GALAXY
Integrating Technology | Driving Growth

TECH TALK

Issue 153 March 2025

Pioneering Tech Leadership with a Legacy of Excellence.

AIM

Galaxy Office Automation Pvt. Ltd.

Galaxy Recognition: Best Employer Brand Award

Galaxy is proud to announce that we have been honoured with the 'Best Employer Brand Award' by the WORLD HRD Congress at the National Best Employer Brands 2024!

This recognition is a testament to our unwavering commitment to fostering a dynamic, innovative, and supportive workplace where every team member can thrive.

We extend our heartfelt gratitude to our incredible team—their passion, dedication, and drive for excellence have made this achievement possible.
Here's to many more milestones ahead!

Foreword

Dear Readers,

One of the technologies that I had predicted would see widespread adoption this year was AI-assisted Cybersecurity. As cyber threats become more sophisticated, traditional security measures struggle to keep up.

Attackers are using advanced tactics such as AI-driven malware, automated phishing, and zero-day exploits, making it essential for organisations to adopt a proactive defense strategy. This is where Artificial Intelligence (AI) is revolutionising cybersecurity—by enabling real-time threat detection, predictive analytics, and automated responses to combat evolving cyber risks.

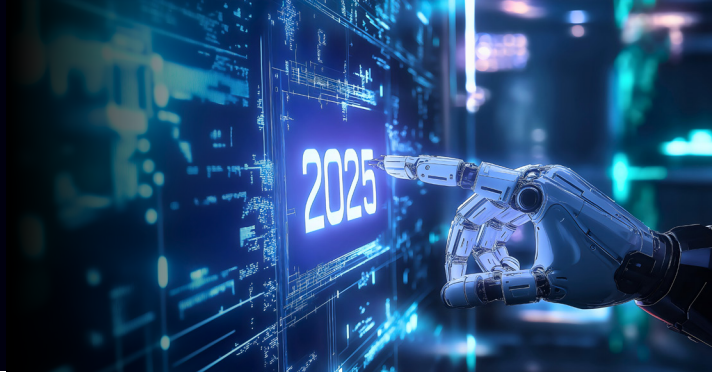
However, AI is not a silver bullet—it requires continuous monitoring, human oversight, and ethical considerations. By combining AI with Zero-trust, SOAR, and threat intelligence, organisations can stay ahead of cybercriminals and build a resilient cybersecurity framework.

At Galaxy, we are at the forefront of bringing AI-based cybersecurity solutions to you. Do reach out to our experts to discuss how they could help your business.

Happy reading.

Anoop Pai Dhungat
Chairman & Managing Director

Future is now!



Pomelo Power:
Scientists Generate Power from Fruit Peel Using Triboelectric Device

Researchers have used waste pomelo-peel biomass to power small electric devices and monitor biomechanical motions. The method was developed by researchers at the University of Illinois Urbana-Champaign after analysing the peels' chemical composition and mechanical properties. The research team used the peel's properties to create devices that convert mechanical energy into electricity and serve as self-powered motion sensors.

"There are two main parts of the pomelo peel – a thin outer layer and a thick, white inner layer. The white part is soft and feels like a sponge when you push on it," said study co-author Yi-Cheng Wang, an assistant professor in the Department of Food Science and Human Nutrition.

Advantage of the Natural Porous, Spongy Structure of the Peel

"Some people have used pomelo peels to extract compounds for essential oils or pectin, but we wanted to take advantage of the natural porous, spongy structure of the peel."

Commonly grown in Southeast and East Asia, the Pomelo is a large citrus fruit with a very thick peel, typically discarded, resulting in a considerable amount of food waste.

A pomelo fruit typically weighs 1 to 2 kilograms (2 to 4.5 pounds), and the peel accounts for 30% to 50%.

Researchers Used Pomelo-peel Biomass and a Plastic (Polyimide) Film

"If we can upcycle the peel to higher-value products instead of simply throwing it away, we can not only reduce waste from pomelo production, consumption, and juice making, but also create more value from food and agricultural waste," added Wang.

