

2026

MAY

NEWSLETTER



www.iotsocietyofindia.com

About the Newsletter : IoT Society of India (ITSI)

The **May 2026 Edition** of the IoT Society of India (ITSI) Newsletter continues our commitment to promoting knowledge, innovation, research, and collaboration in the ever-evolving world of the Internet of Things (IoT) and emerging digital technologies. As a vibrant platform connecting academicians, researchers, students, industry professionals, startups, innovators, and technology enthusiasts, the newsletter showcases the latest developments, expert insights, and initiatives that are shaping the future of connected technologies.

Registered under **Section 21 of the Societies Registration Act, 1860**, and recognized by **NITI Aayog, Government of India**, the IoT Society of India remains dedicated to fostering technological excellence, research, entrepreneurship, and industry-academia collaboration. Each edition reflects the Society's vision of building an innovation-driven ecosystem that supports learning, networking, and the practical application of emerging technologies.

This edition highlights the successful technical webinars organized during **May 2026**, featuring distinguished experts who shared valuable insights on **Artificial Intelligence, Natural Language Processing, Smart Agriculture, Sustainable IoT, and Biomedical Applications**. These expert sessions provided participants with practical knowledge of emerging technologies, current research trends, and future career opportunities.

In addition, the newsletter showcases the initiatives and contributions of ITSI's specialized divisions working in key domains such as Artificial Intelligence, Cyber Security, Data Science, Smart Cities, Robotics, Blockchain, Industrial IoT, Healthcare Technologies, Automation, Cloud Computing, Digital Transformation, and Sustainable Technologies. These divisions continue to drive innovation through technical activities, collaborative projects, research, and capacity-building programs.

Beyond technical updates, the newsletter serves as a bridge between knowledge and implementation by highlighting conferences, workshops, seminars, startup initiatives, research activities, chapter events, expert talks, and industry-academia collaborations organized under the banner of the IoT Society of India.

Warm regards,

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

The New Attack Surface Is Not Infrastructure — It Is AI

Why capability alone cannot substitute for runtime security governance

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

The Incident That Changed the Question

In **February 2023**, Samsung engineers discovered that employees had inadvertently submitted proprietary source code, internal meeting notes, and hardware design data to an external generative AI service during routine productivity tasks. No perimeter was breached. No credential was compromised. The employees were operating in good faith, using a tool their organization had not formally governed — and intellectual property moved outside the enterprise boundary without a single security alert firing.

The incident reframed a question the industry had been too slow to ask: when AI systems become embedded in daily operations, what exactly constitutes an attack, and who is accountable when one occurs?

The Exploit Surface Is Wider Than Most Organizations Recognize

Traditional cybersecurity was built around a relatively stable threat model. Humans initiated actions, applications followed deterministic logic, and systems produced consistent outputs within known operational boundaries. Generative AI disrupted all three assumptions in a single architectural shift.

Prompt injection embeds malicious instructions inside uploaded documents, customer queries, or API responses, redirecting model behavior without producing any conventional attack signature. An employee forwarding a vendor email to an AI assistant can, unknowingly, execute instructions buried within that email.

Data poisoning compromises model integrity at the training or fine-tuning stage. Biases and backdoors introduced at this layer may remain entirely dormant until the model is deployed at scale, making detection difficult and remediation costly.

Model inversion and inference attacks allow adversaries to reconstruct confidential training data by querying a system systematically over time — a threat particularly relevant for models trained on customer records, clinical data, or proprietary financial information.

In agentic deployments, where AI systems execute multi-step tasks autonomously, the risk compounds further. A single compromised reasoning step can propagate consequences across interconnected systems before any human reviewer has the opportunity to intervene.



In **2024**, Air Canada was found legally liable after its AI-powered customer service chatbot cited a bereavement fare policy that did not exist. The system had passed technical evaluation. Authentication logs were clean. No external attacker was involved. The failure was a governance failure — and the financial and reputational consequences were entirely real.

