Unit-II

Overview: Physical Systems

IoT security

Vulnerabilities of IoT applications

IoT applications suffer from various vulnerabilities that put them at risk of being compromised, including:

- **Weak or hardcoded passwords.** Many passwords are easy to guess, publicly available or can't be changed. Some IT staff don't bother changing the default password that shipped with the device or software.
- **Lack of an update process or mechanism.** IT admins unintentionally exclude many IoT apps and devices from updates because they are invisible on the network. Also, IoT devices may not even have an update mechanism incorporated into them due to age or purpose, meaning admins can't update the firmware regularly.
- **Unsecured network services and ecosystem interfaces.** Each IoT app connection has the potential to be compromised, either through an inherent vulnerability in the components themselves or because they're not secured from attack. That includes any gateway, router, modem, external web app, API or cloud service connected to an IoT app.
- **Outdated or unsecured IoT app components.** Many IoT applications use third-party frameworks and libraries when built. If they're obsolete or have known vulnerabilities and aren't validated when installed in a network, they could pose security risks.
- **Unsecured data storage and transfer.** Different data types may be stored and transmitted between IoT applications and other connected devices and systems. All must be properly secured via Transport Layer Security or other protocols and encrypted as needed.

Threats to IoT applications

Threats to IoT applications fall into several general categories: spoofing, information disclosure, distributed denial of service (DDoS), tampering and elevation of service. Attackers typically use these threats as an entry point to a network and then move on to other areas to cause problems, such as stealing data, blocking connections or releasing ransomware.

IoT app threats
Spoofing threats
Attackers intercept or override data streams and spoof the originating app.
Info disclosure threats
Attackers eavesdrop and steal data, then threaten to release it online.
Tampering threats
Attackers replace software on a device and take over anything downstream, including IoT apps.
Elevation of privilege threats
Attackers use unsecured IoT apps to change access control rules for the application to cause damage in connected systems.
TechTarget

Four threats that target IoT app vulnerabilities.

Spoofing threats. Attackers intercept or partially override the data stream of an IoT device and spoof the originating device or system, which is also known as a man-in-the-middle attack. They intercept shared key information, control devices or observe sent data.

Information disclosure threats. Attackers eavesdrop on broadcasts to obtain information without authorization, jam the signal to deny information distribution or partially override the broadcast and replace it with false information. They then threaten to release or sell the data.

Tampering threats. Attackers can gain access to the firmware or OSes of the devices running an IoT app and then partially or completely replace it on the device. They then use the genuine device and application identities to access the network and other connected services. For example, SQL or XML injection attacks and DDoS attacks are tampering threats for IoT apps.

Elevation of privilege threats. Attackers use unsecured IoT apps to change the access control rules of the application to cause damage. For example, in an industrial or manufacturing environment, an attacker could force a valve to open all the way that should only open halfway in a production system and cause damage to the system or employees

How to protect IoT applications

Protecting IoT applications isn't a one-and-done activity. It requires planning, action and regular monitoring. Get started with these nine ways.

1. Learn the most likely threats

Threat modeling can identify, assess and prioritize the potential IoT app vulnerabilities. A model can suggest security activities that will ensure IT admins include IoT apps in overall security strategies. The model should continue to evolve and grow to reflect the state of the IoT app accurately.

2. Understand the risks

Not all risks are the same when it comes to IoT apps and an organization. Prioritize risks in order of concern and act accordingly. Many tech teams forget to align the risk with business scenarios and outcomes. A failure or breach in one IoT app may seem innocuous to IT but have serious financial implications for the company.

3. Update apps regularly

IT admins must deploy updates to IoT apps as quickly as possible to ensure the safety of the entire network. Use only approved and authenticated updates and, if updating apps over the air, use a VPN to encrypt all update data streams. Secure public key infrastructures (PKIs) can also authenticate devices and systems.

4. Secure the network

Firewalls, encryption and secure communication protocols protect IoT apps from unauthorized access. Regularly review the various standards, devices and communication protocols used on the network to ensure adequate security. Add IoT apps to any application security testing.

5. Enable strong authorization

Strong password protection is essential for IoT applications and that includes developing a secure password process for those creating passwords. Change the default passwords on IoT devices and apps and ensure they're changed regularly. Deploying a two- or three-way authentication model with TLS communication protocols reduces the chances that authentication data can be compromised at any point.

