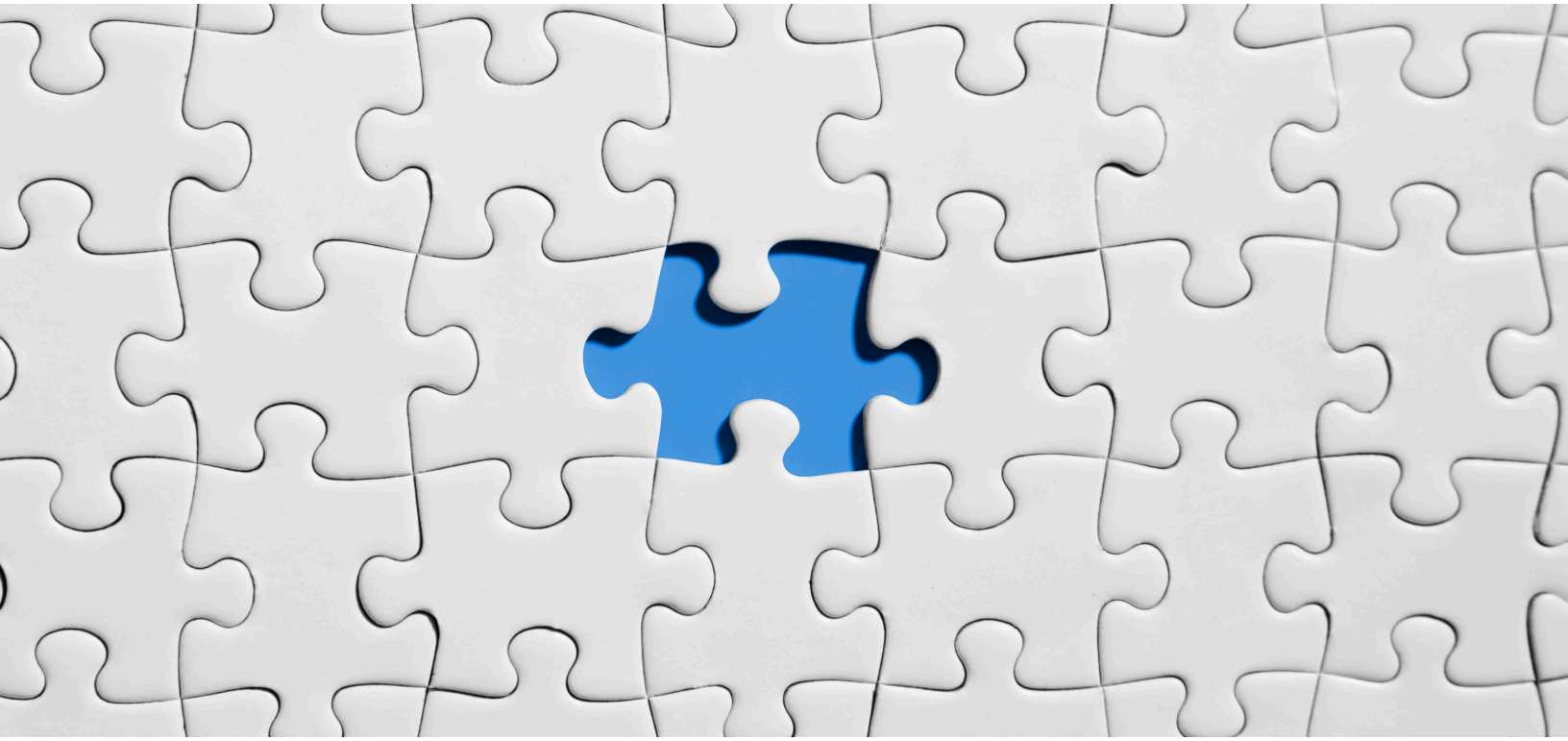
DELL Technologies

IOT SECURITY: CHALLENGES AND FUTURE TRENDS



Ranjisha R

Sales Engineer Analyst

Dell Technologies

Ranjisha.r@dell.com

Sowmya S Gowda

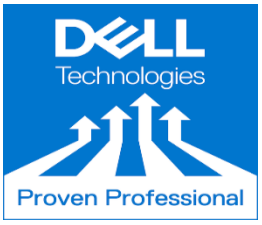
Sales Engineer Analyst

Dell Technologies

SowmyaS.Gowda@dell.com

Knowledge Sharing Article

DELL Technologies Proven Professional



The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Abstract 4
Introduction 5
IoT Management 5
Rise of IoT 6
IoT Architecture 6
Stages of IoT architecture 6
IoT Security Threats 8
Types of IoT threats 8
IoT Security 9
Introduction 9
IoT Security framework 10
Addressing IoT security challenges 11
The Future of IoT Security 12
Conclusion 13
References 14

Abstract

With new technology comes new challenges and opportunities. These opportunities try to leverage Internet of Things (IoT) and embark on creating a connected business. IoT promises technical advances, improved efficiencies, greater revenues and enhanced customer experiences. This clearly indicates that IoT is becoming mainstream and represents a significant opportunity for the global economy, society and business. However, this expansion heightens security as a major concern.

As more and more devices get interconnected, securing them all will be the biggest challenge that we face. Hardware, software and connectivity will all need to be secured for IoT objects to work effectively. All these security concerns could inhibit IoT expansion.

IoT security should protect the systems, network and data from all vulnerabilities. Security is not just a destination; it is a continuous journey which moves and evolves with technology and capabilities. Adopting a security-focused mindset will support IoT product and service providers in mitigating risks ranging from cybersecurity threats to regulatory action. It is always necessary for business to understand the need for the transformation and take a more holistic approach to their IoT journey. This article provides insights on cybersecurity of IoTs and some major applications in industries, research challenges and trends.

