use Cases Of AI In BFSI

The continuous advancement of AI in BFSI promises to enhance the customer experience further, improve decision-making, and fortify security measures.

By Kunal Thakur

Artificial Intelligence has become a hot topic in boardroom discussions for strategy building. AI in Digital transformation is not just an innovation but a disruption that has redefined how financial institutions operate, interact with customers, and manage their resources. If you look at the use cases nowadays, AI is not just a tool but a strategic imperative enabling organizations to stay competitive.

Leveraging AI for data analysis in finance and fraud detection

There is a massive amount of data generated by financial institutions through their internal process and customer interactions. AI can use this vast data. There are multiple cases where this is used currently.

AI is used for fraud detection, which helps prevent scams by identifying potentially fraudulent activities in real-time. The software evaluates the pat-

tern of the regular transaction using a Debit/Credit card or UPI of the person on timings, usage, and payment to vendors. It uses this data to identify any unusual pattern compared to the previous one. Any unusual pattern generates the added confirmation sent to the person for verifying the transaction even before it happens. Also, these patterns can be fed manually and evaluated by AI logic.

Robo Advisory and Predictive Analytics

Robo Advisory and Predictive Analytics for Investments can be done using AI. During my recent discussion with the Senior leadership of an Indian bank, this was the major ask by them on Robo Advisory to be part of their wealth management platform for their customers. It analyses market data, news, and economic indicators to predict stock prices, asset allocation, and investment strategies. This can be beneficial for both individual and institutional investors. The Robo Advisory feature is a significant known ask by the BFSI industry to their WMS software provider in the market.

Sentiment analysis for investment decisions

Sentiment analysis is another used case of AI. AI can analyze social media, news, and other external data sources to gauge public sentiment and market trends, helping in investment decisions.

Enhancing call center quality with AI

The quality evaluation of the bank call center can be done through sentiment analysis of the customer care call center calls. From my earlier experience, real-time evaluation of a bank's customer care calls can be done by evaluating the verbiage used by the customer. It can give you data to showcase if the Agent could make the call from negative to positive. Now, you do not need manual random listening of calls to do quality checks for the customer care center. You can use AI to suggest Agents live on how to handle the situation with customers on call.

The synergy between AI and BFSI is not just a trend but a transformational journey that will shape the financial landscape for years to come.

Customer service automation for enhanced security

Nowadays, Chatbots used for handling customer queries are AI-enabled, which helps to get the queries answered at the first level at the Chatbot level instead of manual intervention.

Voice and Speech recognition is another used case for customer identity and verification to enhance user experience in call centers and mobile apps. To make the interaction more secure, it should not just be data shared by the caller to verify but to check the caller's identity.

The future of AI in the BFSI sector

The world of banking and financial institutions is evolving, and India is leading it from the top and showing the way of digitalization. Integration of Artificial Intelligence in the BFSI sector represents a pivotal moment in the industry's evolution. AI has brought efficiency and automation and redefined how financial institutions interact with customers, manage risks, and stay compliant with evolving regulations. As we look to the future, the continued advancement of AI in BFSI promises to enhance the customer experience further, improve decision-making, and fortify security measures. The synergy between AI and BFSI is not just a trend but a transformational journey that will shape the financial landscape for years to come. This journey is marked by innovation, adaptability, and an unwavering commitment to meeting the evolving needs of customers and the industry. ■

Kunal Thakur is a Next100 winner and Senior Vice President at Winsoft Technologies India Pvt Ltd.

Where Is AI Heading In 2024?

The journey to a responsible and ethical AI future is marked by two foundational factors – robust governance structures and cultivating an ethical mindset.

By Vidhi Chugh

2023 saw the rise of Large Language Models (LLMs); however, it did not take the industry long to realize that we hurriedly made such powerful models accessible to the public without implementing robust and adequate safeguards. Nevertheless, we have learned our lesson, and now is the time to make it right.