6. Secure communication

Encrypting data between IoT devices, apps and back-end systems keeps data safe from attackers. That includes encrypting data at rest and in transit and adopting PKI security models to ensure both senders and receivers get authenticated on the system before transmitting.

7. Secure control applications

Applications and systems that have access to IoT apps should also be secured. When they are secure, it stops the client IoT system from being compromised by outside attacks and prevents it from propagating attacks downstream.

[redacted]

8. Secure API integrations

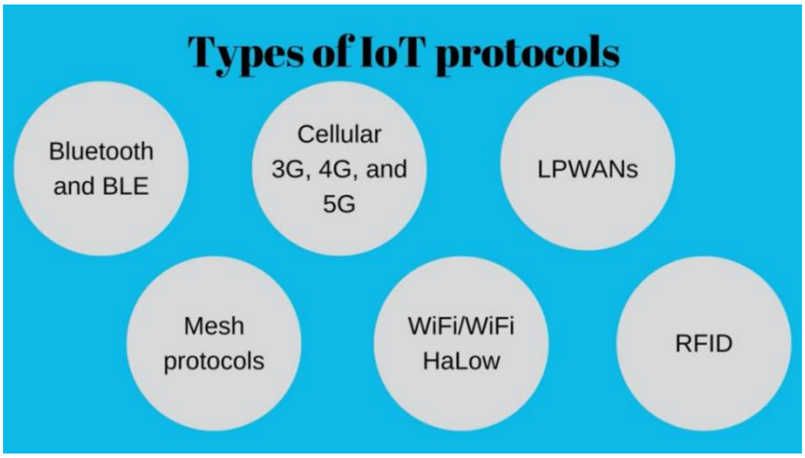
APIs are often used to push and pull data between applications and systems. They are another way for attackers to connect to IoT apps and cause problems. Only authorized devices and applications must communicate with APIs, making it easier to detect threats and attacks immediately. IT admins must also use API version management with old or redundant versions identified and removed regularly.

9. Monitor IoT apps

Monitoring IoT apps is the final step in protecting them. Ensure they're tested and scanned like the rest of the network to get alerts and address IoT security issues quickly.

IoT devices and applications pose a significant risk to organizations today. With hundreds or even thousands of devices connected to an enterprise network, not applying the same level of security measures to each component of IoT deployments can lead to problems beyond the individual device or application. **Six types of IoT protocols and network standards**

Devices are generally connected to the internet with an IP (internet protocol) network. But, devices can also be connected locally via Bluetooth or NFC (near-field communication). The differences between both types of connections are power, range, and memory used. IP connections are complex and require increased power and memory, but there are no range limitations. Bluetooth connections, on the other hand, are simple and require less power and memory, but the range is limited. There are many different types of IP and Bluetooth protocols that IoT devices can use.



Bluetooth and BLE

Bluetooth is a 2.4GHz network for personal wireless network communication. 2.4GHz network is preferred for providing personal networks by network providers as it is cheaper and has a much better range than other networks. Bluetooth low energy (BLE) is the new and optimized version of Bluetooth for connections between IoT applications. BLE consumes lesser power than standard Bluetooth for communication. BLE-enabled devices are commonly used with electronic devices that can act as a hub for data transfer from IoT devices to the cloud. This makes BLE a perfect match for IoT wearables. BLE is widely integrated into health and fitness trackers, as well as some smart home devices like door locks. Data from BLE-enabled IoT wearables can be easily communicated to smartphones.

In the retail context, BLE can be used with beacon technology to provide customer service like in-store navigation. Beacons are essentially small transmitters that use BLE to transmit signals to nearby IoT devices. By transmitting signals to nearby IoT devices, beacons can make location-based searching and navigation much easier and accurate.

Cellular (3G, 4G, and 5G)

Cellular networks, as the name suggests, are well-established in the mobile consumer market. 2G is an “old school” cellular network that, along with 3G, is being phased out in most parts of the world. But, the world is quickly embracing new high-speed cellular networks like 4G and 5G. Cellular networks provide high bandwidth and reliable broadband communication for voice calls or video streaming but with high operational costs and power consumption. Cellular networks cannot be used with most IoT devices due to their frequency, range, and security challenges. However, cellular networks can be viable options in some specific IoT devices like connected cars. Connected cars can use cellular networks for traffic routing with the help of GPS systems. GPS systems and cellular networks can help track road traffic in real-time as cellular networks can transfer high quantities of data over the network.

