Security for the IoT: A survey on existing communication models and protocols

Nithish Reddy Yalaka
40164619
INSE
Concordia University
nithishreddy.12@gmail
.com

***Abstract*— The Internet of Things (IoT) is a next-generation internet network that consists of intelligent objects with software and sensors that are employed in a variety of industries, including automotive, manufacturing, health, textiles, education, and transportation. The devices in an organization communicate with the cloud worker who measures and does the examination using several conventions. Although the ease and dependability that IoT offers is highly valued, new concerns have emerged as well. Current IoT conventions rely on IP Protocols, which are designed to provide security at several layers. Security is the most important aspect of IoT devices, and several protocols are designed to provide dependability and productivity. Several issues remain unsolved despite countless research efforts aimed at lessening the difficulty of these obstacles. In this report I will walk the reader through the IOT design, its layers, its functionality, its existing protocols, and the possible vulnerabilities they possess [1][2][11] [12][13].**

Keywords*— *IoT, IOT-Architecture, communication protocols, IoT Protocols, Security.

I. INTRODUCTION

Kevin Ashton created the phrase IoT (Internet of Things) in 1999. It is defined as a global network of interconnected physical items (also known as "things") capable of gathering and transferring data without the need for human intervention. Embedded systems (software, electronics, networks, and sensors) are used in these devices to collect data about the environment, communicate data over a network, respond to remote commands, and execute actions depending on that data. Wearables, implants, automobiles, machines, cellphones, appliances, computing systems, and any other item that can transmit and receive data are all examples of IoT devices or things available today. IoT can integrate cloud-based storage and computing, Cyber-Physical Systems, and big data networks. The Internet of Things is largely concerned with extending internet connectivity from traditional devices (such as computers, mobile phones, and tablets) to relatively simple items such as toasters. It converts old "dumb" gadgets into "smart" devices by allowing them to send data over the internet, allowing them to communicate with people and other IoT-enabled devices [2][3].

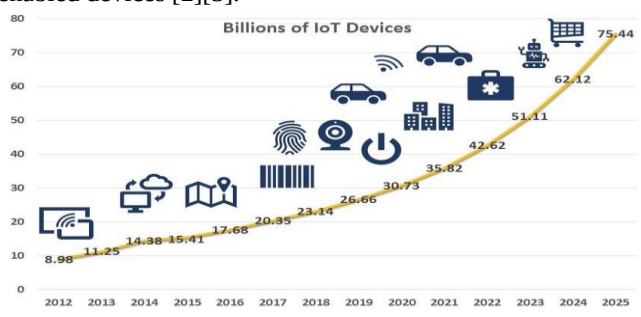

Image Source : Research paper – IoT over the years [1]

IoT is a concept that connects all devices to the internet and allows them to communicate with one another. IoT devices are categorized as sensors that collect data, while actuators serve as a communication and automation interface. The possibilities for IoT in the future are endless. Increased network agility integrated artificial intelligence (AI), and the ability to deploy, automate, coordinate, and secure various use cases at hyperscale will accelerate advancements in the industrial internet. It helps provide advanced healthcare facilities to patients, doctors, and researchers. These facilities include smart diagnosis, wearable devices for tracking health, patient management, and many more. Furthermore, IoT devices have reduced unnecessary strain on the healthcare systems by using the AI models.

As fascinating and advanced as the IoT maybe it does face many challenges in terms of privacy, network connectivity, reliability, insufficient testing, and lack of awareness. IoT applications may require suitable measures to protect communications with sensors if the Internet's network architecture evolves to incorporate them. The IoT has helped many technologies in various fields like smart homes, smart grids, smart cities, automation in industries, health care , energy systems. Hackers can gain access to connected IoT devices. Many IoT devices capture and send personal information over an open network without encryption, leaving it vulnerable to hackers. Cloud endpoints can potentially be used by hackers to target servers. To address the vulnerabilities, these applications will require the best security procedures.

In this report, I will initially discuss how the IoT works, the characteristics of IoT, different components of IoT, advantages and risks involved in IoT, different layers of protocol stack, applications of IoT, existing communication models, and existing threats in IoT as per their layers.

II. HOW IoT WORKS

Artificial Intelligence (AI) is at the heart of Internet of Things (IoT) devices. Sensors, a cloud component, data processing software, and cutting-edge user interfaces are all part of the Internet of Things.

