CHAPTER 4

Issues raised by Internet of Things

The internet of things (IoT) is the vast network of connected physical objects (i.e., things) that exchange data with other devices and systems via the internet. While it refers to the actual devices, IoT is commonly used as an overarching term to describe a highly-distributed network that combines connectivity with sensors and lightweight applications, which are embedded into tools and devices. These are used to exchange data with other devices, applications, and systems for everything from smart plugs and power grids to connected cars and medical devices.

What Is IoT Security?

IoT security is an umbrella term that covers the strategies, tools, processes, systems, and methods used to protect all aspects of the internet of things. Included in IoT security is the protection of the physical components, applications, data, and network connections to ensure the availability, integrity, and confidentiality of IoT ecosystems.

Security challenges abound, because of the high volume of flaws regularly discovered in IoT systems. Robust IoT security includes all facets of protection, including hardening components, monitoring, keeping firmware updated, access management, threat response, and remediation of vulnerabilities. IoT security is critical as these systems are sprawling and vulnerable, making them a highly-targeted attack vector. Securing IoT devices from unauthorized access ensures that they do not become a gateway into other parts of the network or leak sensitive information.

IoT security vulnerabilities are found in everything from vehicles and smart grids to watches and smart home devices. For example, researchers found webcams that could be easily hacked to gain access to networks and smartwatches containing security vulnerabilities that allowed hackers to track the wearer’s location and eavesdrop on conversations.

The Importance of IoT Security

IoT is widely believed to be one of the most significant security vulnerabilities that impact nearly everyone—consumers, organizations, and governments. For all of the convenience and value derived from IoT systems, the risks are unparalleled. The importance of IoT security cannot be overstated, as these devices provide cybercriminals with a vast and accessible attack surface.

IoT security provides the vital protections needed for these vulnerable devices. Developers of IoT systems are known to focus on the functionality of the devices

and not on security. This amplifies the importance of IoT security and for users and IT teams to be responsible for implementing protections.

IoT Security Challenges

As noted above, IoT devices were not built with security in mind. This results in myriad IoT security challenges that can lead to disastrous situations. Unlike other technology solutions, few standards and rules are in place to direct IoT security. In addition, most people do not understand the inherent risks with IoT systems. Nor do they have any idea about the depth of IoT security challenges. Among the many IoT security issues are the following:

- Lack of visibility
  Users often deploy IoT devices without the knowledge of IT departments, which makes it impossible to have an accurate inventory of what needs to be protected and monitored.
- Limited security integration
  Because of the variety and scale of IoT devices, integrating them into security systems ranges from challenging to impossible.
- Open-source code vulnerabilities
  Firmware developed for IoT devices often includes open-source software, which is prone to bugs and vulnerabilities.
- Overwhelming data volume
  The amount of data generated by IoT devices make data oversight, management, and protection difficult.
- Poor testing
  Because most IoT developers do not prioritize security, they fail to perform effective vulnerability testing to identify weaknesses in IoT systems.
- Unpatched vulnerabilities
  Many IoT devices have unpatched vulnerabilities for many reasons, including patches not being available and difficulties accessing and installing patches.
- Vulnerable APIs
  APIs are often used as entry points to command-and-control centers from which attacks are launched, such as SQL injection, distributed denial of service (DDoS), man-in-the-middle (MITM), and breaching
-
- networks
- Weak passwords
  IoT devices are commonly shipped with default passwords that many users fail to change, giving cyber criminals easy access. In other cases, users create weak passwords that can be guessed.

Five security considerations for IoT implementations

If you're considering implementing an IoT strategy for your business, you need a serious security plan. Here's your checklist of five security weak points and what to look for when you attempt to fix them.

Here's my list of five security points:

1. Device security
2. Network security
3. Server security
4. Data security
5. Operating system security

Device security

Devices that gather data have multiple security weak points: physical, operating system, data, and network. Physical security is any device's most vulnerable point. Even the least competent security person will tell you that if your physical security is compromised, then there's very little a thief can't acquire. Physical security of your devices is as important as physical security of your servers.

