GALAXY
Integrating Technology | Driving Growth

TECH TALK

Issue 173
November 2026

Pioneering Tech Leadership with a Legacy of Excellence.

AIM

Galaxy Office Automation Pvt. Ltd.



We are proud to have hosted an exclusive Technology Day in collaboration with **Dell Technologies** in Mumbai, bringing together industry professionals to explore innovations in AI PCs, Cyber Resiliency, Dell Private Cloud, and Cybersecurity.

The session reinforced our commitment to helping enterprises build secure, resilient, and future-ready IT environments.

A sincere thank you to Dell Technologies, our customers, and all participants for making this event a success.

Together, we continue to drive innovation and shape the future of enterprise IT.

Foreword



Dear Readers,

On behalf of Galaxy, I wish all the readers a very happy Diwali and a safe and prosperous year ahead. Speaking of safety, I would like to touch upon the ticking time bomb of the "Quantum Clock".

Quantum computing is advancing rapidly, and while we are still some distance away from machines capable of breaking today's widely used encryption, the cybersecurity implications are already real.

Quantum computers promise extraordinary breakthroughs in science, medicine and computing. However, they also pose a fundamental challenge to the encryption technologies that protect our digital world. The concern is not just what quantum computers might do in the future, but what bad actors are doing today. Encrypted data can be intercepted and stored now, with the intention of decrypting it when quantum computing becomes sufficiently powerful. This Harvest Now, Decrypt Later approach, fundamentally changes how we must think about data security. For organisations handling sensitive information that must remain confidential for years or decades, waiting for quantum computers to become a practical threat before acting could be a costly mistake.

The transition has officially begun. The USA National Institute of Standards and Technology (NIST) has already standardised its first generation of Post-Quantum Cryptography (PQC) algorithms, and its October 2026 migration roadmap provides further direction for organisations preparing to move away from vulnerable encryption standards. More recently, international cybersecurity agencies have called on organisations to assess the post-quantum readiness of their technology vendors.

For enterprises, this is much more than a cybersecurity upgrade. Encryption is embedded across data centres, cloud platforms, enterprise networks, digital identities and business applications. Identifying these dependencies and migrating them without disrupting operations will require careful planning.

At Galaxy, we believe quantum readiness must become part of the enterprise technology roadmap today. Through our expertise in cybersecurity, data centre architecture, networking and cloud, we help organisations build visibility into their technology environments and prepare for the next generation of security challenges.

The quantum era may still be unfolding, but the time to prepare is now. The organisations that act early will be better positioned to protect their data, preserve digital trust and build long-term resilience.

Do reach out to our experts and evangelists to explore how your organisation can begin its journey towards quantum-resilient infrastructure.

Happy reading!



Anoop Pai Dhungat
Chairman & Managing Director



A Lab on Your Wrist: Cambridge Scientists Develop a $10 Chip to Revolutionise Health Monitoring.

A new optical sensor that could make health monitoring easier, faster, and more affordable. The sensor is expected to cost around $10 and could help people check important health information using small wearable devices. One of the most exciting possibilities is checking blood sugar levels without using needles. This could make life easier for people who need to monitor their blood glucose regularly. The same technology could also be useful in food testing, factories, and environmental monitoring.

1 What Is an Optical Sensor?

An optical sensor is a device that uses light to collect information about different materials or substances. It studies how light behaves when it comes in contact with something. These sensors are already used in healthcare, industries, laboratories, and environmental testing. They help identify materials and measure different substances. However, traditional optical sensors are often large, expensive, and difficult to carry. Making them smaller usually reduces their accuracy. This has made it difficult to use them in small wearable devices. The new sensor developed by the Cambridge research team aims to solve this problem. It is small, affordable, and designed to provide highly accurate results.

2 How Does the New Sensor Work?

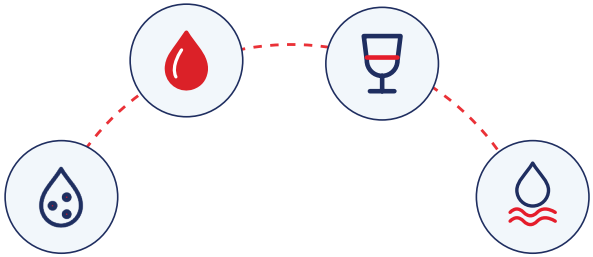
The researchers have developed a new type of device called a Convolutional Spectrometer. It uses light and mathematical calculations to study different substances. Unlike traditional devices, this sensor uses a different method to collect and understand light signals. This helps it deliver accurate results in less time. The device is built using a special material called silicon nitride, which is commonly used in advanced electronic and photonic technologies. It can measure different types of light in less than one second. It is also designed to work in different temperature conditions, from -20°C to 80°C. This makes it useful for wearable devices, industrial machines, and outdoor applications.

