



2026

NEWS LETTER

APRIL MONTH

IOT Society of India, Lucknow
www.iotsocietyofindia.com

About the Newsletter – IoT Society of India (ITSI)

The newsletter of the IoT Society of India continues to serve as an important platform for sharing knowledge, innovation, research, and emerging developments in the rapidly expanding field of the Internet of Things (IoT). Published regularly, the newsletter reflects the society's vision of building a strong and collaborative ecosystem connecting academia, industries, startups, researchers, professionals, innovators, and technology enthusiasts across India and beyond.

Registered under **Section 21** of the **Societies Registration Act – 1860** and **recognized by NITI Aayog, Government of India**, ITSI remains committed to promoting awareness, collaboration, research, and technological advancement in the field of IoT and allied technologies. Through this newsletter, the society highlights major activities, technical achievements, expert insights, chapter initiatives, research contributions, startup engagements, and upcoming opportunities for members and stakeholders.

The newsletter also showcases the efforts of ITSI's specialized divisions working in advanced and emerging domains such as Artificial Intelligence, Cyber Security, Data Science, Smart Cities, Healthcare Technologies, Robotics, Blockchain, Industrial IoT, Automation, Cloud Computing, and Digital Transformation. These divisions are continuously contributing towards creating a future-ready, innovation-driven, and technology-enabled ecosystem.

Apart from highlighting technological trends and innovations, the newsletter acts as a bridge between knowledge and practical implementation by encouraging collaboration among educational institutions, industries, government organizations, startups, innovators, and corporate sectors. It provides readers with updates on conferences, workshops, seminars, expert sessions, research activities, training programs, startup initiatives, and industry-academia partnerships organized under the banner of ITSI.

The **April 2026 Edition** continues this mission by bringing together insightful articles, expert contributions, organizational activities, innovation stories, and emerging opportunities in the IoT and digital technology sector. This edition emphasizes the growing importance of connected technologies, cybersecurity awareness, AI-driven solutions, startup innovation, and digital transformation initiatives shaping the future of society and industry.

The IoT Society of India strongly believes that knowledge-sharing, innovation, and collaboration are essential for technological growth and national development. Through this newsletter, ITSI aims to inspire innovation, encourage research, strengthen industry-academia collaboration, and empower the IoT community for building a smarter, safer, and more connected future.

Warm regards,

*The IoT Society of India Team
Connecting the Future, Today!*

How safe is India's critical national infrastructure?

Over the last few decades, critical infrastructure and services have been scaled up through automation, the Internet of Things and AI. However, this has also made them more vulnerable to attacks through IoT devices, highlighting the need for a policy framework to safeguard our infrastructure

Our everyday life depends on critical services that we often take for granted: water, electricity, cooking gas, petrol and diesel, groceries, banking, communications, transport, internet, healthcare, governance, law and order, courts and defence.



Behind each of these lies a vast network of infrastructure: power plants, refineries, distribution systems, fuel transportation networks, railway stations, airports, hospitals, public utility systems and industrial installations. Any disruption can affect public safety, economic stability and national security. Over the last few decades, these services have been scaled up through digital transformation.

The internet, automation, the Internet of Things (IoT), and artificial intelligence (AI) have improved monitoring, prediction, control and service delivery. However, the same connectivity that improves efficiency also expands the risk horizon. Systems that were earlier isolated or locally controlled are now linked to digital networks, creating opportunities for remote disruption.

Complexities of the digital landscape:

We are familiar with cyber risks in the digital world: server breaches, data theft, denial-of-service attacks, ransomware and online fraud. Governments have responded with cyber-security laws, certifications, protective systems and agencies such as CERT-In (Indian Computer Emergency Response Team). These measures have improved security, but they do not make critical infrastructure completely safe.

The larger emerging concern is that the internet is no longer only a network of people, computers and servers. It has expanded to accommodate billions of connected devices. Cameras, GPS devices, temperature and pressure sensors, wind monitors, water-level sensors and industrial controllers are constantly collecting data and communicating with central systems. In refineries, power plants, chemical plants, manufacturing units and transport networks, such devices enable high levels of automation.

Earlier, many of these systems were local process control systems managed through SCADA (Supervisory Control and Data Acquisition system). Today, they are increasingly connected to the internet for centralised monitoring, optimisation and predictive maintenance. This creates the important triad of IT, OT and IoT. IT operates in the digital space, processing data and enabling computing. OT, or operational technology, operates in the physical world of plants, machinery, transport, industrial automation and critical assets. IoT connects the two by sensing physical conditions, sending real-time data to digital systems and, in many cases, executing commands through controllers and actuators. This connection is powerful, but it can also become the weak link. If the IoT layer is compromised, the data collected from the physical world can be manipulated, or control over physical processes can be misused.