These devices have operating systems, local data, and network connections that, even if secured to the maximum possible level, are vulnerable if a thief gets physical access. At a minimum, your device will be disabled and you'll collect no data from it. This incurs expense and outage for you.

The worst case scenario is that a thief not only takes the device but also recovers the data, network configurations — including usernames and passwords — or is able to temporarily take the device offline, plant malware on it and then replace it. In the case of a malware infection, you might never know that a device has been compromised.

Often the device or its data are not the actual target of the compromise; it's your other assets that can be acquired through malware infection once inside your network or data center.

Network security

Many system administrators see network security as the weakest link in the data transfer and communications chain in IoT implementations. It is true that many hacks, cracks, and compromises are due to some sort of network shortfall but it isn't the only method. To be sure, it's the first one that many hackers try. It's the least risky to the hacker and the method that generally pays the highest dividends in compromised data hacks.

There is a general assumption that virtual private networks (VPNs) are the ultimate network security compromise deterrent. They are good practice but they, in no way, ensure absolute network security. Yes, VPNs are secure because their traffic is encrypted, but the problem with trusting network security to a VPN alone is that it is still susceptible to man-in-the-middle (MITM) attacks.

Just because network traffic is encrypted doesn't mean that it's 100-percent safe or secure. There is a way to ensure that it is — data integrity checks. You should check traffic coming

from your devices to be sure that it hasn't been tampered with by using integrity checks. Some IoT device providers do this and some do not. You'll need third-party software to perform the checks for you.

You also need to check the data that leaves your network. Don't assume that everything bad that can happen happens from the outside in. Some compromises are from the inside to the outside, directionally speaking. You should monitor those leaks as well. Remember that it's not always a break-in situation. Sometimes the compromise is a slow leak of your valuable data from inside your network.

Server security

Server security isn't the same as operating system (OS) security. The difference is that servers or services run on an operating system. A huge number of hacks and compromises occur when such services are left unpatched or unsecured. The rule of thumb is to have as few services as possible exposed on your systems. Typically, services expose themselves via TCP or UDP (Internet protocol) ports such as SSH (22), HTTPS (443), SMTP (25), POP3 (110), DNS (53), and 3389 (RDP).

On Linux hosts, one of the best methods of securing ports is to only allow connectivity from other specific hosts using the /etc/hosts.deny and /etc/hosts.allow files.

Other methods of securing services include using firewall port address translation rules (holes) for securing which networks or hosts may contact a particular system on a specific port number.

Some protocols have secure equivalents available. When they do, or when they support secure connections between client and server, use them. Examples are SMTP's 587 or 465 and POP3's 995. SSH is already a secured port on 22.

Encrypted communications, as stated earlier, isn't a 100-percent effective deterrent but it is still a deterrent for most over-the-network hacks. The problem with network ports is that many run with elevated (root) status and once compromised they drop the successful hacker to a root prompt so that he has unlimited access to your system.

Data security

Data security is something that I've written about before. There are two types of data: data in flight (data during transmission) and data at rest (stored data). Remember that by "data," I'm referring to anything that's transmitted or stored, including passwords, usernames, certificates, keys, configuration files, as well as, actual collected data from remote sensors. Although raw data typically isn't that valuable to a hacker, it's the pathway that the data takes or what the data reveals that's important to him.

Data should be stored in an encrypted manner. That means that all data at rest should be encrypted at a very high level so that its contents are jumbled to the point of diminishing returns for anyone who could collect it, transfer it, and decrypt it.

Especially sensitive data such as credit card numbers, account numbers, usernames, passwords, should be stored and transferred encrypted. And multi-factor authentication should always be used for such sensitive data transactions and transmissions.

Operating system security

Operating system security has to do with patches, strong passwords, encrypted filesystems, antivirus software, antimalware software, and intrusion protection monitoring. Operating systems are a very weak link in the overall security spectrum. You have to be vigilant, proactive, and paranoid to make the OS secure. The OS is often seen as the weakest security link. OSs are a prime target for hackers. They exploit vulnerabilities in operating system code to own a system. Once a system is owned, it's under the control of the malicious actor. To fix such a compromised system usually means reimaging (a complete wipe and reinstall of the OS and applications).

nd don't rely on backups because the compromised system was probably backed up for a long time before you detected the compromise. If you can accurately determine the date of the hack, you can restore from before that point. The problem is that you might not have backups old enough to perform a good restore.