3 How Can It Help in Healthcare?

One of the biggest benefits of this technology is its possible use in healthcare.The researchers tested the sensor to measure different health-related markers, including:

- **Blood glucose (blood sugar levels)**
- **Blood alcohol levels**
- **Blood lactate levels**
- **Skin moisture**

In one test, the researchers also demonstrated that the sensor could track blood glucose without using needles over an extended period in one participant. If this technology is developed further, it could help people monitor their health more easily through wearable devices such as smartwatches and other portable gadgets. However, more research and medical testing are required before it can be used as a regular medical device.





Beyond Healthcare: Other Possible Uses

The sensor is not limited to healthcare. It could also bring major changes to different industries.

Food Testing
It could help identify food products such as coffee, tea, flour, and other materials. It may also help check food quality and detect unwanted changes.

Industrial Quality Control
Factories could use these small sensors to check the quality of materials during production. This could help identify problems quickly and reduce waste.

Environmental Monitoring
The technology could help monitor water quality and detect changes in different substances. This could support environmental testing and pollution monitoring.

Medicine and Chemical Testing
It could help identify medicines and measure the concentration of different chemicals with high accuracy.

3 Why Is This Technology Important?

The biggest advantage of this new sensor is that it combines small size, low cost, and high accuracy. Traditional laboratory equipment can be expensive and requires more space. This new technology could make similar types of measurements possible using much smaller devices. It also requires less computing power, which means it can process information quickly without needing complicated systems. The researchers believe that this technology could be produced on a larger scale in the future, making it more affordable and easier to use.

The Future of Everyday Health Monitoring

This new development could change how people monitor their health in the coming years. Instead of depending only on large laboratory machines, people may be able to check important health information through small wearable devices. From monitoring blood glucose to checking food quality and testing water, this $10 optical sensor has the potential to support many industries. Although more testing is needed before it becomes available for everyday use, it is an important step towards making advanced technology smaller, smarter, and more affordable.

Read more →

TECHNOLOGY FOCUS



What is High Availability?

A Simple Guide for Growing Businesses

High availability (HA) is a term that refers to a system's ability to be accessible and reliable close to 100% of the time.

Highly available systems must be able to withstand outages, including scheduled downtime and site-wide disasters. Typically, HA systems meet two characteristics:

- They must be available for use close to 100% of the time.
- They must be able to meet a certain set of predetermined user expectations.

With the growth of digital transformation initiatives and the subsequent move of many services to the cloud, high availability solutions are now offered by many tech and software as a service (SaaS) companies, including Microsoft, Amazon (AWS), IBM, Red Hat, and more.

High availability of IT systems is particularly important in industries where critical applications rely on having little or no system downtime. For example, in hospitals and data centers, users depend on high availability solutions to perform many routine, daily functions. If users can't access a system for any reason, it is deemed 'unavailable.' The period of time that a system is unavailable to users is known as downtime.

HA versus Disaster Recovery (DR)

Disaster recovery (DR) consists of IT infrastructure technologies and best practices designed to prevent or minimize data loss and business continuity disruption resulting from catastrophic events. High availability (HA), on the other hand, typically concerns smaller failures or faults that might impact a systems' availability.

HA versus fault tolerance

Fault tolerance is a system's ability to operate continuously after one or more of its critical components fail. Like HA, fault tolerance can help make a system available during or after a disruptive event.

However, where fault tolerance and HA differ is in the way they treat downtime. While HA seeks to have as little downtime as possible, the goal of fault tolerance is zero downtime, a goal it can only achieve through redundancy, having a backup or secondary copy of every single component in the infrastructure.



Benefits of high availability

With enterprises relying more than ever on online services and cloud and hybrid cloud architectures to deliver critical applications and services, infrastructure demands are rising, making high availability a priority. Here are some of the most common enterprise benefits of highly available systems.

Increased flexibility

With digital transformation a key objective for most companies, high availability of systems is critical to giving employees and customers unlimited access to critical applications.