Researchers separated the peel from the flesh and removed the outermost layer. According to researchers, the remaining thick, spongy white peel was cut into smaller pieces and freeze-dried to preserve its unique three-dimensional, porous structure, then stored under different humidity conditions.

Researchers used pomelo-peel biomass and a plastic (polyimide) film as triboelectric layers brought into contact when external force is present. They attached a copper foil electrode to each layer and evaluated how well the resulting device could convert external mechanical energy into electricity.

The study reveals that tapping these pomelo-peel-based triboelectric devices with a finger could light up about 20 light-emitting diodes (LEDs).

What Can Be Powered

They also demonstrated that a calculator or sports watch can be powered solely by these mechanical forces, without external electricity, when integrated with a power-management system with an energy-storage unit.

Researchers have revealed that this application has strong potential to convert otherwise wasted energy into useful electricity. This study's optimized pomelo-peel biomass-derived porous material-based triboelectric nanogenerator (PP-TENG) had an open circuit voltage of 58 V and a 254.8 mW/m^2 peak power density.

"We also found that, thanks to the pomelo peel's naturally porous structure, triboelectric devices based on it can be highly sensitive to force and force frequency.

This inspired us to develop sensing devices that can be attached to the human body for biomechanical monitoring," explained Wang.
According to researchers, when attached to various body parts, the researchers' proof-of-concept sensors were able to monitor biomechanical movements such as joint motions and gait patterns.

This was because the movements of different body parts can lead to contact electrification between the triboelectric layers, generating distinct electrical signals corresponding to different motions. According to a press release, this capability has great potential to provide valuable insights for health care and physical rehabilitation professionals.

Read more →

TECHNOLOGY FOCUS

Why Cloud Migration? The Future of Business IT Infrastructure

Cloud migration is the process of moving data, applications, and workloads from an on-premises data center to a cloud-based infrastructure, or from one cloud environment to another, known as cloud-to-cloud migration.

A company might migrate to either a single cloud or multiple. They can use public cloud models, where services are delivered over the public internet, or private cloud models, with a secure, proprietary cloud infrastructure accessible only to them. Many organisations choose a hybrid cloud environment, which combines public and private cloud services to create a single, flexible, cost-effective IT infrastructure that supports and automates workload management across cloud environments.

Multiclouds offer another option, which allows companies to migrate IT infrastructure by using multiple public cloud providers. Multiclouds can be as simple as using software as a service (SaaS) from different vendors to employ portability features across infrastructures. However, they often involve managing enterprise applications on platform as a service (PaaS) or infrastructure as a service (IaaS) across multiple cloud vendors—such as Amazon Web Services, Google Cloud Platform, IBM Cloud® and Microsoft Azure—from a central console.

Types of Cloud Migrations

There are different types of cloud migration, varying in terms of what is being migrated and where it is moving to.

Complete Data Center Migration

This cloud migration is the process of moving all data, applications and services from on-premises data centers to a cloud provider's servers. This process is generally extensive and requires thorough planning and testing to ensure efficient execution.

Hybrid Cloud Migration

Hybrid cloud migration involves moving a portion of resources to public cloud while leaving others in on-premises data centers. This hybrid cloud scenario allows organisations to take advantage of current investments in on-premises infrastructure while also using the flexibility, efficiency, strategic value, and other benefits of public cloud.

Enterprises also use hybrid cloud migration for data backup. In this case, a company backs up its private cloud resources on a public cloud as a mitigation technique when an attack or disaster renders an on-premises data center inoperable.

Cloud-to-cloud Migration

Organisations might move their resources from one public cloud to another for many reasons. These reasons include taking advantage of specific pricing models, security features or products (such as new AI or machine learning tools) or because of changes to company structure or service level agreements.