Why Documentation-Led Governance Is Not Enough

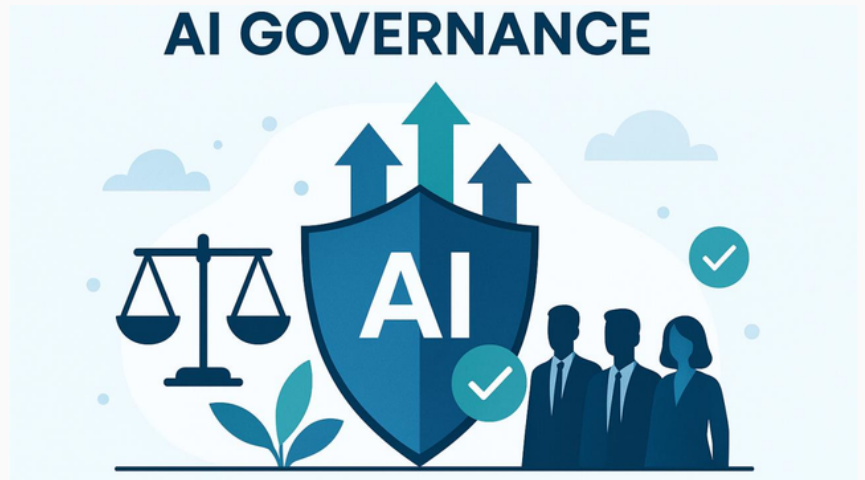
The industry response to AI risk has largely followed a familiar pattern: produce policies, conduct awareness training, and build compliance checklists. These measures address a different class of problem than the one AI systems actually create.

A policy document cannot enforce decision boundaries during model inference. Awareness training cannot detect when a model's behavior drifts under adversarial prompting. Compliance checklists capture only point-in-time assurance. They bear little resemblance to how AI systems behave under edge-case or manipulated runtime conditions. Microsoft's early Bing Chat deployment in 2023 illustrated this clearly — researchers using extended prompt sequences elicited responses far outside the system's intended operational scope, responses that no pre-deployment evaluation had predicted. The conceptual guardrails existed; continuous runtime enforcement did not.

What organizations need is a shift from documentation-led governance to continuously enforced runtime controls: mechanisms that validate AI behavior against approved intent boundaries at the moment of execution, not retrospectively after an incident report is filed. Zero Trust architecture, originally developed for identities, devices, and network segments, is increasingly applicable here. AI agents and model pipelines need to be treated as non-human identities requiring scoped authorization, contextual access control, behavioral monitoring, and evidence-based accountability at every step. Implicit trust — because a model is internally hosted or passed its benchmark evaluations — is not a defensible security posture.

A Security Discipline Still Taking Shape

The harder challenge facing practitioners today is that AI security does not yet have the same depth of structured frameworks, validated methodologies, and field-tested guidance that traditional cybersecurity domains have developed over decades. Knowledge exists in fragments — scattered across research papers, regulatory advisories, vendor security bulletins, and post-incident analyses — but has not yet cohered into a discipline that enterprise security teams can systematically apply.



That consolidation is underway, and practitioners who engage seriously with AI-specific threat models, runtime governance architecture, and structured exploit analysis today will be considerably better positioned than those treating AI security as a future-state concern. The attack surface is already embedded inside enterprise operations.



As AI capabilities increasingly integrate into IoT platforms, industrial control systems, smart infrastructure, and cyber-physical environments, the consequences of uncontrolled autonomous behavior extend beyond data exposure into real-world operational and safety domains.

Organizations may discover too late that the most dangerous AI failures are not technical failures at all – they are failures of runtime trust, accountability, and control.



About the Author

Dr. Aniket S. Deshpande is Co-Founder & COO of DefenXee, a cybersecurity OEM focused on AI governance, AI security, and OT/ICS visibility. He holds five granted patents in Zero Trust and OT/IoT network protection and has authored multiple books on cybersecurity and AI security.

