IOT Security (Lecture 11)

# IoT Vulnerabilities at Different Layers

Device based = Deficient physical security, insufficient energy harvesting

Network based = inadequate authentication, unnecessary open ports, improper encryption

Software based = insufficient access control, improper patch management capabilities, weak programming practices, Insufficient audit mechanisms

# IoT Security Objectives

**Confidentiality**: This security objective is designed to protect assets from unauthorized access and is typically enforced by strict access control, rigorous authentication procedures, and proper encryption.

IoT vulnerabilities which enable unauthorized access to IoT resources and data would be related to Confidentiality.

**Integrity:** The integrity objective typically guarantees the detection of any unauthorized modifications and is routinely enforced by strict auditing of access control, rigorous hashing and encryption (**protecting sensitive info unauthorised access**) primitives, interface restrictions, input validations and intrusion (**intruding**) detection methods. (**mainly detection**)

Integrity issues consist of vulnerabilities which allow unauthorized modifications of IoT data and settings to go undetected.

**Availability:** This security objective is designed to guarantee timely **access** to resources (including data, applications, and network infrastructure). Vulnerabilities which hinder the continuous access to IoT would be related to Availability.

**Accountability:** The accountability objective typically guarantees the feasibility of tracing actions and events to the respective user or systems aiming to establish **responsibility** for actions. Vulnerabilities that hinder proper logging would be related to Accountability.

# Countermeasures

Countermeasures is a classification of the available **remediation** techniques to mitigate the identified IoT vulnerabilities.

• Access and Authentication Controls

* Firewalls, algorithms & authentication schemes, biometric-based models, and context aware permissions

• Software Assurance (**Confidence that the software is free from vulnerabilities**)

* Software assurance is defined as "the level of confidence that software is free from vulnerabilities, and that the software functions in the intended manner"
* Software Assurance elaborates on the available capabilities to assert integrity constraints

• Security Protocols

* Lightweight security schemes for proper remediation ( improving the security situation).

# Situation Awareness

Capabilities categorizes available techniques for **capturing accurate and sufficient information regarding generated** malicious activities in the context of the IoT.

• Vulnerability Assessment

• Honeypots -Generally, a honeypot consists of data that appears to be a legitimate part of the site which contains information or resources of value to attackers. It is actually isolated, monitored, and capable of blocking or analyzing the attackers.

• Intrusion Detection

# Attacks against Confidentiality and Authentication

Aim: To gain unauthorized access to IoT resources and data to conduct further malicious actions.

• Mechanism: executing brute force events, eavesdropping IoT physical measurements, or faking devices identities.

• Dictionary attacks aim at gaining access to IoT devices through executing variants of brute force events, leading to illicit modifications of settings or even full control of device functions.

# Attack against Data integrity

**Injecting false data** or modification of device firmware

**False Data Injection (FDI)** attacks fuse legitimate or corrupted input towards IoT sensors to cause various integrity violations. For instance, launching such attacks could mislead the IoT device’s data, causing dramatic economic impact or even loss of human life.

**Firmware modification** is rendered by malicious alteration of the firmware, which induces a functional disruption of the targeted device

Denial of Service (DoS) attacks against IoT is to prevent the legitimate users’ timely access to IoT resources (i.e., data and services).

• By revoking device from the network or draining IoT resources until their full exhaustion.

Device capture: capture, alter or destroy a device to retrieve stored sensitive information, including secret keys

• Similarly battery draining attacks by flooding with messages

IOT Security (Lecture 10)

**• Profit driven businesses (In the context of IoT devices, many businesses are driven by the desire to generate profit. This focus on financial gains might sometimes lead companies to prioritize cost-cutting measures over investing in robust security mechanisms)**

**• Time-to-market constraint (IoT Technology is rapidly evolving and businesses often face intense competition to bring their IoT device to market quickly. This time to market constraint refers to the pressure companies face to develop and release their IoT product. In this rush to launch products quickly, manufacturers might not have sufficient time to thoroughly assess and implement comprehensive security measures)**

**• Absence of related legislation (Unlike some other industries, the IoT sector might lack specific regulations and legislation concerning security standards. In the absence of stringent laws mandating certain security practices for IoT devices, manufacturers might not be legally obligated to adhere to specific security standards. This absence of regulatory frameworks can lead to a lack of standardized security protocols across IoT devices.)**

**• Manufacturers overlook security considerations that result in potentially vulnerable IoT devices.**

# IOT based known Security Lapses (INTERESTING)

• Unauthorized voice recordings, emails and passwords by Internet-connected IoT toys[1]

• Cloudpet teddy bears could be turned into a remote surveillance devices.

• The company left a database containing customer data completely insecure.

• CloudPets' toys don't use any standard Bluetooth security features such as pairing encryption, when communicating back to their owner's smartphone's app. Anyone within range can connect to the toy, upload a message to the toy, "silently" trigger the toy's recording functionality, and "download the audio that the toy has recorded.

The hacking of traffic lights [2]

• With permission from a local road agency, the University of Michigan researchers hacked into nearly 100 wirelessly networked traffic lights. Weakness were: unencrypted wireless connections, the use of default usernames and passwords that could be found online, and a debugging port that is easy to attack

Hacking of Vehicles

Hackers remotely took control of a Tesla Model S from 12 miles away by exploiting the car's Controller Area Network (CAN bus). They manipulated various functions, including moving seats, triggering indicators, and even controlling brakes. Additionally, a "radio amplifier attack" targeted keyless entry systems in 24 car models from 19 manufacturers, allowing thieves to unlock and drive away these cars using a cheaply constructed device that alters radio frequencies to deceive keyless sensors into recognizing an owner's presence.

