KIET GROUP OF INSTITUTIONS

Department of Computer Applications (MCA)

In This Issue..

- Alumni Section
- Google to start autodeleting search, voice and location records.
- Can tracking hardware-level activity protect children's online privacy?
- Smart devices could convert motion into electricity
- Killing COVID-19 Coronavirus with a Handheld UV Light Device
- Bengal Research Institutes Develop Low Cost Ventilators for COVID-19 Patient
- Donut Robotics developed an internet-connected smart mask
- Mercedes-Benz Cars to Be Built on Nvidia Autonomous Driving Architecture
- Boston Dynamics Spot Dog-Like Robots Now on Sale
- Hackers Can intrude on Your Conversations Using Light Bulbs
- India has joined GPAI (Global Partnership on Artificial Intelligence)
- Qure.ai a Mumbai based startup developed an AI tool which can detect Covid – 19 lung infection in less than a minute
- Google says Indian Gaming Industry to Cross $1 Billion Within Two Years.

Technical NEWS LETTER

Vol III,Issue 7 July 2020

Compiled By-
Naman Kumar (MCA II year)
Arya Mishra (MCA I year)
Shivam Nerwal (MCA I year)

Coordinated By-
Ms. Shalika Arora
(Assistant Prof., MCA)

Design by:- Sujeet Pratap Singh, MCA Deptt.

Alumni Section

Ayushi Singh
Software Engineer
Uneecops Business Solutions

CYBER SECURITY: OPPORTUNITY FOR DEVELOPERS

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." – Stephane Nappo

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. We live in the golden age of data. Today data is more available than ever before, and its mobile access has provided space for no of business and people and opened up no of opportunities for both companies and their customers. A big opportunity comes with a big risk. That big opportunity is data and big risk is cybercrimes.

Things developer should know about cyber security:
IT professionals and networking administrators are responsible for hardware and network security, and software developers are responsible for building secure applications. Data breaches can easily be avoided by implementing best practices and latest upgrade tools. Here we are discussing some of attacks that attackers use to breach security and what are the best practices we can use to avoid them:

1. Brute-Force Attack: It is trial-and-error method used to obtain info such as password/pin. If there is 1000 possible combination for a pin/password, attacker will apply all those combinations. Attackers use some automated software to generate and apply these combinations.
Work Around: Developer should use some good encryption algorithm. If AES encryption used, its key is 128 bit, thus possible keys are 2^128=>5*10^24 years will take to find out correct pin, if one combination takes one sec to decrypt.

2. Http Parameter Pollution Attack: What if we pass same parameter multiple times in a url, Ex: /details/?User=Anderson & User=Smith. How this thing is handled, whether the first parameter or second parameter will be used? This totally depends on backend and server. Some uses first one, some uses last one while some other returns value for all. Would it cause some breach to security? Yes it can be a threat if not properly handled, attacker can trick the url and play malicious activity.
Work Around: Using encrypted url parameter is a solution (remember base64 is not a secret. Use some good algorithms)

3. HTTP Tempering: This is something related to improper use of http methods to handle request. What if a developer is writing an api/method to delete a record by id by using GET method? The url would be like: /del_user/id=1 Now attacker just needs to change the id parameter value in the url and he will be able to delete other records.
Work Around: Use correct HTTP method. We have set of various Http methods like: GET POST, DELETE, PUT, and PATCH. A developer should choose correct http method as per the operation required.

4.Password Protection: Username and password are keys to access resources from an application. Password must be strong enough to detect.
Work Around: Restrict end user to enter strong password and don't use your own algorithm for encryption. Use some standard BCrypt/Scrypt/PBKDF-2 encryption algorithms. - Use of salt and pepper: A salt is random data that is used as an additional input to your data(say password) before hashing, pepper is a secret added to an input (password here) prior to being hashed - hash(strong password + salt + pepper)

5.HTTPS: It is http over a secure connection. Https gives identity, encryption and integrity. You need to take SSL certificate to convert your website into secure website i.e. from http to https. No attacker on the network can actually see or modify any of the traffic.
Work Around: There are certificate authorities that will give you a free certificate and make really automatic and easy to setup

6.CSRF Attacks (Cross Site Reference Forgery): One domain is forging some request to other domain, and modifies values. This is possible as one can get user details from cookies. Ex: There is a website vulnerable.com, having delete account functionality. There is some other website, say evil.com that contains a link that will send delete account request to vulnerable website and hence result in deletion of account on vulnerable.com.
Work Around: Using randomized token also k/a Anti csrf tokens can help here. It will be generated randomly on backend and will be sent to frontend web app on every request. (Request + anti csrf token)

7.SSRF Attacks (Server Site Reference Forgery): This is similar to CSRF but here attacks are intended at server side. There are various ways of ssrf attacks, for example someone can use port scanning to identify the ports that are open or close or their purpose on your server or they can trick to access your secret files on server that you never want to expose or use some other protocol scheme to access your files from server.
Work Around: There is no silver bullet for SSRF mitigation, nut some combination of these can be effective: - Limit connections to only port 80 (HTTP) and 443(HTTPS) to prevent port scanning - Resolve the IP of target host, to ensure that the IP is for that of an external host. - Disable access to any protocol scheme that is not HTTP or HTTPS

8.Injections (SQL, Xss): In these attacks, attacker can inject some malicious code in your website, say he provided some java script in your website comment box that cause alert on your web page or for in your input field user provided such value that can manipulate your query. Ex: your query is: Select * from users where username = 'user input' and password = 'password input'. On login page some provided username = 'OR 1=1-- Now it becomes: select * from users where username= "OR 1=1 -- and password = '**' Thus 1=1 will be true, '--'will comment rest of section of your code and end user will get all users details.
Work Around: Using binding parameter, it will convert whole input into string, and it will not be considered as part of sql query.