Workload-specific Migration

Another option is to migrate specific workloads to the cloud. For example, an organisation might choose to migrate certain databases or mainframes to the cloud as a way to capitalize on lower costs, or for more reliable performance, better security, or other factors.

The Cloud Migration Process

Cloud migration has become a modernisation imperative for businesses looking to streamline IT operations, implement cost-saving measures, and realise end-to-end digital transformation. Tech analysts predict that 75% of organisations will adopt cloud-based data infrastructure by 2026.

To ensure a successful transition, organisations should follow a well-defined workflow that focuses on comprehensive planning, execution, and optimisation.

Read more →

SPECIAL FOCUS

Microsegmentation: A Key Strategy for Modern Security

Microsegmentation is a network security technique that enhances the security of a network by dividing it into smaller, more isolated segments, or "microsegments." Each microsegment is typically a small, self-contained network segment that is isolated from other parts of the network. This isolation is achieved using network security policies and controls.

The Key Principles and Features of Microsegmentation

Granular Access Control

Microsegmentation allows organisations to apply highly granular access controls to network resources. Instead of relying on traditional perimeter-based security measures, such as firewalls at the network edge, access controls are applied at a much finer level, often down to the individual workload or application.

Zero-trust Security Model

Microsegmentation aligns with the zero-trust security model, which assumes that no entity, whether inside or outside the network, should be trusted by default. Access to network resources is restricted based on the principle of "least privilege," meaning that users or systems are granted only the minimum access necessary to perform their tasks.

Isolation

Microsegments are isolated from one another, which means that even if an attacker gains access to one segment, they will have a difficult time moving laterally within the network because the communication paths between segments are restricted. This containment helps limit the potential impact of a security breach.

Application-centric

Microsegmentation is often application-centric, focusing on securing individual applications or workloads rather than entire subnets or network segments. This approach allows organisations to tailor security policies to the specific requirements of each application.

Dynamic Policies

Microsegmentation can be dynamic, meaning that security policies can be adjusted in real-time based on changing network conditions, user behavior, or threat intelligence. This adaptability is crucial in responding to evolving security threats.

Network Visibility and Monitoring

To effectively implement microsegmentation, organisations need robust network visibility and monitoring tools. These tools help administrators understand network traffic patterns, detect anomalies, and enforce security policies effectively.

Automation

Automation plays a significant role in microsegmentation, as it can help manage and enforce policies at scale. Automation tools can respond to security events and policy changes rapidly.

Microsegmentation can be implemented using various technologies and tools, such as virtual firewalls, software-defined networking (SDN), and network access controls (NAC). It is commonly used in data centres and cloud environments to enhance security and prevent lateral movement by attackers. This approach to network security is especially valuable in modern, complex IT environments where traditional perimeter-based security measures may be insufficient to protect against advanced threats.

Advantages of Microsegmentation

Microsegmentation offers several advantages for network security and is increasingly adopted by organisations to enhance their cybersecurity posture. Some of the key benefits of microsegmentation include:

Improved Security Posture

Microsegmentation significantly enhances security by reducing the attack surface. It limits lateral movement within the network, making it more challenging for attackers to compromise multiple systems once they gain access to one segment. This containment helps prevent the spread of threats.

Zero-trust Security

Microsegmentation aligns with the zero-trust security model, which means that trust is not assumed, and access is restricted by default. This proactive approach to security reduces the likelihood of unauthorized access and data breaches.

Granular Access Control

With microsegmentation, organisations can implement highly granular access controls. They can specify who or what has access to specific resources or applications, providing a finer level of control compared to traditional perimeter-based security.

Tailored Security Policies

Microsegmentation allows organisations to tailor security policies to individual applications or workloads. This customization ensures that security measures are appropriate for the specific needs and vulnerabilities of each asset.

Reduced Attack Surface

By isolating segments from one another, microsegmentation minimizes the exposure of critical assets to potential threats. Even if one segment is compromised, it doesn't automatically grant access to other parts of the network.