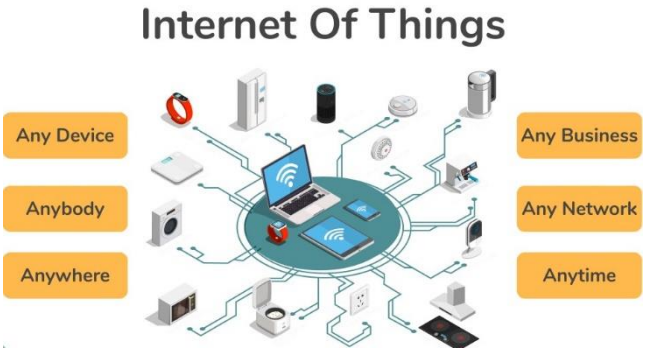

Image Source : Google Images – understanding the IoT

Sensors and gadgets are connected to the cloud via some sort of connectivity in IoT systems. For IoT devices, a Raspberry Pi with a quadcore processor can be utilized as an "Internet gateway." It's a card-sized computer with GIPO (general purpose input/output) pins for controlling outputs and sensors for collecting data about real-world circumstances. A sensor collects real-time data from the environment and sends it to the cloud infrastructure. Once the data has arrived in the cloud, the software program can evaluate it and determine what action to take, such as issuing an alert or proactively altering the sensors/devices without the need for user participation.

If user input is required or if they want to check in on the system, a user interface is used. The user's changes are then relayed back and forth via the system, from the user interface to the cloud, and from the cloud to the sensors/devices to adjust. As a result, a gadget that is highly reactive and intuitive is built, considerably increasing automation.

III. IoT CHARACTERISTICS

The most important characteristics of IoT on which it operates are connectivity, sensing, active engagements, scalability, and AI.

Connectivity: The most crucial part of IoT is connectivity. Without flawless communication among the interconnected components or objects, the IoT ecosystem (sensors, compute engines, data hubs, and so on) cannot function properly. Radio waves, Bluetooth, Wi-Fi, and Li-Fi are all options for connecting IoT devices.

Sensing: The next stage is to analyze the data that is being collected and apply it to develop effective business intelligence once all of the necessary objects have been connected. Extracting insight from the generated data is critical. A sensor, for example, generates data, but that data is useless unless it is properly understood by humans.

Active Engagements: Passive engagement accounts for a large portion of today's interactions with linked technologies. Multiple goods, cross-platform technology, and services collaborate on an active engagement basis through the Internet of Things. The usage of cloud computing in blockchain enables active engagements among IoT components in general.

Scalability: More and more elements are connecting to the IoT zone every day. As a result, IoT systems should be able to handle significant expansion. The amount of data generated as a result is enormous, and it must be properly managed.

Artificial Intelligence: The Internet of Items (IoT) uses data collecting, artificial intelligence algorithms, and networked technology to make things like mobile phones, wearables, and automobiles smart and improve people's lives. For example, if the coffee machine's beans are about to run out, it will place an order with the shop of user's choice.

IV. IoT COMPONENTS

The following are the four major components of IoT devices:

Sensors: A sensor or gadget is a critical component for collecting real-time data from the environment. This data can be of various types. This could be as simple as a temperature sensor, GPS, or accelerometer on the mobile phone, or as complex as a social media platform's live video capability. Sensors allow IoT devices to communicate with the real world and the environment. Different types of sensors are Gas sensors, Temperature sensors, IR sensors, Smoke sensors, proximity Sensors, Motion detection sensors, and Pressure sensors.

Connectivity: All data is collected and transferred to a cloud infrastructure. This could be accomplished by employing a variety of communication means to connect the sensors to the cloud, such as mobile or satellite networks, Bluetooth, WI-FI, WAN, and so on. Different methods of connectivity are used by different IoT devices.

Data Processing: It is the obligation of the data processors to process the data once it has been collected and transferred to the cloud. From regulating the temperature of the air conditioner to identifying faces on mobile phones, data processing software may improve IoT devices in a variety of ways.

User Interface: A User Interface is how an IoT device communicates with a user. A user interface is the visible and tactile part of an IoT system that users can interact with. It entails presenting data in a way that is beneficial to the end user. Users will be more likely to interact with a well-designed user interface because it will make their experience easier. End-users must be able to obtain information in some way, for as by receiving alerts by notification, email, or text message [4].