Operating system hacks and compromises are among the most costly of all because of the amount of time required to restore the crippled system to full operation and the data losses that have occurred on it. Microsoft has Patch Tuesday to provide users with a weekly patch bundle to keep systems updated and safe. Linux distributions have their software repositories that should be checked on a daily basis for new security patches. Those checks can be performed automatically in a CRON job that grabs the latest patches, downloads them, and installs them to the system to keep it updated.

Security is all about due diligence. You have to show, in the case of a significant hack or compromise, that you and your staff were diligent in applying patches to your systems. Since patching these days is easy to automate, there's really no excuse for not staying up to date.

These five security considerations in the context of The Internet of Things gives you an idea of the depth and the breadth of the security issues facing you, your devices, and your data. I'm not trying to spread fear, but I am attempting to make you aware of the security issues you're facing and what actions you need to take. A little bit of paranoia never hurt anyone.

IoT Privacy and Security: Challenges and Solutions

The Internet of Things (IoT) is one of the fastest growing technologies today due to its wide potential of applications. However, it also comes with security concerns like cyber attacks and software vulnerabilities, which makes customers hesitant in using IoT devices. This is especially true for organizations that deal in sensitive data such as healthcare, retail, manufacturing, finance, and logistics industries.

So, what is IoT? Simply put, it is a network of connected smart devices that can exchange data via internet without requiring any human involvement. The technology finds its applications in a number of industries including logistics, agriculture, healthcare, automotive, and more. Depending upon the requirements, smart devices can range from a simple sensor to high-level DNA analysis hardware.

What Is IoT Privacy and Security?

IoT security involves a set of practices and approaches that protect all the devices, processes, networks, and technologies from a wide range of cyber threats. IoT security matters because organizations with IoT applications need to be extra vigilant about system security and critical customer data. A small vulnerability can result in a cyber attack or system failure, which can directly affect hundreds of people. For instance, traffic lights that stop working suddenly can result in road accidents. Moreover, it is important to protect Personally Identifiable Information (PII) of customers, which is a requirement that must be fulfilled according to cybersecurity standards and regulations. Failure to protect it can result in loss of customer trust and eventually reputational damage to the organization.

Common IoT Privacy and Security Challenges

Maintaining security of IoT systems is a challenging task and it is important to have awareness of potential risks and challenges. Here are some common privacy and security challenges with the Internet of Things.

1. Software Vulnerabilities

Many smart devices have limited computing power and are unable to run powerful security functions. This leads to them having more software vulnerabilities as compared to other non-IoT devices.

Some of the reasons IoT devices have security vulnerabilities include:

- Poor access control

- Lack of computational capacity
- Lack of regular updates and software patches due to technical limitation or limited budget
- User negligence in updating IoT devices
- Inability to protect device from physical attack by a hacker. E.g., a criminal adding a chip or accessing device through radio waves.

2. Unsecured Communication

Most of the security mechanisms existing today were originally developed for desktop devices and are not as efficient when applied to IoT devices. One of the biggest threats resulting from unsecured communication within IoT networks is Man-in-the-Middle (MitM) attacks, where hackers can take control of your device, change its functionality, or install malware in it. The data exchanged between different IoT devices can also be read by cybercriminals if there is no encryption or the messages are in cleartext.

3. Data Leakage from IoT Systems

In addition to data leakage from IoT devices, hackers can also access data that is transferred and stored in the cloud. Cloud hosting services can experience attacks from external sources and include sensitive information like your bank account credentials, health records, and location.

4. Malware

According to a study by Zscaler, devices that were at high risk of being hacked by malware were smartwatches, smart TVs, and set-top boxes. By injecting malware into an IoT system, cyber criminals can collect all data, meddle with the system's functionality, and launch further attacks at other devices in the system.