Secure data with a high availability architecture, organizations' most important data is always available, accessible, and protected from unauthorized breaches

Improved brand reputation. System failures that cause hours or even minutes of downtime can cause public relations nightmares for enterprises across a broad range of industries, including SaaS, aviation, and mobile technology. High availability infrastructure ensures a brand's reputation doesn't suffer due to an outage or unexpected downtime.

Better customer service, Managed Service Providers (MSPs) must deliver high availability of networks or risk not fulfilling their service level agreements (SLAs). HA systems help MSPs deliver networks that their most valuable clients can depend on, like one that helps autonomous vehicles drive safely or a healthcare facility manage patient records.

Read more →

Galaxy enables organizations to achieve high availability by building resilient, always-on IT systems that minimize downtime and ensure seamless business continuity. Our approach leverages robust infrastructure design, redundancy, and proactive monitoring to keep critical applications accessible, secure, and reliable—helping businesses enhance customer experience, protect data, and maintain operational excellence in a digital-first world.

To connect with our experts, write to us at marketing@goapl.com



SPECIAL FOCUS

Beyond Connectivity: Strengthening Digital Security with Intelligent DNS Protection

Domain Name System (DNS) is a fundamental component of modern IT infrastructure, translating domain names into IP addresses to enable seamless communication across networks. As almost every online interaction relies on DNS, it has become a key target for cyberattacks.

DNS Security provides an additional layer of protection by monitoring, filtering, and analyzing DNS traffic to detect and block malicious activities. It helps prevent access to harmful domains, identify suspicious communication, and protect users, applications, and networks from evolving cyber threats. DNS Security is a critical layer of modern cybersecurity.

Key Features of DNS Security

DNS Security combines threat intelligence, real-time monitoring, and automated protection to safeguard an organization's DNS infrastructure.

- **Threat Intelligence:** Identifies malicious domains, phishing sites, malware sources, and command-and-control (C2) servers using updated threat intelligence.
- **DNS Filtering & Protection:** Blocks access to malicious and unauthorized domains, protecting users from phishing, malware, and ransomware.
- **DNS Tunnelling Detection:** Detects suspicious DNS traffic that may indicate data exfiltration or unauthorized communication.
- **DNS Integrity Protection:** Uses DNSSEC validation to protect against DNS spoofing and cache poisoning.
- **Real-Time Monitoring:** Monitors DNS traffic and identifies unusual activities and potential security threats.
- **DDoS Protection:** Helps detect abnormal DNS traffic and mitigate DNS-based service disruptions.
- **Centralized Management & Reporting:** Enables unified policy enforcement, security dashboards, activity monitoring, and compliance reporting across enterprise and cloud environments.

Benefits of Using DNS Security

DNS Security strengthens an organization's cyber resilience by proactively preventing threats and improving network visibility.

- **Threat Intelligence:** Identifies malicious domains, phishing sites, malware sources, and command-and-control (C2) servers using updated threat intelligence.
- **DNS Filtering & Protection:** Blocks access to malicious and unauthorized domains, protecting users from phishing, malware, and ransomware.
- **DNS Tunnelling Detection:** Detects suspicious DNS traffic that may indicate data exfiltration or unauthorized communication.
- **DNS Integrity Protection:** Uses DNSSEC validation to protect against DNS spoofing and cache poisoning.
- **Real-Time Monitoring:** Monitors DNS traffic and identifies unusual activities and potential security threats.
- **DDoS Protection:** Helps detect abnormal DNS traffic and mitigate DNS-based service disruptions.
- **Centralized Management & Reporting:** Enables unified policy enforcement, security dashboards, activity monitoring, and compliance reporting across enterprise and cloud environments.

DNS Security Use Cases

DNS Security protects organizations across diverse IT environments and industries:

- **Enterprise Network Protection:** Secures corporate networks, branch offices, and data centers against malicious domains.
- **Phishing & Malware Prevention:** Blocks access to phishing, ransomware, and malware-hosting websites.
- **Data Exfiltration Detection:** Identifies DNS tunnelling and suspicious data transfers.
- **Cloud & Hybrid Security:** Ensures consistent DNS protection across on-premises and cloud environments.
- **Remote Workforce Protection:** Secures remote users through DNS filtering and threat prevention.
- **SOC & MSSP Operations:** Enhances threat monitoring, investigation, and incident response through DNS intelligence.
- **Critical Infrastructure Security:** Protects business-critical systems across BFSI, healthcare, manufacturing, and telecom sectors.