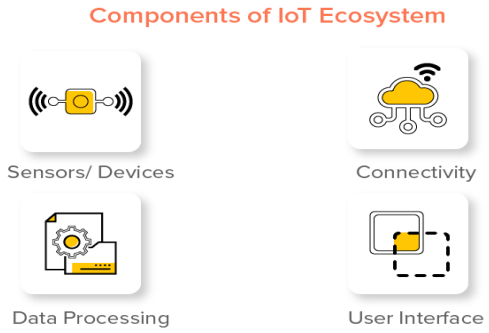

Image Source : Google Images – IoT Components [4]

V. ADVANTAGES of IoT

An Internet of Things (IoT) system is a sophisticated automation and analytics system that combines networking, big data, sensors, and artificial intelligence to deliver a comprehensive solution. It has the following advantages:

Ease of access: The Internet of Things has now made it possible to access real-time data from (nearly) anywhere. All it required is an internet-connected smart device.

Improved security measures: Access control systems can give additional security to companies and individuals by utilizing the Internet of Things. IoT technology in surveillance, for example, can help a business improve security standards and spot any illegal practices.

Improved insights: Currently the judgments are made based on superficial data, but IoT gives real-time data that leads to more efficient resource management.

Technical optimization: Technology has developed and become more efficient as a result of the Internet of Things. It has made even ancient "dumb" gadgets "smart" by allowing them to send data via the internet, allowing them to communicate with people and other IoT-enabled equipment. Coffee machines, smart toys, smart microwaves, and other smart devices are examples.

Effective time management: Overall, the Internet of Things can help save a significant amount of time. It is very well visible on the latest news, on our phones, peruse a blog about our favorite activity, or shop online while commuting to work.

Improved customer service and retention: By automating tasks, the Internet of Things makes for a better customer experience. The collection of user-specific data made possible by smart devices also aids organizations in better understanding client expectations and behavior. IoT also improves customer service by providing post-sale follow-ups such as automatic tracking and reminders of required

maintenance of acquired equipment after its predetermined duration of usage, the expiration of warranty periods, and so on.

VI. APPLICATIONS of IoT

In practically every business, the Internet of Things (IoT) is now being employed. Some of the most commonly utilized real-world applications of IoT are.

Medicine and Health: Real-time monitoring and patient care are possible with connected health systems. Patient information aids in the making of better medical decisions. In addition, the Internet of Things improves the power, precision, and availability of existing devices. Devices that track the health of generic people and share the data with the health-care system can help with disease identification early on.

Farming: Drip irrigation, analyzing crop trends, water distribution, drones for agricultural surveillance, and other techniques are being developed. These solutions will allow farmers to enhance yields while also addressing problems.

Smart Homes: One of the most practical IoT applications is smart houses. Though IoT is used at various levels in smart homes, the greatest one combines intelligent systems with entertainment. For instance, a set-top box with remote recording capabilities, an intelligent lighting system, a smart lock, and so on.

Wearables: Wearable gadgets have arisen as one of the first sectors to implement the Internet of Things on a large scale. Fit Bits, heart rate monitors, and smartwatches are just a few of the wearable technologies accessible today.

Hospitality: The use of IoT in the hotel business results in a greater degree of service quality. Using electronic keys supplied directly to guests' mobile devices, several interactions can be automated. As a result of IoT technology, integrated applications can track visitors' positions, give offers or information about interesting activities, place orders for room service or room orders, and automatically charge the room account.

Smart self-driving cars: Self-driving and operating cars were once thought to be a thing of the future; today they're a reality. Smart car technology allows user to use a phone app to keep track of the car's status, including its position, oil levels, gas, and more. Internet connectivity and onboard sensors are used by connected cars to optimize their operation, maintenance, and passenger comfort. Tesla, BMW, Apple, and Google are among the main automakers aiming to deliver the next revolution to the automobile industry [4][5][10].

Image Source : hackr.io blog – IoT Applications [5]

VII. IoT Architecture

There is no one-size-fits-all architecture for IoT projects due to the ever-evolving nature of IoT devices and the wide variety of sensors. Some of the building blocks, however, will be the same from project to project. First and foremost, the architecture must be constructed with scalability in mind. The amount of data that will be acquired over time will be vast, and a platform is required so that it can handle this in the long run. Availability in almost every possible time is expected. In the best-case scenario, system failures could cost huge finances, but in the worst-case scenario, they could be fatal. Finally, it is needed to design a system that is flexible enough to accommodate quick and frequent changes. As the architecture evolves, or the business needs change, it is required to iterate quickly without breaking the existing architecture [9].