9. DDOS (Distributed Denial of Services): API DDos attacks are exec to overload an API service. Since each hacker sends normal traffic volumes, these attacks are difficult to detect.
Work Around: Pagination limits to prevent DDOS. Most endpoints that return a list of entities will need to have some sort of pagination. Without pagination, a simple search could return large data set causing extraneous traffic. Most sql provides feature of limit and offset that is used to limit number of records.

10. Authorization: You must implement proper authorization technique in order to control access to resources from server. If you are making apis for third parties, you must implement OAuth2.0 authentication method. In case of client server model you can implement token based authorization. You have various options like JWT Token or SessionId + Redis. Along with all these practices, filter and monitoring incoming traffic, Unit test are the steps you must take care along with development. Day by day cybercrime is increasing, Most of the companies want to implement security best practices but due to the lack of knowledge, expertise, finances, and awareness, they are unable to do so, there is a great market for developers. They can also look for ethical hacking. According to a report by IDC, there will be a shortage of 3.5 million cyber security experts by the year 2021. If you're looking for a career change or a new opportunity, cyber security field would be a decent option and will continue to be for the next several years.

Google to start autodeleting search, voice and location records

Google has announced that it will begin automatically deleting some user data which is presently retained indefinitely by default.

Google CEO Sundar Pichai, in a blog post announcing a new set of privacy-focused features, emphasised the company's commitment to privacy: "As we design our products, we focus on three important principles: keeping your information safe, treating it responsibly and putting you in control. Today, we are announcing privacy improvements to help do that, including changes to our data retention practices across our core products to keep less data by default."

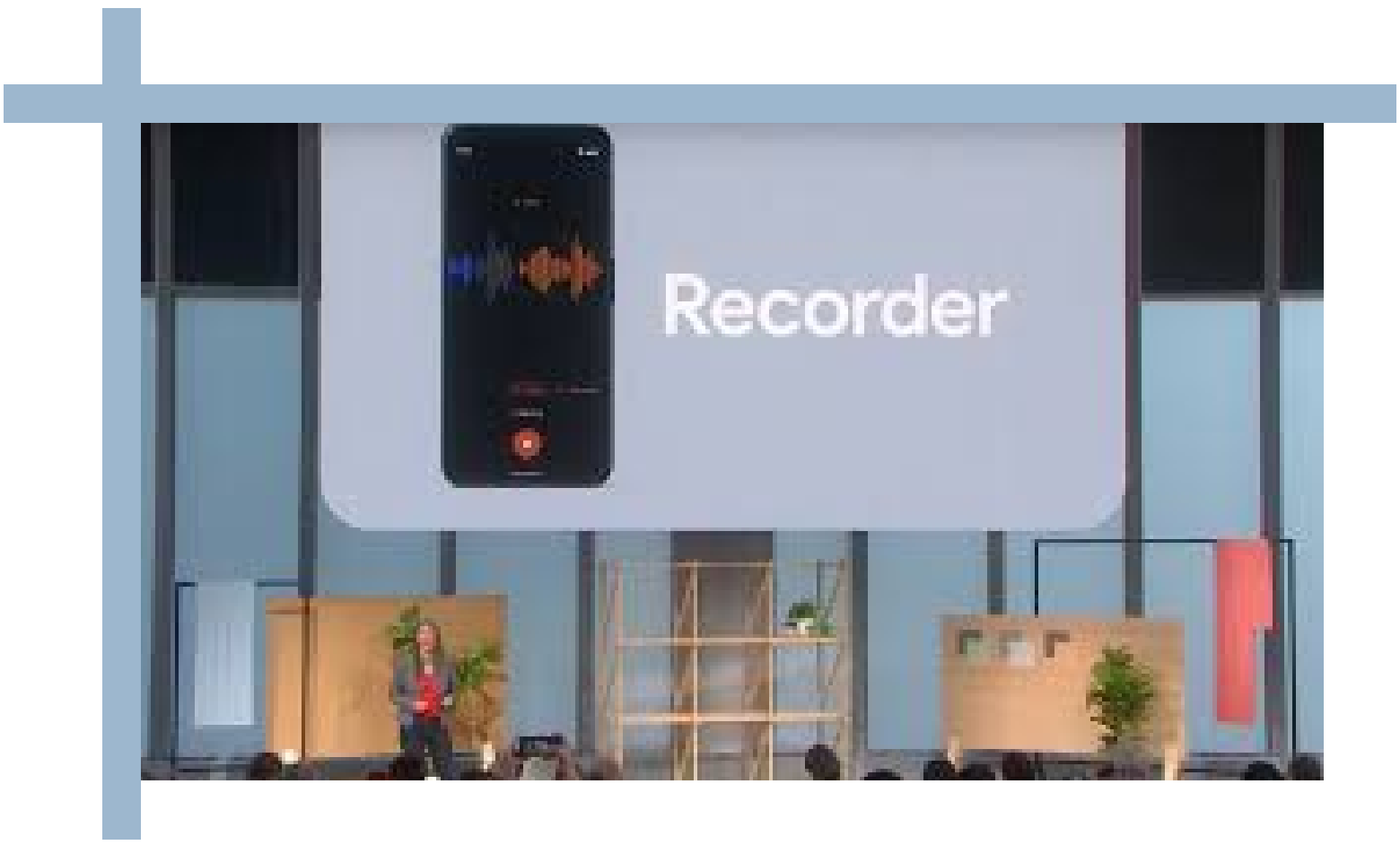
Most notably, Google will be moving from offering users the option to auto delete data (introduced last year and accessible in Google's Activity Controls section) after three months or 18 months to deleting data after 18 months for new users by default. This will affect location history; search history; voice commands collected via Google Assistant, and YouTube viewing history (although viewing history will be automatically deleted after 36 months instead, such that viewing history can still be used to inform the platform's recommendations). Data will not be auto deleted from apps intended to store personal data such as Gmail, Drive and Photos.