(The RF amplifier essentially amplifies the signal transmitted by the key fob. When the key fob is inside the owner's house, the amplifier extends the range of the keyless entry system. It tricks the car's keyless sensor technology into thinking that the key fob is nearby, even though it may be far away, inside the owner's house. This makes the car's security system believe that the owner is present and authorized to unlock or start the vehicle.)

# Technical Difficulties

**Limited Computational Capabilities:**

IoT devices often have restricted computing power, which limits their ability to process complex tasks or run sophisticated software applications. This limitation impacts their ability to perform advanced operations.

**Limited Storage:**

IoT devices typically have limited storage capacity for data. Storing large volumes of information locally can be challenging, especially for devices with minimal built-in storage capabilities. This constraint can affect the amount of data the device can store and process.

**Limited Power:**

Many IoT devices operate on battery power, making energy efficiency crucial. Power limitations require IoT devices to be designed to consume minimal power, enabling them to operate for extended periods without frequent battery replacements. This constraint affects the device's functionality and operational duration.

**Limited Update Mechanism:**

IoT devices often lack robust mechanisms for software updates. Ensuring that devices receive timely security patches and feature upgrades is challenging due to limited connectivity, compatibility issues, and the potential to disrupt device functionality during updates

**IoT communication protocols and technologies differ from traditional IT realms, their security solutions ought to be different as well**

# IOT Vulnerabilities

**Deficient physical security**

• Unauthorized physical access possible

**• Insufficient energy harvesting**

• Stored energy can be drained by an attacker by legitimate or corrupt messages.

**• Inadequate authentication**

• Simple authentication due to limited processing power and energy

**Improper Encryption**

• Resource limitations of IoT affects encryption

**• Unnecessary open ports**

• IoT devices have unnecessarily open ports while running vulnerable services

**• Insufficient Access control**

• IoT devices in conjunction with their cloud management solutions do not force a password of sufficient complexity

• Default user credentials not forced to change

• Most of the users have elevated permissions and can be misused.( **Insufficient access control refers to a situation where the permissions and privileges granted to users within a system are not properly restricted or regulated. In this scenario, most users have elevated permissions, meaning they have access to more resources and functionalities than necessary for their roles. This lack of control can lead to misuse, as users might exploit**)

.Improper patch management capabilities

• Manufacturers either do not recurrently maintain security patches or do not have in place automated patch-update mechanisms.

• Moreover, even available update mechanisms lack integrity guarantees, rendering them susceptible to being maliciously modified (**it refers to situations where the update files have been tampered with by malicious individuals or hackers.**)

(**Specifically, security patches are updates released by software manufacturers or developers to address vulnerabilities and security issues discovered in their software.**)

• Weak programming practices (**these devices lack robust systems to track and monitor user activities and system events effectively. Without proper auditing, it becomes challenging to identify and analyze security breaches,**)

• IoT manufacturers release firmware with known vulnerabilities

• Insufficient audit mechanisms

• IoT devices lack thorough logging procedures, rendering it possible to conceal IoT-generated malicious activities

Effect of Smart Products on Industry Structure (Lecture 09)

# Effect of Smart Products on Industry Structure

In any industry, competition is driven by five competitive forces:

• The bargaining power of buyers

• The nature and intensity of the rivalry among existing competitors

• The threat of new entrants

• The threat of substitute products or services

• The bargaining power of suppliers

**• Industry structure changes when new technology, customer needs, or other factors shift these five forces.**

**• Smart, connected products will substantially affect structure in many industries, as did the previous wave of internet-enabled IT.**

# Bargaining power of buyer’s

Knowing how customers actually use the products enhances a company’s ability to segment customers, customize products, set prices to better capture value

Smart, connected products also allow companies to develop much closer customer relationships.

• All of this serves to mitigate or reduce buyers’ bargaining power

(For example, if an engine is not operating as efficiently as expected or if there are any deviations in its performance parameters, this data can be used to pinpoint the issue. By detecting these discrepancies early on, GE Aviation and the airlines can take proactive measures, such as scheduling maintenance or making necessary adjustments, to optimize engine performance and ensure safe and efficient flights.)

GE Aviation, for example, is now able to provide more services to end users directly—a move that improves its power relative to its immediate customers, the airframe manufacturers.

• Information gathered from hundreds of engine sensors, for example, allows GE and airlines to optimize engine performance by identifying discrepancies between expected and actual performance.

**GE’s analysis of fuel-use data, for example, allowed the Italian airline Alitalia to identify changes to its flight procedures, such as the position of wing flaps during landing, that reduced fuel use (VERY USEFUL)**

• Buyers may also find that having access to product usage data can decrease their reliance on the manufacturer for advice and support. **(This information can include usage patterns, performance metrics, and other relevant data points. With this knowledge, buyers become more self-sufficient. They can troubleshoot issues, optimize product usage,)**

• Finally, compared with ownership models, “product as a service” business models or product-sharing services can increase buyers’ power by reducing the cost of switching to a new manufacturer.