2023 will be the year of Generative-AI (GenAI), and 2024 will be the year of its GOVERNANCE.

Regulations are making their way!

Let us draw inspiration from the EU AI Act, the most comprehensive approach to AI regulation thus far. The Act underscores the importance of categorizing AI applications according to their risk profiles and enforces stricter measures commensurate with their potential impact, mitigating severe consequences.

The global consortium, comprising academic researchers, leading technology companies, and policymakers, increasingly emphasizes the need for robust governance of large models to ensure their responsible adoption. The foundation model developers have

also started demonstrating accountability for their models. It is evident by Microsoft's recent announcement to protect customers from legal repercussions stemming from copyright infringement related to their products.

Governance finds Its roots in ethics

As an AI Ethicist, one of the biggest challenges I often face is aligning everyone on the definition of ethics. Frequently, questions arise such as, "Whose ethical principles, whose code of moral conduct, ethical according to which standards?"

The recent technological developments in the form of GenAI systems place even higher equity in enforcing ethical AI.

As the law becomes enforceable, it prompts a fundamental question: How can we guarantee that AI systems are built in a responsible and trustworthy manner, working for the greater good of society? This concern extends beyond just the organizations utilizing LLMs or the developers of foundational models; it encompasses all of us, including the users of these systems.

The actual test lies in whether we would uphold the highest standards of responsibility and ethics, even in the absence of legal oversight. What actions and choices would we make when no one monitors or enforces compliance?

The rise of AI Governance

As we ponder these questions, the underlying theme of AI governance starts to surface. Let us define it first. AI governance includes all things ethics, regulations, and policies. It places a significant responsibility on the policymakers and regulators.

As the use of AI technologies becomes increasingly ubiquitous, the challenge lies in fostering innovation while upholding ethical considerations.

I have outlined five crucial components to balance innovation with governance:

- Having interoperable global regulations that transcend borders is vital for creating a shared foundation for evaluation and oversight.
- Ensuring industry-specific regulations are in place is equally important to address the unique risks associated with different sectors and domains.
- Building an independent audit committee responsible for assessing the ethical implications of AI systems is a critical step. This committee can provide unbiased evaluations and recommendations.
- Establishing ethics review boards within organizations should assess potential biases, discrimination, privacy violations, and other ethical concerns, not just during the ideation phase but also throughout the development and deployment process.
- Recognizing that risks in AI manifest in diverse ways, no single entity can foresee and manage them comprehensively. Therefore, all stakeholders in the AI governance ecosystem, including regulators, developers, data scientists, and decision-makers, should stay updated to understand the evolving implications of complex AI systems and make timely amendments.

Such collaboration brings a diversity of perspectives that creates a robust governance framework. It helps address the challenge of "unknown unknowns," where authorities may not even be aware of what they don't know, making it challenging to design comprehensive guardrails.

Awareness

The formal processes and systems take time to develop and come to life; meanwhile, it is crucial to foster awareness and promote an ethical mindset.

It requires a thorough understanding of the technical aspects of what it means for a system to be fair and unbiased. This includes grasping the technical underpinnings of machine learning algorithms and how they can introduce bias.

Ensuring future developers are well-versed in techniques to detect and mitigate bias in AI systems.

The art of asking the right questions, overcoming impostor and self-doubt. Encourage developers to ask questions such as, "How can I explain the internal workings of an algorithm to foster trust in its decision-making process?" and "How can I codify ethical expectations in the AI system?"

Conducting ethical and responsible AI awareness sessions, which include discussions about the social and ethical implications of AI technology. Providing real-world case studies and practical examples that illustrate the impact of AI on society helps developers understand the consequences of their work.

Encouraging diversity and inclusion in AI development teams, as they bring a more comprehensive range of perspectives and are more likely to identify and address potential biases.