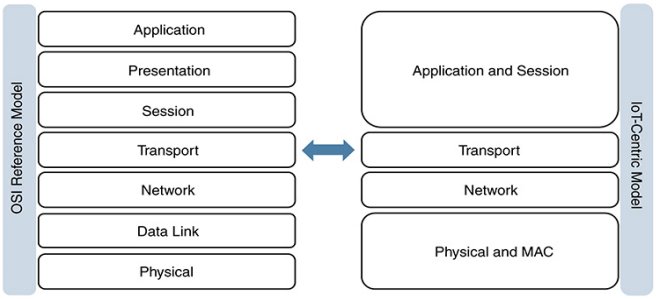

Image Source : Google Images – OSI vs IoT centric

While no two IoT projects are alike, the fundamental layers have always remained the same. The four-layer architecture has been the prevalent approach for IoT applications since the beginning of IoT research. Physical, Network, Transport, and Application are the four levels.

A. **Application Layer**:
This layer is where the user communicates. This layer is in charge of supplying application-specific resources to the consumer. Among other things, it distinguishes between smart houses, smart communities, and smart transportation. Restricted nodes use the CoAP protocol, whereas unconstrained nodes use HTTP.

B. **Transport Layer**:
This layer is responsible for end-to-end connectivity management, which includes characteristics such as packet repetition, congestion avoidance, and ensuring that packets are sent in the same order as those sent by the previous layer. UDP provides security at this layer. To preserve secrecy and honesty, IPsec protections are utilized.

C. **Network Layer**:
This layer contains network communications software as well as physical components such as architectures, servers, network nodes, and network components that enable devices to connect with one another. Its main purpose is to transport data between devices and between receivers and devices. This layer is made up of data transmission networks that are accessible via the internet. At this layer, the 6LoWPAN and IPsec protocols provide security. 6LoWPan is used in the WSN and the internet to secure low-power and computing-capable PCs. IPsec protocols are used by unrestricted nodes, while 6LoWPAN protocols are used by restricted nodes. The data from this layer is delivered to the cloud source as a payload and is encrypted using Internet protocol protection.

D. **Physical Layer**:
The physical layer, which acts as the IoT's foundation layer for networking smart devices, is made up of everyday hardware like

physical components, smart appliances, and power sources. The data from the sensors, actuators, and RFID is collected at this layer. Force, transmission speed, and energy utilization are all factors to consider in this layer. On the Internet of Things, a low-power wide area network (LPWAN) is used to transmit data to the organization layer. This layer's security is encoded via cryptographic calculations. The Link layer is in charge of connecting clever content, workers, and organizational devices. It uses various advancements depending on the type of sensors, such as Zigbee, 3G, 4G, and Wi-Fi. IEEE802.15.4 is used to provide security in this layer.

VIII. CHALLENGES ASSOCIATED with IoT

Though the benefits of the Internet of Things are particularly appealing in terms of enhancing business profitability, it also poses some risks.

Network Connectivity: Many IoT devices have trouble connecting to the internet. Especially if the devices are widely scattered, in remote places, or if bandwidth is scarce. The massive volume of interconnections between diverse devices and connectivity to the global network is the Internet of Things' defining feature. As a result, IoT devices necessitate an infrastructure that assures continuous wired and wireless connectivity with high throughput, low latency, and continual Internet access. To reap the benefits of iOS, a company must first provide all of the necessary networking equipment, such as cables, routers, hubs, and local data storage devices.

Reliability: It might be challenging to assure the stability of IoT systems due to the extremely scattered nature of IoT devices. Natural disasters, cloud service disruptions, power outages, and system failures can all have an impact on the components that make up an IoT system.

Privacy: Hackers can gain access to connected IoT devices. Many IoT devices capture and send personal information over an open network without encryption, leaving it vulnerable to hackers. Cloud endpoints can potentially be used by hackers to target servers.

High Skill Requirements: Responsible, experienced individuals with a thorough understanding of the scope and potential repercussions of their activity are required for IoT solutions. Deploying, setting up, maintaining, and altering the size of IoT solutions in a corporate enterprise necessitate highly qualified administrators, who may be difficult to find and hire due to the high wages they require. All staff who will be dealing with the smart device network should be properly trained and given clear instructions. While the Internet of Things decreases the demand for human resources, the remaining personnel must be well-trained to avoid disrupting smart device operations and causing the "snowball effect."