Dynamic Adaptation

Microsegmentation can dynamically adjust security policies in response to changing conditions, such as the detection of suspicious activities or emerging threats. This flexibility enables organisations to respond quickly to security events.

Compliance and Regulatory Benefits

Microsegmentation can help organisations meet compliance and regulatory requirements more effectively. It allows for the enforcement of access controls and data protection measures, which are often mandated by industry-specific regulations.

Network Visibility

To implement microsegmentation effectively, organisations typically invest in network visibility and monitoring tools. This enhanced visibility allows administrators to gain insights into network traffic patterns, detect anomalies, and make informed decisions to strengthen security.

Easier Incident Response

In the event of a security incident, microsegmentation can aid in containment and isolation, limiting the scope of the breach and making it easier for security teams to investigate and respond.

Scalability

Microsegmentation is scalable, making it suitable for environments with varying sizes and complexities. It can be applied to both on-premises data centers and cloud environments, allowing organisations to maintain consistent security measures across their infrastructure.

Automation

Automation plays a significant role in microsegmentation, helping manage and enforce policies at scale. Automated responses to security events or policy changes enhance overall security and operational efficiency.

Compliance

- **Payment Card Industry Data Security Standard (PCI DSS) Compliance**

  Organisations handling credit card transactions can use microsegmentation to isolate systems that store, process, or transmit cardholder data, helping meet PCI DSS requirements.

- **Healthcare and Health Insurance Portability and Accountability Act (HIPAA) Compliance**

  Healthcare providers can implement microsegmentation to safeguard electronic protected health information (ePHI) and ensure compliance with HIPegulations.

We at Galaxy can help you design and implement a solution to make it more efficient to stop or prevent ransomware attacks within the environment including insider threat vectors. Microsegmentation is a solution that will enhance security posture on applications and microservice levels by enforcing granular access controls and limiting the spread of threats, organisations must implement robust microsegmentation strategies to strengthen their security posture. To talk to our experts, email us at marketing@goapl.com

TECH NEWS

Elon Musk Launches 'Scary Smart' AI Chatbot Grok 3

Elon Musk's AI company unveiled, on Monday, the latest version of its chatbot, Grok 3, which the billionaire hopes will find traction in a highly competitive sector contested by the likes of ChatGPT and China's DeepSeek.

The launch comes as the world's richest man is deploying the enormous powers granted to him by US President Donald Trump to restructure and dismantle federal agencies.

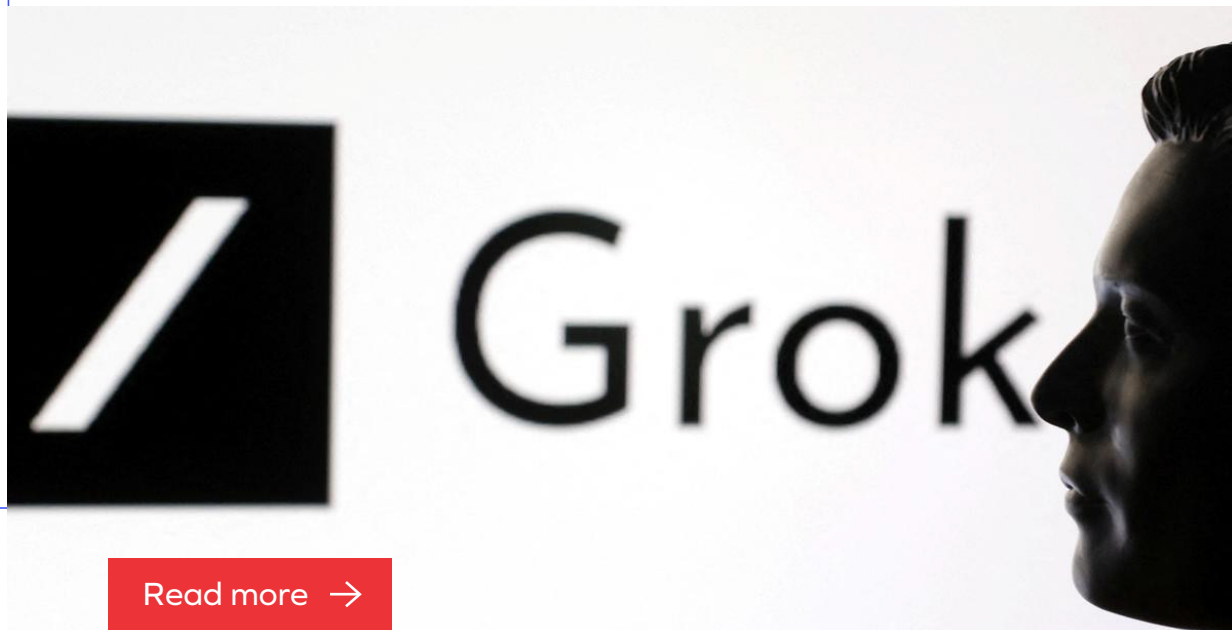
The unprecedented cost-cutting drive has raised conflict-of-interest questions, given that many of those agencies have regulatory oversight on elements of Musk's sprawling business empire.

Musk has promoted Grok 3 as "scary smart," with 10 times the computational resources of its predecessor that was released in August last year.

The flagship product of his xAI company was trained on synthetic data and employs self-correction mechanisms that avoid errors - known as "hallucinations" - that plague some AI chatbots and lead them to process false or misleading data as fact.

"Grok 3 has very powerful reasoning capabilities, so in the tests that we've done thus far, Grok 3 is outperforming anything that's been released, that we're aware of, so that's a good sign," Musk said in a video call last week with the World Governments Summit in Dubai.

The upgraded chatbot enters a crowded field with countries racing to introduce more sophisticated - and cost-effective - AI products.



Read more →

TECH NEWS

DeepSeek to Share Some, Doubling Down on Open Source

The startup DeepSeek will make its models' code publicly available, it said on Friday (Feb 21), doubling down on its commitment to open source AI.

The company said in a post on social media platform X that it will open source five code repositories next week, describing the move as "small but sincere progress" that it will share "with full transparency."

"These humble building blocks in our online service have been documented, deployed, and battle-tested in production." the post said. DeepSeek rattled the global AI industry last month when it released its open source R1 reasoning model, which rivaled western systems in performance while being developed at a lower cost.

The company's commitment to open source has distinguished it from most AI firms in China, which like their US rivals lean towards closed-sourced models. DeepSeek's low-key founder Liang Wenfeng said in a rare interview with a Chinese media outlet last July that the firm did not prioritize commercializing its AI models and that there was soft power to be gained from open source.

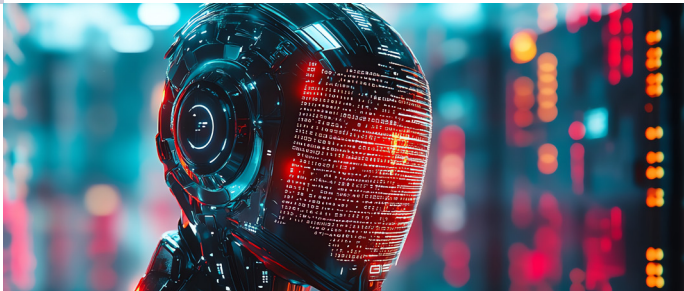
"Having others follow your innovation gives a great sense of accomplishment," Liang said in July.

"In fact, open source is more of a cultural behaviour than a commercial one and contributing to it earns us respect" he added.

The newly released open source code will provide infrastructure to support the AI models that DeepSeek has already publicly shared, building on top of those existing open-source model frameworks.

The announcement came after DeepSeek on Tuesday released a new algorithm called Native Sparse Attention (NSA), designed to make long-context training and inference more efficient.

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