To summarize, the journey to a responsible and ethical AI future is marked by two foundational factors – robust governance structures and cultivating an ethical mindset. While formal processes are underway, let us demonstrate accountability to ensure that AI-developed systems bring benefits to society and humanity at large. ■

Vidhi Chugh is an AI expert, recognized as a top innovator, and founded "All About Scale" for AI governance.

Artificial Intelligence (AI) In The Automotive Manufacturing Industry

Traditionally, the manufacturing sector is slow to adopt new technologies but is now realizing AI's potential and has started adopting it and integrating it with their processes gradually.

By Anup Awasthi

The new era of technological advancement is here, and the technology that is making it possible is Artificial Intelligence (AI), which has the potential to change every field and industry in the coming years. Artificial Intelligence (AI) has already touched all of us in one way or another, whether it's Google Maps, Spotify, or Alexa. Although AI as a technology has been in the works for decades, it has been in recent years that it has started to make its impact felt in every industry. This has been possible only because of technological advancements in computational powers and the designing of new machine-learning platforms.

AI has enormous potential to transform every industry by automating repetitive learning and discovery through data. Instead of just automating manual tasks, AI performs

frequent, high-volume, computerized tasks. And it does so constantly, reliably, and without any sort of fatigue. AI adds intelligence to existing products by getting the most out of data. This holds true for the automotive manufacturing industry also. Although automation has been a part of the Automotive Industry for decades with AI, it is different works based on data, machine learning, and algorithms that help produce the desired outcomes.

Artificial intelligence (AI) holds the promise of revolutionizing the manufacturing process in several key ways, bringing in a new era of efficiency and innovation on factory floors. Traditionally, the manufacturing sector is slow to adopt new technologies but is now realizing the immense potential of AI and has started adopting it and integrating it with their processes gradually.

Automotive Industry has traditionally been labor-intensive, with the manufacturing of hundreds of various parts consisting of different materials, shapes, and sizes.

AI can drastically improve overall efficiency and produce superior results by employing a mix of robotics, human-machine interactions, and quality assurance parameters. This would affect the working of entire production and Assembly lines in the Automotive Manufacturing industry.

Use cases of AI in the Automotive Manufacturing Industry

1. Automation of manufacturing process

Collaborative robots work in conjunction with humans in the shared assembly space. Robots can easily handle manual, labor-intensive tasks like welding, painting, and component assembly with great speed, precision, and safety. These robots can also identify defects and irregularities in materials and components used for production and raise alerts if necessary.

2) Enhanced quality control

AI systems closely and continuously inspect and analyze finished products and identify defects with pinpoint accuracy. This ensures the production of only high-quality products while reducing the risk of faulty items reaching customers. By focusing on data rather than complex AI systems, manufacturers can enhance their operations significantly. AI can continuously monitor data from factory operations, enabling real-time analysis and early detection of anomalies and patterns that might be imperceptible to human operators.

AI systems have transformed data into operable entities by assigning intelligent attributes; the algorithm can undertake data segmentation and establish patterns from the derived data sets.

3) Maintenance predictions

AI's ability to monitor equipment and machinery through Data Analysis can predict equipment failures and maintenance requirements well in advance, reducing downtime.

4) Warehouse sorting & management

The addition of robots in the warehouse has enabled them to automate a considerable part of the logistics network where these machines can track, lift, and sort items. It is instrumental in reducing costs and improving quality control, besides maintaining traceability.

5) Fleet monitoring system

AI can collect and compile complex data from various sources to figure out patterns not possible by ordinary human beings to automate and enhance the decision-making process regarding fleet management.