**In the context of transportation, traditional ownership models involve individuals purchasing and owning their own cars. However, the rise of ride-sharing services, such as Uber and Lyft, represents a "product as a service" model in the transportation industry.**

**In this scenario:**

**Ownership Model: If someone owns a car, they are responsible for maintenance, insurance, fuel, and other associated costs. Switching to a new car or a different manufacturer typically involves selling the existing car, purchasing a new one, and dealing with the associated financial transactions and paperwork.**

**Product as a Service (Ride-Sharing): Alternatively, with ride-sharing services, consumers don't own the vehicles but instead pay for rides as a service. They can easily switch between different service providers (Uber, Lyft, or similar services) without the complexities of selling or buying a car**

# Rivalry among competitors

• Smart products also enable firms to tailor offerings to morespecific segments of the market, and even customize products for individual customers.

**(Smart products, equipped with sensors and connectivity features, enable businesses to collect vast amounts of data on how these products are used. By analyzing this data, companies gain valuable insights into customer behaviors, preferences, and needs. With this information, businesses can customize their products and services to cater to specific market segments more effectively. Moreover, they can even tailor products to individual customers, offering personalized experiences)**

• Smart, connected products also create opportunities to broaden the value proposition beyond traditional products, to include valuable data and enhanced service offerings. (**For instance, a smart home security system not only includes physical sensors but also offers real-time monitoring services and data analytics to improve home security. EXPANDING HORIZONS**)

Babolat, for example, has produced tennis rackets and related equipment for 140 years. • With its new Babolat Play Pure Drive system, which puts sensors and connectivity in the racket handle, the company now offers a service to help players improve their game through the tracking and analysis of ball speed, spin, and impact location, delivered through a smartphone application.

This transfers the cost structure of smart, connected products toward higher fixed costs and lower variable costs.

• This results from the higher upfront costs of software development, more-complex product design, and high fixed costs of developing the technology stack, including reliable connectivity, robust data storage, analytics, and security.

**When companies develop smart, connected products, they face higher upfront costs due to the complexity of software development, intricate product design, and creating a robust technology infrastructure. This includes costs for reliable connectivity, data storage, analytics, and security features. These initial expenses contribute to higher fixed costs.**

**However, once these fixed costs are incurred and the technology stack is established, the cost of producing additional units becomes significantly lower. This shift results in a higher upfront investment (fixed costs) but lower costs per unit in the long term (variable costs). The company invests heavily initially but benefits from economies of scale, making each additional unit more affordable to produce.**

# Threats to new Entrants

New entrants in a smart, connected world face significant new obstacles, starting with the high fixed costs of morecomplex product design, embedded technology, and multiple layers of new IT infrastructure. • Broadening product definitions can raise barriers to entrants even higher. **Biotronik, a medical device company, initially manufactured stand-alone pacemakers**, insulin pumps, and other devices. Now it offers smart, connected devices, such as a home health-monitoring system that includes a data processing center that allows physicians to remotely monitor their patients’ devices and clinical status.

Smart, connected products can also increase buyer loyalty and switching costs, further raising barriers to entry.

• Alternatively, barriers to entry may go down, when smart, connected products leapfrog or **invalidate the strengths and assets of existing** manufacturers.

• Existing manufacturers may **hesitate** to fully embrace the capabilities of smart, connected products, **preferring to protect hardware-based strengt**hs and profitable **legacy parts** and service businesses.

This opens the door to new competitors, such as the OnFarm, which is successfully competing with traditional agricultural equipment makers to provide services to farmers through collecting data on multiple types of farm equipment to help growers make better decisions, avoiding the need to be an equipment manufacturer at all. (**companies like OnFarm can compete successfully with traditional agricultural equipment manufacturers by offering services to farmers. Instead of manufacturing equipment, these new competitors focus on collecting data from various farm equipment. This data is then used to provide valuable insights**)

Product companies are also facing challenges from other nontraditional competitors like Apple, which recently launched a simpler, smartphone-based approach to managing the connected home with Homekit.

# Threat of Substitutes

In many industries smart, connected products create new types of substitution threats, such as wider product capabilities that can include the conventional products.

• For example, Fitbit’s wearable fitness device, which captures multiple types of health-related data including activity levels and sleep patterns, is a substitute for conventional devices such as running watches and pedometers.

**(In the past, people used specific devices like running watches or pedometers for tracking fitness-related activities. However, products like Fitbit's wearable fitness device go beyond these conventional devices. Fitbit captures diverse health-related data, including activity levels and sleep patterns, providing a comprehensive overview of the user's health and fitness.**)

New business models enabled by smart, connected products can create a substitute for product ownership, reducing overall demand for a product. (**Smart, connected products allow for innovative business models where consumers can access the benefits of a product without having to own it outright.**)

• Product-as-a-service business models, for example, allow users to have full access to a product but pay only for the amount of product they use.

**Another example is shared bike systems, which are springing up in more and more cities. A smart phone application shows the location of docking stations where bikes can be picked up and returned, and users are monitored and charged for the amount of time they use the bikes. • This shared usage will reduce the need for urban residents to own bikes. (USEFUL FOR EXAMPLES)**

The auto OEMs (Original Equipment Manufacturer) lacked the specialized capabilities needed to develop a robust embedded operating system that delivers an excellent user experience while enabling an ecosystem of developers to build applications.

**Auto OEMs’(ORIGINAL EQUIPMENT MANUFACTURER) traditional clout relative to suppliers is greatly diminished with suppliers like Google, which have not only substantial resources and expertise but also strong consumer brands and numerous related applications (for example, consumers may prefer a car that can sync with their smartphone, music, and apps). (FARHAN’s CAR vs Obi’s car)**

**Smart Product (Lecture 8)**

# Smart Products

Smart Products have complex systems that combine

• hardware • sensors • data storage • Computing entity • software • connectivity

In the energy sector, ABB’s smart grid technology enables utilities to analyze huge amounts of real-time data across a wide range of generating, transforming, and distribution equipment (manufactured by ABB as well as others), such as:

• Changes in the temperature of transformers and secondary substations.

• This alerts utility control centers to possible overload conditions, allowing adjustments that can prevent blackouts before they occur

**(1. Real-time Data Analysis:**

**ABB's smart grid technology allows utilities to analyze vast amounts of real-time data from various generating, transforming, and distribution equipment. This data includes information about crucial parameters such as the temperature of transformers and secondary substations.**

**2. Monitoring Changes and Alerts:**

**By monitoring changes in the temperature of transformers and substations, ABB's technology detects anomalies or fluctuations in the equipment's operating conditions. Unusual temperature variations can indicate potential issues like overload conditions, which, if not addressed, could lead to system failures or blackouts.**

**3. Proactive Prevention:**

**When these abnormal conditions are detected, the smart grid technology sends alerts to utility control centers in real-time. These alerts serve as early warnings, allowing utility operators to take proactive measures.**)

In consumer goods, Big Ass ceiling fans sense and engage automatically:

• When a person enters a room • Regulate speed on the basis of temperature and humidity • Recognize individual user preferences and adjust accordingly.

•At UWA, the Big Ass fans are in the E -Zone Building (INTERESTING)

# Smart Products: Tech Infrastructure

Smart, connected products require that companies build an entirely new technology infrastructure, consisting of a series of layers known as a “technology stack”.

**This technology stack includes** :

• Modified hardware

• Software applications

• Operating system embedded in the product itself

• Network communications to support connectivity

• Product cloud (software running on the manufacturer’s or a third-party server) containing the product-data database

• A platform for building software applications

• An analytics platform

• Smart product applications that are not embedded in the product (**When we talk about "smart product applications that are not embedded in the product," we mean software functionalities and applications that enhance the capabilities of a smart product but are not physically built into the product itself**)

All the layers are accessed through an identity and security structure, a gateway for accessing external data, and tools that connect the data from smart, connected products to other business systems. For example, ERP(Enterprise resource planning ), Product lifecycle management (PLM) and CRM (Customer relationship management) systems.

• ERP system track business resources (cash, raw material, production capacity, orders and payroll etc.

• PLM is the process of managing the entire life cycle of a product from its inception through the engineering, design, manufacture as well as service and disposal of manufactured products.

• CRM manages the company’s relationship and interaction with customers and potential customers

IoT enables not only rapid product application development and operation but the collection, analysis, and sharing of the potentially huge amounts of data generated inside and outside the products that has never been available before.

• Building and supporting the technology stack for smart, connected products requires substantial investment and a range of new skills—such as software development, systems engineering, data analytics, and online security expertise—that were rarely found in manufacturing companies in the **past**.

# Capabilities of Smart Product

The capabilities of smart, connected products can be grouped into four areas:

• Monitoring • Control • Optimization • Autonomy

# Monitoring

Smart, connected products enable the comprehensive monitoring of a product’s condition, operation, and external environment through sensors and external data sources.

• Using data, a product can alert users or others to changes in circumstances or performance.

• Monitoring also allows companies and customers to track a product’s operating characteristics and history and to better understand how the product is actually used.

**1. Design Improvement (Reducing Over-Engineering):**

**By analyzing usage data, companies can gain insights into how their products are used in real-world scenarios. This information helps in optimizing product design by eliminating unnecessary features (reducing over-engineering) and focusing on aspects that customers truly value. This targeted approach leads to more efficient and cost-effective product designs.**

**2. Market Segmentation (Analyzing Usage Patterns):**

**Collected data allows companies to analyze usage patterns based on customer types. This analysis enables businesses to understand the specific needs and preferences of different customer segments. By tailoring marketing strategies and product offerings to match these segments, companies can effectively target their audience, resulting in improved sales and customer satisfaction.**

**3. After-Sale Service Enhancement (Dispatching the Right Technician):**

**Monitoring data helps in diagnosing issues remotely and understanding the nature of problems faced by customers. This knowledge enables companies to dispatch technicians equipped with the right parts and tools, improving the efficiency of after-sale service. Swift and accurate repairs enhance customer experience and satisfaction, leading to positive reviews and brand loyalty.**

**• In some cases, such as medical devices, monitoring is the core element of value creation.**

**• Medtronic’s digital blood-glucose meter uses a sensor inserted under the patient’s skin to measure glucose levels in tissue fluid and connects wirelessly to a device that alerts patients and clinicians up to 30 minutes before a patient reaches a threshold blood-glucose level, enabling appropriate therapy adjustments. (INTERESTING)**

**Monitoring capabilities can span multiple products across distances.**

**• Joy Global, a leading mining equipment manufacturer, monitors operating conditions, safety parameters, and predictive service indicators for entire fleets of equipment far underground.**

**• Joy Global also monitors operating parameters across multiple mines in different countries for benchmarking purposes. (WE COULD HAVE DONE SOMETHING LIKE THIS)**

• Smart, connected products can be controlled through remote commands or algorithms that are built into the device or reside in the product cloud.

• For example, “if pressure gets too high, shut off the valve” or “when traffic in a parking garage reaches a certain level, turn the overhead lighting on or off, or display the filled capacity”.

# Control

• Control through software embedded in the product or the cloud allows the customization of **product performance** to a degree that previously was not **cost effective** or often even possible.

• The same technology also enables users to control and personalize their interaction with the product in many new ways. **For example, users can adjust their Philips Lighting hue lightbulbs via smartphone, turning them on and off, programming them to blink red if an intruder is detected, or dimming them slowly at night.**

• Doorbot (now named as Ring, https://ring.com), a smart, connected doorbell and lock, allows customers to give visitors access to the home remotely after screening them on their smartphones.

**(Mainly talks about control remotely)**

# Optimization

The rich flow of monitoring data from smart, connected products, coupled with the capacity to control product operation, allows companies to **optimize** product performance in numerous ways, many of which have not been previously possible.

• Smart, connected products can apply algorithms and analytics to dramatically improve output, utilization, and efficiency.

• In wind turbines, for instance, a local microcontroller can adjust each blade on every revolution to capture maximum wind energy. And each turbine can be adjusted to not only improve its performance but minimize its impact on the efficiency of those nearby.

• Real-time monitoring data on product condition and product control capability enables firms to optimize service by performing preventative maintenance.

• Advance information about what is broken, what parts are needed, how to accomplish the fix reduces the repair costs.

# Autonomy ()

**In the context of the Internet of Things (IoT), autonomy refers to the ability of connected devices or systems to operate and make decisions independently, without the need for constant human intervention or control.**

**These autonomous devices can collect and process data from their environment, make decisions based on predefined algorithms or artificial intelligence, and take appropriate actions. For example, in smart home systems, autonomous IoT devices like smart thermostats can analyze temperature patterns, learn user preferences, and adjust the temperature settings automatically without the homeowner manually adjusting the thermostat.**

• Monitoring, control, and optimization capabilities combine to allow smart, connected products to achieve a previously unattainable level of autonomy.

• At the simplest level is autonomous product operation like that of the iRobot Roomba, a vacuum cleaner that uses sensors and software to scan and clean floors in rooms with different layouts.

• More-sophisticated products are able to learn about their environment, self-diagnose their own service needs, and adapt to users’ preferences.

Autonomy not only can reduce the need for operators but can improve safety in dangerous environments and facilitate operation in remote locations.

• Autonomous products can also act in coordination with other products and systems. For example, the energy efficiency of the electric grid increases as more smart meters are connected, allowing the utility to gain insight into and respond to demand patterns over time.

**Ultimately, products can function with complete autonomy, applying algorithms that utilize data about their performance and their environment—including the activity of other products in the system—and leveraging their ability to communicate with other products. • Example, The Google self-driving car project , Waymo**

**FUTURE WORK OF THE BRIDGE PROJECT (I DID NOT PUT MUCH EMPHASIS)**

**• The IoT-based sensor data transmission to AWS needs further investigation to reduce the transmission rate. Edge computing at the source will reduce the amount of data to transmit to AWS, thus reducing the transmission cost and energy consumption. • The above research work need to be in line with bridge health monitoring parameters such as shifts in the fundamental frequency etc. • The future research work further encompasses comparison of digital accelerometer against analog wired accelerometer.**

**Smart Product (Lecture 6)**

# Smart Products – Transforming Businesses

Smart, connected products offer opportunities for

• New functionality

• Far greater reliability

• Much higher product utilization

• Capabilities that cut across and transcend traditional product boundaries

**The statement "The changing nature of products is also disrupting value chains, forcing companies to rethink and retool nearly everything they do internally" suggests that advancements in technology, market demands, and other factors are causing significant shifts in the way products are developed, produced, and distributed. As a result, traditional value chains, which outline the various steps involved in bringing a product from conception to the hands of the customer, are being disrupted.**

**This disruption necessitates companies to reevaluate and adapt their internal processes and strategies. In the face of changing products and consumer expectations, companies must reconsider their methods of production, supply chain management, marketing, and even organizational structure. They need to adopt new technologies, innovative approaches, and flexible strategies to keep up with the evolving market trends.**

The changing nature of products is also disrupting value chains, forcing companies to rethink and retool nearly everything they do internally.

• The idea of the value chain is based on the process view of organizations, the idea of seeing a manufacturing (or service) organization as a system, made up of subsystems each with inputs, transformation processes and outputs

•. Inputs, transformation processes, and outputs involve the acquisition and consumption of resources – money, labour, materials, equipment, buildings, land, administration and management. How value chain activities are carried out determines costs and affects profits.

• These new types of products alter industry structure and the nature of competition, exposing companies to new competitive opportunities and threats. They are reshaping industry boundaries and creating entirely new industries.

**The way companies acquire, transform resources into products, and deliver them affects costs and profits. New innovative products can disrupt industries, creating opportunities and threats.**

**They reshape existing markets and can lead to the emergence of entirely new industries, forcing companies to adapt or diversify their strategies to stay competitive.**

**In the context of the statement provided, "value" refers to the utility or worth that a product or service provides to customers.**

**(MAINLY TALKS ABOUT BUSINESS CHANGE ONCE SMART PRODUCTS ARE CHOSEN TO BE MADE)**

• Smart, connected products raise a new set of strategic choices related to

• How value is created and captured

• How the huge amount of new (and sensitive) data they generate is utilized and managed

• How relationships with traditional business partners are redefined

• What role companies should play as industry boundaries are expanded

**It is the expanded capabilities of smart, connected products and the data they generate that are ushering in a new era of competition.**

Before modern information technology, products were mechanical, and value chain activities relied on manual, paper-based processes and verbal communication. The first wave of IT in the 1960s and 1970s automated specific activities, boosting productivity. The internet ushered in the second wave in the 1980s and 1990s, enabling coordination across activities, suppliers, customers, and geography.

Now, IT has evolved further, integrating with products. Embedded sensors, processors, and connectivity enhance product functionality. Data analysis using product-usage data drives improvements, making IT an integral part of the product itself. This integration leads to enhanced product features and performance.

# Smart Products

Smart, connected products have three core elements:

• Physical components

• “Smart” components

• Connectivity components

Smart components amplify the capabilities and value of the physical components.

Connectivity amplifies the capabilities and value of the smart components and enables some of them to exist outside the physical product itself.

**Smart components, embedded with sensors and software, gain enhanced capabilities. Connectivity amplifies their functions, allowing them to communicate with other devices and exist independently, expanding their value beyond the physical product.**

• Physical components comprise the product’s mechanical and electrical parts. In a car, for example, these include the engine block, tyres, and batteries.

• Smart components comprise the sensors, microprocessors, data storage, controls, software, and typically an embedded operating system and enhanced user interface. In a car, for example, smart components include the **engine control unit, antilock braking system, rain-sensing windshields with automated wipers, and touch screen displays.**

• In many products, software replaces some hardware components or enables a single physical device to perform at a variety of levels.

# Smart Products: Connectivity

Connectivity components comprise the ports, antennae, and protocols enabling wired or wireless connections with the product.

• Connectivity takes three forms, which can be present together:

• One-to-one: An individual product connects to the user, the manufacturer, or another product through a port or other interface. Example, when a car is hooked up to a diagnostic machine.

• One-to-many: A central system is continuously or intermittently connected to many products simultaneously. For example, many Tesla automobiles are connected to a single manufacturer system that monitors performance and accomplishes remote service and upgrades.

• Many-to-many: Multiple products connect to many other types of products and often also to external data sources. An array of types of farm equipment are connected to one another, and to geo-location data, to coordinate and optimize the farm system. For example, automated tillers inject nitrogen fertilizer at precise depths and intervals, and seeders follow, placing corn seeds directly in the fertilized soil.

**1. \*\*One-to-One Connectivity:\*\***

**- \*\*Definition:\*\* A single product connects to a user, manufacturer, or another product through a specific port or interface.**

**- \*\*Example:\*\* When a car is connected to a diagnostic machine in an auto repair shop. The diagnostic machine communicates directly with the car to identify issues and perform diagnostics, enabling the mechanic to assess and fix problems.**

**2. \*\*One-to-Many Connectivity:\*\***

**- \*\*Definition:\*\* A central system is connected to multiple products simultaneously, either continuously or intermittently.**

**- \*\*Example:\*\* Tesla automobiles are connected to a central manufacturer system. This allows Tesla to monitor the performance of numerous cars in real-time. The system can accomplish remote services and upgrades for multiple cars simultaneously, enhancing efficiency and providing timely updates to improve performance or fix issues.**

**3. \*\*Many-to-Many Connectivity:\*\***

**- \*\*Definition:\*\* Multiple products connect with various other products and often external data sources, enabling complex interactions and optimizations.**

**- \*\*Example:\*\* In agriculture, different types of farm equipment, such as automated tillers and seeders, are interconnected. These machines are also connected to external data sources like geo-location data. By sharing information, the equipment coordinates their actions. For instance, the tillers inject nitrogen fertilizer at precise depths and intervals, and the seeders follow, placing seeds directly in the fertilized soil. This interconnected system optimizes the farming process for higher efficiency and better yields.**

**In summary, one-to-one connectivity involves a single product interacting with a specific user, manufacturer, or another product. One-to-many connectivity connects multiple products to a central system for monitoring and remote services. Many-to-many connectivity allows multiple products to interact with various other products and external data sources, enabling complex and optimized systems, as seen in agricultural practices.**

• Connectivity serves a dual purpose. First, it allows information to be exchanged between the product and its operating environment, its maker, its users, and other products and systems.

**• Second, connectivity enables some functions of the product to exist outside the physical device**, in what is known as the product cloud. For example, in Bose’s new Wi-Fi system, a smartphone application running in the product cloud streams music to the system from the internet. (**Example of product cloud functions is smart home security systems. These systems often have cameras, sensors, and alarms that are physically installed in a home. Through connectivity to the product cloud, homeowners can remotely monitor their security cameras, receive real-time alerts, and even control the system using a smartphone app or a web interface, regardless of their physical location. This allows users to enhance their home security, even when they are away from home, by accessing and managing the system through the cloud-based platform.)**

• To achieve high levels of functionality, all three types of connectivity are necessary.

**Smart, connected products require that companies build an entirely new technology infrastructure, consisting of a series of layers known as a “technology stack”.**

Components of IoT (Continuation)(Lecture 5)

# Components of IoT

• Sensors

• Connectivity

• Platform

• Analytics

• User Interface

**The provided text discusses different types of wireless connectivity based on frequency bands, licensing, and infrastructure requirements:**

**1. \*\*Frequency Band:\*\***

**- \*\*Licensed:\*\* These wireless systems operate on specific frequencies allocated by regulatory authorities. They require licenses and typically have better control and reliability. Examples include traditional cellular networks.**

**- \*\*Unlicensed:\*\* These systems operate on open frequency bands, allowing anyone to use them without a license. They are more flexible but may experience interference. Examples include Wi-Fi and Bluetooth connections.**

**2. \*\*Infrastructure Requirements:\*\***

**- \*\*With Infrastructure:\*\* These systems rely on established network infrastructures, such as cellular towers or Wi-Fi routers. They provide stable and widespread coverage.**

**- \*\*Infrastructure-less (Adhoc and Peer to Peer, Self-Organizing):\*\* These systems operate without a centralized infrastructure. Devices communicate directly with each other, forming ad hoc networks. Examples include peer-to-peer connections in Bluetooth devices.**

**3. \*\*Types of Wireless Systems:\*\***

**- \*\*Cellular:\*\* Traditional mobile phone networks that use cell towers to provide coverage.**

**- \*\*Paging:\*\* Communication systems used for one-way messaging, commonly seen in hospitals or public safety services.**

**- \*\*Fixed Wireless:\*\* Wireless communication used to provide high-speed internet access to fixed locations, often in rural areas.**

**- \*\*Satellite:\*\* Communication systems that use satellites to enable global coverage, useful in remote areas or for satellite TV services.**

**- \*\*Cordless:\*\* Wireless phones used within a limited range from their base station.**

**- \*\*WLAN (Wireless Local Area Network):\*\* Localized wireless networks commonly used in homes, offices, and public places.**

**- \*\*Bluetooth, UWB (Ultra-wideband):\*\* Short-range wireless technologies enabling data exchange between devices, such as smartphones, laptops, and peripherals.**

**- \*\*M2M (Machine-to-Machine):\*\* Wireless communication between devices without human intervention, often used in IoT applications.**

**- \*\*PAN (Personal Area Network):\*\* Short-range network for personal devices, allowing data sharing between devices like smartphones, tablets, and laptops.**

**In summary, the text provides an overview of various wireless connectivity options, ranging from licensed to unlicensed frequencies, with infrastructure-based and infrastructure-less approaches. Each type serves specific purposes and is suited for different applications, depending on factors like coverage, reliability, and range.**

**IMPORTANT**

**Certainly! Here's a more detailed explanation of the differences between Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS):**

**1. \*\*IaaS (Infrastructure as a Service)\*\*:**

**- \*\*Definition\*\*: IaaS provides virtualized computing resources over the internet. It offers virtual machines, storage, and networking, allowing users to rent virtualized hardware.**

**- \*\*Control\*\*: Users have the most control over their environment. They can install, configure, and manage software applications and operating systems.**

**- \*\*Examples\*\*: Amazon Web Services (AWS) EC2, Microsoft Azure Virtual Machines, Google Cloud Compute Engine.**

**- \*\*Use Case\*\*: IaaS is suitable for businesses that require complete control over their infrastructure, need to host custom software applications, or want to run virtualized environments.**

**2. \*\*SaaS (Software as a Service)\*\*:**

**- \*\*Definition\*\*: SaaS delivers software applications over the internet on a subscription basis. Users can access the software through a web browser without worrying about maintenance, updates, or infrastructure concerns.**

**- \*\*Control\*\*: Users have little to no control over the underlying infrastructure or software. They use the application as-is, without the ability to modify its code or backend.**

**- \*\*Examples\*\*: Google Workspace (formerly G Suite), Microsoft 365, Salesforce, Dropbox.**

**- \*\*Use Case\*\*: SaaS is suitable for businesses and individuals who want ready-to-use software applications without the hassle of managing and maintaining them.**

**3. \*\*PaaS (Platform as a Service)\*\*:**

**- \*\*Definition\*\*: PaaS provides a platform that includes tools and services for application development, such as development frameworks, databases, and operating systems. It abstracts the underlying infrastructure, allowing developers to focus on building and deploying applications.**

**- \*\*Control\*\*: Users have control over the deployed applications and data, but they do not manage or control the underlying platform or infrastructure.**

**- \*\*Examples\*\*: Heroku, Google App Engine, Microsoft Azure App Services.**

**- \*\*Use Case\*\*: PaaS is suitable for developers who want to build, deploy, and scale applications without managing the complexity of the underlying infrastructure. It is ideal for rapid application development and deployment.**

**In summary, IaaS provides virtualized hardware and maximum control, SaaS offers ready-to-use software applications with minimal control, and PaaS provides a development platform with a balance between control and abstraction, allowing developers to focus on coding and deploying applications. The choice among these services depends on the specific needs and technical expertise of the users or businesses.**