5. Cyber Attacks

Apart from MitM and malware attacks, IoT systems are also susceptible to a number of other cyber attacks such as Denial of Service (DoS) attacks, device spoofing, application-based attacks, and physical intrusion, to name a few.

Solutions to IoT Security Challenges

By following IoT security solutions and best practices, we can ensure that the three main components of IoT are protected, i.e., network, data, and devices. Let's look at some of the solutions.

1. Secure your Smart Devices

- Ensure that your devices are tamper-resistant by using camera covers or port locks. You can also apply strong boot-level password that disables the device in case of a tampering attempt.
- Device security and maintenance requires regular patches and updates. Establish regular automatic security updates for your devices.

Conduct regular vulnerability assessments and penetration tests to detect vulnerabilities in your IoT firmware.

2. Secure Your Network

- Ensure strong authentication by using unique default credentials. Also use multi-factor authentication where possible.
- To ensure secure communication between network devices, enable encryption. You can also used optimized security protocols such as Secure Sockets Layer (SSL) and IPsec.
- Separate big networks into smaller ones to apply next-generation firewall security.
- Implement VPN for secure internet communication.
- Minimize your device bandwidth by limiting network traffic to the amount required for device functioning.

3. Secure Your Data

- Protect your sensitive data by using unique default password or requiring immediate password change after first use.
- Only collect data necessary for the functioning of your IoT system. This protects consumer privacy and lowers the risk of noncompliance with data protection standards and regulations.
- Secure your internal communications by restricting access to data within the IoT network.

Conclusion

It is important to think about privacy and security from early on when implementing an IoT system. However, it is difficult to implement robust security

for IoT projects. Not only does it have hardware limitations, it also increases development time and cost, which is quite challenging for businesses. But with appropriate solutions and proactive measures in place, it is possible to overcome these challenges and implement secure IoT solutions.

Internet of Things Privacy Background

IoT privacy refers to the issue where the manufacturer of the device has the ability to monitor and to use the data that they get from these devices. As the user connects more and more devices to the system, it increases the threat surface of the system. The ability to limit privacy is necessary to establish trust with an IoT system device.

Is the Internet of Things Secure?

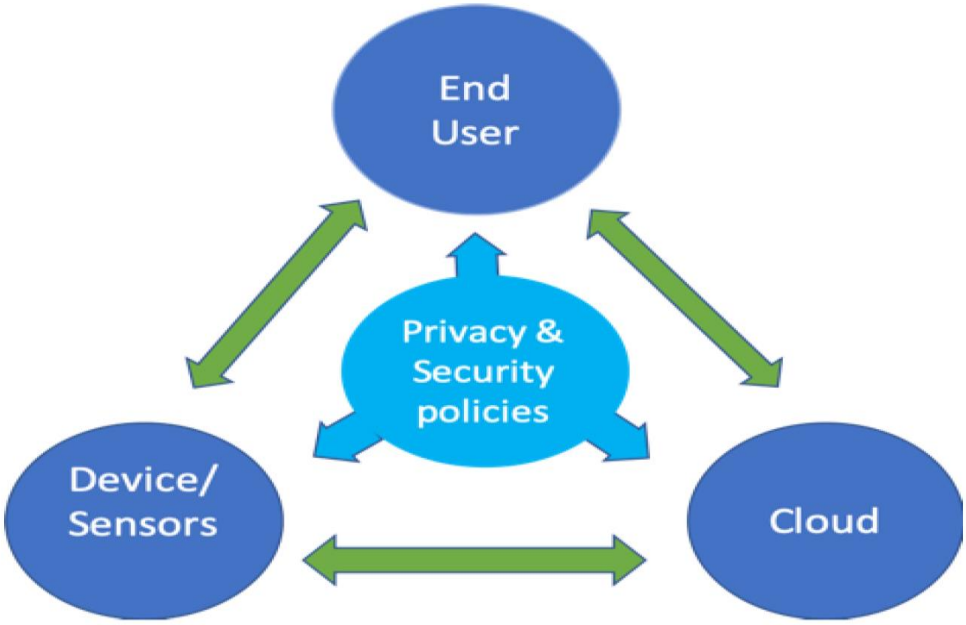
In a world where we already face numerous security and privacy risks, IoT creates even more exposure.