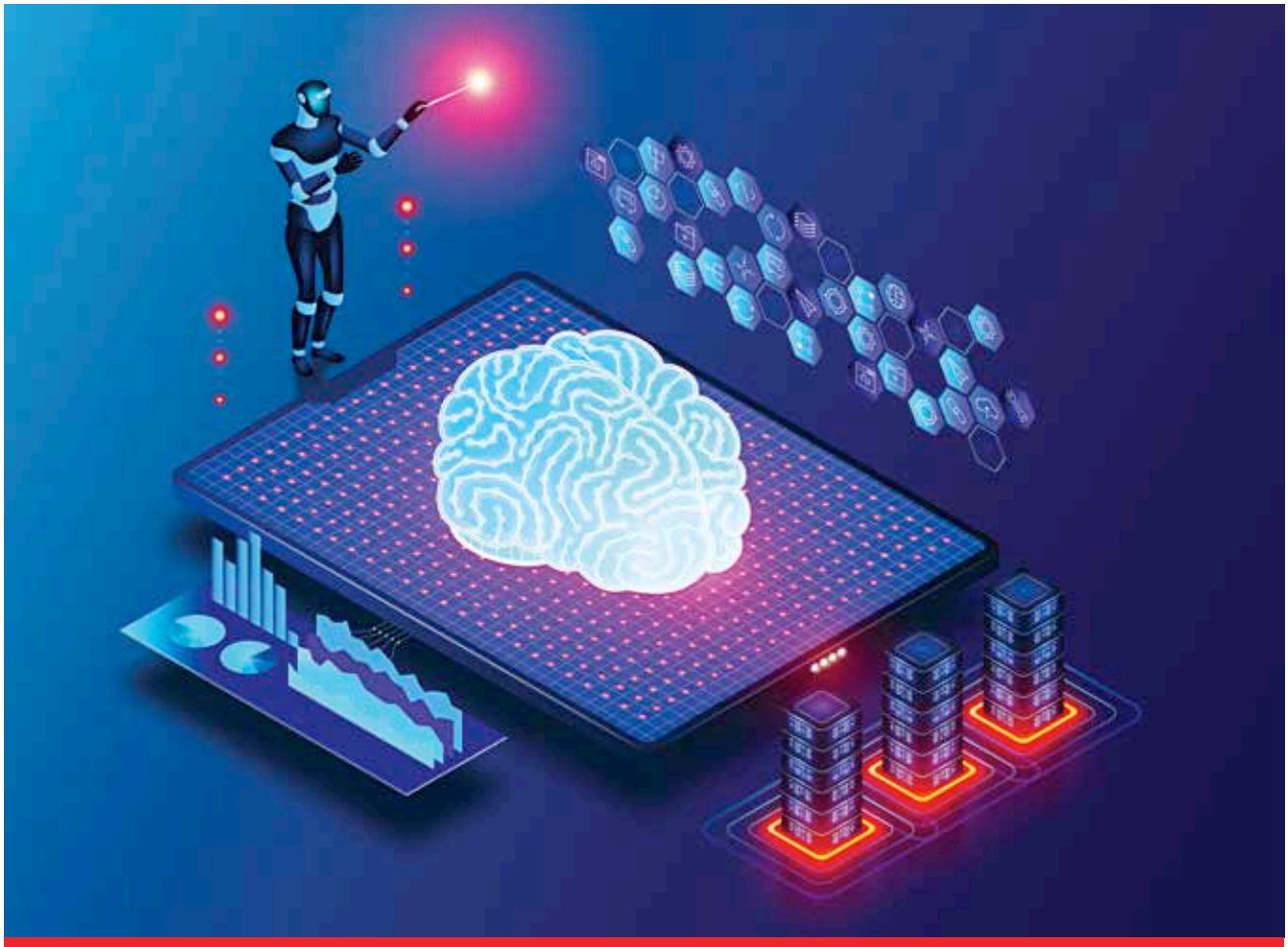
6) Shop floor monitoring system through AI-based video analytics

AI-based video analytics has many more use cases beyond just building surveillance and security purposes. In fact, with new integrated computer vision, surveillance systems, along with AI, can take smart and immediate actions, making the shop floor a much more safer place for the technicians and workforce. For this, AI systems have transformed data into operable entities by assigning intelligent attributes; the algorithm can undertake data segmentation and establish patterns from the derived data sets. These systems use real-time feed and historical data to understand ideal behavior and violations and, in case of any variations, can raise an immediate alert, thereby drastically reducing any chances of accidents or mis-happenings on the shop floor or in the entire assembly lines.