Security Flaws: Inadequate security measures are the most common flaw that stymies the growth of IoT as a whole. The danger of data leaks is constantly present since smart gadgets capture and transmit sensitive data that, if revealed, might have disastrous effects. IoT solutions, on the other hand, rarely have suitable anti-tampering features or comply with all necessary data protection standards, encryption protocols, and other policies and technologies aimed at preventing unwanted access to sensitive data. Failure to maintain adequate data security can result in costly, terrible, and even deadly repercussions, such as identity theft, the loss of corporate secrets, equipment, or products, and so on. As a result, expert development, and deployment of IoT solutions in businesses are required.

IX. EXISTING COMM. PROTOCOLS IN IOT

The existing IoT communication protocols will be thoroughly discussed in this section, which are meant to communicate with sensing devices. The techniques are intended to keep data safe and secure communication possible [12][13][14][15].

Layer	Protocol
Application layer	• Advanced Message Queuing Protocol (AMQP) • Message Queue Telemetry Transport (MQTT) • Constrained Application Protocol (CoAP)
Transport layer	• User Datagram Protocol (UDP) • Transmission Control Protocol (TCP)
Network layer	• 6LoWPAN • IP
Datalink layer	• LPWAN • IEEE 802.15.4 MAC
Physical layer	• IEEE 802.15.4 MAC • Near field communication (NFC) • Radio frequency identification (RFID) • Bluetooth Low Energy (BLE) • Ethernet

Image Source : Google Images – existing IoT protocols associated with layers

A. **Security Protocols for Application Layer**:

The HTTP protocol was used to request and receive data in this tier. This method is not appropriate for IoT devices. Because HTTP consumes more bandwidth, CoAP and MQTT were created to support devices.

1. Message Queue Telemetry Transport (**MQTT**): This protocol is widely used in devices that require only a moderate amount of bandwidth. The publish-subscribe messaging mechanism is used in this protocol. MQTT uses a binary format that requires only a tiny amount of bandwidth to operate. Message patterns include CONNECT, CONNACK, PUBLISH, and SUBSCRIBE. Using this protocol, messages are sent in open text format. It is simple to gain access to user information. The authentication technique is aided by Transport Layer Security (TLS). SSL and TLS transport encryption secure the information. Because any client must support TCP and the link to the broker must still be available, the disadvantages of MQTT packet loss are severe.
2. Constrained Application Protocol (**CoAP**): This protocol is designed to assist devices with minimal control transmission capacity. In accordance with the web's illustrated state move (REST) engineering, the CoAP convention implements a number of ways for packing application-layer convention metadata without including application interoperability. In the CoAP convention, communications between two endpoints are not exchanged at the same time. Using this method, Confirmable CoAP messages could be distinguished, with the sender performing a simple pause-and-stand-by retransmission component with the dramatic back-off. A Confirmable message should be recognized with a corresponding Acknowledge message, or it should be rejected with a Reset message if it requires setting to properly process the message. A Confirmable message containing a Message-ID and the location of the corresponding endpoint is used to identify Recognize or Reset messages. When marked apart as Non-Confirmable, CoAP communications may also be

communicated less reliably if the beneficiary does not identify the message.

B. **Security Protocols for Transport Layer**:

The transport layer is responsible for end-to-end communication and includes features like as reliability, congestion avoidance, and ensuring that packets arrive in the same sequence as they were sent. For performance reasons, UDP (User Datagram Protocol) is frequently used for IoT transport. This layer includes protocols such as TCP (Transport Control Protocol), UDP (Uniform Datagram Protocol), and others. Other protocols used in this layer include Secure Socket Layer (SSL), Datagram Transport Layer Security (DTLS), and Fast UDP Internet Connections.

C. **Security Protocols for Network Layer**:

Devices on the Internet of Things are resource constrained, which implies that their size, power, and memory space are all limited. IPV4 is a 32-bit address with a device capacity of 4 billion. Because each computer on the internet has an IP address, IPv4 is insufficient to accommodate all of them. IPV6, a 128-bit address, was introduced to combat this. A total of 2128 devices can be delegated.

The IPv6 Low Power Personal Area Network (IPv6 LoWPAN) protocol uses lightweight IP-based communication to traverse over low data rate networks. It has limited processing power when it comes to transferring data wirelessly via the internet protocol. As a result, it is mostly employed in the automation of homes and buildings. Only the 2.4 GHz frequency range and a 250-kbps transfer rate are supported by the 6LoWPAN protocol. 128-bit header packets are the maximum length. For the 6LowPAN communication protocol, security is a critical concern. At the 6LoWPAN security level, there are various assaults that try to direct the network's destruction. Because it is a hybrid of two systems, it is possible for an attack from both sides to target all layers of the 6LoWPAN stack. Fragmentation, 6LoWPAN Header, Dispatch Header, Mesh Addressing Mesh addressing, broadcast, fragmentation, and dispatch headers are optional, but they must occur in this order: mesh addressing, broadcast, fragmentation, and dispatch [6].

The IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) working group was established by the Internet Engineering Task Force in 2007 to develop a standard that would allow IPv6 packets to be transmitted over low-energy IEEE 802.15.4 and related wireless networking circumstances. There is a maximum packet size of 127 bytes, varying addresses and lengths, and limited bandwidth with this protocol. By compressing packet headers and establishing techniques for supporting IPv6 operations and address auto-configuration, the 6LoWPAN adaptation layer maximizes the utilization of available payload space. The information provided by the connection and adaption layers is utilized to condense network and transport protocol headers. RFC 6282 defines how User Datagram Protocol (UDP) headers can be compressed in the form of the 6LoWPAN adaptation layer.

D. **Security Protocols for Datalink and Physical Layer**:

The deployed IoT connectivity and internet solution is inadequate. New communications and security standards are being developed by the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE), which will be important in supporting future IoT applications. An organized protocol stack is possible because to the IEEE and IETF exchange protocols.
Due to the applicability of low-energy wireless networking situations, IEEE 802.15.4e constructs protocols with established technologies such as CoAP or 6LoWPAN in the Phy and Mac Layer. Other protocols, such as ZigBee, have proven to be industry standards in areas like smart energy. The IEEE 802.15.4e specification is utilized in critical industrial systems. The IEEE 802.15.4 PHY's main goal is to achieve reliability. Modulation techniques such as "Direct Sequence Spread Spectrum (DSS), Direct Sequence Ultra-Wideband (UWB), and Chirp Spread Spectrum (CSS)" can also aid. Using RFD (Reduced-function device) and FFD (Full-function device) interactions with IEEE 802.15.4, network topologies such as peer-to-peer, star, and cluster networks can be facilitated.

IEEE 802.15.4 computers can be identified using a 16-bit short identifier or a 64-bit IEEE EUI-64 identifier. Data frames, acknowledgement frames, beacon frames, and MAC commands frames are the four frames defined by IEEE 802.15.4 for data transmission. Collisions are handled at this layer using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The Advanced Encryption Standard (AES) is used by IEEE 802.15.4e to safeguard data at the hardware level. Secrecy, data authenticity, and honesty are all basic security needs that are met by the security mechanisms outlined below. The Security Enabled Bit field of the Frame Control field is set at the start of the header to define a protected frame.

X. COMMUNICATION MODELS in IoT

The operational perspective of the Internet of Things is all about connecting various devices and sensors to the Internet, but how to link them isn't always obvious. The Internet Architecture Board, which is part of the Internet Society and controls the technical growth of the Internet. Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing are four popular communication methods used by IoT "smart things" [7].

A. **Device-to-Device Communication**:

Two or more devices that are directly connected and communicate with one another are referred to as device-to-device communication. They can interact across a variety of networks, including IP networks and the Internet, although Bluetooth, Z-Wave, and ZigBee are the most common. This approach is frequently used in home automation systems to transport short data packets of information at a low data rate across devices. This might include light bulbs, thermostats, and door locks exchanging modest quantities of data. Because there is this short-range radio technology [and a] one-to-one interaction between these two devices, security is notably simplified with Device-to-Device.

Image Source : Research paper – D2D Communication model [7]

Wearable IoT devices, such as a heart monitor connected with a smartwatch, are appealing since data doesn't have to be shared with numerous people. There are several standards being developed for Device-to-Device communication, including Bluetooth Low Energy also known as Bluetooth Smart, which is popular among wearable and portable devices due to its low electricity needs, which could allow devices to run for months or even years on a single battery. Its smaller size and reduced cost are due to its decreased complexity.

B. **Device-to-Cloud Communication**:

To communicate and exchange data in this approach, an internet cloud service such as an application service provider is used. To exchange data and control message flow, an IoT device connects directly to an Internet cloud service like an application service provider via device-to-cloud communication. It typically connects via wired Ethernet or Wi-Fi, although it can also use cellular technologies. Wi-Fi or Ethernet is used to establish a link between the device and the IP network. Large corporations, such as Samsung Smart TV, adopt this type of communication technique. The Internet connection is utilized to send viewing data from users to Samsung for analysis. This model adds value to the end user by expanding the device's capabilities. Cloud connectivity allows a user (and an application) to access a device remotely. It may also be used to push software updates to the device.