LPWANs

LPWANs (Low Power Wide Area Networks) are new sets of protocols developed for IoT solutions but can also be used by other devices to communicate over a wide area. Even cellular networks can provide a wide-area communication network, but the cost of communication over cellular networks is high because of its high power consumption. LPWANs enable communications over wide area with the help of small and inexpensive batteries that can last for long-term making it a cost-saving option in comparison with cellular networks.

There are different types of licensed (NB-IoT, LTE-M) and unlicensed (MIOTY, LoRa) LPWANs that are built differently for different purposes. While power consumption is one of the big challenges for licensed LPWANs, Quality of Service (QoS) and scalability are some challenges faced by unlicensed LPWANs.

Generally speaking, LPWANs can connect almost all types of sensors and enable data sharing among themselves and with the cloud. With the help of LPWANs, IoT sensors can facilitate numerous applications. For instance, sensors can allow remote monitoring of everything. However, LPWANs can send only small blocks of data over the network in a single instance, and it cannot send a large amount of data at a time.

Mesh protocols

A mesh usually refers to a rich interconnection network of devices that are made up of devices organized in a mesh topology. Mesh topology is a networking infrastructure in which all connected devices can cooperate to transfer and share data amongst each other.

ZigBee is one of the most popular mesh protocols used for IoT applications. It is a short-range, low-power protocol that is commonly deployed to extend communication over multiple IoT devices. When compared with LPWANs, ZigBee provides large data transfer at a single instance but with much less power-efficiency due to mesh infrastructure.

Due to its short physical range, ZigBee and other similar mesh protocols are best suited for medium-range IoT devices that are distributed within small areas. For instance, ZigBee protocols can be best suited for smart home sensor networks like smart lighting.

WiFi/WiFi HaLOW

Everyone would know what WiFi is because of its pervasiveness in both industrial and home environments. However, WiFi is not used with most of the IoT devices. Except for a few applications like digital signages and security cameras, WiFi does not provide a feasible option for IoT connectivity. The use of the WiFi network is limited in IoT devices, mainly because of its low range, high power consumption, and low scalability. A lesser-known derivative of WiFi known as WiFi HaLow is introduced for IoT devices. WiFi HaLow offers increased range and improved power efficiency. However, the use of WiFi HaLow has received less support from industries as the network offers low security.

RFID

RFID (Radio-frequency identification) uses radio waves to transfer small data packets over the network within small areas. It is easy to embed an RFID chip in IoT devices. RFID readers can then read the tags and give information about the product that is attached to tags. One of the common applications of RFID is inventory management. By attaching RFID tags to all products and connecting it to IoT devices, businesses can keep track of the number of products available in stock. Thus RFID can help in better stock planning leading to an optimized supply chain management. RFID tags can also help smart home IoT devices. For instance, a smart washing machine that can read RFID tags can be controlled.

The use of IoT devices is increasing globally. According to an estimate, there will be 41.6 billion IoT devices generating 79.4ZB (zettabytes) of data in 2025. Simultaneously the chances of cyber-attacks on data may also increase. With the increased use of IoT devices and vulnerability to cyber-attacks, it is time for businesses and other stakeholders to know and choose IoT protocols and standards that can potentially keep the possibilities of cyber breaches at bay. To choose the best IoT protocol for businesses means accurately weighing the criteria of range, power consumption, bandwidth, latency, QoS, and security

Countermeasures for Security Issues of IoT

There are some countermeasures available; using which the security issues of IoT can be reduced [5]. Those includes access control, data encryption, cloud computing and certification, communication security etc, discussed as below.

Data Encryption Mechanism

Encryption is the process of converting plaintext in to an unintelligible form known as cipher text. The network layer of IoT adopts hop-by-hop encryption mechanism to secure the nodes at network layer. This way the information is encrypted in transmission process, besides it needs to keep plaintext in each node through a encryption and decryption process. While the application layer of IoT adopts end-to-end encryption mechanism to securely transmit the information between the sender and the receiver. According to the needs of business one can choose any encryption mechanism. Additional to this with secure key management and secure key exchange one can prevent attacks like eavesdropping, fabrication record, etc on IoT [10].