Existing Google account holders will have the auto-delete option promoted to them on the search page and on YouTube, prompting them to examine their privacy settings.

By autodeleting user data after 18 months by default, Google will be able to position itself as a platform which values data privacy while simultaneously retaining a very large quantity of the most recent (and hence most valuable user) data.

Other changes include Google making it easier to switch to Incognito mode in Google apps (a mode in which browsing history is not saved locally) with a long press on their profile picture. This feature will be introduced to iOS users this week and later for Android OS users. Google will also soon offer the option to remain in incognito mode across all Google apps, such that users will not need to switch it on in every app they use. Google will also be integrating 'Password Checkup' – a tool which checks if any passwords associated with the user's Goggle account have been compromised – to the 'Google Security Checkup' centre, whilst removing the 'Password Checkup' Chrome extension.

Although Google is widely credited with creating the lucrative business model of ad targeting based on mass collection and analysis of user data, the company has been increasingly attempting to position itself as privacy-conscious, including by publicly backing the EU's General Data Protection Regulation.



Can tracking hardware-level activity protect children's online privacy?

Researchers have developed a tool that can determine whether a mobile game or app complies with a US federal law aimed at protecting children's privacy online.
The tool, created by a researcher at the University of Texas at Dallas, comes after a study at the university which found that 72 out of 100 mobile apps for children violated the federal Children's Online Privacy Protection Act (COPPA).
Dr Kanad Basu, assistant professor of electrical and computer engineering, along with colleagues elsewhere, developed and tested their 'COPPA Tracking by Checking Hardware-Level Activity' (COPPTCHA) tool, which was found to have 99 per cent accuracy.
The researchers said they are continuing to improve on the technology, which they intend to make available to download for free.According to Basu, games and other apps that violate COPPA pose privacy risks that could make it possible for someone to determine a child's identity and location. He added this risk is heightened as more people are accessing apps from home, rather than public places, due to the Covid-19 pandemic.

Basu explained: “Suppose the app collects information showing that there is a child on Preston Road in Plano, Texas, downloading the app. A trafficker could potentially get the user's email ID and geographic location and try to kidnap the child. It's really, really scary.”
Apps can access personal, identifiable information. This includes names, email address and location, and unique identifiers for devices such as an international mobile equipment identity (IMEI) and media access control (MAC) addresses.

“When you download an app, it can access a lot of information on your cellphone,” Basu said. “You have to keep in mind that all this info can be collected by these apps and sent to third parties. What do they do with it? They can pretty much do anything. We should be careful about this.” The researchers' technique accesses a device's special-purpose register, a type of temporary data storage location within a microprocessor that monitors various aspects of the microprocessor's function. Whenever an app transmits data, the activity leaves footprints that can be detected by the special-purpose register.

Under COPPA, websites and online services directed at children must obtain parental consent before collecting personal information from anyone younger than 13. However, as Basu's research found, many popular apps do not comply.
According to the research, many popular games designed specifically for young children revealed users' Android IDs, Android advertising IDs and device descriptions.
Basu recommends that parents use caution when downloading or allowing children to download apps. He also advised keeping downloads to a minimum.
“If your kid asks you to download a popular game app, you're likely to download it,” Basu said. “A problem with our society is that many people are not aware of – or don't care about – the threats in terms of privacy.”
In May, a coalition of 20 advocacy groups accused TikTok of violating US child privacy laws and breaching a settlement agreed in February 2019 with the Federal Trade Commission (FTC). Back in January, the UK's data regulator published standards that would force tech companies to prioritise children's privacy online.

Smart devices could convert motion into electricity

Scientists have developed small, flexible generators that enable smart devices to charge themselves using energy harnessed from the movements of their user.