Image Source : Research paper – D2C Communication model [7]

A smart tag that tracks the dog when the owner is not around would be a use case for cellular-based Device-to-Cloud, which would require wide-area cellular communication because it is not known where the dog was. From a security standpoint, this is more complicated than Device-to-Device since it involves two sorts of credentials: network access credentials (such as the SIM card on a mobile device) and cloud access credentials.

C. **Device-to-Gateway Communication**:

IoT devices link to an intermediary device to access a cloud service under the Device-to-Gateway architecture. This strategy often entails application software running on a local gateway device (such as a smartphone or "hub") that functions as a bridge between an IoT device and a cloud service. This gateway could provide security as well as other features like data and protocol translation. This application software may take the form of an app that pairs with the IoT device and communicates with a cloud service if the application-layer gateway is a smartphone. Gateway devices may also be able to bridge the gap between devices that communicate using various protocols. SmartThings' Z-Wave and Zigbee transceivers, for example, can connect with both types of devices.

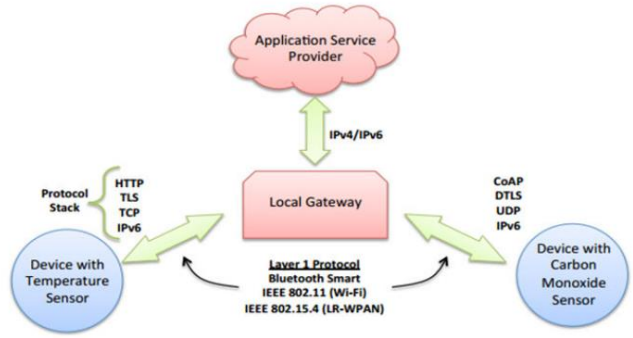

Image Source : Research paper – D2Gateway Communication model [7]

This may be a fitness tracker like Nike's that links to the cloud via a smartphone app, or home automation apps like Samsung's SmartThings ecosystem that involve gadgets that connect to a hub. Today, the general public either have to buy a dedicated gateway or utilize one of these multi-purpose gateways. All the gadgets are connected to that gateway, and it does something like data aggregation or transcoding, and depending on the use case, it either hands locally to the home or shuffles it out to the cloud.

D. **Backend Data Sharing Model**:

Back-End Data-Sharing fundamentally extends the single device-to-cloud communication concept to allow authorized third parties to access IoT devices and sensor data. Users can export and analyze smart object data from a cloud service, as well as data from other sources, and transfer it to other services for aggregation and analysis, using this approach. This approach defies the fear that everything will be trapped in a silo.

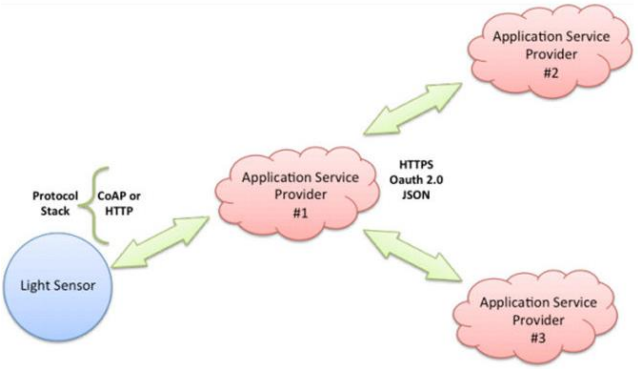

Image Source : Research paper – Backend Data Sharing Model [7]

Map My Fitness is an excellent example of this, as it gathers data from a variety of devices, including the Fitbit, Adidas miCoach, and Wahoo Bike Cadence Sensor. They provide Map My Fitness with hooks and REST APIs that enable for secure and private data sharing. This means that a workout can be evaluated from the perspective of multiple sensors.