Most privacy issues related to the Internet of Things come from the internet-connected devices we use every day. And whenever these devices connect, they deliver an amazing amount of sensitive information to third parties.

And more often than not, these transfers aren't secure or obvious to the user.

With more businesses and individuals connecting critical devices and systems, Internet of Things privacy is a bigger issue than ever.

And while sending data isn't always risky, collecting and analyzing info from multiple locations can often reveal sensitive information.



What are Two Privacy Issues Regarding the Internet of Things? (CO-5)

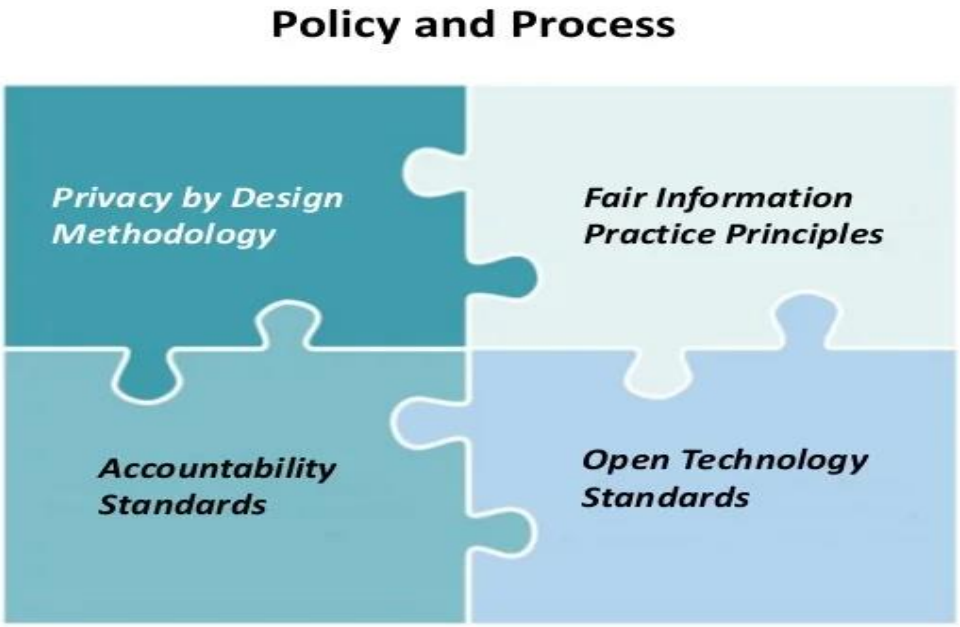
1. Data Overload

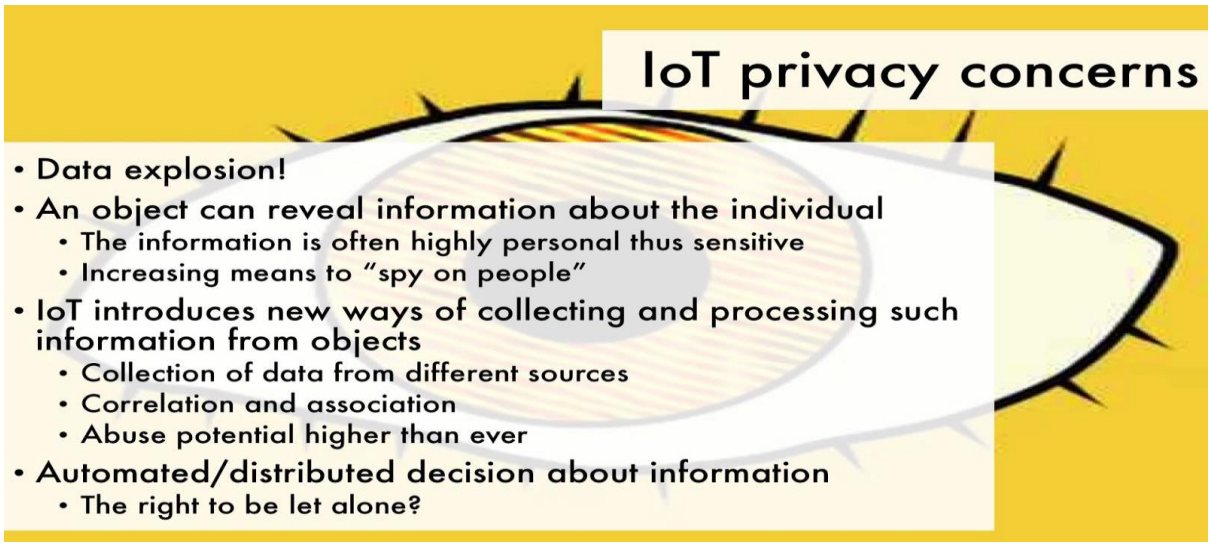
The amount of data IoT devices generate is staggering. Studies show that 10,000 households can create 150 million distinct data points every day. This risks not only your own information but details about your family, daily habits, changes in routine and more.