In conclusion, artificial intelligence is reshaping manufacturing by improving the overall design processes, automating labor-intensive tasks, predicting maintenance needs, ensuring product quality, and warehouse management, among others.

Artificial Intelligence has come as a blessing for multiple industries, including the automotive industry, and the way it is evolving and transforming the manufacturing landscape, it can be safely implied that it is no longer optional for the Manufacturing Industry to adopt it, but they are forced to do so, for their own survival. ■

The author is AVP (IT) at Imperial Auto Industries Ltd., leads key IT projects, including SAP S4 Hana and cloud-based solutions.



AIOps: A New Horizon In IT Operations

With the high number of false positives, prioritizing alerts is time-consuming and increases the chances that engineers miss the real alerts.

By Nitesh Sharma

In the ever-evolving world of technology, staying ahead of the curve has become more critical than ever. Today, businesses, irrespective of their size or industry, are racing to embrace the transformative power of Artificial Intelligence (AI) and Machine Learning (ML) in their IT operations. Hence, AI and ML are not just buzzwords anymore; they're the fuel driving the next wave of innovation toward building NextGen IT operations, also referred to as "AIOps." It has the potential to revolutionize the way organizations manage their IT infrastructure, delivering greater efficiency, agility, and cost-effectiveness, and address some critical challenges like:

1. **Managing large datasets of events/alerts:** IT ops are overwhelmed with the flood of data and alerts due to more complex IT environments with disparate data sources (e.g., Infrastructure Log data, ITSM tools, inventory tools, etc.). With the high number of false positives, prioritizing alerts is time-consuming and increases the chances that engineers miss the real alerts.
2. **Provide faster response with reduced downtime:** SLA requirements for IT are increasing before, 96%, then 99.5%, and due to digital transformation imperatives, now users demand 100% availability. Need for predictive maintenance, to monitor in real-time, and any anomalies are flagged before they lead to costly breakdowns.
3. **Align with Agile working methods:** DevOps adoption drives faster release cycles, increasing pressure on ops teams to continually operate and support new releases.
4. **Increasing Security Risks:** Cyber threats are rising, and traditional security measures are insufficient. Need to be able to detect even the most subtle anomalies in network traffic or user behavior, enabling rapid response to potential security breaches.

Get started in the AIOps journey

Embedding AI and ML into IT operations is a complex plug-and-play affair. It involves several key components:

Identifying foundational AIOps use cases: The starting step for any organization in the AIOps journey is identifying core use cases. It's essential to differentiate AIOps from chatbot monitoring tools and focus on use cases that analyze operations data and telemetry to improve IT service delivery and operations. They can be categorized into three:

- **Eyes on Glass** – Enhanced transparency to IT landscape
- **Provide Deep Insights** – Transparency translated into actionable root cause analysis.
- **Proactive Action** – Deep understanding translated into the automated response.

Selecting AIOps tools: Most monitoring tools, like Datadog, Device42, PagerDuty, Big Panda, etc., have built-in features and functionalities like anomaly detection, event correlation, or noise reduction. For enabling AIOps capability, features beyond monitoring, like intelligent remediation capability and integration with other ITSM tools like CMDB, Incident Management, DevOps, etc., are necessary. Strategy and architecture teams are crucial in selecting the right tool for the organization.

Data Management: The foundation of AI and ML is data. Quality data collection, storage, and integration are essential. Without a solid data strategy, the potential of AI and ML remains untapped.

Runbook Automation: Automation processes should be designed, integrated, and tested meticulously to ensure they function as intended and do not disrupt critical operations.

Start of the journey and not the end: Establishing continuous improvement feedback loops to capture and implement improvements is crucial. AI and ML systems should learn and adapt as the IT environment changes.