Why Choose Us for DNS Security?

As a System Integrator (SI), we deliver end-to-end DNS Security solutions tailored to your business and security requirements.

- **End-to-End Integration:** From assessment and design to deployment, customized solutions and ongoing support.
- **Vendor-Agnostic Approach:** Recommending the right technology based on business needs and budget.
- **Technical Expertise:** Highly skilled in implementation, configuration, and troubleshooting.
- **Scalability:** Solutions designed for evolving enterprise, cloud, and hybrid environments.
- **Ongoing Support:** Continuous assistance, optimization, and managed security services.

As your trusted System Integration partner, we deliver tailored, scalable, and integrated DNS Security solutions that strengthen your security posture, minimize cyber risks, and ensure business continuity.

As cyber threats continue to evolve across enterprise networks, DNS Security has become an essential layer of modern cybersecurity. Intelligent DNS protection helps organizations detect and block malicious domains, prevent phishing and malware attacks, identify suspicious DNS traffic, and strengthen security across on-premises, cloud, and hybrid environments, ensuring secure connectivity and business continuity.

To connect with our experts, write to us at marketing@goapl.com



TECH NEWS

The Future of EV Batteries:

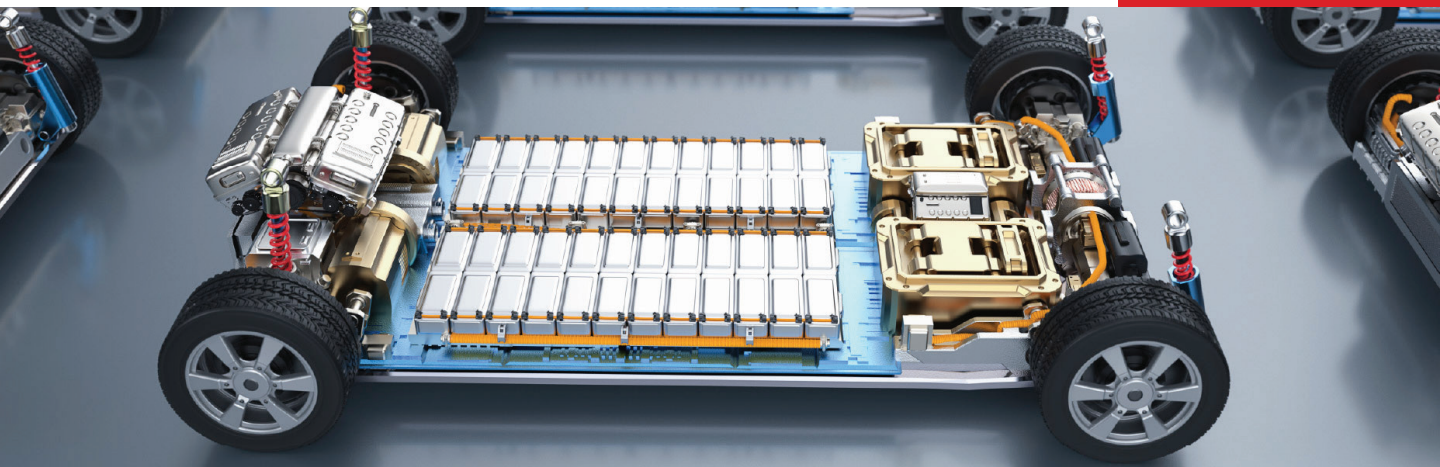
The Future of EV Batteries: How General Motors Is Advancing Battery Innovation
General Motors is challenging China's dominance in EV batteries. Alongside developing a different battery chemistry for electric trucks and large SUVs, the automaker is encouraging engineers to question senior leaders, acknowledge uncertainty and turn down work that distracts from their priorities. According to a Fortune report, that cultural shift helped GM move forward with a battery technology it had spent more than a decade researching.
"I want to grant myself permission to speak fearlessly." GM has encouraged employees to use this phrase when opening a disagreement with their seniors, Kurt Kelty, its vice president of battery and sustainability, told Fortune. Battery engineer Andy Oury said the approach helped open up the debate over lithium manganese-rich batteries, or LMR, which GM plans to produce commercially with LG Energy Solution

