

Internet of Things:

IoT is creating an environment of unification in the society. Today, IoT is being implemented everywhere which is of human concern like smart city, security, smart agriculture and home automation. This has created a lot of buzz among industries and right now all the companies are looking for candidates who has practical experience in IoT.

You can develop practical skills in IoT by building the following projects.

- Weather monitoring system using Raspberry Pi
- Smart irrigation system using IoT
- Home automation using IoT
- Weather monitoring system using Arduino
- Smart building using IoT
- Automated street lighting using IoT
- Smart water monitoring system using IoT
- Surveillance camera using IoT

The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play. Projections for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than \$11 trillion by 2025.

At the same time, however, the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits. Attention-grabbing headlines about the hacking of Internet-connected devices, surveillance concerns, and privacy fears already have captured public attention. Technical challenges remain and new policy, legal and development challenges are emerging.

This overview document is designed to help the Internet Society community navigate the dialogue surrounding the Internet of Things in light of the competing predictions about its promises and perils. The Internet of Things engages a broad set of ideas that are complex and intertwined from different perspectives. Key concepts that serve as a foundation for exploring the opportunities and challenges of IoT include:

- **IoT Definitions:** The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.
- **Enabling Technologies:** The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. The recent confluence of several technology market trends, however, is bringing the Internet of Things closer to widespread reality. These include *Ubiquitous Connectivity*, *Widespread Adoption of IP-based Networking*, *Computing Economics*, *Miniaturization*, *Advances in Data Analytics*, and the *Rise of Cloud Computing*.
- **Connectivity Models:** IoT implementations use different technical communications models, each with its own characteristics. Four common communications models described by the Internet Architecture Board include: *Device-to-Device*, *Device-to-Cloud*, *Device-to-Gateway*, and *Back-End Data-Sharing*. These models highlight the flexibility in the ways that IoT devices can connect and provide value to the user.

- **Transformational Potential:** If the projections and trends towards IoT become reality, it may force a shift in thinking about the implications and issues in a world where the most common interaction with the Internet comes from passive engagement with connected objects rather than active engagement with content. The potential realization of this outcome – a “hyperconnected world” — is testament to the general-purpose nature of the Internet architecture itself, which does not place inherent limitations on the applications or services that can make use of the technology.

Five key IoT issue areas are examined to explore some of the most pressing challenges and questions related to the technology. These include security; privacy; interoperability and standards; legal, regulatory, and rights; and emerging economies and development.

Security

While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber attack and expose user data to theft by leaving data streams inadequately protected.

The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments.

As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues.

Privacy

The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services.

Indeed, the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users. While these are important challenges, they are not insurmountable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

Interoperability / Standards

A fragmented environment of proprietary IoT technical implementations will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in.

In addition, poorly designed and configured IoT devices may have negative consequences for the networking resources they connect to and the broader Internet. Appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet. The use of generic, open, and widely available standards as technical building blocks for IoT devices and services (such as the Internet Protocol) will support greater user benefits, innovation, and economic opportunity.

Legal, Regulatory and Rights

The use of IoT devices raises many new regulatory and legal questions as well as amplifies existing legal issues around the Internet. The questions are wide in scope, and the rapid rate of change in IoT technology frequently outpaces the ability of the associated policy, legal, and regulatory structures to adapt.

One set of issues surrounds crossborder data flows, which occur when IoT devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing. Further, data collected by IoT devices is sometimes susceptible to misuse, potentially causing discriminatory outcomes for some users. Other legal issues with IoT devices include the conflict between law enforcement surveillance and civil rights; data retention and destruction policies; and legal liability for unintended uses, security breaches or privacy lapses.

While the legal and regulatory challenges are broad and complex in scope, adopting the guiding Internet Society principles of promoting a user's ability to *connect, speak, innovate, share, choose, and trust* are core considerations for evolving IoT laws and regulations that enable user rights.

Emerging Economy and Development Issues

The Internet of Things holds significant promise for delivering social and economic benefits to emerging and developing economies. This includes areas such as sustainable agriculture, water quality and use, healthcare, industrialization, and environmental management, among others. As such, IoT holds promise as a tool in achieving the United Nations Sustainable Development Goals.

The broad scope of IoT challenges will not be unique to industrialized countries. Developing regions also will need to respond to realize the potential benefits of IoT. In addition, the unique needs and challenges of implementation in less-developed regions will need to be addressed, including infrastructure readiness, market and investment incentives, technical skill requirements, and policy resources.

The Internet of Things is happening now. It promises to offer a revolutionary, fully connected "smart" world as the relationships between objects, their environment, and people become more tightly intertwined. Yet the issues and challenges associated with IoT need to be considered and addressed in order for the potential benefits for individuals, society, and the economy to be realized.

Ultimately, solutions for maximizing the benefits of the Internet of Things while minimizing the risks will not be found by engaging in a polarized debate that pits the promises of IoT against its possible perils. Rather, it will take informed engagement, dialogue, and collaboration across a range of stakeholders to plot the most effective ways forward.