Challenges and Considerations

Despite the tremendous potential of AI and ML in IT operations, there are challenges and considerations to address before you get started:

Data Security and Privacy: Safeguarding sensitive data and ensuring compliance with data privacy regulations are paramount.

Talent and Skills: The need for more AI and ML expertise can be a hurdle. Organizations must invest in training or consider outsourcing.

Change Management: Employees need to adapt to the new AI-driven environment. Change management strategies are critical to secure a smooth transition.

Ethical Concerns: Algorithmic bias, transparency, and accountability must be addressed to ensure responsible AI and ML use.

Define and measure the agreed Value / Outcomes

To gauge the effectiveness of AI and ML integration, define key performance indicators (KPIs). These might include metrics like mean time to resolution (MTTR), uptime, and cost savings. A few examples are:

- Enable Self Service by end users with knowledge-backed self-services and an intuitive Product Service Catalog that reduces the demand on IT staff.
- Improve operational efficiency by X%

1. AI improves efficiency by reducing tickets and identifying opportunities for process improvements.
2. Noise reduction helps shift newly available capacity to proactive event management.

- Reduce downtime by ~X%

1. Reduce Incident volume by using event patterns to predict problems and intervene before downtime.
2. Resolve incidents faster by starting resolution actions earlier, being more efficient.

Conclusion

Accelerating toward AIOps transformation is necessary for organizations to have reliable and secure Digital Products and Services. Achieving this operational maturity requires upskilling people, redesigning processes, and embedding new technology tools. Organizations ahead in the journey will undoubtedly be the ones to lead the way and help businesses maximize returns on their Digital investments. ■

Nitesh Sharma is a NEXT100 winner and CTO / Head of IT Advisory at ISSC.

Cloud Computing's Role In Environmental Sustainability

Exploring sustainable solutions is crucial as the demand for cloud services rises, along with its environmental challenges.

By Logesh R

In the digital age, cloud computing has revolutionized data management, offering businesses and individuals an efficient infrastructure for innovation and data handling. The convergence of technology, from manufacturing to software development and the automobile industry, along with the burgeoning startup ecosystem, has led to an unprecedented surge in data generation. However, alongside the transformative capabilities of cloud computing arises a pressing concern: the ecological footprint of data centers and cloud infrastructure. As the demand for cloud services continues to surge, it is imperative to explore the environmental challenges and, more critically, the innovative and sustainable solutions that can mitigate them.

The environmental challenge

The environmental challenges cloud computing poses predominantly hinge on energy consumption, e-waste management, and the necessity of elaborate cooling systems. Data centers, the linchpin of cloud computing, demand prodigious energy resources for uninterrupted operation, predominantly derived from non-renewable

sources, contributing significantly to carbon emissions. Additionally, the fast-paced obsolescence of hardware components leads to copious electronic waste, necessitating precise recycling and disposal procedures. Inefficient cooling mechanisms only compound the environmental burden imposed by data centers.

Sustainable solutions-paving the way to a greener cloud

To counter these challenges, the cloud computing industry is actively engaged in the pursuit of sustainable solutions driven by cutting-edge technologies:

Renewable energy utilization and energy efficiency

The transition to renewable energy sources is pivotal in curtailing the environmental impact of cloud computing. Major cloud service providers like Amazon, Google, Microsoft, and Oracle have heavily invested in wind, solar, and hydroelectric power, marking significant strides toward sustainable cloud infrastructure. This commitment is complemented by the design of energy efficient data centers, prioritizing energy efficiency through inventive cooling methodologies, server virtualization, and optimized hardware utilization to curtail energy wastage.

Edge computing-enhanced data processing efficiency

Edge computing, a paradigm that processes data at its source, significantly reduces the energy demand associated with long-distance data transmission while diminishing latency. This augments real-time data processing capabilities, not only minimizing energy consumption but also elevating data processing agility. Edge computing has gained traction in many sectors.