Critical infrastructure security :

Therefore, critical infrastructure security must go beyond conventional cyber security. Physical installations may have heavy security and restricted access, but the devices connecting them to digital systems may still expose them to invisible risks. The real question is whether these devices can be trusted. They must not contain hidden vulnerabilities, unauthorised data-sharing mechanisms, malicious control pathways or embedded Trojans that can be exploited later.

This issue becomes serious when imported devices are deployed in sensitive installations without rigorous scrutiny. India speaks strongly about Atmanirbhar Bharat and Made in India, but this intent has not always translated into procurement practices at lower levels of government departments and public sector undertakings (PSUs). Tender conditions often do not insist on trusted Indian-made products or deep security evaluation. Eligibility is frequently assessed through template-based compliance checks rather than careful examination of design origin, manufacturing authenticity and operational vulnerability. Existing IT guidelines and IoT policies are also not enforced with the seriousness required for national-level infrastructure.

Fuel transportation is a practical example. Earlier, tankers carrying fuel from oil terminals to retail outlets were protected with ordinary seals, locks and keys, leaving room for pilferage. Over time, the system moved to IoT-based keyless and OTP-based e-locking, supported by GPS tracking and digital monitoring. These solutions improve accountability and security, but they also become critical control points in the fuel supply chain. If vehicle tracking systems or e-locks are imported or unverified or dubiously certified, the oil supply chain can become vulnerable to remote disruption. There are increasing instances of electronic locks with GPS and communication capabilities that are manufactured in China getting certifications in India as an Indian product.

Need for strengthening certification :

The recent certification of cameras, by STQC tests devices ensures that they do not perform unintended control or data-sharing functions. However, the certification process is onerous and lengthy. More importantly, similar mechanisms are not yet available or strongly enforced for many other IoT devices used in critical infrastructure.

High level of awareness is needed for economic security. Future attacks may target the industrial base, supply chains, utilities and automated infrastructure that support national growth. A recent attack on systems that monitor U.S. gas stations' fuel storage, reported by CNN is a case in point.

As India moves toward becoming a major global economy and digitally empowered nation, the safety of critical infrastructure cannot be treated merely as a technical issue. It is a matter of sovereignty, resilience and economic security. India must embrace IoT, AI and automation, but it must do so with trust, transparency and strong safeguards. The need of the hour is stricter policy enforcement, rigorous certification, preference for trusted indigenous technologies and continuous vigilance across government and industry. The question is not whether we should adopt connected technologies, but whether we are deploying them securely enough to protect the nation's future.



About the Author

L.N. Rajaram is the National Division Chairman, IoT application in Government, Public, and Private Organisations, IoT Society of India. He is also Co-Founder , Kritilabs Technologies Pvt. Ltd.,Chennai

Courtesy:https://epaper.thehindu.com/ccidist-ws/th/th_international/issues/186568/OPS/GKKG0I80R.1+GROG1I6NS.1.html

Where Nature Meets Innovation: A New Blueprint for Human Flourishing

How India's 5,000-year-old forest school tradition holds the answer to today's learning crisis – and how nature-inspired robotics is the bridge back

Thousands of years before the first classroom was built, before the first exam was written, before the first child was ranked against another – there was the Gurukul. Deep in the forests of ancient India, students lived beside their Guru for twelve years, not within walls but beneath trees, beside rivers, under the open sky. .



Nature was not a backdrop to their education. Nature was the curriculum itself. And in the urgent, screen-saturated, anxiety-ridden world of today's young people, that ancient wisdom may be the most radical and necessary idea we can return to.

My work in nature-inspired robotics – building machines that learn from birds, insects, and living systems – has led me to an unexpected conclusion: the most advanced educational philosophy for the 21st century was already perfected in ancient India. The Gurukul system and modern biomimetic robotics are not opposites. They are the same truth expressed across millennia

The Forest Cure: Nature, Robots, and Mental Health

The Gurukul's insistence on seclusion in natural environments was not poetic – it was profoundly practical. The Guru knew what modern neuroscience has now confirmed: that the human nervous system was shaped by millions of years of life in natural environments, and that removing people from those

environments produces measurable cognitive and emotional deterioration. Anxiety, hyperactivity, loss of focus, depression – these are not character flaws in today's children. They are symptoms of a profound environmental mismatch.



Curiosity Is the Cure: From Scrolling to Self-Learning

Mobile addiction does not happen to curious children. It happens to bored ones – children who have been told that learning is sitting still, absorbing facts, and being compared to their peers. The Gurukul produced no such boredom, because in a forest there is no such thing as a dead end. Every question leads to three more.



Every observation opens a door. A child who has spent a morning studying why a dragonfly can hover in four directions and then builds a drone that tries – and fails, and tries again – has crossed into a state of intrinsic motivation that no algorithm can manufacture and no exam can measure.