The device, developed by scientists from Loughborough University and the University of Surrey, is based on triboelectric nanogenerators (Tengs) and generates electricity from movement similar to how static electricity is produced. The University of Surrey researchers previously proposed a system based on Tengs in 2018.

Previously, using Tengs has been incompatible with many day-to-day electronic devices due to their inability to produce a constant current. However, the researchers have said they found a way to produce a direct current from a unique Teng design, creating a steady flow of electricity and opening up the potential for real-world applications.

"Triboelectric nanogenerators are effectively small-scale, flexible, and sometimes stretchable, energy generators that convert movements in our surroundings such as human motion, machine vibrations, vehicle movements, wind and wave energy into electricity," said Dr Ishara Dharmasena, of Loughborough's School of Mechanical, Electrical and Manufacturing Engineering.

Dharmasena said these generators are versatile and can be constructed in a wide variety of shapes, weights and sizes – from a few mm2 to several m2. "Unlike conventional mechanical energy harvesting methods, such as piezoelectric or electromagnetic devices which contain heavy and bulky components, toxic materials and rigid structures, Tengs can be constructed using low cost, lightweight, non-toxic and flexible materials."

Potential applications of the generators include next-generation wearable and implantable electronics, smart textiles, medical devices, IoT (Internet of Things) and 5G related sensors, smart pavements, smart floors, mobile phones and tablets, the researchers said. Tengs are made from dielectric materials, such as plastics, which accumulate static charge when they rub against each other. As these charged materials move back and forth, they generate uneven instantaneous alternating electrical current signals. The current is then further processed and stored in a battery or capacitor to be used when needed. Therefore, a typical Teng produces sharp positive and negative current peaks during its operation.

"In our new technology, converting the alternating current into a direct flow involves phase shifting," Dharmasena said, adding that an assembly of Teng units (poles) are used as a single device, where they are systematically excited to obtain a phase difference among their outputs. This systematic excitation is obtained through their geometry and spatial arrangement, he explained. The outputs with different phases are then superimposed to obtain the final DC output signal.

In a paper on the research, the team demonstrated the applicability of this technology by continuously lighting a set of LED lights and a photodetector.

Dharmasena said: "This new invention overcomes one of the most critical challenges of Teng technology and will enable countless real-time low-power applications in wearable electronics, such as IoT related applications and smart sensing, getting us one step closer towards a sustainable, autonomous and portable energy source."

Killing COVID-19 Coronavirus with a Handheld UV Light Device

A personal, handheld device emitting high-intensity ultraviolet light to disinfect areas by killing the novel coronavirus is now feasible, according to researchers at Penn State, the University of Minnesota, and two Japanese universities.

There are two commonly employed methods to sanitize and disinfect areas from bacteria and viruses — chemicals or ultraviolet radiation exposure. The UV radiation is in the 200 to 300 nanometer range and known to destroy the virus, making the virus incapable of reproducing and infecting. Widespread adoption of this efficient UV approach is much in demand during the current pandemic, but it requires UV radiation sources that emit sufficiently high doses of UV light. While devices with these high doses currently exist, the UV radiation source is typically an expensive mercury-containing gas discharge lamp, which requires high power, has a relatively short lifetime, and is bulky.

The solution is to develop high-performance, UV light emitting diodes, which would be far more portable, long-lasting, energy-efficient, and environmentally benign. While these LEDs exist, applying a current to them for light emission is complicated by the fact that the electrode material also has to be transparent to UV light.

“You have to ensure a sufficient UV light dose to kill all the viruses,” said Roman Engel-Herbert, Penn State associate professor of materials science, physics, and chemistry. “This means you need a high-performance UV LED emitting a high intensity of UV light, which is currently limited by the transparent electrode material being used.”

While finding transparent electrode materials operating in the visible spectrum for displays, smartphones and LED lighting is a long-standing problem, the challenge is even more difficult for ultraviolet light.