Sustainable hardware practices and eco-friendly design

Eco-friendly hardware design is gaining prominence among cloud providers. This entails the production of robust and recyclable equipment, extending the lifecycle of data center components. The dual advantage of curbing electronic waste and conserving resources is an instrumental step towards ecological sustainability.

Rise of containerization adoption

Adopting containerization solutions such as Docker and Kubernetes have gained wide traction within the cloud computing industry. These technologies, equipped with auto-scaling functions, enable dynamic server capacity adjustments in response to demand fluctuations, eliminating the necessity for over-provisioned servers that excessively consume power and cost. Also, this technology had the advantages of application availability and fault tolerance compared to traditional Virtualization architecture.

Artificial Intelligence and machine learning

Artificial intelligence and machine learning technologies are indispensable in orchestrating sustainable solutions within the cloud computing realm. These intelligent systems optimize resource allocation, forecast energy consumption patterns, and automate data center management, efficaciously curtailing energy wastage while elevating environmental sustainability.

Innovation in action-putting "Cloud" into the "Ocean"

A striking illustration of innovation driving environmental sustainability is epitomized by Microsoft's Project Natick, which pioneers the submergence of data centers underwater, harnessing the natural cooling properties of the ocean. This pioneering approach substantially mitigates the energy requirements associated with conventional cooling systems. Notably, several other cloud industry leaders are following suit, experimenting with submerged data centers as part of their pursuit of sustainable and eco-friendly operations. Companies such as Google and Facebook have undertaken similar ventures, exploring the possibilities of underwater data centers across diverse geographical locations.

Transition to green computing data centers

As we advance toward a more sustainable future, the cloud computing industry is realigning its focus toward green computing data centers. These data centers are meticulously engineered with environmental considerations at the forefront, emphasizing energy efficiency, renewable energy sources, and eco-friendly hardware. The adoption of green computing approaches endeavors to reduce the ecological footprint of data centers while upholding the same high caliber cloud services.

Conclusion- a greener cloud on the horizon

Cloud computing has redefined data management paradigms, furnishing unparalleled convenience and operational efficiency. As we embrace innovative and sustainable solutions and transition to green computing data centers, the cloud computing sector spearheads the transition toward a more sustainable and ecologically responsible future. In this ever-evolving digital landscape, the future of cloud computing promises a greener, more sustainable world. Through the collective efforts of industry leaders and pioneering projects such as submerged data centers, we are progressively attaining a cloud infrastructure that not only caters to our technological exigencies but also champions our planet's well-being. ■

The author is an Assistant Vice President at Cloud Infra Architect

डिजिट
अब हिंदी में

देश का सबसे लोकप्रिय और विश्वसनीय टेक्नोलॉजी वेबसाइट डिजिट अब हिंदी में उपलब्ध हैं। नयी हिंदी वेबसाइट आपको टेक्नोलॉजी से जुड़े हर छोटी बड़ी घटनाओ से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यु से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओ में उपलब्ध होगा।

digit.in
NOW IN HINDI

www.digit.in/hi
www.facebook.com/digithindi

डिजिट

To follow the latest in tech,
follow us on...