About the Author

Mr. Rajesh Patanaik is a nature enthusiast and entrepreneur in Robotics and AI. His skills includes Robotics, Internet of Things (IoT), Team Building, Leadership, and Management. He has done B.Tech. in Mechanical Engineering and Advance Certification Program in IoT& Cloud computing from Indian Institute of Technology, Madras. He was a Scholar in Global Tech Initiative.org working on AI, ML & Product Management

How to become an IoT Member

Download requisite form from IoT website <https://iotsocietyofindia.com>.
Home > Download

Individual Membership

Print/Download Individual Membership Form (7) > Fill > Pay > Scan > Send

Institutional/Corporate Membership

Print/Download Institutional/Corporate Membership Form (6) > Fill from and details of authorized person > Nominate 3 faculty members to whom individual certificate to be issued > Pay > Scan > Send

Student Chapter Accreditation

Student Chapter – IoT Application Accreditation Form III > Fill form details > prepare list of min 50 students with under noted details > Pay > Scan Form III and send the Form with excel sheet of the students for printing certificates.

Note: The following documents are to be sent via email to iotsocietyofindia@gmail.com

Interesting Applications of IoT

IoTJi –Tussi Great Ho!

IoT enabled Intelligent Engines

Rolls-Royce is collaborating with Microsoft to transform the aerospace industry. The Rolls-Royce's Total Care Services is incorporating advanced analytics and IoT to aggregate data from disparate sources, integrate large quantities of airline operational data and apply smart data analysis capabilities and predictive tools to help airlines reduce fuel usage and fly routes more efficiently.

This information will also be useful for ensuring that the right teams and equipment are in place to optimally service the engines.

Courtesy: <https://www.clariontech.com/blog/10-cool-iot-applications-around-the-world>



IoT enabled smart agriculture

IoT enabled smart agriculture system, uses IoT and Big Data system and sensors to monitor the soil health, moisture levels, wind speed, solar radiation, rainfall, air and soil temperature, and leaf wetness and sends this data to farmers. The farmers can use this information to make more timely and accurate irrigation decisions.

Courtesy: <https://www.clariontech.com/blog/10-cool-iot-applications-around-the-world>



IoT enabled Virgin Atlantic

Do you know that every component of Virgin Atlantic's Boeing 787 is attached to a wireless airplane network? Per flight, the aircraft creates more than 1/3rd of a terabyte of data and gathers real-time IoT data on the flight performance, maintenance etc. With this, if there is even a small problem with, say, the engines, the ground staff knows about it even before the plane lands and the staff can make sure that the parts are ready before the plane lands. It has helped Virgin Atlantic in ensuring safer flights, lesser delays, and of course, happier customers.

Courtesy: <https://www.clariontech.com/blog/10-cool-iot-applications-around-the-world>



Funny & Creative IoT Applications

1. Smart Tea/Coffee Cup

A cup that sends a mobile alert:

"Your tea is getting cold!"

"Time for another coffee break!"

It can even track how many cups you drink during office hours.



2. IoT-Based Snooze Alarm Punisher

If you press snooze too many times:

Curtains automatically open

Room lights switch on

Speaker plays loud motivational quotes

Bed starts vibrating

Perfect for students and office-goers!



3. Smart Refrigerator with Attitude

The fridge detects repeated opening and says:

"You already checked me 5 minutes ago."

"No new food has appeared magically."

It can also recommend recipes from available ingredients.



"Yes, it's self-defrosting. It also does a daily inventory, searches for the best deal and runs over to the store for you."

4. Intelligent Plant Complainer

A plant pot that sends emotional notifications:

"I am thirsty."

"Too much sunlight today!"

"Please stop forgetting me."

Excellent beginner IoT project for students



Join IoT Society Membership

Unlock a world of opportunities with IoT Society of India membership!

- ♦ Professional Development: Access training, research, capacity building programs, and industry insights to propel your career forward. Stay ahead of emerging trends in your field!
- ♦ Networking Opportunities: Connect with users and experts in your domain for invaluable insights and resources. Expand your professional network and collaborate with like-minded individuals.
- ♦ Conferences, Workshops, and Events: Stay updated with the latest developments through engaging events. Participate in workshops, seminars, and online sessions led by industry leaders with years of experience.



Ready to be part of the future? Connect with us today!
Scan this QR code



Website: www.iotsocietyofindia.com

Email: iotsocietyofindia@gmail.com, iotsocietyofindia@rediff.com

Phone: +91-9839017309, 7080604446

Office Address: IOT Society of India, Lucknow D 315, Church Rd, Block D, Indira Nagar, Lucknow, Uttar Pradesh 226016.