Certification and Access control

Using public key infrastructure (PKI) one can achieve authentication by public key certification for preserving the authenticity and confidentiality of an IoT system. It is also a secure way of finding the identity of the parties who involved in information transfer. The identification of parties can also be done through trusted third party known as notarization [11]. Access control will give a secure IoT environment by limiting the access for devices, things or a person's which are illegal to access the resources of an IoT system. For correct access control an IoT system should provide secure certification system.

Cloud Computing

Cloud is name given to store a huge data. The performance of cloud is high with low cost. The IoT can adopt cloud computing for data storing, processing the data, which has been collected from the many sensor nodes. It also provides the third party security to an IoT system [12].

Security of Communication in IoT

IoT consists of smaller devices with less power, this leads that communication security is week in IoT system. We need a very strong, secure communication protocol that provides a security to communication.

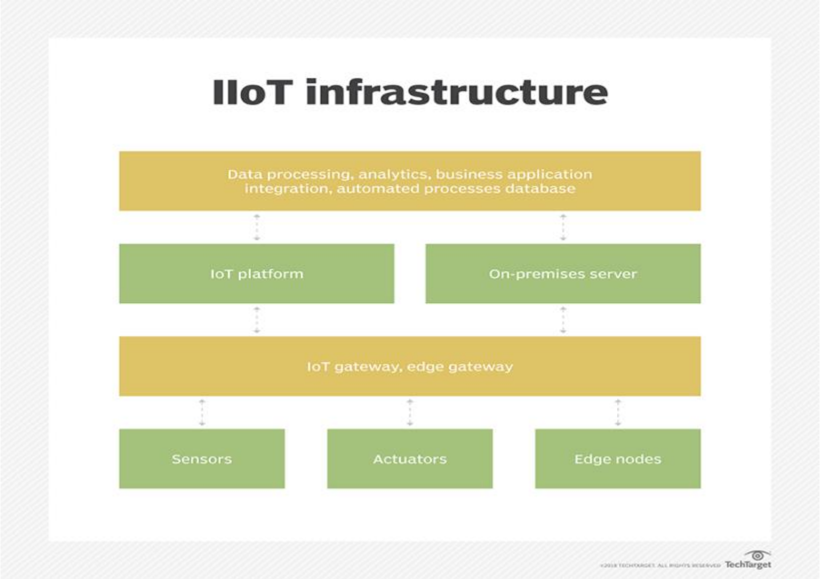
The Figure 2 summarizes the kind of device, security issues and countermeasures for those issues at each layer of an IoT.

IIOT and IOMT

What is the industrial internet of things?

The industrial internet of things (IIoT) is the use of smart sensors and actuators to enhance manufacturing and industrial processes. Also known as the industrial internet or Industry 4.0, IIoT uses the power of smart machines and real-time analytics to take advantage of the data that "dumb machines" have produced in industrial settings for years. The driving philosophy behind IIoT is that smart machines are not only better than humans at capturing and analyzing data in real time, but they're also better at communicating important information that can be used to drive business decisions faster and more accurately.

Connected sensors and actuators enable companies to pick up on inefficiencies and problems sooner and save time and money, while supporting business intelligence efforts. In manufacturing, specifically, IIoT holds great potential for quality control, sustainable and green practices, supply chain traceability, and overall supply chain efficiency. In an industrial setting, IIoT is key to processes such as Predictive maintenance (PdM), enhanced field service, energy management and asset tracking.


IIoT infrastructure
Data processing, analytics, business application integration, automated processes database
IoT platform
On-premises server
IoT gateway, edge gateway
Sensors
Actuators
Edge nodes
©2018 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

How does IIoT work?

IIoT is a network of intelligent devices connected to form systems that monitor, collect, exchange and analyze data. Each industrial IoT ecosystem consists of:

- connected devices that can sense, communicate and store information about themselves;
- public and/or private data communications infrastructure;
- analytics and applications that generate business information from raw data;
- storage for the data that is generated by the IIoT devices; and
- people

IoMT

The Internet of Medical Things (IoMT) is the network of Internet-connected medical devices, hardware infrastructure, and software applications used to connect healthcare information technology. Sometimes referred to as IoT in healthcare, IoMT allows wireless and remote devices to securely communicate over the Internet to allow rapid and flexible analysis of medical data.