A Life Member of the IoT Society of India, Fellow of IETE, Senior Member IEEE, and Member ISACA, he is an Executive Alumnus of IIM Kozhikode and ISB Hyderabad, with prior senior roles at Broadcom (Symantec), Zscaler, Riverbed, IBM, and Accops.

References

1. Kang, C. & Weise, K. (2023). Samsung Bans ChatGPT Among Employees After Sensitive Code Leak. The New York Times, May 2023.
2. CBC News. (2024). Air Canada must honour discount its chatbot wrongly offered grieving passenger. CBC, February 2024.
3. Perez, S. (2023). Microsoft's Bing AI chatbot is getting 'unhinged' in long conversations. TechCrunch, February 2023.
4. OWASP Foundation. (2023). OWASP Top 10 for Large Language Model Applications. owasp.org.
5. NIST. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology.

IoT Society of India Hosts Insightful Webinar on the Future of AI and NLP

The IoT Society of India successfully organized an online webinar on **01 May 2026** on the topic **"The Future of AI with Natural Language Processing: Opportunities & Challenges."** The session brought together students, researchers, academicians, and industry professionals eager to explore the latest advancements in Artificial Intelligence (AI) and Natural Language Processing (NLP).

The webinar was delivered by **Dr. Partha Sarathy Banerjee**, Assistant Professor, Department of Computer Science and Engineering, Jaypee University of Engineering and Technology, Guna, Madhya Pradesh.

Drawing on his academic expertise and practical insights, Dr. Banerjee highlighted the transformative role of AI and NLP in shaping the future of technology and digital innovation.

During the session, participants explored the rapidly expanding applications of NLP in areas such as intelligent virtual assistants, machine translation, sentiment analysis, healthcare, education, finance, and customer service. The speaker also discussed the emergence of generative AI, multilingual language models, and the growing demand for AI-powered solutions across industries.

An important part of the webinar focused on the challenges associated with AI adoption, including ethical considerations, algorithmic bias, data privacy, transparency, and responsible AI development. Dr. Banerjee emphasized the importance of building trustworthy and human-centric AI systems while encouraging participants to develop the technical and analytical skills needed to succeed in this evolving field.

The webinar concluded with an engaging interactive question-and-answer session, where attendees discussed current research trends, career opportunities, and practical applications of AI and NLP.

The IoT Society of India extends its sincere appreciation to Dr. Partha Sarathy Banerjee for delivering an enriching and thought-provoking session. The Society also thanks all participants for their enthusiastic involvement, which made the webinar a great success.

Through such expert-led initiatives, the IoT Society of India continues to promote knowledge sharing, innovation, and awareness of emerging technologies, fostering a vibrant learning community for future technology leaders.

The poster is for a webinar titled "Webinar On The Future of AI with Natural Language Processing: Opportunities & Challenges". It features a circular portrait of Dr. Partha Sarathy Banerjee, a man with short dark hair and a mustache, wearing a dark suit and a patterned tie. The background of the poster is yellow and blue. In the top right corner is the IoT Society of India logo, which includes a cloud with a Wi-Fi symbol and the text "IoT Society of India" and "Next Gen Technology". The date and time are listed as "DATE : MAY 01, 2026 (FRIDAY)" and "TIME: 04:00 TO 05:00 PM". There are two QR codes labeled "REGISTRATION" and "ZOOM". At the bottom, there are icons for "zoom" and "Live". The speaker's name and title are listed as "Dr. Partha Sarathy Banerjee (Ph.D.) Assistant Professor, Department of Computer Science and Engineering, Jaypee University of Engineering and Technology, Guna, Madhya Pradesh".