facebook.com/digitgeek

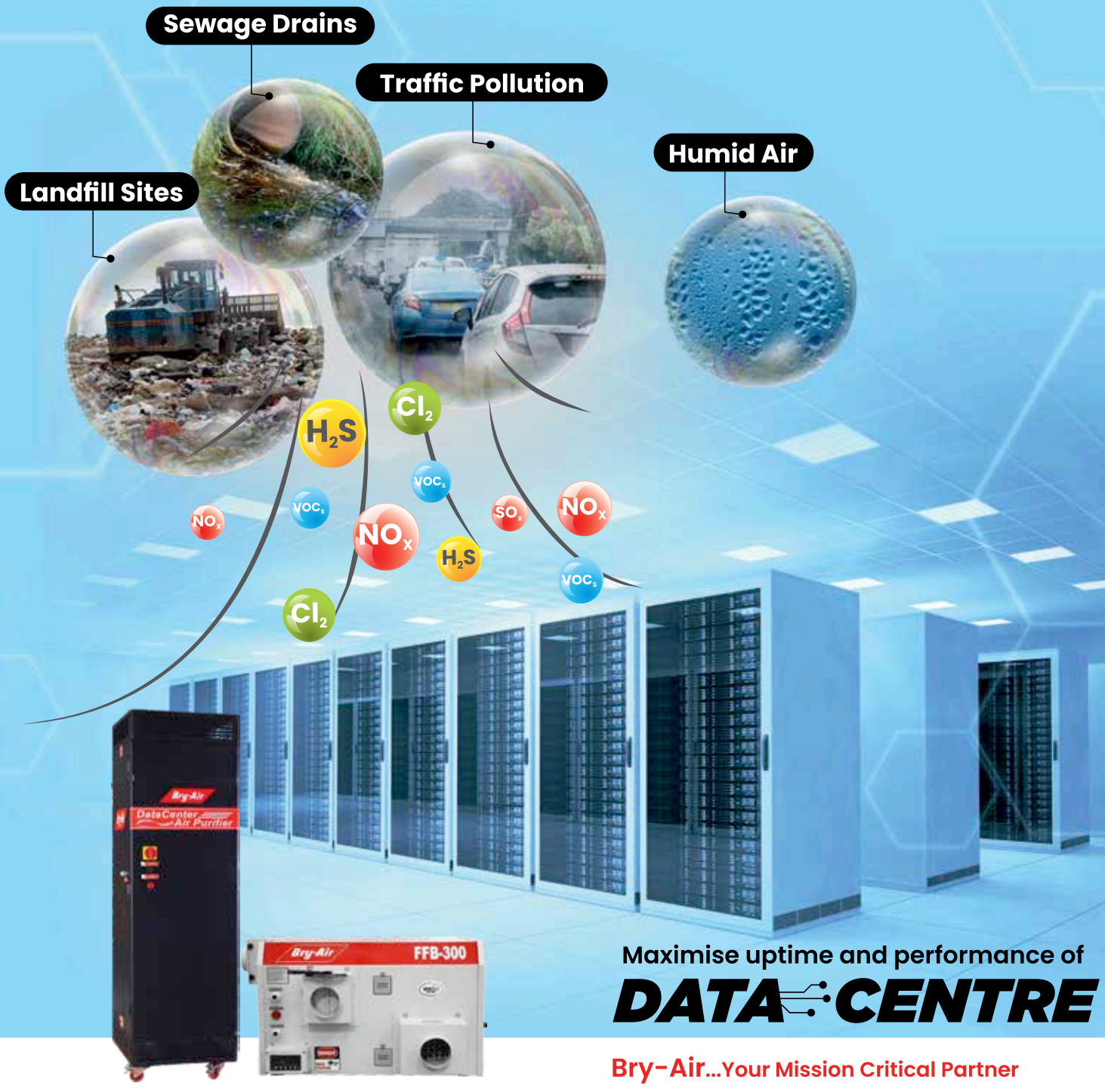
digit.in/facebook

PAHWA GROUP
Innovation is life

DELENG/2010/33560

Bry-Air®

Bry-Air solutions help neutralise corrosive gases and control moisture



Maximise uptime and performance of DATA CENTRE

Bry-Air...Your Mission Critical Partner

BRY-AIR (ASIA) PVT. LTD.
21C, Sector-18, Gurugram - 122015
Haryana, India

+918826990350
1800 102 7620

bryairmarketing@pahwa.com
www.bryair.com

OVERSEAS OFFICES
Malaysia • China • Switzerland • Brazil • Nigeria • Vietnam • Indonesia • Philippines • Korea • Japan • UAE • Saudi Arabia • Bangladesh • USA • Canada

BAA/Data Centre/ 2022-23