



2026 **NEWS LETTER**

MARCH 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 serves as an important platform for sharing knowledge, innovation, research, and developments in the rapidly growing field of the Internet of Things (IoT). Published regularly, the newsletter reflects the society's vision of building a strong ecosystem that connects academia, industries, startups, researchers, professionals, 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** is dedicated to promoting awareness, collaboration, and technological advancement in emerging domains of IoT and allied technologies. Through this newsletter, the society highlights significant activities, technical achievements, expert insights, chapter initiatives, research developments, and upcoming opportunities for members and stakeholders.

The newsletter also showcases the role of ITSI's specialized divisions that focus on cutting-edge areas such as Artificial Intelligence, Cyber Security, Data Science, Smart Cities, Healthcare Technologies, Robotics, Blockchain, Industrial IoT, Automation, and Digital Transformation. These divisions contribute towards creating a future-ready and innovation-driven IoT ecosystem.

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

The **March 2026 Edition** continues this mission by bringing together informative articles, expert contributions, organizational updates, and emerging opportunities in the IoT sector. It reflects the society's commitment to **"Connecting the Future, Today"** by empowering the community with valuable insights and fostering meaningful engagement in the digital and connected world.

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

Most OT Environments Are Already Exposed : They Just Don't Know It Yet

By **Dr. Aniket S. Deshpande**, B.E. (CSE), M.Tech (CSE), Ph.D(CSE), DSc. (CSE), MBA (IT&SM)

In **2021**, an attacker gained access to the water treatment controls at a facility in Oldsmar, Florida, and attempted to increase sodium hydroxide levels to more than one hundred times the safe concentration. The entry point was not a sophisticated zero-day exploit. It was TeamViewer — a remote access tool installed on an operator workstation and left accessible. The operator noticed the cursor moving on his screen and intervened manually. That was the only thing that prevented a public health emergency.

The remote access pathway existed because someone needed operational convenience at the time, and nobody later questioned whether it should still exist.

That pattern appears across sectors with uncomfortable regularity.

A Las Vegas casino was breached through a smart aquarium thermometer connected to the corporate network for remote temperature monitoring. A German steel mill suffered physical damage to a blast furnace after attackers entered through the business network, moved laterally into industrial systems, and issued commands that appeared operationally legitimate until the equipment itself began failing. The Mirai botnet recruited hundreds of thousands of IP cameras, consumer routers, and networked industrial sensors into a global attack infrastructure — because those devices had never been inventoried, much less secured.

Different sectors. Different technologies. Same underlying problem: organizations frequently do not understand the true exposure surface of their connected environments. This is the real OT and IoT security challenge today. Not the theoretical threat of nation-state actors dismantling power grids — though Industroyer demonstrated that threat is entirely real — but the practical reality that most industrial environments carry connectivity that was never fully mapped and devices that were never fully governed. IIoT sensors deployed by operations teams optimizing throughput. Engineering workstations bridging network zones for convenience. Vendor remote access credentials never revoked after a service engagement closed. Building automation systems managing HVAC, access control, and energy infrastructure across shared network segments with no monitoring in place.

Each represents an exposure pathway. Most organizations could not list them accurately today. And in many environments, nobody owns that visibility problem end-to-end. In many plants, those assumptions may have existed for years without being revisited.

Addressing this in OT is harder than in enterprise IT because of the operational

constraint. A discovery tool routine in corporate networks can cause unexpected behavior in a Distributed Control System or a Programmable Logic Controller. The Triton attack on a petrochemical facility illustrated precisely how dangerous it is when IT security assumptions are applied to industrial environments without understanding what those systems actually do. What made it especially alarming was that the attackers targeted the safety instrumented systems themselves — the very mechanisms designed to prevent catastrophic physical failure — and the malware had been resident for an extended period before anyone detected it.



This is where passive visibility approaches become important. Rather than interrogating systems directly, they capture what is already happening — traffic between assets, communication patterns, deviations from established process baselines. When an engineering workstation begins communicating with a controller it has no process reason to contact, or a sensor transmits outside its normal cycle, those deviations surface without anyone touching the underlying system. No disruption. No additional risk introduced by the security tool itself.

In several environments, teams discover legacy engineering laptops or forgotten remote-access pathways only after passive monitoring is deployed. Until then, those assets are simply assumed to be inactive.

After the Colonial Pipeline attack in 2021, investigators found the entry point was a legacy VPN account with no multi-factor authentication — an account not in active use and never formally decommissioned. The organization did not know it was exposed because neither the credential nor the access pathway was being actively monitored. The attacker did not need to be clever. The environment had already done the work for them. The IoT layer compounds this. As smart sensors, connected building systems, and industrial IoT devices proliferate, the asset surface grows faster than most inventory and governance processes can track. Mirai demonstrated what happens when that surface remains unmanaged at scale. It is not an abstract risk. It is a demonstrated outcome.

Regulators, cyber insurers, and critical infrastructure oversight bodies are increasingly requiring organizations to demonstrate a defensible understanding of their industrial environments — not as an aspirational capability, but as a baseline expectation. The question has moved from "do you have security tools?" to "can you show us what your environment actually looks like and whether it is behaving as designed?"

For a significant number of organizations, that question remains genuinely difficult to answer.

The organizations making meaningful progress are usually not the ones starting with the most advanced detection platforms. They are starting with an accurate picture of what is connected, what it is communicating, and whether that behavior is consistent with what the plant actually requires.

Without that foundation, most security discussions in OT become architecture diagrams disconnected from operational reality.



Dr. Aniket S. Deshpande

*Co-Founder & Chief Operating Officer, DefenXee Private Limited,
Board Member – Alterego Technology, Visiting Faculty
Organization/Institution: DefenXee*

Aniket Deshpande is a cyber-security and technology leader specializing in OT/ICS security, Zero Trust architecture, AI governance, and cyber resilience. He is the Co-Founder & COO of DefenXee. He has previously held leadership roles at Broadcom (Symantec), Zscaler, Riverbed, IBM, and Accops across global cybersecurity and enterprise transformation initiatives. He is also a life member of IoT Society of India, Fellow IETE, Sr Member IEEE, Member ISACA, etc.

Email Address: aniket@drdeshpande.in / anik.deshpande@gmail.com

Interesting Applications of IoT

IoT Ji – Tussi Great Ho!

IoT enabled Kitchen Table

A kitchen table which you can use to check your emails and phone calls make video calls, and it comes with integrated charging and syncing capabilities. An oven which is controlled by a Smartphone app, allows you to monitor the cooking with a live video stream, and sends notifications to your mobile device once the food is cooked. A fridge that detects the items inside and their expiration date and give you suggestions on how to use the groceries before they go bad. All such things may seem like objects from some sci-fi movie, right? Well, these are actual devices which will be soon hitting the stores for all of us to use. Thanks to IoT, what was yesterday's fantasy is today's reality.

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



IoT enabled Wristband

While Apple Pay verifies the payments using fingerprints, the IoT enabled wristband uses your heartbeat for that. It uses your “unique cardiac rhythm” to verify your identity. As long as you wear the band in your hand, the authentication is active and it is automatically deactivated when the band is removed from your hands. Forget about carrying your wallet when you go for a run but that will not stop you from shopping for a can of milk on your way back though – as far as you are wearing IoT enabled wristband.

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



IoT enabled Infant Monitor

This infant monitor uses sensor technology and gives parents insight into their baby's sleep. It provides them real-time information about their baby's breathing patterns, body temperature, body position, activity level, and early warnings – all on their smart phones.

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



The Advisory Panel Members

Sr. No.	Advisory Panel Members
1	Dr. Subimal Kundu, M.Com., Ph.D., Ex CEO, Management & Computer Services, Patron & Fellow, Computer Society of India, Kolkata
2	Dr. Brijendra Kumar Saxena, Ph.D., Retired Founder Principal of Tolani Maritime Institute, Talegaon, Pune, Maharashtra
3	Dr. Shreedhar A. Joshi, Professor and Head, Department of Electronics and Communication, SDM College Of Engineering & Technology, Dharwad, Karnataka
4	Prof. Vineet Kansal, Director, Indian Institute of Information Technology, Pune, Maharashtra & Ex Director, Institute of Engineering & Technology (IET), Lucknow, Uttar Pradesh
5	Prof. (Dr.) Neelendra Badal, Professor, Department of Computer Science & Engineering, Kamla Nehru Institute of Technology, (KNIT), Sultanpur (U.P.), affiliated to Dr A.P.J. Abdul Kalam Technical University (AKTU), Lucknow UP (On-Leave) and presently Director of Rajkiya Engineering College, Bijnor, Uttar Pradesh
6	Dr. Ghanshyam Singh, Professor, Department of Electronics & Communication Engineering, Malaviya National Institute of Technology, Jaipur, Rajasthan
7	Dr. Amiya Kumar Tripathy, Professor & Dean (Research & Innovation), Computer Engineering Department, Don Bosco Institute of Technology (DBIT), Mumbai, Maharashtra

IoT Society of India, Lucknow Chapter Management Committee Members

Immediate Past Chairman	Shri Harish Chandra Gupta, Senior Consultant, Uptron Powertronics Limited & Ex-Senior Manager (Systems), Uttar Pradesh Development Systems Corporation (UPDESCO), a U.P. Government Undertaking, Lucknow
Chairman	Dr Rohitashwa Pandey, Associate Professor, Head of Department (CSE), Bansal Institute of Engineering and Technology (BIET) , Lucknow
Vice Chairman cum Chairman-elect	Mr Pankaj Kumar Agarwal, Founder & CEO, Docket Care System, Lucknow
Secretary	Mr Puneet Pandey, Manager, Maharishi University Incubation Centre, Lucknow
Treasurer	Mr Vineet Garg, Director, ADRI Technosoft Pvt. Ltd., Lucknow
Management Committee Members	Dr Shahnaz Fatime, Associate Professor, Amity Institute of Information Technology, Amity University, Lucknow, Uttar Pradesh
	Mr Dheeraj Jotwani, Founder & Director, Urbanelinks Private Limited, Lucknow
	Mr Rafaqat Jalil, Skynet Digital solution, Lucknow
	Ms Ayati Mishra, Freelance Biotechnologist, Lucknow
IoT/AI School Coordinators	Mrs Awanti Mishra, Project Based Learning Leader (AI), City Montessori School, Lucknow
	Mrs Preeti Saxena, Coordinator (AI), City Montessori School, Lucknow

Divisional Chairpersons of 16 Divisions of the IoT Society of India

Division1: *Internet of Things (IoT) & Internet of Everything (IoE).*

Chairperson: Dr. Aditya Dubey, Department of Cyber Security & Digital Forensics, Assistant Professor, National Forensic Sciences University, Jaipur, Rajasthan

Division 2: *Artificial Intelligence, Machine Language, Cloud and Edge Computing.*

Chairperson: Dr. K. Dasaradharami Reddy, Associate Professor & Head, Dept. of Computer Science & Engineering, Navodaya Institute Of Technology (Autonomous), Raichur, Karnataka.

Division3: *Data Science, Data and Cyber Security ,Quantum Technology*

Chairperson: Dr Aniket Satish Deshpande, Ph.D. (CSE), DSc. (CSE), MBA, Co-Founder, COO and Executive Director, DefenXee Private Limited, Pune, Maharashtra

Division 4: *IoT application in Health (IoHT), Life Science and Biomedical Engineering*

Chairperson: Prof. (Dr.) Shubhajit Roy Chowdhury, Professor, School of Computing and Electrical Engineering, Indian Institute of Technology, Mandi, Himachal Pradesh

Division5: *IoT application in the Educational Sector.*

Chairperson: Dr. Umakant D Butkar, Associate Professor, Department of Computer Engineering, Guru Gobind Singh College of Engineering and Research Centre, Nashik, Maharashtra

Division6: *IoT application in Industries–Industrial IoT.*

Chairperson: Dr. M. V. N. Srujan Manohar, Department of Internet of Things, Malla Reddy University, Hyderabad, Telangana

Division7: *IoT application in Government, Public and Private Organizations*

Chairperson: Dr. L.N. Rajaram, Co-Founder and Director, Kriti labs Technologies Pvt. Ltd., Chennai, Tamil Nadu..

Division 8: *IoT application in Banking, Financial Services, and Insurance (BFSI).*

Chairperson: Mr. Sushant Kataria, Product Owner, Tata Consultancy Services, Gurugram, Haryana

Division9: *IoT application in Law and Law enforcement.*

Chairperson: Dr. Aman Deep Singh, Associate Professor, Dr. Ram Manohar Lohiya National Law University, Lucknow. Uttar Pradesh

Division 10: *IoT application in Smart City / Transportation, Smart Hospitality, Smart Agriculture, etc.*

Chairperson: Dr. Anbunathan Ramaiah, Co-founder and CEO, Digitaltransols AI Private Limited, Bengaluru, Karnataka

Division11: *IoT application in Defense, Aeronautics and Marine.*

Chairperson: Prof. (Dr.) Subrata Mohan Paul, Independent Director, registered with the Ministry of Corporate Affairs, Govt. of India & Academic Counselor, IGNOU, Kolkata, West Bengal

Division12: *Information and Communication Technology (ICT).*

Chairperson: Dr. Dilip S. Aldar, Associate Professor, Electronics Engineering and Telecommunication, K B P College of Engineering, Satara, Maharashtra

- Division 13:** Research, Entrepreneurship, Startups, Innovation & Skill Development.
Chairperson: Dr. S. Hemalatha, PhD, DSc., Professor/CSBS, Panimalar Engineering College, Chennai, TamilNadu
- Division 14:** Robotics, Cobotics & Autonomous Systems, Blockchain Technology.
Chairperson: Mr. Rajesh Patanaik, Head, BiSy Hub, Berhampur, Odisha
- Division 15:** Cognitive Computing, Social Sensing, Cognitive IoT and Human-Computer Interfaces.
Chairperson: Dr. Ranjana Rajnish, Associate Professor, Amity Institute of Information Technology(AIIT), Amity University, Lucknow, Uttar Pradesh
- Division 16:** Computer Vision, AR/VR, Speech, Video & Text Analytics, Image Processing.
Chairperson: Dr. Vasantha Kumara M, Associate Professor, Department of Computer Science and Engineering, Government Engineering College, Hassan, Karnataka

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: iotsocietyofindia1@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.