IoMT's impact on the healthcare market is undeniable and irreversible. According to a recent Deloitte survey, the overall IoMT market is expected to grow from $41 billion in 2017 to $158 billion by 2022.

The broader Internet of Things (IoT) includes the network of all Internet-connected devices, including: internet connected factory equipment, biometric cybersecurity scanners, and autonomous farming equipment. IoMT is focused specifically on healthcare and medical applications. Given the sensitivity and strict regulations around healthcare data, IoMT requires a more comprehensive security infrastructure than other IoT systems.

IoMT Challenges

IoMT comes with some unique legal, regulatory, technical, and privacy challenges, mainly because the IoMT ecosystem has so many stakeholders, including:

- Medical device providers

- Connectivity providers
- Original equipment manufacturers (OEM)
- Systems/software providers
- System integrators

IOT in Smart Home and Cities

- To understand how IoT (internet of things) affects our lives in our smart homes, the cities we live in, and our lives. We need to grasp our knowledge of what IoT is. The internet of things explains the cluster of physical objects comprising sensors, software, and other technological devices to interlink and exchange data with other devices and systems. The internet of things also refers to the skyrocketing number of digital devices. These devices share data by communicating through the internet all over the world. You can control these devices remotely through a user interface or even your smartphones. In fact next-generation technologies like IoT, AI are transforming our homes and living.

- **Technology advancing**

- Because of technological advancements in our digital society, embedded systems, user-interactive software, control systems, wireless sensor systems, and more enable the internet of things. The consumer market relates IoT technology to the concept of smart homes, which includes devices such as home security systems, thermostats, lighting, and cameras. All these devices include Bluetooth. They can use the internet to share data and store data in a database to support an ecosystem.

- Because it enables the data to be shared, users can control devices via devices linked to the ecosystem, such as smartphones

To what extent does it affect our lives
IoT has changed the way we carry out simple tasks, and it has made our lives convenient since we can control devices around us by the touch of a screen on our smartphones. Before IoT, people would physically get up to do things around the house, such as turn on the water heater or turn the lights on.

IoT also includes mobile devices; since they can communicate with others and manage data, it is a device everywhere. Everyone carries a smartphone all day. You can control objects using a mobile device.

Today, you can get brilliant smart refrigerators with work-in cameras, so you can look at their substance while you are shopping. In the future, you will see fridges that detect you are coming up short on supplies and send an essential food rundown to your cell phone.

Stores could then push suggestions to add food and different things, considering previous purchases and average purchasing patterns. When strolling through the supermarket, reminders will get sent to your smartphone to ensure you never need to make that second trip back to the store.

Using IoT can decimate costs for firms that are operating in the economy. Organizations use IoT for innovative management and for observing scattered data. Thus, they can handle the latter from far-off places as they feed data into applications and information stockpiling (data storage).

IoT gives the benefit of realizing things ahead of time. Because of the minimal expense of IoT, it is now possible to screen and manage previously inaccessible activities. The monetary aspect is the best benefit since this innovation could replace people responsible for observing and keeping up with provisions. Therefore, expenses can essentially decrease and get optimized. IoT likewise makes it conceivable to gain new bits of knowledge. For example, they are associating the climate impact to mechanical productions.

GNU Radio

GNU stands for GNU's Not UNIX. It is a UNIX like computer operating system, but unlike UNIX, it is free software and contains no UNIX code. Its goal is to give computer users freedom and control in their use of their computers and computing devices by collaboratively developing and publishing software that gives everyone the rights to freely run the software, copy and distribute it, study it, and modify it. GNU software grants these rights in its license.

GNU Radio is an open-source toolkit to implement SDRs. It provides basic blocks to perform different steps of signal processing, for example, filters, decoders, demodulators, and many more. It works with all of the major SDR hardware. The major benefit is the huge extensibility of the framework. It is possible to write blocks in C++, or Python.

GNU radio companion (GRC):

GNU Radio Companion (GRC) is a frontend visualization tool that is part of the Gnu radio framework. We should keep in the back of our mind that GRC was created to simplify the use of GNU Radio by allowing us to create python files graphically as opposed to creating them in code alone. It allows one to simply drag, modify parameters, and start processing the signal. We’ll focus on it more as we proceed.

- End usersities

IoT Impact Our Lives In Smart Homes And Cities

To understand how IoT (internet of things) affects our lives in our smart homes, the cities we live in, and our lives. We need to grasp our knowledge of what IoT is. The internet of things explains the cluster of physical objects comprising sensors, software, and other technological devices to interlink and exchange data with other devices and systems. The internet of things also refers to the skyrocketing number of digital devices. These devices share data by communicating through the internet all over the world. You can control these devices remotely through a user interface or even your smartphones. In fact next-generation technologies like IoT, AI are transforming our homes and living.

Technology advancing

Because of technological advancements in our digital society, embedded systems, user-interactive software, control systems, wireless sensor systems, and more enable the internet of things. The consumer market relates IoT technology to the concept of smart homes, which includes devices such as home security systems, thermostats, lighting, and cameras. All these devices include Bluetooth. They can use the internet to share data and store data in a database to support an ecosystem.

Because it enables the data to be shared, users can control devices via devices linked to the ecosystem, such as smartphones.

Table of Contents

To what extent does it affect our lives

IoT has changed the way we carry out simple tasks, and it has made our lives convenient since we can control devices around us by the touch of a screen on our smartphones. Before IoT, people would physically get up to do things around the house, such as turn on the water heater or turn the lights on.

IoT also includes mobile devices; since they can communicate with others and manage data, it is a device everywhere. Everyone carries a smartphone all day. You can control objects using a mobile device.

Today, you can get brilliant smart refrigerators with work-in cameras, so you can look at their substance while you are shopping. In the future, you will see fridges that detect you are coming up short on supplies and send an essential food rundown to your cell phone.

Stores could then push suggestions to add food and different things, considering previous purchases and average purchasing patterns. When strolling through the supermarket, reminders will get sent to your smartphone to ensure you never need to make that second trip back to the store.

Using IoT can decimate costs for firms that are operating in the economy. Organizations use IoT for innovative management and for observing scattered data. Thus, they can handle the latter from far-off places as they feed data into applications and information stockpiling (data storage).

IoT gives the benefit of realizing things ahead of time. Because of the minimal expense of IoT, it is now possible to screen and manage previously inaccessible activities. The monetary aspect is the best benefit since this innovation could replace people responsible for observing and keeping up with provisions. Therefore, expenses can essentially decrease and get optimized. IoT likewise makes it conceivable to gain new bits of knowledge. For example, they are associating the climate impact to mechanical productions.

Concerns about IoT

One of the critical drivers of the IoT is information. The accomplishment of interfacing gadgets to make them more productive is subject to access to and capacity and data preparation. For this reason, organizations dealing with the IoT gather information from many sources and store it in their cloud network for additional handling.

The data is vulnerable, and hackers target it to access private information. This welcomes protection and security risks and single point weakness of different frameworks.

Conclusion on IoT and its impact

The future of IoT is limitless. It gives solutions in all areas, including producing, style, medical services, schooling, etc. Innovative sites can share a typical smart city platform, which bonds well, particularly for tiny urban communities. The cloud-based nature of IoT solutions for Smart Cities gets fitted by sharing a stage-dependent on the information. Small urban communities can shape a typical metropolitan ecosystem.

Along these lines, small and enormous smart cities’ solutions get organized and controlled through the central cloud platform. At last, yet critically, the size of a town isn’t a snag while heading to becoming “smart.” Urban communities in each group can profit with insightful technological advancements

Risks in IOT world

1. Lack of physical hardening

The lack of physical hardening has always been a concern for devices within the internet of things. Since most IoT devices are remotely deployed, there is no way to properly secure devices that are constantly exposed to the broader physical attack surface. Devices without a secure location and the inability for continual surveillance allow potential attackers to gain valuable information about their network’s capabilities which can assist in future remote attacks or gaining control over the device. For example, hackers can facilitate the removal of a memory card to read its contents and access private data and information that may allow them to access other systems.

2. Insecure data storage and transfer

As more people utilize cloud-based communications and data storage, the cross-communication between smart devices and the IoT network increases. However, any time data is transferred, received, or stored through these networks, the potential for a breach or compromised data also increases. This is due to the lack of encryption and access controls before data is entered into the IoT ecosystem. For this reason, it is important to ensure the secure transfer and storage of data through robust network security management tools like firewalls and network access controls.

3. Lack of visibility and device management

Many IoT devices remain unmonitored, untracked, and improperly managed. As devices connect and disconnect from the IoT network, trying to monitor them can grow to be very difficult. Lack of visibility into device status can prevent organizations from detecting or even responding to potential threats. These risks can become life-threatening when we take a look into the healthcare sector. IoT pacemakers and defibrillators have the potential to be tampered with if not secured properly and hackers can purposefully deplete batteries or administer incorrect pacing and shocks. Organizations need to implement device management systems to properly monitor IoT devices so all avenues for potential breaches are accounted for.

4. Botnets

Botnets are a series of internet-connected devices that are created to steal data, compromise networks, or send spam. Botnets contain malware that allows the attacker to access the IoT device and its connection to infiltrate an organization's network, becoming one of the top threats for businesses. They are most prominent in appliances that were not initially manufactured securely (smart fridges, for example). These devices are continuously morphing and adapting. Therefore, monitoring their changes and threat practices is necessary to avoid attacks.

5. Weak passcodes

Although intricate passcodes can prove to be secure for most IoT devices, one weak passcode is all it takes to open the gateway to your organization's network. Inconsistent management of passcodes throughout the workplace enables hackers to compromise your entire business network. If just one employee does not adhere to advanced password management policies, the potential for a password-oriented attack increases. Practicing good password hygiene is essential to ensure your business is covering all bases within standard security practices.

6. Insecure ecosystem interfaces

Application programming interfaces (APIs) are software intermediaries that allow two applications to talk to each other. With the connection of the two servers, APIs can introduce a new entrance for attackers to access a business's IoT devices and breach a network's router, web interface, server, etc. It is crucial to understand the intricacies and security policies of each device in the ecosystem before connecting them to ensure complete network security.

7. AI-based attacks

While AI attacks have been around since 2007, the threats they present within IoT are becoming increasingly more prominent. Hackers now can build AI-powered tools that are faster, easier to scale, and more efficient than humans, to carry out their attacks. This poses a serious threat within the IoT ecosystem. While the tactics and elements of traditional IoT threats presented by cyber attackers will look the same, the magnitude, automation, and customization of AI-powered attacks will make them increasingly hard to battle.

Software-defined radio powers the IoT(SDR)

For many years, the evolution of wireless communication standards depended on large-scale hardware upgrades. Today, however, the adoption of SDR technologies makes it easier to find alternatives to expensive hardware.

The primary motivation of the SDR concept is to overcome added costs. The three essential methods used in SDR are to move the broadband analog-digital conversion (ADC) and digital-to-analog converter (DAC) as close as possible to RF devices, use hardware as the basis of wireless communication, and maximize software options to enable functions that are traditionally only available in the RF and intermediate frequency (IF) analog domain.

To make the system more flexible at a lower cost, items such as the operating frequency band and modulation method are configured by software in the digital domain. SDR lets the same hardware handle multiple frequency bands by loading the relevant software as required. This scheme works for products ranging from smartphones to sensor networks. Meanwhile, market forces are driving the steady development of high-speed, high-precision ADC technology to enable fast and accurate processing of wireless broadband signals. ADC limitations previously constituted one of the main bottlenecks to SDR.

Receiver design is a critical priority for SDR. So it is useful to review the special requirements for SDR receiver implementation. The key is the front-end. Implementation of the entire SDR system dictates how to partition specifications for the ADC and other key components. High speed, dynamic range, and richness in software configurations are essential in the ADC.

SDR receivers generally can be divided into three categories based on their signal bands: RF sampling receivers, IF sampling receivers, and baseband sampling receivers. RF sampling most resembles the ideal SDR structure: An ADC connected to an antenna to form a receiver and a

DAC connected to an antenna to form the transmitter. However, the two major performance bottlenecks — RF devices and ADCs — make the ideal structure the most difficult to realize at a reasonable cost.