KIET GROUP OF INSTITUTIONS
Connecting Life with Learning
www.kiet.edu
Delhi-NCR, Ghaziabad
CELEBRATING 25 YEARS OF EXCELLENCE
DEPARTMENT OF COMPUTER APPLICATIONS (MCA)

# TechEdge Technical Newsletter

Vol. VII Issue 2, Feb 2024


- Alumni Section
- Google announces the development of Lumiere, an AI-based next-generation text-to-video generator
- AI discovers that not every fingerprint is unique
- Researchers create first functional semiconductor made from graphene
- CoRover.ai Introduces BharatGPT, India's First Large Language Model
- Swedish Scientists Create 'e-soil' That Accelerates Plant Growth
- Google DeepMind Introduces Mobile ALOHA Humanoid Technology


**Disclaimer**

The newsletter you received is intended for information purposes only and does not constitute a binding offer. The institute does neither give any guarantee nor assume any liability (of whatever content or nature) for the transmission of its news as well as for the timeliness, completeness and accuracy of the information contained in the newsletter and the contents on websites (including all information, services, software, etc.) directly or indirectly referred to by links or references named in the newsletter.

**Compiled by:-**
*Aditya Sharma,Manmeet Chauhan*
*Rahul Singh Negi (MCA 3rd sem)*

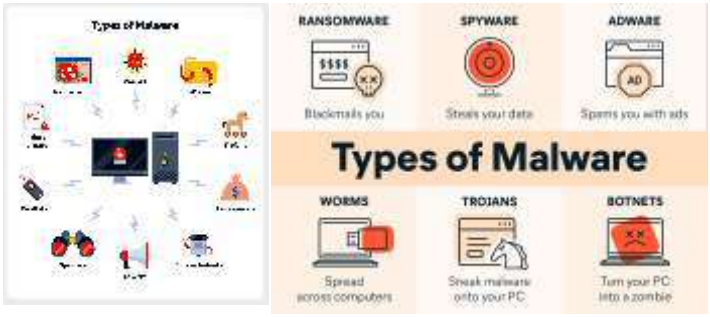
**Coordinated by:-**
*Ms. Shalika Arora*
*(Asst. Prof.,MCA)*

## Cyber-attack

**Rishi Indolia**
***Sr. Principal engineer (Mac & iOS)@Sophos***

### 1. Malware

Malware or malicious software is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, crypto-jacking, and any other type of malware attack that leverages software in a malicious way.




### 2. Denial-of-Service (DoS)

DoS Attacks is a malicious, targeted attack that floods a network with false requests in order to disrupt business operations.

In a DoS attack, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network. While most DoS attacks do not result in lost data and are typically resolved without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

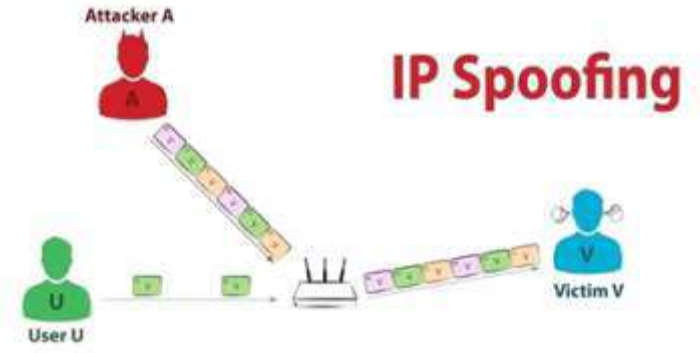
The difference between DoS and Distributed Denial of Service (DDoS) attacks has to do with the origin of the attack. DoS attacks originate from just one system while DDoS attacks are launched from multiple systems. DDoS attacks are faster and harder to block than DOS attacks because multiple systems must be identified and neutralized to halt the attack.


### 3. Phishing

Phishing is a type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information-such as passwords or account numbers - or to download a malicious file that will install viruses on their computer or phone.

### 4. Spoofing

Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.




### 5. Identity-Based Attacks

CrowdStrike's findings show that 80% of all breaches use compromised identities and can take up to 250 days to identify. Identity-driven attacks are extremely hard to detect. When a valid user's credentials have been compromised and an adversary is masquerading as that user, it is often very difficult to differentiate between the user's typical behaviour and that of the hacker using traditional security measures and tools.

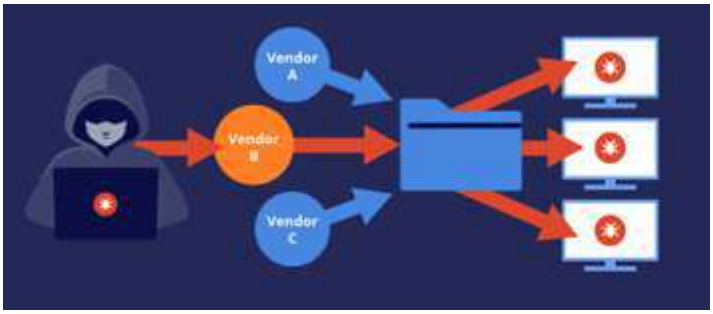
Pass-the-Hash (PtH) is a type of attack in which an adversary steals a “hashed” user credential and uses it to create a new user session on the same network. It does not require the attacker to know or crack the password to gain access to the system. Rather, it uses a stored version of the password to initiate a new session.


**6. Code Injection Attacks**

Code injection attacks consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action. There are multiple types of code injection attacks.


**7. Supply Chain Attacks**

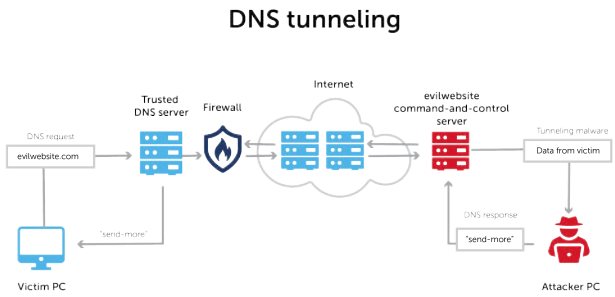
A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. Software supply chain attacks inject malicious code into an application in order to infect all users of an app, while hardware supply chain attacks compromise physical components for the same purpose. Software supply chains are particularly vulnerable because modern software is not written from scratch: rather, it involves many off-the-shelf components, such as third-party APIs, open source code and proprietary code from software vendors.




**8. DNS Tunnelling**

DNS Tunnelling is a type of cyberattack that leverages domain name system (DNS) queries and responses to bypass traditional security measures and transmit data and code within the network. Once infected, the hacker can freely engage in command-and-control activities. This tunnel gives the hacker a route to unleash malware and/or to extract data, IP or other sensitive information by encoding it bit by bit in a series of DNS responses.

DNS tunnelling attacks have increased in recent years, in part because they are relatively simple to deploy. Tunnelling toolkits and guides are even readily accessible online through mainstream sites like YouTube.

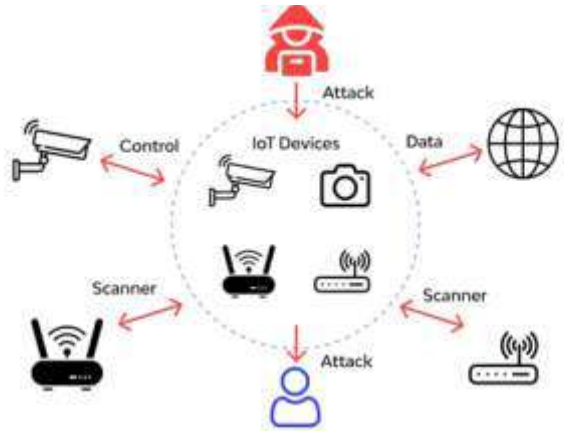



**9. IoT-Based Attacks**

An IoT attack is any cyberattack that targets an Internet of Things (IoT) device or network. Once compromised, the hacker can assume control of the device, steal data, or join a group of infected devices to create a botnet to launch DoS or DDoS attacks.

[According to the Nokia Threat Intelligence Lab, connected devices are responsible for nearly one-third of mobile network infections-more than double the amount in 2019.]

Given that the number of connected devices is expected to grow rapidly over the next several years, cybersecurity experts expect IoT infections to grow as well. Further, the deployment of 5G networks, which will further fuel the use of connected devices, may also lead to an uptick in attacks.




**How To Protect Against Cyber Attacks**

A comprehensive cybersecurity strategy is absolutely essential in today's connected world. From a business perspective, securing the organization's digital assets has the obvious benefit of a reduced risk of loss, theft or destruction, as well as the potential need to pay a ransom to regain control of company data or systems. In preventing or quickly remediating cyberattacks, the organization also minimizes the impact of such events on business operations.

Finally, when an organization takes steps to deter adversaries, they are essentially protecting the brand from the reputational harm that is often associated with cyber events-especially those that involve the loss of customer data.

**Below are some recommendations we offered in our 2023 Global Threat Report to help organizations improve their security posture and ensure cybersecurity readiness:**

**1. Protect All Workloads:**
In the digital landscape, safeguarding all data and applications-referred to as workloads-is imperative. This involves implementing robust security measures across every aspect of your systems, whether they are on-premises, in the cloud, or across various devices. Utilize encryption, access controls, and regular security updates to fortify these workloads against potential threats like unauthorized access or data breaches.

**2. Know Your Adversary:**
Understanding the motives, tactics, and potential vulnerabilities of potential threats is crucial. This involves comprehensive threat intelligence gathering to identify and analyse potential attackers. By studying past incidents, emerging trends, and the techniques used by adversaries, organizations can better prepare defences and proactively thwart potential attacks.

**3. Be Ready When Every Second Counts:**
In the realm of cybersecurity, time is of the essence. Incidents can unfold rapidly, and swift response times are critical in mitigating their impact. Establishing a well-defined incident response plan, with clearly outlined roles and procedures, enables organizations to react promptly in the event of a security breach, minimizing damage and swiftly restoring normalcy.

**4. Adopt Zero Trust:**
The Zero Trust model operates on the principle of 'never trust, always verify.' It involves eliminating the assumption that entities within or outside an organization's network can be trusted by default. Instead, access to systems and resources is granted on a least-privileged basis and continuously verified, irrespective of location or user identity. This approach significantly reduces the attack surface and enhances overall security posture.

**5. Monitor the Criminal Underground:**
Keeping an eye on illicit online forums, hacker communities, and the dark web provides insights into potential threats. By monitoring these channels, organizations can identify discussions or activities related to planned cyberattacks, stolen data sales, or emerging vulnerabilities. This information can be used to bolster defences and proactively protect against imminent threats.

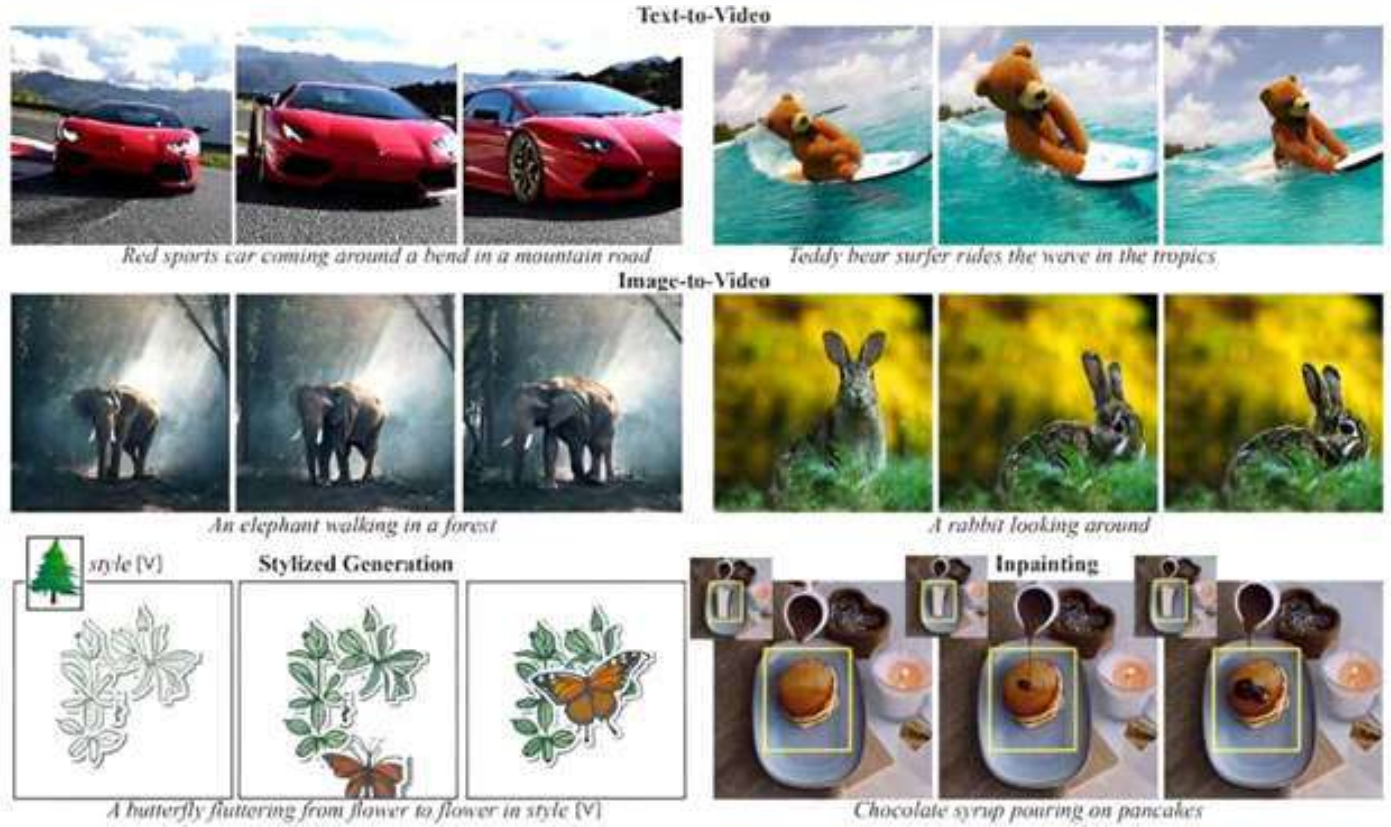
**6. Invest in Elite Threat Hunting:**
Employing skilled cybersecurity professionals for proactive threat hunting is crucial. These experts use advanced tools and methodologies to actively seek out potential threats within an organization's network, identifying anomalies or potential indicators of compromise that automated systems might miss. This proactive approach allows for early detection and mitigation of potential threats before they escalate.

**7. Build Comprehensive Cybersecurity Training Program:**
Human error remains a significant factor in cybersecurity breaches. A comprehensive training program is essential to educate employees about potential threats, best practices for data protection, recognizing phishing attempts, and adhering to security protocols. Regular training sessions ensure that staff remains updated on the latest threats and security measures, significantly reducing the risk of inadvertent security breaches.
DNS tunnelling attacks have increased in recent years, in part because they are relatively simple to deploy. Tunnelling toolkits and guides are even readily accessible online through mainstream sites like YouTube.

# Google announces the development of Lumiere, an AI-based next-generation text-to-video generator

Highlights

- *Google Research Launches Lumiere: A Breakthrough in Text-to-Video Generation*
- *Lumiere's high-resolution output transforms simple sentences into captivating videos*
- *Powered by the revolutionary Space-Time U-Net Architecture, enabling single-pass animated video creation*
- *Advanced features include real-time video editing and diverse output styles, redefining AI-generated content.*




A team of AI researchers at Google Research has developed a next-generation AI-based text-to-video generator called Lumiere. The group has published a paper describing their efforts on the arXiv preprint server.

Over the past few years, artificial intelligence applications have moved from the research lab to the user community at large-LLMs such as ChatGPT, for example, have been integrated with browsers, allowing users to generate text in unprecedented ways.

More recently, text-to-image generators have allowed users to create surreal imagery. And text-to-video generators have allowed users to generate short video clips using nothing but a few words. In this new effort, the team at Google has taken this last category to new heights with the announcement of a text-to-video generator called Lumiere.

Lumiere, likely named after the Lumiere brothers who pioneered early photography equipment, allows users to type in a simple sentence such as "***two raccoons reading books together***" and get back a fully finished video showing two raccoons doing just that-and it does it in stunningly high resolution. The new generator represents a next step in the development of text-to-video generators by creating much better-looking results.

Google describes the technology behind the new generator as a "*groundbreaking Space-Time U-Net architecture*."It was designed to generate animated video in a single model pass.

Here is a YouTube video link of the same
https:/youtu.be/wxLr02Dz2Sc?feature=shared

The demonstration video shows that Google added extra features, such as allowing users to edit an existing video by highlighting a part of it and typing instructions, such as "***change dress color to red***."The generator also produces different types of results, such as stylizations, where the style of a subject is created rather than a full-color representation. It also allows substyles, such as different style references. It also does cinemagraphics, in which a user can highlight part or all of a still image and have it animated.

In its announcement, Google did not specify if they plan to release or distribute Lumiere to the public, likely due to the obvious legal ramifications that could arise due to the potential creation of videos that violate copyright laws.

# AI discovers that not every fingerprint is unique

Highlights

- *Columbia Engineering Team Challenges Forensic Norms: Intra-Person Fingerprints Found Matchable*
- *Undergraduate Gabe Guo Uses AI to Challenge Uniqueness of Different Fingerprints from the Same Person*
- *Modified AI System Achieves 77% Accuracy in Matching Fingerprints of Different Fingers; Potential Tenfold Increase in Forensic Efficiency*
- *AI-based Forensic Marker: Columbia Engineering's Innovative Approach Challenges Traditional Minutiae Analysis*

From "***Law and Order***" to "**CSI**," not to mention real life, investigators have used fingerprints as the gold standard for linking criminals to a crime. But if a perpetrator leaves prints from different fingers in two different crime scenes, these scenes are very difficult to link, and the trace can go cold.

It's a well-accepted fact in the forensics community that fingerprints of different fingers of the same person-"intra-person fingerprints"-are unique and, therefore, unmatchable.

A team led by Columbia Engineering undergraduate senior Gabe Guo challenged this widely held presumption. Guo, who had no prior knowledge of forensics, found a public U.S. government database of some 60,000 fingerprints, and fed them in pairs into an artificial intelligence-based system known as a deep contrastive network. Sometimes the pairs belonged to the same person (but different fingers), and sometimes they belonged to different people.

Over time, the AI system, which the team designed by modifying a state-of-the-art framework, got better at telling when seemingly unique fingerprints belonged to the same person and when they didn't. The accuracy for a single pair reached 77%. When multiple pairs were presented, the accuracy shot significantly higher, potentially increasing current forensic efficiency by more than tenfold.

The project, a collaboration between Hod Lipson's Creative Machines lab at Columbia Engineering and Wenyao Xu's Embedded Sensors and Computing lab at University at Buffalo, SUNY.

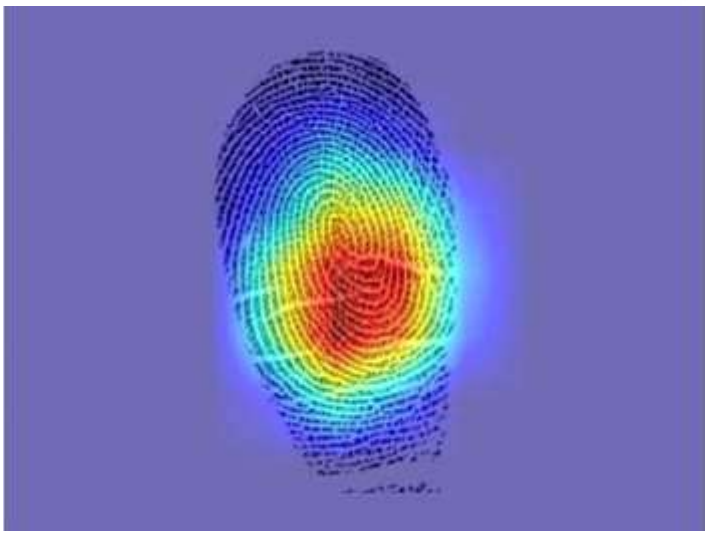
Video Link https:/youtu.be/s5esfRbBc18

**Study findings challenge and surprise forensics community**

Once the team verified their results, they quickly sent the findings to a well-established forensics journal, only to receive a rejection a few months later. The anonymous expert reviewer and editor concluded that "It is well known that every fingerprint is unique," and therefore, it would not be possible to detect similarities even if the fingerprints came from the same person.

The team did not give up. They doubled down on the lead, fed their AI system even more data, and the system kept improving. Aware of the forensics community's skepticism, the team opted to submit their manuscript to a more general audience. The paper was rejected again, but Lipson, who is the James and Sally Scapa Professor of Innovation in the Department of Mechanical Engineering and co-director of the Makerspace Facility, appealed.

"I don't normally argue editorial decisions, but this finding was too important to ignore," he said. "If this information tips the balance, then I imagine that cold cases could be revived and even that



innocent people could be acquitted."

While the system's accuracy is insufficient to decide a case officially, it can help prioritize leads in ambiguous situations. After more back and forth, the paper was finally accepted for publication by Science Advances.

**A new kind of forensic marker to precisely capture fingerprints**.

One of the sticking points was the following question: What alternative information was the AI actually using that has evaded decades of forensic analysis? After carefully visualizing the AI system's decision process, the team concluded that the AI was using a new forensic marker.

"*The AI was not using 'minutiae,' which are the branching and endpoints in fingerprint ridges-the patterns used in traditional fingerprint comparison,*" said **Guo**, who began the study as a first-year student at Columbia Engineering in 2021. "Instead, it was using something else, related to the angles and curvatures of the swirls and loops in the center of the fingerprint."

Columbia Engineering senior Aniv Ray and Ph.D. student Judah Goldfeder, who helped analyze the data, noted that their results are just the beginning. "Just imagine how well this will perform once it's trained on millions instead of thousands of fingerprints," said Ray.

The team is aware of potential biases in the data. The authors present evidence that indicates that the AI performs similarly across genders and races where samples were available. However, they note that more careful validation needs to be done using datasets with broader coverage if this technique is to be used in practice.

# Researchers create first functional semiconductor made from graphene

Highlights

- *Georgia Tech Researchers Achieve Milestone: World's First Functional Graphene Semiconductor*
- *Graphene Breakthrough: Semiconductor with 10 Times Silicon's Mobility Overcomes Band Gap Challenge*
- *Walter de Heer and Team at Georgia Tech Pave the Way for New Electronics Era*
- *Epitaxial Graphene on Silicon Carbide Wafers Unleashes Semiconducting Properties, Surpassing Limits of Silicon*

Researchers at the Georgia Institute of Technology have created the world's first functional semiconductor made from graphene, a single sheet of carbon atoms held together by the strongest bonds known. Semiconductors, which are materials that conduct electricity under specific conditions, are foundational components of electronic devices. The team's breakthrough throws open the door to a new way of doing electronics.

Their discovery comes at a time when silicon, the material from which nearly all modern electronics are made, is reaching its limit in the face of increasingly faster computing and smaller electronic devices.

Walter de Heer, Regents' Professor of physics at Georgia Tech, led a team of researchers based in Atlanta, Georgia, and Tianjin, China, to produce a graphene semiconductor that is compatible with conventional microelectronics processing methods—a necessity for any viable alternative to silicon..

In this latest research, published in Nature, de Heer and his team overcame the paramount hurdle that has been plaguing graphene research for decades, and the reason why many thought graphene electronics would never work. Known as the "band gap," it is a crucial electronic property that allows semiconductors to switch on and off. Graphene didn't have a band gap-until now.

"We now have an extremely robust graphene semiconductor with 10 times the mobility of silicon, and which also has unique properties not available in silicon," de Heer said. "But the story of our work for the past 10 years has been, 'Can we get this material to be good enough to work?'"

**A new type of semiconductor**

De Heer started to explore carbon-based materials as potential semiconductors early in his career, and then made the switch to exploring two-dimensional graphene in 2001. He knew then that graphene had potential for electronics.

Video Link: https://youtu.be/gWUX2OTqkEo

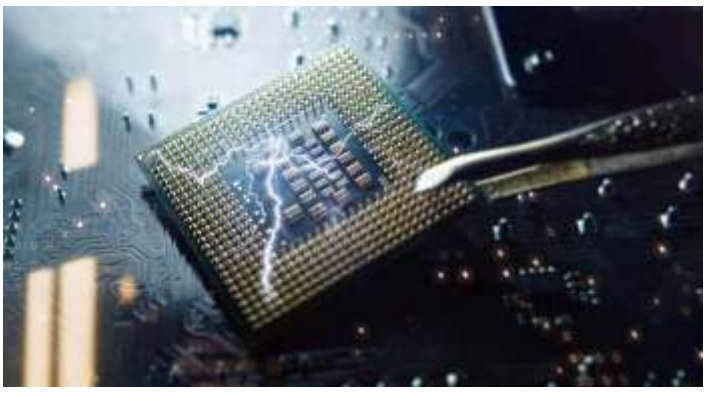
"We were motivated by the hope of introducing three special properties of graphene into electronics," he said. "It's an extremely robust material, one that can handle very large currents, and can do so without heating up and falling apart."

De Heer achieved a breakthrough when he and his team figured out how to grow graphene on silicon carbide wafers using special furnaces. They produced epitaxial graphene, which is a single layer that grows on a crystal face of the silicon carbide. The team found that when it was made properly, the epitaxial graphene chemically bonded to the silicon carbide and started to show semiconducting properties.

Over the next decade, they persisted in perfecting the material at Georgia Tech and later in collaboration with colleagues at the Tianjin International Center for Nanoparticles and Nanosystems at Tianjin University in China. De Heer founded the center in 2014 with Lei Ma, the center's director and a co-author of the paper.

**How they did it**

In its natural form, graphene is neither a semiconductor nor a metal, but a semimetal. A band gap is a material that can be turned on and off when an electric field is applied to it, which is how all transistors and silicon electronics work. The major question in graphene electronics research was how to switch it on and off so it can work like silicon.



# CoRover.ai Introduces BharatGPT, India's First Large Language Model

Highlights

- *CoRover.ai, a prominent player in Conversational AI, introduces BharatGPT, India's inaugural Large Language Model, aiming to transform AI dialogues across 22 Indian languages.*
- *This groundbreaking development aims to revolutionize AI conversations across 22 Indian languages.*
- *Data remains in India*

CoRover has launched its own Indigenous Large Language Model (LLM), BharatGPT. BharatGPT is integrated for voice modality in more than 14 Indian languages & 22 languages for text modality, in partnership with BHASHNI, a National Language Translation Mission (NLTM) under The Ministry of Electronics and Information Technology (MeitY). CoRover, the world's first and the highest ROI-delivering human-centric conversational AI platform, also has Generative AI capabilities. It provides all the required features needed to build and manage Chabot's across communication channels like dialogue/conversation management tool.

CoRover, the world's first and the highest ROI-delivering human-centric conversational AI platform, also has Generative AI capabilities. It provides all the required features needed to build and manage Chatbot's across communication channels like dialogue/conversation management tool. CoRover is presently offering AI Virtual Assistants (ChatBots, VoiceBots, VideoBots) to hundreds of organizations, that includes IRCTC, LIC, IGL, KSRTC, Indian Navy (GRSE), Max Life Insurance, NPCI, BHIM-UPI, Mahindra, Government of India, and many more. Most of these existing Virtual Assistants by CoRover.ai, having a user base of1 Billion+, would be using BharatGPT.

CoRover has partnered with Google to scale BharatGPT, BharatGPT is hosted in Google CloudPlatform (GCP) to ensure data sovereignty, privacy, and security. Additionally, Vertex AI is integrated with CoRover's Conversational AI platform, allowing organizations to utilize Google's AI services.

Using CoRover's BharatGPT developers and business users can create text and voice enabled multi-lingual Virtual Assistant in a few seconds by just adding the content/documents specific to their business and/or use case(s). Additional Benefits of CoRover Conversational AI platform is the data remains in India. It also has an option to add custom knowledge base and can be integrated with any Enterprise Resource Planning (ERP)/Customer Relationship Management (CRM) systems, and Application Programming Interfaces (APIs) for real-time transactions. CoRover also has the capability of integrating payment gateway and Aadhar-based authentication for KYC. Furthermore, CoRover has many components, viz., Dialogue/Conversational Management, Real Time Analytics, Speech to Text (STT)/ Automatic Speech Recognition (ASR), Text to Speech (TTS), Speech to Speech (STS), Video to Text, Documents-to-Text (fine-tuned AI-based OCR, hand-written documents are also supported),Text-to-Q&A (Q&A Generator), Text-to-Voice (voice cloning), Text-to-Video (Video Cloning),Sentiment Analysis and many more.


On the other hand, the existing platforms having LLM(s) are not capable enough, to create Enterprise Virtual Assistants (ChatBots, VoiceBots, VideoBots). A Conversational AI platform also requires other components, such as user interface; a dialogue management system; integration with other systems and data sources; voice and video capabilities, to create Virtual Assistants. Bharat GPT has many additional features and should be considered as EnterpriseGPT. Idea is to implement a responsible AI with generative capabilities, with better Governance and Safety Net, along with informational and end-to-end transactional capabilities, for various organizations. CoRover with BharatGPT now offers Gen AI as a Service (GaaS).

Some of the examples of BharatGPT implementations are: IncomeTaxGPT, GSTGPT, HealthGPT, MediaGPT, BusGPT, ShipGPT, ExternalAffairsGPT, EducationGPT, SkillGPT, KaramYogiGPT, ECIGPT, LegalGPT, JusticeGPT, DARPGGPT, GeMGPT, SpaceGPT, EnergyGPT, ComsumerGPT, BFSIGPT, and more. Even for each state, like: KarnatakaGPT, GujaratGPT, J&KGPT, and more.

Now CoRover.ai with BharatGPT becomes a human-centric conversational AI platform with contextual Generative AI (LLM) and faster Machine Learning, which takes substantially less compute and memory. We aim to build BharatGPT as a Sovereign Gen AI platform, that is accurate, grounded, and reliable with a better Governance and Safety Net.

CoRover along with Bhashini is also removing the language barriers, if one user speaks in one languages, other can listen in their preferred languages at the same time.

Adding to the accolades, the President & CEO of NeGD and DIC (Digital India), Mr. Abhishek Singh, after an insightful demo of BharatGPT, observed, “BharatGPT will be transformational for Conversational AI in India. Its potential applications in the government sector are numerous. BharatGPT will not only make India proud but will also position us as an AI-first country.”

# Swedish Scientists Create 'e-soil' That Accelerates Plant Growth

**Highlights**

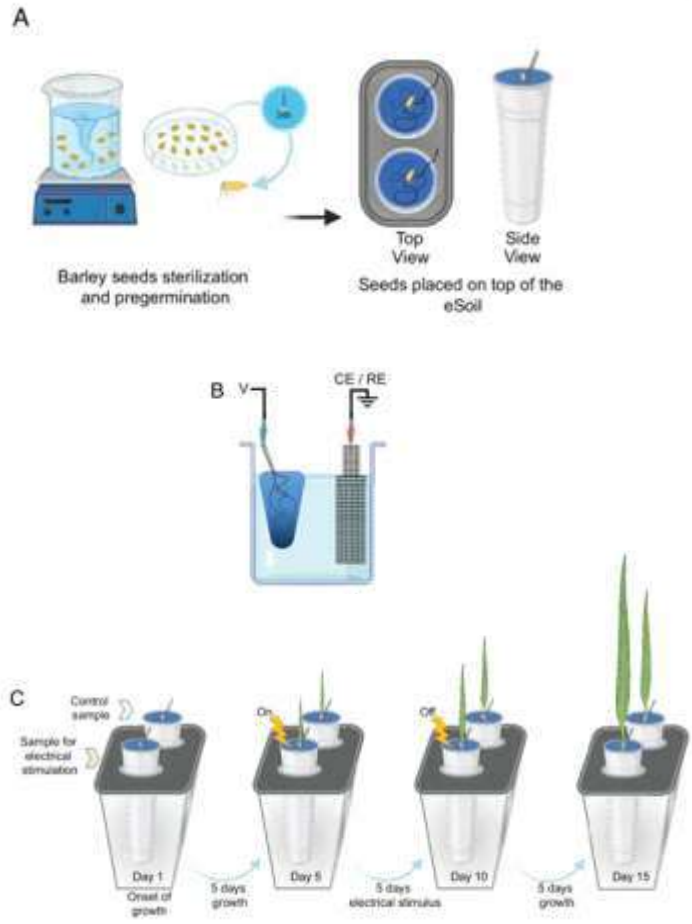
- *Scientists have unveiled an electrically conductive soil engineered to foster exceptional growth in crops.*
- *This innovative soilless cultivation method, termed hydroponics, harnesses a sophisticated root system activated through a novel cultivation substrate.*
- *It can speed up the growth of plants in hydroponic spaces, or farms that grow plants without soil in environments made up of mostly water.*

Researchers from Linköping University in Sweden developed a 'bioelectronic soil' that can speed up the growth of plants in hydroponic spaces, or farms that grow plants without soil in environments made up of mostly water and a place for roots to attach. After integrating the engineered 'eSoil' into the framework where seedlings grow, researchers discovered that sending electrical signals through the soil made plants grow 50 percent more on average.

The eSoil is made up of organic substances mixed with a conductive polymer called PEDOT, which can be found in things like sensors and OLED displays. Eleni Stavrinidou, the supervisor of the study, told Engadget that the soil's conductivity was necessary for stimulating the plant roots. In this particular study, the researchers examined the effect of sending signals to barley seedlings over the span of 15 days before harvesting them for analysis. Applying a voltage as small as 0.5V on the eSoil electrically stimulates the roots, Stavrinidou explained. This, in turn, resulted in a recordable increase in the biomass of the electrically stimulated plants when compared to the non-stimulated seedings.

The stimulation's effect on the barley seedlings was described as “steady” and “transient.” Stavrinidou told Engadget that nitrogen, one of the main nutrients involved in plant growth, was processed more efficiently through the stimulation. "We found that the stimulated plants could process the nutrients more efficiently however we don't understand how the stimulation is affecting this process,” Stavrindou explained, adding that the reason behind the growth process will be a focus of future studies.

While hydroponic techniques are mainly used to grow leafy greens and some vegetables like cucumbers and tomatoes, the eSoil could offer a solution to create new ways to increase crop yields in commercial settings and especially in places where environmental conditions impact plant growth. The study highlights that this technique could minimize the use of fertilizers in farming.



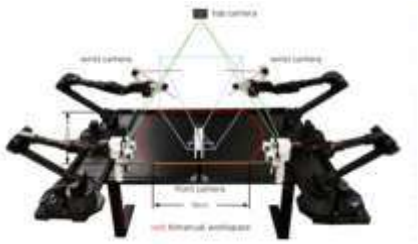

The opportunity for technological innovation in farming is huge considering the number of US farms has steadily declined since 1982, according to the Department of Agriculture. Last year, the number of US farms reached 2 million, down from 2.2 million in 2007. Not only are farms on the decline, but the US is losing acres of land due to a host of reasons that range from climate change to worsening economic outlook for farmers due to inflation. But beyond improving crop yield, the implementation of eSoil in hydroponic farms could make them more energy conscious. While traditional hydroponic farms use up less water, they require more energy to run. “*The eSoil consumes very little power in the microwatt range*,” Stavrinidou said. Before this technology can be applied to large-scale agriculture and other types of crops, more studies need to be conducted to observe how electrical stimulation can impact the whole growth cycle of a plant throughout its entire lifespan and not just in the early stages of seedling maturation. Stavrinidou also said that her team plans on studying how the technique affects the growth of other plant species.

# Google DeepMind Introduces Mobile ALOHA Humanoid Technology

Highlights

- *Scientists have unveiled an electrically conductive soil engineered to foster exceptional growth in crops.*
- *This innovative soilless cultivation method, termed hydroponics, harnesses a sophisticated root system activated through a novel cultivation substrate.*
- *It can speed up the growth of plants in hydroponic spaces, or farms that grow plants without soil in environments made up of mostly water.*


Google DeepMind and Stanford University have leveraged cutting-edge technology to revolutionise household tasks. Together, they have unveiled Mobile ALOHA, an innovative and affordable open-source hardware system designed for bimanual teleoperation, specifically aimed at enhancing capabilities in cooking and cleaning.unloading from the dishwasher.



It is a humanoid robot that can be remotely operated by a user and perform autonomously by imitation learning. This development was highlighted by a researcher in a X post, wherein he showed that ALOHA could autonomously cook and serve shrimps, call and take the elevator and store a 3lbs pot in a cabinet - tasks it learned through imitation of 50 demos. Both the hardware and machine-learning algorithms of ALOHA are open-sourced. Additionally, the robot can do laundry and can be used as a vacuum cleaner. It could also perform other tasks such as watering plants, loading and

Mobile ALOHA can also self-charge and use a coffee machine. While these are some listed chores by the robot, the open-source invention is capable of doing many other tasks that are yet to be announced. The whole system will reportedly cost less than USD 20,000 with off-the-shelf robots and 3D-printed components. Currently, ALOHA is available on the Trossen Robotics website where buyers can place an order.