XI. SECURITY THREATS in IoT

When cyber security is neglected, the IoT devices potentially contain serious risks and authorities for users. Some of the threat types and their counter measures in IoT are presented below:

Threat types	IoT devices	Countermeasures
Privacy, data, and identity theft	Parking garage, EV charging station, surveillances feeds	Authentication, encryption, and access control
Man in the middle	Wastewater overflow	Authentication, encryption, security lifecycle managements
Application level distributed denial of service (DOS)	Parking meters, plethora devices, etc.	Device identification, access control, security monitoring, and analysis [8]
Device hijacking	Smart meter, stealthily siphon energy, etc.	Device identification, access control, security lifecycle managements
Permanent denial of services (PDoS)	Parking meter replacement or reinstallation of updated software, etc.	Authentication, encryption, access control and application level DDOS protection, security monitoring, and analysis

Image Source : Research paper –Threat types and their countermeasures [8]

Because of particular aspects of the underlying technology, threats against IoT systems and devices translate to higher security risks. These properties make IoT settings functional and efficient, but threat actors are likely to take advantage of them. When it comes to security standards, the Internet of Things is a bit of a wild west. Because there is no universal standard for firms and niches, each company must set its own rules and guidelines. The lack of standardization makes it more difficult to protect IoT devices, as well as to allow machine-to-machine (M2M) communication without increasing security risks.

IoT have seen many attacks in the previous years and Different

types of defense mechanism are adopted to prevent the attacks in different layers of IoT and are presented below:

Layer	Attack	Countermeasures
Physical	Jamming (networks)	Channel surfing, priority messages, spatial retreat
	Tampering	Tamper proofing, hiding
	Radio interference	Delayed disclosure of keys
	Unfairness	Small frames
	Exhaustion	Rate limitation
	Collisions	Error-correcting code
Network	Sinkhole	Geo-routing protocol
	blackhole, wormhole	Authorizations, monitoring, redundancy
	Misdirection	Egress filtering, authorization, monitoring
	Homing	Encryption
Transport	De-synchronization	Authentication
	Flooding	Client puzzles
Application	Reprogram	Authentication
	Overwhelm	Rate-limiting

Image Source : Research paper – Attacks in different layers of IoT with their countermeasures [8]

XII. Conclusion

In this survey, I have summarized the evolution and architecture of IoT, understanding IoT, characteristics of IoT, components of IoT, advantages of IoT, applications of IoT, different layers in IoT and their existing protocols, challenges associated with IoT, existing communication models in IoT, and current security threats in IoT relevant to its layers. The research presented in this paper has revealed that IoT devices are a perfect target for assaults, with major ramifications for the services deployed. The IoT has evolved as an important technology. Data transmitted between IoT devices may contain sensitive information that must be kept safe from unauthorized access. IoT connectivity between two nodes is insecure, therefore IoT devices' physical security should not be compromised. IoT must incorporate services like encryption, end-to-end environments, and access control for real-time and critical infrastructure security to achieve secure communication. Staying one step ahead of the attacker in cybercrime is difficult. Improved security for smart devices in the future is expected, as well as higher privacy standards for IoT connectivity, allowing users to automate jobs more easily with this technology.

In the interconnected world, IoT with superior privacy, data protection mechanisms, and ethical standards will undoubtedly garner user trust and gain a competitive advantage. To enable safe communication at multiple stages in IoT, a detailed investigation of security protocols and processes is performed. In addition, Internet protocol security solutions provide security to sensing devices that are linked together. The research difficulties and advancements in existing protocols present possibilities for future research in this field.

XIII. REFERENCES

[1] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[2] https://en.wikipedia.org/wiki/Internet_of_things

[3] Waqas Toor, Maira Alvi, Mamta Agival: “Combined Access Baring Scheme for IoT Devices using Bayesian Estimation”

[4] https://appinventiv.com/blog/what-is-internet-of-things/

[5] https://hackr.io/blog/top-10-iot-applications

[6] https://www.javatpoint.com/iot-network-layer-protocols

[7] Husamuddin Mohammed, Mohammed Qayyum- “Internet of Things: A Study on Security and Privacy Threats”

[8] Debabrata Singh, Bibudhendu Pati, Chhabi Rani Panigrahi, Shrabanee Swagatika: “Security Issues in IoT and their Countermeasures in Smart City Applications”

[9] SA Kumar – “Security in IoT: Challenges, Solutions and Future Directions”

[10] Stefan Marksteiner, V´ıctor Juan Expo´sito Jime´nez, Heribert Vallant, Herwig Zeiner “An Overview of Wireless IoT Protocol Security in the Smart Home Domain”

[11] Tariq Aziz Rao, Ehsan ul Haq - ”Security Challenges Facing IoT layers and its Protective Measures”

[12] Cynthia Jayapal, Parveen Sultana, Saroja M N.J.Senthil – “Security Protocols for IoT”

[13] Sutaria R, Govindachari R (2013) “Making sense of interoperability: protocols and standardization initiatives in IOT”

[14] G Nebbione, M C Calzarossa, “Security of IoT Application Layer Protocols: Challenges and Findings”

[15] Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues: Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva