CURRENT TRENDS IN INTERNET OF THINGS (IOT) AND SMART TECHNOLOGIES: A COMPREHENSIVE REVIEW

K. Kasturi and Y. Kalpana

Applied Computing and Emerging Technologies,

Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamil Nadu

Corresponding author E-mail: kasturi.scs@vistas.ac.in, kalpana.scs@vistas.ac.in

Abstract:

The rapid evolution of the Internet of Things (IoT) has transformed traditional systems into intelligent, interconnected smart environments. IoT, combined with emerging smart technologies such as artificial intelligence (AI), edge computing, big data analytics, and cloud platforms, has enabled innovative applications across healthcare, smart cities, industrial automation, agriculture, and transportation. This review paper presents a comprehensive overview of current trends in IoT and smart technologies, highlighting recent advancements in architectures, communication protocols, data analytics, and security mechanisms. Furthermore, it discusses key challenges including scalability, interoperability, privacy, and energy efficiency, and outlines future research directions for sustainable and intelligent IoT ecosystems. The objective of this work is to provide researchers and practitioners with a consolidated reference to understand the state of the art and identify open research problems in the rapidly evolving IoT domain.

Keywords: Internet of Things, Smart Technologies, Edge Computing, AIoT, Smart Cities, Industry 4.0, IoT Security.

Introduction:

The Internet of Things (IoT) refers to a paradigm in which physical objects such as sensors, actuators, appliances, and machines are interconnected through the Internet, enabling continuous data exchange and intelligent decision-making. The concept of IoT has gained remarkable attention due to the exponential growth of connected devices and advancements in wireless communication, embedded systems, and cloud infrastructures.

Smart technologies represent the integration of IoT with artificial intelligence (AI), machine learning (ML), big data analytics, and automation techniques to build systems that can sense, learn, reason, and act autonomously. These technologies are playing acrucial role in enabling digital transformation across sectors including healthcare, manufacturing, transportation, and public services.

The motivation for this review arises from the rapid diversification of IoT applications and the emergence of new paradigms such as AIoT, edge intelligence, and digital twins. This paper aims to systematically analyze current trends, discuss enabling technologies, identify challenges, and explore future research directions in IoT and smart systems.

Background and Evolution of IoT

The roots of IoT can be traced back to early developments in radio frequency identification (RFID) and machine-to-machine (M2M) communications, where devices were connected for basic monitoring and control. Over time, advancements in sensor technology and wireless communication protocols enabled large-scale wireless sensor networks (WSNs), laying the foundation for modern IoT systems.

The introduction of IPv6 significantly accelerated IoT adoption by providing a vast address space to uniquely identify billions of devices. With the emergence of cloud computing, IoT systems gained scalable storage and processing capabilities, enabling real-time analytics and visualization of massive data streams generated by connected devices.

More recently, the convergence of IoT with AI and big data technologies has given rise to intelligent IoT ecosystems capable of autonomous decision-making and predictive analytics. The evolution from centralized cloud-based models to distributed edge and fog architectures further enhanced system responsiveness and reliability. This evolution reflects a shift from simple data collection to intelligent cyber-physical systems that tightly integrate the physical and digital worlds, supporting complex smart applications in dynamic environments.

IoT Architecture and Enabling Technologies

A typical IoT architecture is organized into multiple layers that collectively support data acquisition, communication, processing, and service delivery. The perception layer consists of sensors and actuators responsible for sensing physical parameters such as temperature, humidity, motion, and pressure. These devices form the interface between the physical world and digital systems.

The transport layer enables data transmission using wired or wireless technologies such as Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT, and cellular networks including 4G and 5G. This layer ensures reliable and scalable connectivity among heterogeneous devices.

The processing layer provides storage and computational resources using cloud, fog, and edge computing infrastructures. While cloud computing offers high scalability and powerful analytics, edge and fog computing bring computation closer to data sources, reducing latency and bandwidth consumption.

The application layer delivers user-centric services tailored to specific domains such as healthcare, smart homes, and industrial automation. Middleware platforms play a crucial role in managing devices, data flows, and application integration.

Enabling technologies for IoT include cloud platforms, virtualization, big data frameworks, AI/ML algorithms, blockchain for secure transactions, and digital twins for system modeling. Together, these technologies enhance scalability, intelligence, and reliability of IoT ecosystems.

Current Trends in IoT

The rapid advancement of IoT has led to several emerging trends that are redefining smart systems. One of the most prominent trends is AI-enabled IoT (AIoT), where machine learning and deep learning techniques are embedded into IoT pipelines to enable predictive analytics, anomaly detection, and autonomous control.

Edge and fog computing have gained importance as they enable real-time data processing near the source, which is critical for latency-sensitive applications such as autonomous vehicles, industrial control, and healthcare monitoring. These paradigms also reduce dependency on cloud resources and improve privacy.

The deployment of 5G networks has opened new opportunities for massive IoT by providing ultra-low latency, high bandwidth, and support for a large number of connected devices. Alongside, low-power wide-area networks (LPWAN) such as LoRaWAN and NB-IoT are widely adopted for long-range and energy-efficient communication.

TinyML is another emerging trend that focuses on deploying lightweight ML models on resource-constrained devices, enabling on-device intelligence without continuous cloud interaction. Digital twins provide virtual replicas of physical systems, facilitating real-time monitoring, simulation, and optimization.

Blockchain technology is being explored to ensure decentralized security, trust, and data integrity in IoT networks. Furthermore, energy harvesting and green IoT solutions aim to build sustainable systems by reducing power consumption and extending device lifetime.

Smart Technologies and Applications

IoT serves as the backbone for a wide range of smart technologies that enhance efficiency, safety, and sustainability. Smart cities leverage IoT for traffic management, smart lighting, waste management, environmental monitoring, and public safety, leading to improved urban living conditions.

In healthcare, IoT enables remote patient monitoring, wearable health devices, smart diagnostics, and telemedicine platforms. These solutions improve accessibility to healthcare services and enable proactive disease management.

Smart homes integrate sensors and automation systems to control lighting, heating, security, and appliances, providing comfort and energy efficiency. Voice assistants and mobile applications offer intuitive user interfaces for home management.

In agriculture, smart farming utilizes IoT sensors for soil monitoring, weather prediction, and automated irrigation, enabling precision agriculture and improving crop yield while conserving resources.

Industry 4.0 represents the application of IoT in manufacturing environments, where smart sensors, robotics, and analytics enable predictive maintenance, asset tracking, and optimized production processes.

Smart transportation systems employ IoT for vehicle tracking, traffic optimization, fleet management, and intelligent public transport, contributing to reduced congestion and enhanced safety.

Security, Privacy, and Interoperability

Despite its benefits, IoT faces significant challenges in terms of security and privacy. Many IoT devices are resource-constrained and lack robust security mechanisms, making them vulnerable to attacks such as malware injection, spoofing, denial-of-service, and unauthorized access.

Privacy concerns arise due to continuous data collection from personal and sensitive environments. Unauthorized data sharing and user profiling can lead to serious ethical and legal issues. Therefore, privacy-preserving data analytics and access control mechanisms are essential.

Interoperability is another critical challenge due to the heterogeneity of devices, platforms, and communication protocols. The lackof common standards hinders seamless integration and large-scale deployment. Protocols such as MQTT, CoAP, and standards like oneM2M and IEEE 2413 aim to address these issues.

Security solutions include lightweight cryptography, secure boot mechanisms, authentication and authorization frameworks, intrusion detection systems, and blockchain-based trust models. A holistic approach is required to ensure end-to-end security in IoT systems.

Challenges and Open Issues

Although IoT has matured significantly, several challenges still limit its widespread adoption. Energy efficiency remains a major concern as many devices operate on limited battery power and are deployed in inaccessible environments.

Scalability is critical for supporting billions of connected devices while maintaining reliable performance and manageable overheads. Efficient device management, firmware updates, and fault tolerance mechanisms are required.

Real-time data processing and low-latency communication are essential for mission-critical applications such as healthcare and industrial automation. Network congestion and bandwidth limitations pose additional challenges.

Other issues include data heterogeneity, lack of skilled workforce, regulatory compliance, ethical considerations, and ensuring user trust. Addressing these challenges requires collaborative efforts from academia, industry, and policymakers.

Future Research Directions

Future IoT research is expected to focus on integrating next-generation communication technologies such as 6G to support ultra-reliable and low-latency communication with intelligent network management.

Autonomous IoT systems capable of self-configuration, self-healing, and self-optimization will become increasingly important. Federated and privacy-preserving learning approaches will enable collaborative intelligence without sharing raw data.

Green IoT initiatives will emphasize energy-efficient hardware, energy harvesting techniques, and sustainable network designs to reduce environmental impact.

Human-centric IoT will focus on improving usability, accessibility, and ethical design to ensure technology serves societal needs. Context-aware systems will enable adaptive behavior based on environmental and user conditions.

The convergence of IoT with emerging technologies such as quantum computing, extended reality, and robotics will further expand the scope of smart applications.

Conclusion:

This paper presented a comprehensive review of current trends in IoT and smart technologies. The evolution of IoT from simple connectivity solutions to intelligent cyber-physical systems highlights its transformative impact on modern society.

The integration of AI, edge computing, advanced communication networks, and smart analytics is enabling a new generation of applications across diverse domains. However, challenges related to security, privacy, interoperability, scalability, and energy efficiency remain significant.

Addressing these challenges through interdisciplinary research, standardization, and innovative system design is essential for realizing the full potential of IoT. Future developments will continue to shape smart environments and contribute to building sustainable, intelligent, and human-centric digital ecosystems.

References:

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.
2. Chen, M., Miao, Y., Hao, Y., & Hwang, K. (2017). Narrowband Internet of Things. *IEEE Access, 5*, 20557–20577.
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.
4. Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal, 3*(6), 854–864.

5. Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers, 17*, 243–259.
6. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*, 680–698.
7. Jalali, F., Ranjbari, A., & Khondoker, R. (2021). Edge computing in IoT: A survey, applications, and research challenges. *Future Generation Computer Systems, 115*, 301–323.
8. Fortino, G., Russo, W., Zhou, M., & Savaglio, C. (2020). Internet of Things as system of systems: A review of methodologies, frameworks, platforms, and tools. *IEEE Access, 8*, 22386–22415.
9. Aazam, M., Khan, I., Alsaffar, A. A., & Huh, E. N. (2014). Cloud of Things: Integrating Internet of Things with cloud computing and the issues involved. In *Proceedings of the IEEE International Conference on Compatibility, Power Electronics, and Power Engineering* (pp. 877–884).
10. Ning, H., & Hu, Z. (2012). IoT security: Advances and challenges. In *IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 326–331).
11. Liu, J., Feng, C., & Xiang, Y. (2021). Survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal, 8*(8), 6320–6340.
12. Han, K., Song, J., Park, Y., & Moon, S. (2020). TinyML: Enabling machine learning on IoT devices. *IEEE Pervasive Computing, 19*(1), 76–82.
13. Yi, S., Hao, Z., Qin, Z., & Li, Q. (2013). Fog computing: Platform and applications. In *Proceedings of the Third IEEE Workshop on Hot Topics in Web Systems and Technologies* (pp. 73–78).
14. Giang, N. K., Giang, N. M., Dang, L. A., Nguyen, C. T., & Abraham, A. A. (2015). Security and privacy in the Internet of Things: Issues and challenges. In *IEEE International Conference on Computational Advances in Bio and Medical Sciences* (pp. 1–6).
15. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. In *Proceedings of the ACM Workshop on Mobile Cloud Computing* (pp. 13–16).
16. Bandyopadhyay, S., & Sen, S. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*, 49–69.
17. Xiao, Y. (2017). *Internet of Things: Architecture, protocols, and standards*. Wiley.

18. Kim, H., & Park, J. (2019). Digital twin-driven smart systems: Framework and applications. *IEEE Access, 7*, 104739–104751.
19. Zhang, X., Chen, M., Mao, S., & Leung, V. (2018). Mobile edge computing and cloud for IoT: A survey. *IEEE Communications Surveys & Tutorials, 20*(4), 2300–2322.
20. Evans, D. (2011). *The Internet of Things: How the next evolution of the Internet is changing everything*. Cisco White Paper.
21. Li, X., Lu, W. D., Zhang, D., & Wang, X. (2010). Smart grid as a cyber physical system: An overview. *IEEE Transactions on Smart Grid, 1*(1), 45–49.
22. Buyya, R., Srirama, S., & Giorgini, M. (2020). Edge computing for IoT: The big picture. *IEEE Internet of Things Magazine, 3*(1), 42–49.
23. Xu, Q., Zheng, R., & Zhang, Q. (2020). A survey on deep learning for IoT big data. *IEEE Communications Surveys & Tutorials, 22*(2), 126–157.
24. Ray, P. (2018). A survey on IoT architectural frameworks and communication protocols. *Journal of King Saud University – Computer and Information Sciences, 30*(3), 291–319.
25. Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics, 56*(10), 4258–4265.