2. Spying

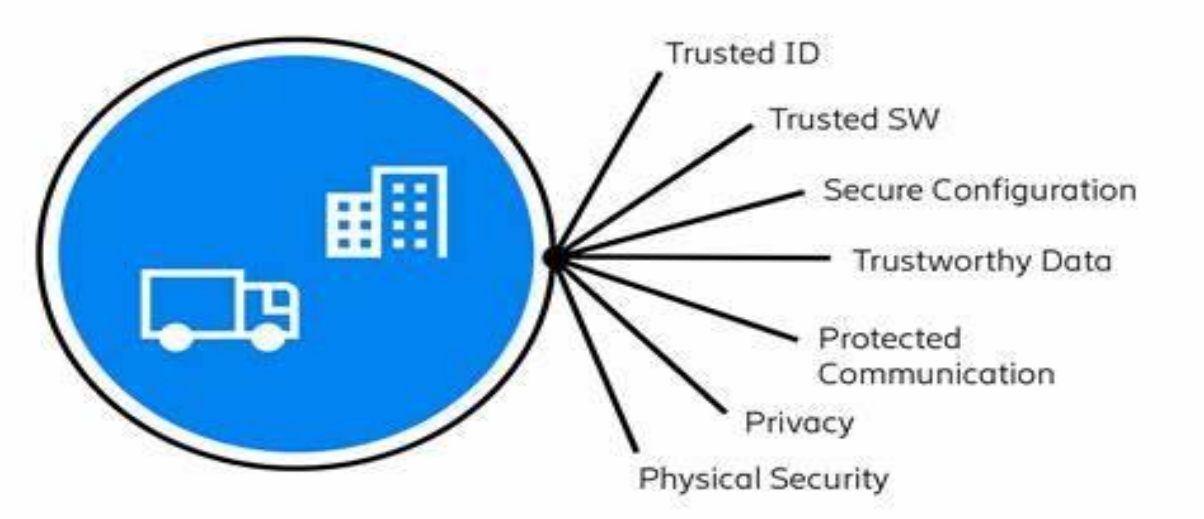
The more internet-enabled devices we use, the more open we are to online threats. When these devices are connected, an attack on any one of them opens the door to all of them, providing access to all kinds of personal information.

For example, say you want to keep an eye on your devices. In that case, all the Internet-enabled devices that make communication easy should be accounted for. This includes all sensors, light bulbs, video cameras, Wi-Fi routers, and more. Attackers could exploit weaknesses and password recovery processes to gain access to your system.