Introduction

Internet of Things (IoT) is a network of connected devices that acts as a system of interrelated Physical Objects, Sensors, Actuators, Virtual Objects, People, Services, Platforms, and Networks each of which have separate identifiers and an ability to exchange data over a network.

IoT has triggered numerous technological changes that span a wide range of fields. As per a Gartner forecast there would be 20.8 billion connected 'things' in use worldwide by 2020.

The development in IoT provides opportunity to make our lives easier and improve efficiency, productivity, and safety for many businesses.

IoT and digital transformation together would enable businesses to connect with customers and partners in open digital ecosystems, share digital insights, collaborate on solutions, and benefit from the value created.

IoT doesn't just connect devices; it connects people too. This makes IoT device security a high priority crucial for the future wellbeing of the internet ecosystem.

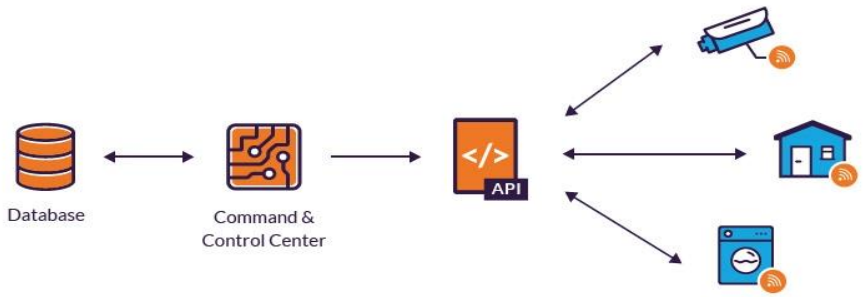
IoT spans sectors and industries, including:

- Consumer applications – IoT consumer products include smartphones, smart watches and smart homes, which control everything from air conditioning to door locks, all from a single device.
- Business applications – Businesses use a wide range of IoT devices, including smart security cameras, trackers for vehicles, container ships and goods, as well as sensors that capture data about industrial machinery.
- Governmental applications – Governmental IoT applications include devices used to track wildlife, monitor traffic congestion, and issue natural disaster alerts and more.

IoT Management

IoT devices can be managed internally and externally by connecting every IoT device to a management unit, known as a command and control center. These Centers are responsible for software maintenance, configurations, and firmware updates to patch bugs and vulnerabilities. It also helps provisioning and authentication of tasks, such as device enrollment.

The image below depicts how IoT devices are managed:



Application program interface (API) is used for communication between devices. All the devices or applications can use it to gather data and communicate with each other. Some APIs can also be used to control other devices. A simple example would be where a building manager uses an API to remotely lock doors inside a specific office.

Rise of IoT

IoT devices are finding their ways into our lives through various sectors like homes, businesses, and so on. With this rapid increase in embedded device connectivity, solutions are aimed to revolutionize manufacturing, industrial, supply chain management, logistics, retail, infrastructure management, food production, surveillance, and many other sectors that combine data gathering, tracking, and analysis.

At the same time, there is a need to process and understand the huge amounts of data evolving from thousands of devices, artificial intelligence, machine learning, Big Data, and other trending technologies.

Making everything "smart" in the consumer space often looks like a solution in search of a problem. Manufacturers of household appliances like smart TVs, wearables, toys, home automation systems, cars, etc. are rushing to bring the next big thing to the market and add connectivity to seemingly every new product.

As the market and technology advances, more standards and best practices should emerge to guide IoT device manufacturers in developing and delivering more secure products.

IoT devices can pose a security threat in more ways since they are often connected to higher-value targets. Hence, with this rapid innovation, it is imperative to ensure security and management of IoT devices.

IoT Architecture

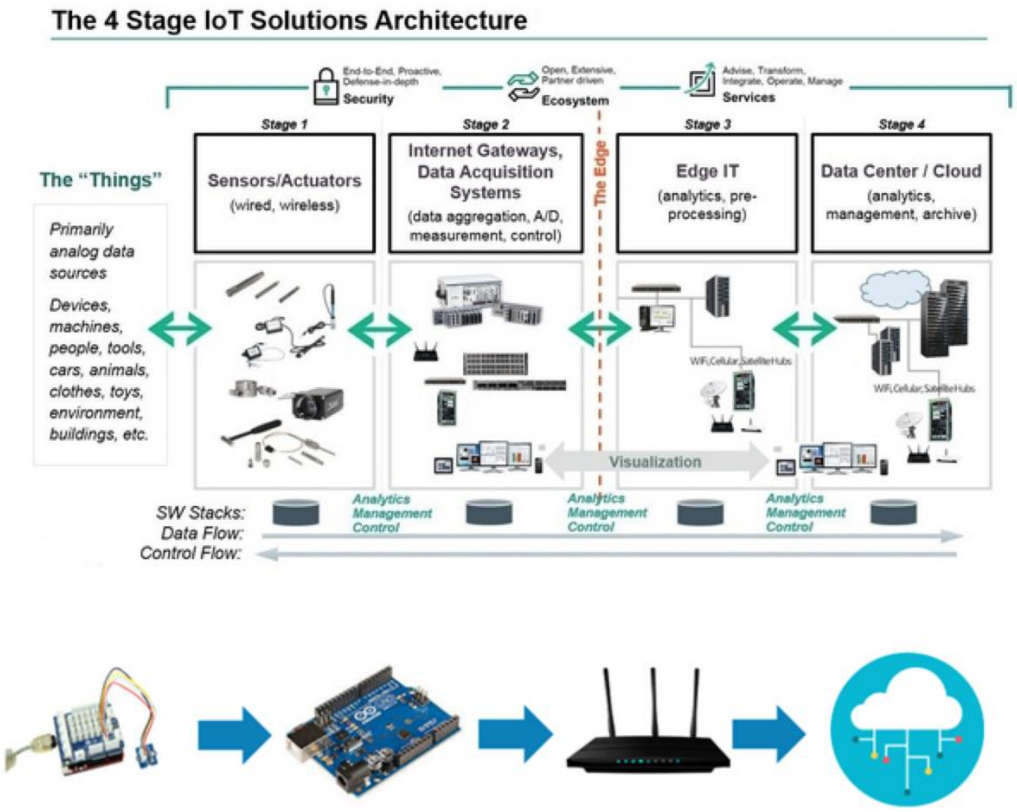
There are three IoT architecture layers:

- The client side (IoT Device Layer)
- Operators on the server side (IoT Getaway Layer)
- A pathway for connecting clients and operators (IoT Platform Layer)

Stages of IoT architecture

The fundamental features of IoT architecture include functionality, scalability, availability, and maintainability. These are addressed in 4 stages of IoT architecture:

- Sensors and actuators
- Internet getaways and Data Acquisition Systems
- Edge IT
- Data center and cloud



Stage 1. Networked things (wireless sensors and actuators)

Sensors or Actuators accept data, process data and emit data over network. They convert the information obtained in the outer world into data for analysis. It is very important to start with the inclusion of sensors in all four stages of an IoT architecture framework to get information in a format that can be processed.

Actuator devices are used to intervene on the physical reality. For example, they can switch off the light and adjust the temperature in a room. This process of sensing and actuating covers and adjusts everything that is needed in the physical world to gain the necessary insights for further analysis.

Stage 2. Sensor data aggregation systems and analog-to-digital data conversion

Stage 2 makes data both digitalized and aggregated.

This stage also works in close proximity to sensors and actuators, Internet getaways and data acquisition systems (DAS) which performs data aggregation and conversion function. The latter connect to the sensor network and aggregate output, while Internet getaways work through Wi-Fi and wired LANs and perform further processing.

The main activity of this stage is to process the enormous amount of information collected on the previous stage and condense it to optimal size for further analysis. Conversion in terms of timing and structure also occurs here.

Stage 3. The appearance of edge IT systems

In this stage, the prepared data is transferred to the IT world. Edge IT systems perform enhanced analytics and pre-processing. This is a processing unit of IoT ecosystem.

Here data is analyzed and pre-processed before sending it to a data center. From there, data is accessed by software applications, i.e. business applications, where data is monitored and managed and further actions are also prepared. For example, it refers to machine learning and visualization technologies. At the same time, additional processing may happen here, prior to the stage of entering the data center.

Stage 3 is closely linked to the previous phases in building an IoT architecture. Because of this, the location of edge IT systems is close to where sensors and actuators are situated, which creates a wiring closet.

Stage 4. Analysis, management, and storage of data

The last stage of IoT architecture happen in the data center or cloud which enables in-depth processing, along with revision and feedback. Data from other sources may be included here to ensure in-depth analysis.

After meeting all the quality standards and requirements, the information is brought back to the physical world which is in a processed and precisely analyzed appearance already.

Data centers or cloud will act as the management stage of data where data is managed and is used by end-user applications, i.e. agriculture, healthcare, aerospace, farming, defense, etc.

IoT Security Threats

IoT comes with lots of benefits and risks. Threats to IoT systems and devices can translate to bigger security risks because of certain characteristics that the underlying technology possesses.

IoT environments are functional and efficient, but they are likely to be abused by threat actors. IoT security threats is a major issue in IoT implementation. Threats such as distributed denial-of-service (DDoS), ransomware, and social engineering can be used to steal critical data from people as well as organizations.

Attackers exploit security vulnerabilities in IoT infrastructure to execute sophisticated cyber-attacks. Such threats can be more concerning for consumers as they are unaware of their existence and do not own the resources to mitigate them. Hence business must identify and address these security threats to offer high-end products and services to their consumers.

Types of IoT threats

Botnets

A botnet is a network that combines various systems together to remotely take control of a victim's system and distribute malware. Command-and-Control-Servers are used to steal confidential data, acquire online-banking data, and execute cyber-attacks like DDoS and phishing. Cybercriminals can utilize botnets to attack IoT devices that are connected to several other devices such as laptops, desktops, and smartphones.

Denial of service

A denial-of-service (DoS) attack cause a capacity overload in the target system by sending multiple requests. The attackers intention is not to steal critical data, but to slow down or disable a service to hurt the reputation of a business and affect their revenue.

Man-in-the-Middle

In a Man-in-the-Middle (MiTM) attack, a hacker breaches the communication channel between two individual systems in an attempt to intercept messages among them. Attackers gain control over their communication and send illegitimate messages to participating systems leading to critical malfunction.

Identity and data theft

Hackers can now attack IoT devices such as smart watches, smart meters, and smart home devices to gain additional data about several users and organizations. By collecting such data, attackers can execute more sophisticated and detailed identity theft.

In this manner, attackers can infiltrate multiple enterprise systems and obtain sensitive business data. Hence, IoT security threats can give rise to data breaches in multiple businesses.

Social engineering

Hackers also use social engineering to manipulate people into divulging sensitive information such as passwords and bank details. Alternatively, cybercriminals may use social engineering to access a system for installing malicious software secretly. This is typically executed using phishing emails, where an attacker has to develop convincing emails to manipulate people.

Ransomware

Ransomware attacks have become one of the most notorious cyber threats. In this attack, a hacker uses malware to encrypt data that may be required for business operations. An attacker will decrypt critical data only after receiving a ransom.

This can be the most sophisticated IoT security threat. There are several research reports that demonstrate the impact of ransomware. This can also be used to attack IoT devices and smart homes.

IoT Security

Introduction

IoT security is the act of securing Internet of Things devices and the networks they're connected to. IoT devices include industrial machines, smart energy grids, building automation, plus whatever personal IoT devices employees bring to work. The biggest challenge is that IoT devices were not built with security in mind. In the majority of cases, there is no way to install security on the device itself. In addition, they sometimes ship with malware on them, which then infects the network they are connected to.

IoT is perhaps the most complex and undeveloped area of network security. The figure below shows the main elements of interest for IoT security. At the center of the network are the application platforms, data storage servers, and network and security management systems. These central systems gather data

from sensors, send control signals to actuators, and are responsible for managing the IoT devices and their communication networks. At the edge of the network are IoT-enabled devices, some are simple constrained devices, others are more intelligent unconstrained devices. Gateways may perform protocol conversion and other networking service on behalf of IoT devices. Unconstrained devices may or may not implement some security capability. Constrained devices generally have limited or no security features. Gateway devices can provide secure communication between the gateway and the devices at the center, such as application platforms and management platforms.

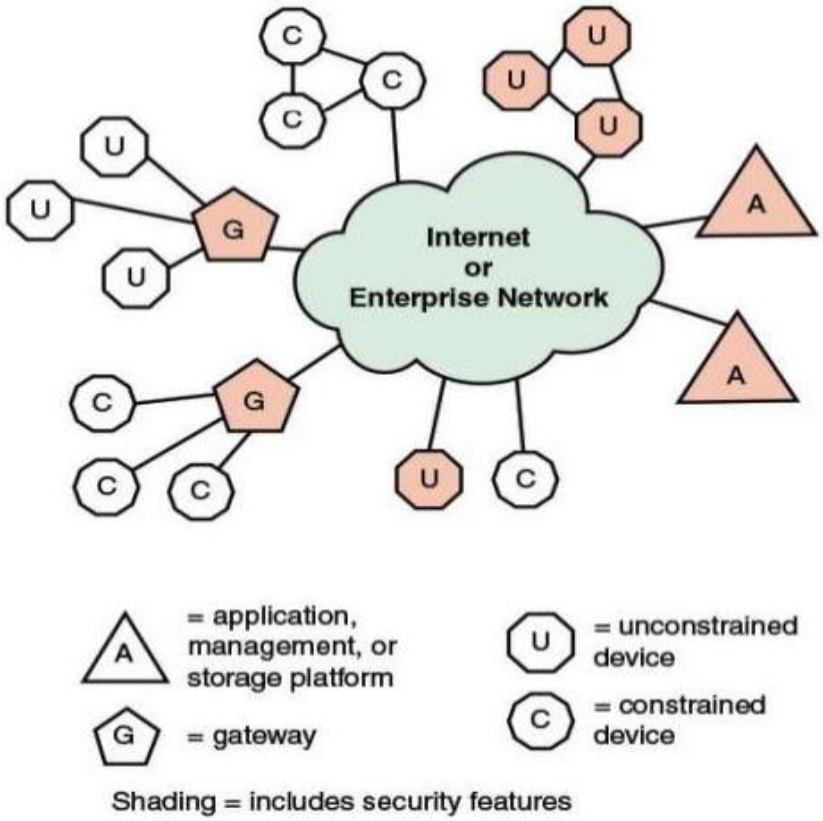


Figure: Elements of IOT Security

IoT Security framework

To address the highly diverse IoT environment and the related security challenges, a flexible security framework is required. The figure below illustrates the security environment from an IoT perspective.

It consists of

- Smart objects/embedded systems
- Fog/edge network
- Core network
- Data center/cloud

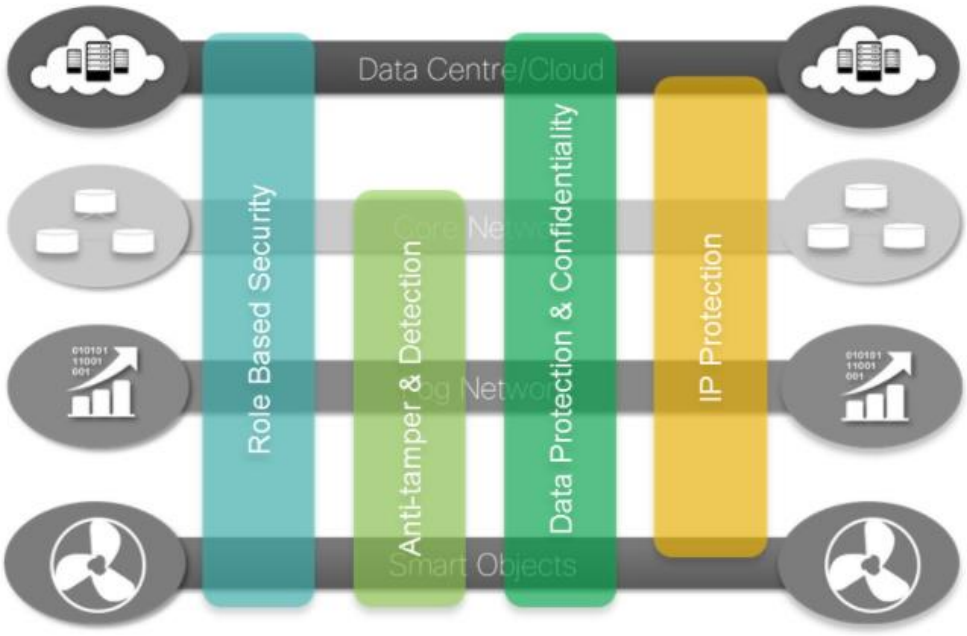


Figure: IOT Security Environment

Smart objects/embedded systems: Consists of sensors, actuators, and other embedded systems at the edge of the network. The devices may not be in a physically secure environment. Need to be concerned about the authenticity and integrity of the data generated by sensors. Protecting actuators and other smart devices from unauthorized use, privacy and protection from eavesdropping may also be requirements.

Fog/edge network: This level is concerned with the wired and wireless interconnection of IoT devices. A key issue of concern is the wide variety of network technologies and protocols used by the various IoT devices and the need to develop and enforce a uniform security policy.

Core network: Provides data paths between network center platforms and the IoT devices. The security issues here are those confronted in traditional core networks. However, the vast number of endpoints to interact with and manage creates a substantial security burden.

Data center/cloud: This level contains the application, data storage, and network management platforms. IoT does not introduce any new security issues at this level, other than the necessity of dealing with huge numbers of individual endpoints.

Addressing IoT security challenges

Businesses are subject to numerous critical market forces that keep changing how they need to execute their cyber programs. As IoT technology becomes more sophisticated and distributed within IT environments from the cloud to edge architectures, cybersecurity grows more complex. Hence, it is necessary to address the potential vulnerabilities.

Gain visibility into your IoT assets and continuously monitor them for risk

The first step in securing IoT is knowing what's connected. This includes using a device identification and discovery tool that automatically and continuously detects, profiles, and classifies what's on the network, maintaining a real-time inventory of devices.

Employ good cyber-hygiene and educate employees and device admins/owners

It is imperative to avoid hardcoded or default passwords and educate device admins on this. Limit the ability of IoT devices to initiate network connections; instead, only connect to them using network firewalls and access control lists which will limit attackers' ability to move laterally within the network. Segment by assigning policies and separating assets, which also stops the threat from moving laterally, as assets are classified and grouped together.

Maintain a separate network

The idea of separate networks is a strategy that will gain some traction. The reasoning behind this is: By keeping all the IoT equipment on a separate network, any compromise of a "smart" device will prevent the attacker from having a direct route to the user's primary devices where most sensitive data are stored. Also, jumping across the two networks will require considerable effort from the attacker.

Use honeypots

Internet honeypots are another strategy being used to secure IoT. These are decoy programs that look legitimate but are specifically designed to trap intruders trying to attack a system. During the process, the attackers are stealthily observed, without the intruder's knowledge. Information ollected through the honeypot can be sent to a sandbox for automated analysis. This makes it possible to preempt attacks, collect and assess malware targeting IoT devices, and take quick remediation actions.

Securing the future of IoT

We are just beginning to scratch the surface of what IoT can provide. However, there are many challenges that can be circumvented with edge and fog-based computing. With an edge node or a fog node, we can control and monitor traffic leaving the premises of the IoT device. IoT future scope or the future of IoT is very bright.

IoT is a full system of all the interconnected computing devices, that involves all the mechanical and digital machines. IoT devices can help develop more flexible and agile business environments. They also can help gather new types of information.

The Future of IoT Security

More Data Monitoring

The current issue in IoT security concerns the access IoT has to sensitive data and the movement of sensitive data overall. With enough time, hackers could theoretically use a connected kettle to gain your business' WIFI password.

Therefore, IoT security depends on intra-network data loss prevention. This tool helps ensure that IoT devices can't simply access data to which they aren't entitled. Further, it prevents malicious actors from

moving data through network nodes or out of the network; instead, it keeps all the data stored securely until an authorized user decides to move it. This can apply to devices as much as people.

Integration with Backup

When we discuss IoT security, the conversation usually hinges on endpoint security. Certainly, this stems from accurate beliefs. After all, IoT devices represent one more aspect of the hardware-based digital perimeter; each device opens another potential attack vector for external threat actors. Without visibility into every device brought by endpoint security, hackers could find a solid foothold for infections.

Unnecessary Capabilities

Of course, the future of IoT security depends largely on your own commitment to cybersecurity and the steps you take to ensure it. For example, many IoT devices come with default administrator passwords which are easily guessed or cracked. Your security team needs to take the time to reset these passwords wherever possible. Further, you need to turn off unnecessary capabilities on each device which could hamper cybersecurity efforts and protections.

Updates and Patches

Security depends on making sure that IoT devices receive regular updates to their security firmware and software. Like all devices, the updates these devices receive contain vital security patches and threat intelligence. Unfortunately, many IoT developers fail to make patching these devices a priority.

Conclusion

IoT connects the virtual world of information technology to the real world of things. It dramatically increases the availability of information and transforms business and organizations. As the technology advances, IoT could change our everyday lives, our everyday work, and our everyday communities. At the same time it is equally important to ensure security at all the phases to ensure your company, data and processes are protected.

References

- https://www.bbntimes.com/technology/iot-ai-and-blockchain-catalysts-for-digital-transformation
- https://www.imperva.com/learn/application-security/iot-internet-of-things-security/
- https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f#:~:text=In%20essence%2C%20IoT%20architecture%20is,a%20sophisticated%20and%20unified%20network.https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f#:~:text=In%20essence%2C%20IoT%20architecture%20is,a%20sophisticated%20and%20unified%20network
- https://www.intellectsoft.net/blog/biggest-iot-security-issues/