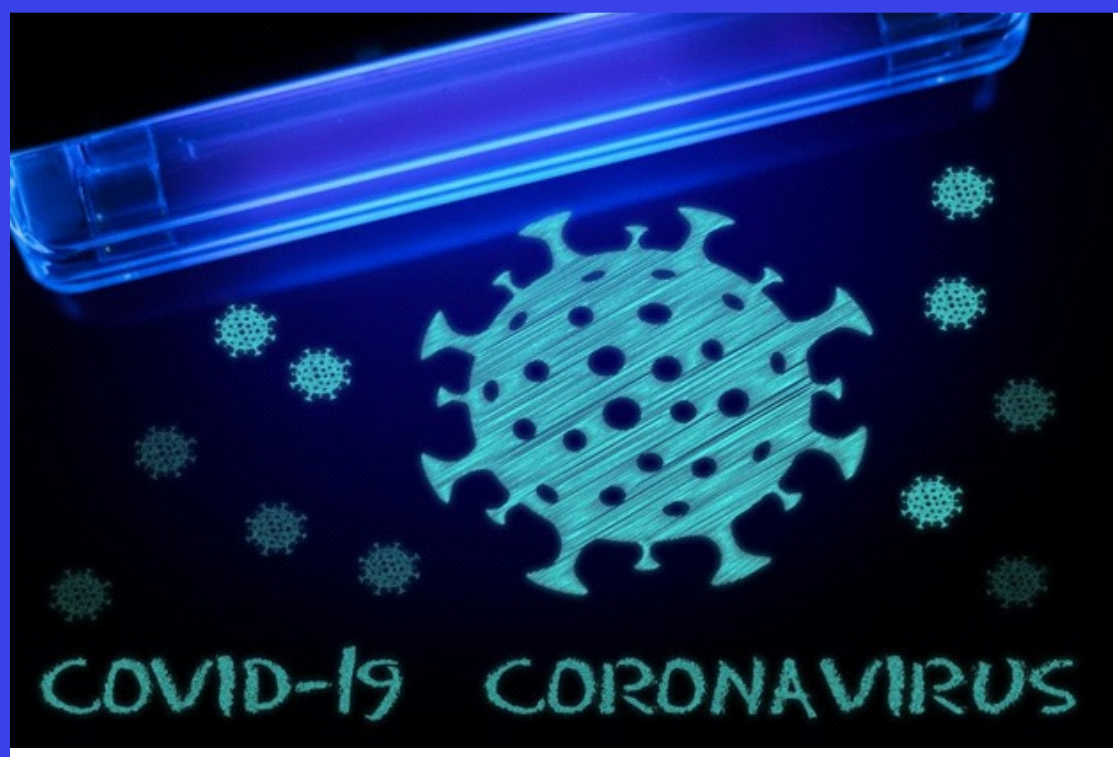
“There is currently no good solution for a UV-transparent electrode,” said Joseph Roth, doctoral candidate in Materials Science and Engineering at Penn State. “Right now, the current material solution commonly employed for visible light application is used despite it being too absorbing in the UV range. There is simply no good material choice for a UV-transparent conductor material that has been identified.”

Finding a new material with the right composition is key to advancing UV LED performance. The Penn State team, in collaboration with materials theorists from the University of Minnesota, recognized early on that the solution for the problem might be found in a recently discovered new class of transparent conductors. When theoretical predictions pointed to the material strontium niobate, the researchers reached out to their Japanese collaborators to obtain strontium niobate films and immediately tested their performance as UV transparent conductors. While these films held the promise of the theoretical predictions, the researchers needed a deposition method to integrate these films in a scalable way.

“We immediately tried to grow these films using the standard film-growth technique widely adopted in industry, called sputtering,” Roth said. “We were successful.”

This is a critical step towards technology maturation which makes it possible to integrate this new material into UV LEDs at low cost and high quantity. And both Engel-Herbert and Roth believe this is necessary during this crisis.

“While our first motivation in developing UV transparent conductors was to build an economic solution for water disinfection, we now realize that this breakthrough discovery potentially offers a solution to deactivate COVID-19 in aerosols that might be distributed in HVAC systems of buildings,” Roth explains. Other areas of application for virus disinfection are densely and frequently populated areas, such as theaters, sports arenas, and public transportation vehicles such as buses, subways, and airplanes.



Bengal Research Institutes Develop Low Cost Ventilators for COVID-19 Patient

Kolkata:

The CSIR-Central Mechanical Engineering Research Institute (CMERI), Durgapur, has developed a mechanical ventilator with indigenous technology which can be used for the treatment of COVID-19 patients and those experiencing breathing difficulty.

Portability and cost-effectiveness are the two most important features of the product, a senior official of the institute said. The mechanical ventilator developed by the institute will cost around Rs 90,000-1,00,000.

A ventilator is a device which works as an assistive oxygen supply support system when normal functioning of the lungs is disrupted owing to some infection.

Elaborating on the device, Director CSIR-CMERI, Durgapur, Prof (Dr) Harish Hirani said on Friday, "Its bellow design, controllers and embedded electronics have all been customised to ensure price efficacy as well as meeting the requirements of relevant industries.

"The ventilator has undergone multiple technical and design changes after adopting critical feed backs from healthcare professionals of Health World Hospital and Vivekananda Hospital, Durgapur."

The device will be further upgraded to meet the requirements of other patients, he said.

The mechanical ventilator was unveiled on June 3 after clinical trials at two hospitals.

Steadily the approach of the institute will be to harness Artificial Intelligence capabilities to automate the functioning of the mechanical ventilator, so that the device automatically responds to fluctuating variables of a patient, he said.

Chairman and Managing Director, Health World Hospitals Pvt. Ltd, Durgapur, Dr Arunangshu Ganguly, said, "The CSIR-CMERI in coordination with Critical Care Experts of Health World Hospitals developed the mechanical ventilator."

"Since the individual parts of the ventilator can be independently developed by different industries, mass-development of this unit will help a broad spectrum of industries."

“The reduced cost of the ventilators will help the economically marginalised sections of the society the most. This will also help in massive upgrading of the tertiary health care infrastructure of the nation."

Donut Robotics developed an internet-connected smart mask

Donut Robotics a Japanese startup has developed SMART MASK with features like transmitting messages and translate from Japanese into eight other languages.

This white plastic mask fits over standard face masks and connects via Bluetooth to a smartphone and tablet application that can transcribe speech into text messages, make calls, or amplify the mask wearer's voice.

Idea for the smart masks came while Donut Robotics' engineers working for a product that would help the company survive the coronavirus pandemic.

Donut Robotics built a prototype connected mask within a month by adapting translation software developed for its robot and a mask design that one of the company's engineers name Shunsuke -Fujibayashi created four years ago for a student project to interpret speech by mapping face muscles. The cost of one mask is about $40 around Rs. 3,000.

Mercedes-Benz Cars to Be Built on Nvidia Autonomous Driving Architecture

German luxury carmaker Mercedes-Benz has joined hands with semiconductor manufacturer Nvidia Corp, under which the latter will provide the Daimler owned automaker a chip and software platform that can be used for autonomous driving functions.

Under this partnership, Mercedes-Benz cars will come built on Nvidia's autonomous driving platform from 2024 onwards, claims the automaker.

As the automaker said, the new software-defined architecture will be built on Nvidia Drive platform and will be standard in Mercedes-Benz' next-generation fleet, enabling automated driving functionalities.

Commenting on this, Ola Kallenius, Chairman of the Board of Management of Daimler AG and Mercedes-Benz AG, said, “We are delighted to be able to extend our cooperation with Nvidia. Jensen and I know one another well and we have spent a great deal of time talking about the goals and potential of the next-generation vehicle computing architecture. This new platform will become an efficient, centralized and software-defined system in our future Mercedes-Benz vehicles.”

He also said, "Nvidia's AI computing architecture will help us streamline our journey towards autonomous driving. These new capabilities and upgrades will be downloaded from the cloud, improving safety, increasing value and extending the joy of ownership for all Mercedes-Benz customers.”

Mercedes-Benz and Nvidia have been already working together on autonomous driving and artificial intelligence car technology for over five years.

Jensen Huang, founder and CEO of Nvidia, said, “We are excited to work with Mercedes-Benz. It's the perfect partner for us given its long record of innovation and our strong technical relationship. It's clear from our extensive discussions with Ola and his team, that we share a common vision of the automobile of the future."

Boston Dynamics Spot Dog-Like Robots Now on Sale

Boston Dynamics an American engineering and robotics design company known for developing dextrous robots said that they started selling its four-legged Spot robots online for just under $75,000 approx. Rs. 57 lakh each unit.

The agile robots can walk, climb stairs, and observe their surroundings with cameras and other sensors. But people who buy them online must agree not to harm them or intentionally use them as weapons, among other conditions.

“The key goal for us is to make sure people trust robots,” Michael Perry, the company's vice president for business development, said in an interview with The Associated Press. “Somebody wanted to use Spot for a haunted house and we said no to that. It frames the robot in a negative context.”

The terms and conditions state that “Spot is an amazing robot, but is not certified safe for in-home use or intended for use near children or others who may not appreciate the hazards associated with its operation.”

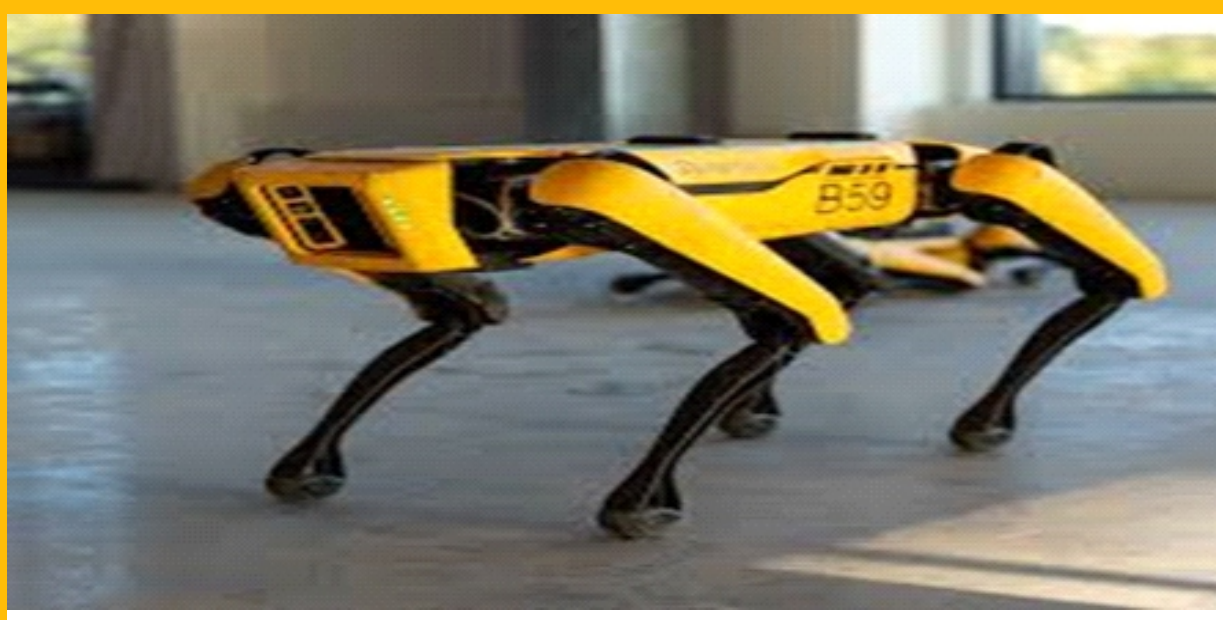
Perry said if a buyer violates the conditions, the company can nullify its warranty, decline to repair the robot and not renew its license, which would eventually cause the machine to deactivate.