Unique Privacy Aspects of IoT



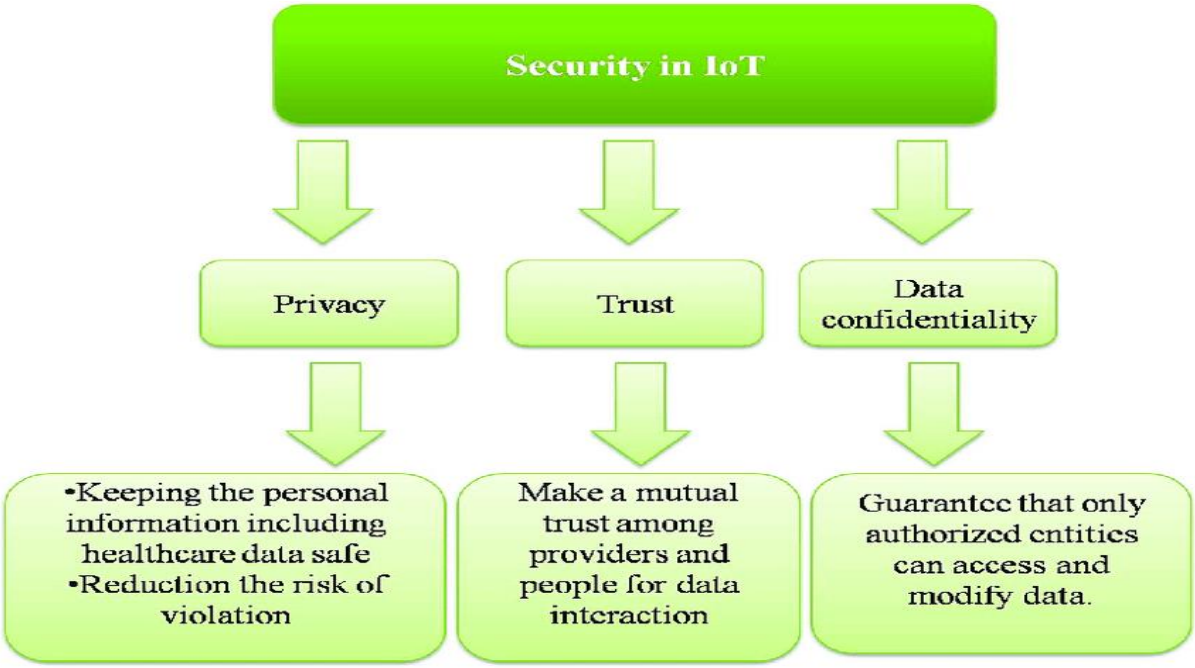
Privacy Concerns in IoT

While the challenges to security are quite prevalent in IoT, the concerns of privacy are also another critical factor. Many people also want to find out 'What are the privacy concerns in IoT?' and the answers could help in improving IoT for large-scale adoption. Let us take a look at some of the common privacy concerns in IoT which you can find today.

1. Abundance of Data

2. Eavesdropping

3. Unwanted Public Exposure



INTEROPERABILITY

The urgency in the requirement for interoperability and interoperable solutions in IoT arose mainly due to the following reasons:

(i) Large-scale Cooperation: There is a need for cooperation and coordination among the huge number of IoT devices, systems, standards, and platforms; this is a long-standing problem

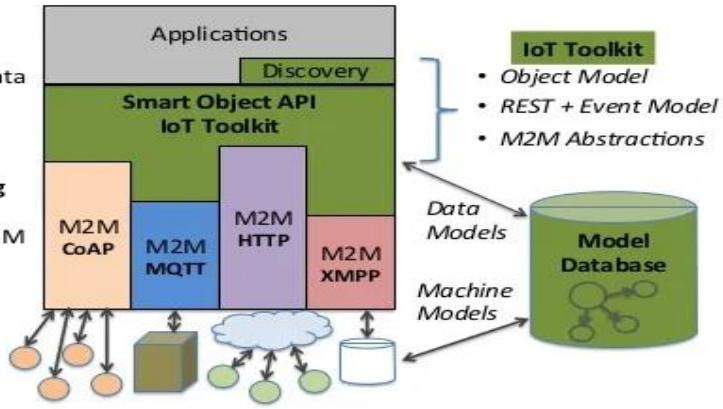
(ii) Global Heterogeneity: The network of devices within and outside the purview of gateways and their subnets are quite large considering the spread of IoT and the applications it is being adapted to daily.