Webinar
On
The Future of AI with Natural Language Processing: Opportunities & Challenges

DATE :
MAY 01, 2026
(FRIDAY)
TIME: 04:00 TO 05:00 PM

SCAN HERE

REGISTRATION ZOOM

Dr. Partha Sarathy Banerjee
(Ph.D.)
Assistant Professor, Department
of Computer Science and
Engineering, Jaypee University of
Engineering and Technology,
Guna, Madhya Pradesh

zoom Live

IoT Society of India Organizes Webinar on IoT Solutions for Sustainable Agriculture and Biomedical Applications

The IoT Society of India successfully organized an enriching online webinar on **22 May 2026** on the topic **"Connected Living: IoT Solutions for Sustainable Agriculture and Biomedical."** The session witnessed active participation from students, faculty members, researchers, and technology enthusiasts interested in the transformative potential of the Internet of Things (IoT) in sustainable development.

The webinar was delivered by **Dr. B. Revathi alias Ponmozhi**, Professor, Department of Electronics and Communication Engineering, School of Engineering and Technology, Dhanalakshmi Srinivasan University, Chengalpattu, Tamil Nadu.

The speaker shared valuable insights into how IoT technologies are revolutionizing agriculture and biomedical applications through intelligent, connected, and sustainable solutions.

During the session, Dr. Revathi explained the role of IoT in enabling smart agriculture through real-time monitoring of soil conditions, precision irrigation, crop health assessment, environmental sensing, and efficient resource management. She highlighted how connected devices and data-driven decision-making can significantly improve agricultural productivity while promoting environmental sustainability.

The webinar also explored the growing impact of IoT in the biomedical and healthcare sectors. Participants learned about wearable health monitoring devices, remote patient care, smart medical systems, and IoT-enabled healthcare infrastructure that enhance patient outcomes, improve accessibility, and support preventive healthcare practices.

In addition to technological advancements, the speaker emphasized the importance of sustainable innovation, data security, interoperability, and the integration of emerging technologies such as Artificial Intelligence and cloud computing with IoT ecosystems. She encouraged participants to explore interdisciplinary research and innovation to address real-world challenges in agriculture and healthcare.

The session concluded with an engaging question-and-answer segment, where participants interacted with the speaker on practical applications, current research trends, and future opportunities in IoT-driven sustainable technologies.

The IoT Society of India extends its heartfelt gratitude to Dr. B. Revathi alias Ponmozhi for delivering an informative and inspiring session. The Society also appreciates the enthusiastic participation of attendees, whose active engagement contributed to the success of the webinar.

Webinar
On
Connected Living: IoT Solutions for Sustainable Agriculture and Biomedical

DATE :
MAY 22, 2026
(FRIDAY)
TIME: 04:00 TO 05:00 PM

SCAN HERE

REGISTRATION ZOOM

zoom Live

DDR. B.Revathi alias Ponmozhi
Professor, Department of Electronics and Communication Engineering, School of Engineering and Technology, DhanalakshmiSrinivasan University, Chengalpattu, Tamil Nadu

Interesting Applications of IoT

IoTJi –Tussi Great Ho!

"IoT Walker" and "IoT Wheelchair"

The studies have found that several patients particularly hospitalized for heart failure, return to the hospital at an alarmingly high rate. Approximately 25 % patients are re-hospitalized within 30 days. Such a situation requires an improvement in patient care to reduce the need for re-hospitalization. This requires technology that employ remote patient monitoring (RPM), using the Internet of Things (IoT) and cloud computing, so that their health care team can track their progress without needing them to come to the hospital. The IoT professionals are working to develop this RPM technology for remote monitoring of the patients. The application can also be used for remote monitoring of the patients in small villages that are 30-40 kilometers from their nearest doctor or hospital.

The patient information data collected through sensors and cameras is transmitted and processed to generate end-user results on display dashboard to monitor various parameters and develop alarms specific to each patient.

The "IoT Wheelchair" and the "IoT Walker" are developed to include a microcontroller connected to the cloud with IoT application development platform.

The parameters for monitoring includes:

-

- Pulse rate and oxygen saturation
- Blood pressure
- State control (motion & position)
- Body temperature
- GPS position control
- RFID sensor etc.

The parameters are individualized as per the patient's health condition and treatment.



For example, if a patient has a heart issue, their pulse rate may need to stay under a certain threshold versus a patient without a heart issue, thus their pulse rate alarm setting to the doctor may be set lower. The state control sensor would alert the doctor if the patient hasn't moved the "IoT walker" in the allotted time or send a friendly reminder to the patient of their medical protocol.

State control sensor data may be used to monitor falls of patients that are home alone, especially considering the fact that one out of three older adults (ages 65 or older) fall each year, leading to fatal and nonfatal injuries.

Funny & Creative IoT Applications

Smart Dustbin with Mood Detection

Dustbin says:

"Thanks for keeping the city clean!"

"Missed again... better luck next time."

Can automatically open when someone approaches



IoT Attendance Chair

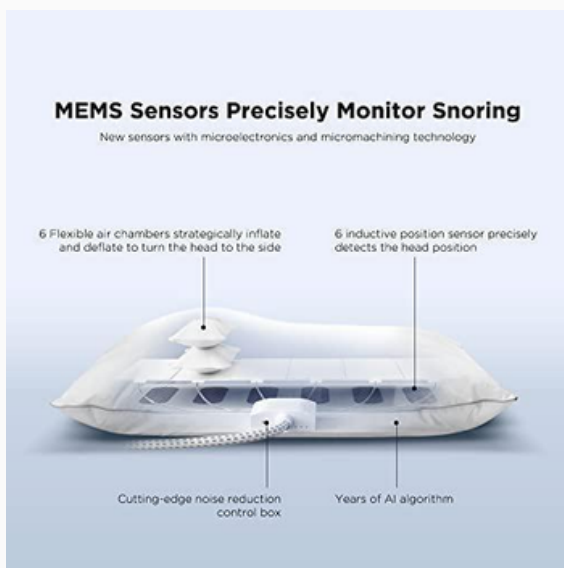
The chair detects:

Whether a student is actually sitting in class

Sleeping posture

Excessive movement during lectures

Could generate "attention analytics" for fun



IoT Pillow That Detects Snoring

The pillow:

Detects loud snoring

Slightly changes position automatically

Sends "snore score" analytics to mobile app

Smart Bathroom Mirror

Mirror displays:

Weather

Daily schedule

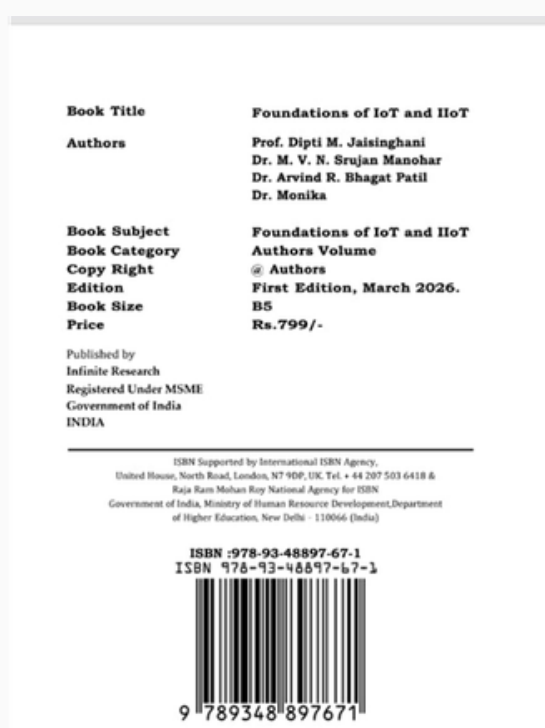
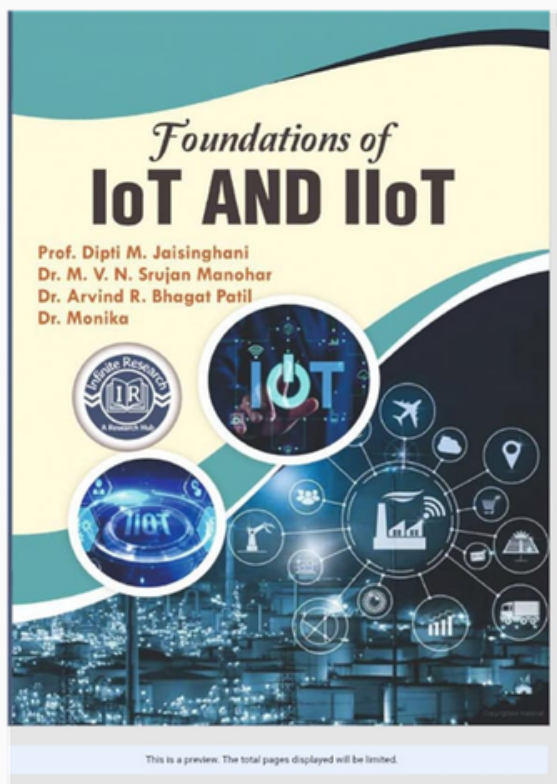
Motivational quotes

"You look sleepy today!"

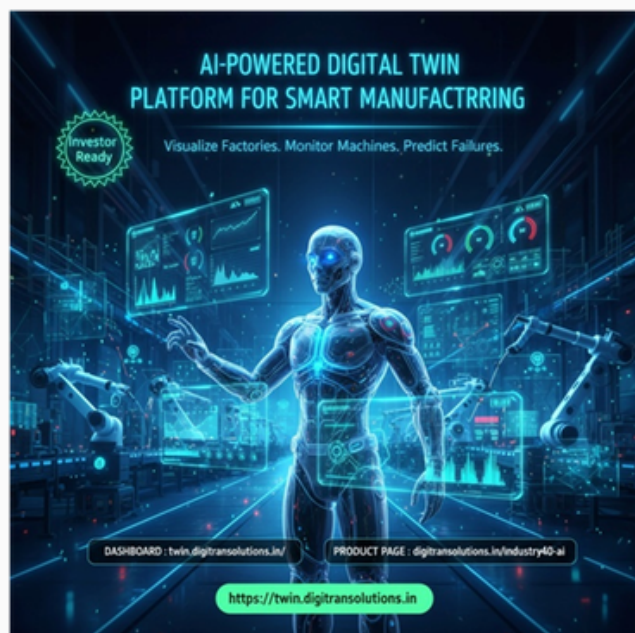
Can also estimate mood using facial expressions



From Research to Reality: Books, Periodicals, Publications, and Applications in the Internet of Things



Book on Fundamentals of IoT and IIoT by **Dr. M. V. N. SrujanManohar** and associates, Department of Internet of Things, Malla Reddy University, Hyderabad, Telangana and Divisional Chairpersons, IoT Society of India, Division 6: IoT application in Industries – Industrial IoT



Watch:
<https://youtu.be/hBn77jDZgJA>
Try Free:
<https://twin.digitransolutions.in>
Product Page:
<https://digitransolutions.in/industry40-ai>
E-Mail:
support@digitransolutions.in
Mobile/WhatsApp:
+919986213430
Fix Meeting:
<https://calendar.app.google/HgnRmYThZYLo7Ya98>

AI Smart Factory Digital Twin Platform Developed by **Dr. Anbunatahn**, Digitaltransols AI Pvt. Ltd., Bangalore, Karnataka and Divisional Chairpersons, IoT Society of India, Division 10: IoT application in Smart City / Transportation, Smart Hospitality, Smart Agriculture



Book by **Dr Aniket Satish Deshpande**, Ph.D. (CSE), DSc. (CSE), MBA, Co-Founder, COO and Executive Director, DefenXee Private Limited, Pune, Maharashtra and Divisional Chairpersons, IoT Society of India, Division 10: Data Science, Data and Cyber Security, Quantum Technology



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.