Boston Dynamics has been developing its dexterous robots through decades of military-funded research. The Waltham, Massachusetts, company is now finding commercial applications for them for the first time since it was founded in 1992.

The company announced last year that it would begin mass production of Spot. As a pilot project, it leased more than 150 of the robots to select customers for such uses as monitoring construction sites, inspecting energy facilities and performing in theme parks. A human can operate the robots remotely, and in certain settings they can operate autonomously. The robots can run for about 90 minutes before they need recharging.

In one recent pilot in Singapore, a Spot robot was deployed in a public park to broadcast prerecorded messages asking people to maintain distance from one another to prevent spread of the coronavirus. It was also used to interview patients at a Boston hospital's COVID-19 triage center and check their body temperature and other vitals.

Boston Dynamics says its sales are intended for commercial and industrial users and that the robots can only be purchased in the US.

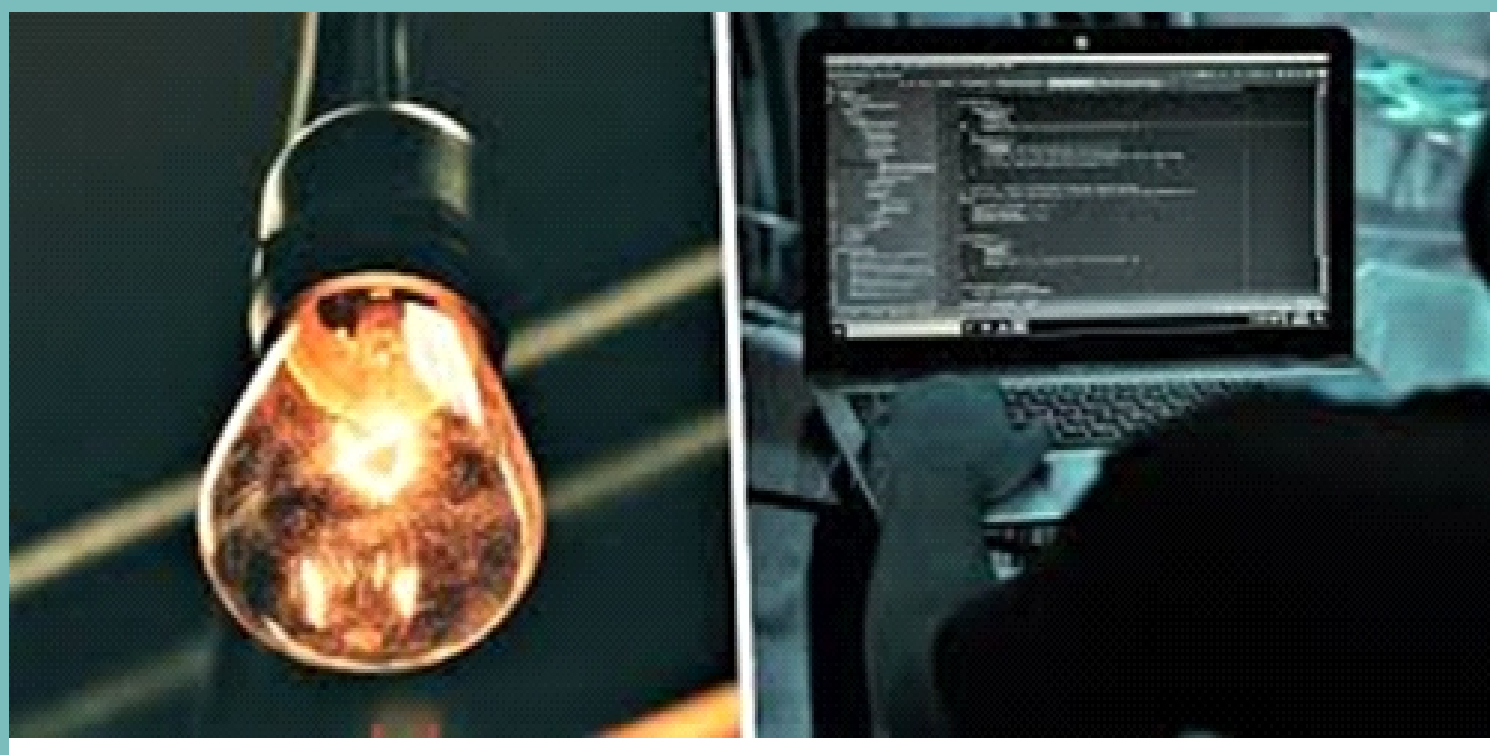


Hackers Can intrude on Your Conversations Using Light Bulbs

According to a study in Israel proves that hackers could use an ordinary or “dumb” light bulb to listen in on your conversations. If there is a hanging light bulb in close proximity of where the conversation is taking place. A conversation can be eavesdropped from 25 metres away. Recovering audio from optical signals obtained from afar has been named 'Lamphone'. It requires a remote electro-optical sensor that analyses a light bulb's frequency response with sound.