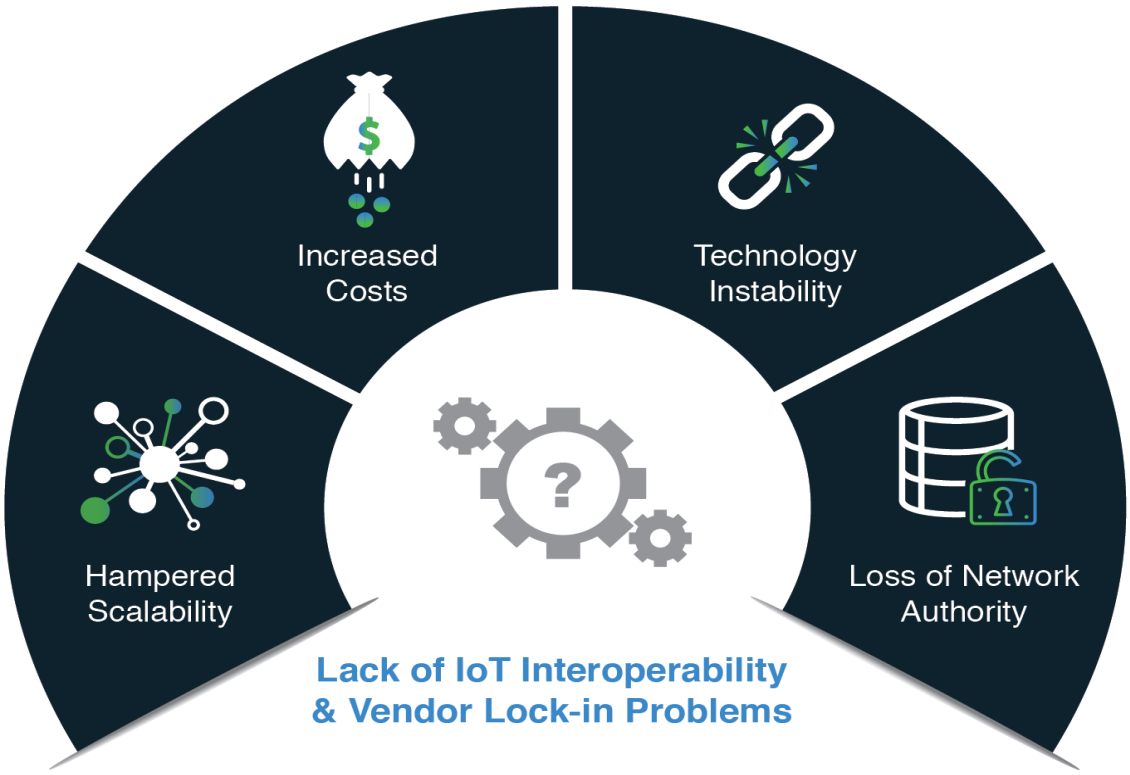
(iii) Unknown IoT Device Configuration: Device heterogeneity is often accompanied by further heterogeneity in device configurations.

(iv) Semantic Conflicts: The variations in processing logic and the way data is handled by the numerous sensors and devices making up a typical IoT implementation, makes it impossible for rapid and robust deployment. Internet of Things (IoT) is an ever-growing network of physical devices embedded with sensors, actuators and wire-less connectivity to communicate and share their information among themselves. The application of IoT is in diverse areas such as agriculture, poultry and farming, smart city, and health care, where a sensor node must support heterogeneous sensors/actuators, and varying types of wireless connectivity. Interoperability is the ability of two or more devices, systems, platforms or networks to work in conjunction. Interoperability enables communication between heterogeneous devices or system in order to achieve a common goal. However, the current devices and systems are fragmented with respect to the communication technologies, protocols, and data formats. This diversity makes it difficult for devices and systems in the IoT network to communicate and share their data with one another. The utility of IoT network is limited by the lack of interoperability.

IoT 2.0 – Interoperability

- Easy to deploy new things and applications using data models
- Write once, run anywhere software
- **Any app** to **any thing** via **any M2M**, use-case appropriate M2M
- Network effect enabled





Summary

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.