What GM's battery bet means for competition with China

Much of the world's inexpensive EV battery supply uses lithium iron phosphate, or LFP, a chemistry dominated by China. GM's LMR cells replace much of the nickel and cobalt with cheaper, more plentiful manganese and additional lithium.GM says the technology can deliver roughly a third more energy density than leading LFP cells at comparable cost. Higher energy density means batteries can store more energy for their size or weight. We're not licensing this from China, Kelty told Fortune. "We're developing this here."The company's $900 million investment in battery development facilities in Warren, Michigan, is intended to help engineers develop cells and work out how to manufacture them. Previously, GM relied on partners to turn its cell designs into physical batteries.The commercial outcome remains uncertain. Kelty said GM

had enough supporting data to get about 60% to 70% of the way to its LMR decision, with further development needed to close the gap.

Read more →



TECH NEWS

Centre's key cybersecurity agency secures access to Anthropic's Mythos AI model

The Indian Computer Emergency Response Team (CERT-In), one of the country's key cybersecurity agencies, has recently received access to Anthropic's Claude Mythos artificial intelligence (AI) model, and is conducting small, controlled experiments on identifying software vulnerabilities, a senior government official said.

The experiments are being carried out on a limited scale because of concerns within CERT-In, which operates under the IT Ministry, over sharing sensitive information with a powerful AI model hosted on third-party servers. The agency is wary of exposing large volumes of potentially sensitive government and critical infrastructure data to a system over which it has limited direct control, the official said. As a result, the initial testing is being restricted to smaller datasets and controlled environments, rather than allowing the model to extensively scan sensitive systems.

The development comes amid CERT-In's recent revelation that AI agents broke safety parameters and gained unauthorised access to sensitive data of Indian firms. The Indian Express reported that the AI agents belonged to Anthropic and OpenAI.

In June, this paper had also reported that CERT-In was among a select group of Indian government cybersecurity agencies in contention to receive access to Mythos, as part of Anthropic's Project Glasswing initiative.

Launched in April, Project Glasswing is Anthropic's initiative to give select cybersecurity organisations early access to its most powerful AI models to identify and fix vulnerabilities in critical software systems before malicious actors can exploit them.

Claude Mythos Preview, the model at the centre of the initiative, demonstrated unusually advanced cybersecurity capabilities, including the ability to autonomously discover previously unknown software vulnerabilities, known as zero-day vulnerabilities, and develop techniques to exploit them.

According to Anthropic, the model had identified thousands of serious security flaws, including vulnerabilities in major operating systems and web browsers. In May, the company said it and its initial partners had discovered more than 10,000 high- or critical-severity vulnerabilities using the model.

Anthropic initially decided against making the model publicly available, warning that it could substantially lower the technical expertise required to discover and exploit weaknesses in widely used software systems.

Instead, the company restricted access to vetted organisations through Project Glasswing, whose initial partners included Microsoft, Google, Amazon Web Services, Apple, Cisco, and CrowdStrike. In June, Anthropic announced that it was expanding the initiative to approximately 150 additional organisations across more than 15 countries.

For India, access to Mythos could help government cybersecurity agencies identify weaknesses in systems underpinning critical sectors such as banking, telecom and power.



To help Enterprise Customers fortify their perimeter against emerging threats, Galaxy Professional Services delivers end-to-end surface attack assessment and compliance automation tailored for modern IT environments. Our vulnerability assessment services conduct rigorous scanning of public-facing web applications to identify zero-day risks, unpatched exposures and unauthorized access vectors before malicious actors can exploit them. Additionally, Galaxy deploys automated compliance tools designed to benchmark enterprise IT assets continuously against the latest CERT-In directives, streamlining posture tracking and ensuring seamless regulatory readiness. Through proactive surface management and intelligent automation, Galaxy empowers organization infrastructure to remain resilient, compliant and securely managed.

To connect with our experts, write to us at marketing@goapl.com

All product names, logos, brands, trademarks, and registered trademarks are the property of their respective owners

Read more →



GALAXY
Integrating Technology | Driving Growth

Galaxy Office Automation Pvt. Ltd. B-602,
Lotus Corporate Park, Graham Firth
Compound, Off. Western Express Highway,
Goregaon (E), Mumbai - 400 063.

+91 22 46108999

marketing@goapl.com

www.goapl.com

© 2026 Galaxy Office Automation Pvt Ltd . All Rights Reserved.
All product names, logos, brands, trademarks, and registered
trademarks are the property of their respective owners.