“Lamphone recovers sound optically via an electro-optical sensor which is directed at a hanging bulb,” the study reads. This means, for this type of attack to work, an electro-optical sensor is required. The researchers also pointed out that a telescope and a voice-to-text application like Google Speech are required as well.

Additionally, the range of this attack depends on the microscope and can be increased by using a bigger and more powerful microscope.



India has joined GPAI (Global Partnership on Artificial Intelligence)

India has joined the Global Partnership on Artificial Intelligence (GPAI) as a founding member to support responsible and human-centric development and use of Artificial Intelligence.

GPAI is an international and multi-stakeholder initiative to guide the responsible development and use of AI, grounded in human rights, inclusion, diversity, innovation, and economic growth.

The first-of-its-type initiative for evolving better understanding of challenges and opportunities around AI using the experience and diversity of participating countries, the alliance will look to bridge the gap between theory and practice by supporting advanced research and applied activities on AI-related priorities.

"In collaboration with partners and international organisations, GPAI will bring together leading experts from industry, civil society, governments, and academia to collaborate to promote responsible evolution of AI and will also evolve methodologies to show how AI can be leveraged to better respond to the present global crisis.

GPAI will be supported by a Secretariat, to be hosted by the Organisation for Economic Cooperation and Development (OECD) in Paris, as well as by two Centers of Expertise -- one each in Montreal and Paris. India recently launched National AI Strategy and National AI Portal, and has also started leveraging AI across various sectors such as education, agriculture, healthcare, e-commerce, finance, telecommunications.

"By joining GPAI as a founding member, India will actively participate in the global development of Artificial Intelligence, leveraging upon its experience around use of digital technologies for inclusive growth," the release added.

Qure.ai a Mumbai based startup developed an AI tool which can detect Covid – 19 lung infection in less than a minute

Mumbai-based Qure.ai has developed a solution that can interpret coronavirus-related lung abnormalities in seconds. This helps triage patients who need to be tested further for COVID-19 using a RT-PCR test.

With a population of 1.3 billion, India has relatively low cases of Covid-19- 33,050 infections and a death toll of 1,074. However, behind the numbers is a doubt on whether India is testing enough to be confident about the count. And, scaling up the number of tests is itself a challenge. So far, only one homegrown testing kit has been approved by the Indian Council of Medical Research (ICMR) and the imported kits are either faulty or delayed because of huge global demand.

Further, the traditional methods of testing each person take nearly eight hours and results come out within a day or two. In places like Delhi, where the number of testing has one up in the recent days, it is taking about 10 days in some cases to get a report. To help boost the testing process, Mumbai-based Qure.ai has developed an AI-powered solution which can classify patients as High, Medium or Low risk for Covid Covid-19 patients need consistent monitoring of lung infection by screening chest X-rays and Qure.ai's solution reads and interprets chest X-ray in seconds and identifies how much of the lung is infected.

“Our Chest X-Ray AI solution named qXR can help triage patients who need to be tested further for COVID-19 using a RT-PCR test. As many nations see a shortage of test kits, this can prioritize who needs to be tested and who needs to be asked to self-isolate,” said Prashant Warier, CEO .. and co-founder, Qure.ai told ET Digital.

Tracing Covid-19 abnormalities in seconds

According to Warier, qXR is capable of detecting ground-glass opacities (an area indicating hazy lung opacity), lung consolidation (when the small airways in the lungs are filled with something other than air) and other abnormalities that are indicative of Covid-19. It also gives metrics such as percentage of the volume and size of the lung affected by the abnormalities. qXR's algorithm then uses a compilation of the location, size and type of abnormalities and presents the results.

“By quantifying the extent of the lung infected, qXR can help objectively track disease progression, which can help measure response to different therapeutic approaches. This could help optimize treatment plans for patients at different stages of COVID-19, and also potentially help in drug discovery,” he said.

Google says Indian Gaming Industry to Cross $1 Billion Within Two Years

There are more than 300 million gamers in India at this time. Many of these gamers take part in gaming activities most days of the week. This in itself creates impressive potential for the Indian gaming industry.

To understand the full potential that the industry has, it's important to factor in other developments. This includes the rise of new technologies such as AI and Computer Vision. These technologies have established huge global markets in themselves. They are also starting to become a feature of game development, thereby having a significant impact on the gaming industry in India and internationally.

Overall, the future of the Indian gaming industry is bright and the market seems certain to continue expanding.

Globally, Android has over 2 billion active devices, and over 250 million apps are downloaded every day from the Play Store. There remains a huge opportunity for developers across the globe to develop successful and scalable businesses across the platform. In India, the developer ecosystem is on the rise. Google Play supports Indian developers throughout their lifecycle — from indie, to big-name.

According to a Google-KPMG report, 100+ online game developers are expected to be added in the next four to five years. The mission for Android and Google Play is to empower the game developer community through education, comprehensive support, and cutting-edge tools that enable them to carve out a path towards success and sustainability on Play.