**PaaS provides a platform that enables developers to build, deploy, and manage applications without dealing with the complexity of underlying infrastructure. It sits between IaaS and SaaS, offering a middle ground where developers can focus on coding and deploying applications without worrying about the hardware, operating system, or server software.**

**Imagine you're a software developer building a web application. With PaaS:**

**You don't need to worry about setting up servers, operating systems, or databases.**

**You can focus entirely on writing the application code using the tools and frameworks provided by the PaaS platform.**

**The platform takes care of deploying your application, managing database connections, and ensuring that the application scales smoothly based on user demand.**

**In summary, PaaS simplifies the development process by providing a ready-to-use platform with all the necessary tools and services, allowing developers to concentrate on creating applications without getting bogged down by infrastructure management.**

**Lecture 4**

**MQTT (Message Queuing Telemetry Transport) is a machine-to-machine connectivity protocol that runs over TCP/IP.**

**Publisher sends message to specific topics, then broker which acts as a server or middleware It receives messages from Publishers and then routes these messages to Subscribers based on the topics they have subscribed to.**

**A Subscriber is a client that receives messages from specific topics**

**MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol designed for efficient communication between devices and applications, especially in IoT (Internet of Things) contexts. It operates on a publish-subscribe model, where publishers send messages on specific topics, brokers route these messages to interested subscribers, and subscribers receive messages based on their topic interests. MQTT is known for its simplicity, low bandwidth usage, and ability to work in resource-constrained environments, making it widely used for IoT and other messaging applications.**

**TTN, or The Things Network, is a global open-source IoT network infrastructure that enables devices to connect and communicate wirelessly over long distances.**

**In summary, TTN facilitates the communication between the smart street lights and the operator dashboard. It receives uplink messages from the devices, which are then processed, timestamped, and stored in a local SQLite database. The second tier of the operator dashboard utilizes this stored data to provide a user interface for the system operator, enabling efficient monitoring and management of the Smart Street Light System**

**Lecture 3 (IMPORTANT)**

**ARDUINO I/O pins**

**Pins RX0, TX1, and D2 through D13 are digital input/output pins. We often refer to these as just “pin 0” through “pin 13”, respectively. • Pins A0 through A5 can be used either as analog input or digital input/output (but not at the same time).**

**Certainly! Here's a brief overview of Zigbee, LPWAN (Low Power Wide Area Network), LoRaWAN, NB-IoT (Narrowband IoT), and Wi-Fi:**

**### Zigbee:**

**- \*\*Type:\*\* Short-range wireless communication protocol.**

**- \*\*Range:\*\* Typically up to 10-100 meters.**

**- \*\*Power Consumption:\*\* Low power consumption, suitable for battery-operated devices.**

**- \*\*Topology:\*\* Mesh networking, allowing devices to relay data to extend coverage.**

**- \*\*Applications:\*\* Home automation, industrial automation, smart lighting, healthcare, and sensor networks.**

**### LPWAN (Low Power Wide Area Network):**

**- \*\*Type:\*\* Long-range wireless communication network.**

**- \*\*Range:\*\* Several kilometers, often more than 10 km in rural areas.**

**- \*\*Power Consumption:\*\* Designed for low-power devices, enabling long battery life.**

**- \*\*Topology:\*\* Supports star, mesh, or hybrid network architectures.**

**- \*\*Applications:\*\* Smart cities, agriculture, industrial IoT, environmental monitoring, and asset tracking.**

**### LoRaWAN (Long Range Wide Area Network):**

**- \*\*Type:\*\* LPWAN technology based on LoRa (Long Range) modulation.**

**- \*\*Range:\*\* Several kilometers to tens of kilometers.**

**- \*\*Power Consumption:\*\* Extremely low power, enabling battery-operated devices with long lifespan.**

**- \*\*Topology:\*\* Star-of-stars topology, where end-devices communicate with gateways.**

**- \*\*Applications:\*\* Smart agriculture, smart metering, asset tracking, and environmental monitoring.**

**### NB-IoT (Narrowband IoT):**

**- \*\*Type:\*\* Low-power wide-area cellular network technology.**

**- \*\*Range:\*\* Similar to 2G/3G/4G cellular networks, covering wide areas.**

**- \*\*Power Consumption:\*\* Low power consumption, optimized for IoT devices.**

**- \*\*Topology:\*\* Uses existing cellular infrastructure, supporting massive device connectivity.**

**- \*\*Applications:\*\* Smart utilities, healthcare, logistics, and smart city applications.**

**### Wi-Fi:**

**- \*\*Type:\*\* Short to medium-range wireless communication technology.**

**- \*\*Range:\*\* Typically up to 100 meters indoors, longer outdoors with proper equipment.**

**- \*\*Power Consumption:\*\* Relatively higher power consumption compared to LPWAN technologies.**

**- \*\*Topology:\*\* Point-to-point or multipoint, connecting devices to a central access point or router.**

**- \*\*Applications:\*\* Home and office networks, public Wi-Fi hotspots, smart homes, and various consumer electronics.**

**In summary, Zigbee is ideal for short-range, low-power IoT applications; LPWAN and LoRaWAN offer long-range connectivity with low power consumption; NB-IoT provides cellular-based IoT connectivity; and Wi-Fi offers higher data rates for local area network applications. The choice depends on factors like range, power consumption, data rate, and specific use case requirements.**