# Internet of things (IoT) and Security

Nagaraja Seshadri
REVA Academy for Corporate Excellence
REVA University
Bengaluru, India

Sivakumar Dhakshinamoorthy
REVA Academy for Corporate Excellence
REVA University
Bengaluru, India

***Abstract*— This paper introduces IoT (Internet of Things), which is creating a digital environment where every device is connected and is becoming more and more intelligent and increasing the efficiency of different processes. The Architecture, Technologies, Components, and Applications of the Internet of Things along with the challenges involved are highlighted. IoT increases productivity, shortens the processes involved, creates better products, and has a huge potential for innovation by integrating both digital and physical components.**

**This paper briefly describes the design of smart home automation architecture that utilizes a smartphone application to remotely control various appliances like door access, fans, geysers, CCTV, lights, air-conditioning, power and water supply at home. Different components with advanced technology are used to create a home automation application. The whole system which includes different appliances are preprogrammed, remotely controlled, and are constantly monitored.**

**We will also discuss key IoT challenges and security risks, and security requirements in this paper.**

***Keywords - Internet of Things (IoT); Gateway; Threats; Security; Home automation; Data Privacy***

## I. INTRODUCTION

Internet of Things is turning the world to more intelligent and advanced through digitization and by inter-connecting smart devices. IoT is useful in public utilities, manufacturing, transportation, agriculture, medical care, finance, emergency actions to natural disasters where it is difficult for human participation. IoT promotes digital transformation through improvement in connectivity by integrating a large number of devices. This is achieved by creating value from different forms of analysis of data that is created in this automated process.

IoT based Smart city project initiatives taken by the Government of India increase the city management efficiency and improves the quality of life by involving and connecting many public utilities like management of water, electricity, traffic, parking, fire protection, gas supply connections, and other various services through an intelligent platform.

IoT is becoming the major driver for digital transformation which is creating more and more innovations in products, optimization and automation of data analysis, new applications, R&D investments, new business, and revenue models across all sectors. Fig. 1 below shows IoT Utilities across various sectors [1].

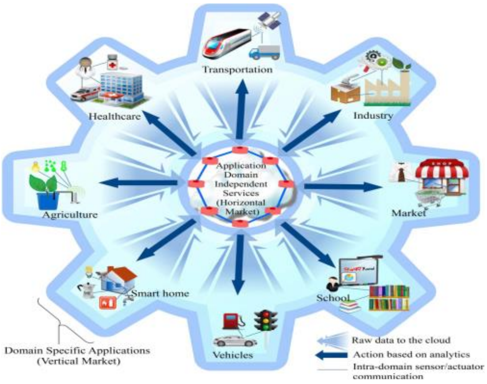
Transportation
Healthcare
Industry
Application Domain Independent Services (Horizontal Market)
Agriculture
Market
Smart home
School
Vehicles
Domain Specific Applications (Vertical Market)
Raw data to the cloud
Action based on analytics
Intra-domain sensor/actuator communication

Fig 1. IoT Utilities

## II. EXPONENTIAL GROWTH OF INTERNET OF THINGS

The number of devices getting connected, from computers to household devices to enterprise and industries has grown in the last 6 years at an annual rate of 23.1%, touching 50.1 billion things in 2020 [2]. Worldwide spending on IoT will cross $1 trillion in 2022 and $1.1 trillion in 2023 as per the IDC report [3].

IoT is primarily comprised of mobile devices and consumer-oriented things but lately, industrial automation is increasingly capturing a larger share in the IoT market.

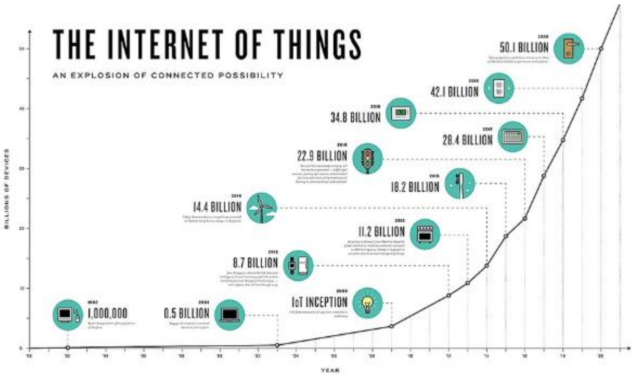

Fig 2 IoT connected things till 2020

Fig. 2 above shows the trend of IoT usage over time [3] [4].

## III. IoT Characteristics [5]

The Internet has seen phenomenal growth in the last few decades since more and more physical devices are getting connected every day and this is prompting organizations and governments to invest more in research activities surrounding IoT. This brings huge economic value when the industries are transformed digitally by intelligently connecting to smart devices. The data collection through IoT and analysis are further developing industries globally.

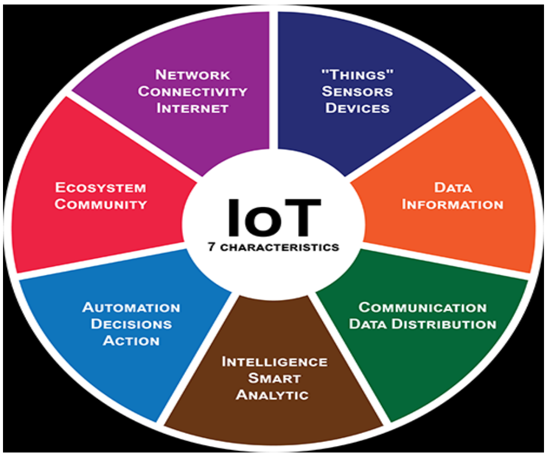

Fig. 3. IoT Characteristics

IoT Characteristics are depicted in Fig. 3 [5] above. The dimension of networks and connectedness is a major part of IoT definition. IoT enables ease of use of smart devices which will be tracked, located, and monitored through efficient network functions by the consolidation of IT infrastructure and physical infrastructure.

A regular device is converted into a smart device using the underlying technologies like pervasive computing, communication technologies, embedded devices, Internet protocols, sensor networks, and applications. A “thing” that contains technology which gives it additional capability to "do something", such as recording sound, measuring temperature or humidity levels, sensing movement, capturing location data. The device is capable of capturing and registering these forms of actions and context and convert it into data.

Data information intelligence is the essence of IoT. The data collected from different IoT devices must be communicated and converted into useful information, knowledge, insight, and actions.

There is no IoT without ("big") data, and no matter what actions the IoT system is addressing or solving, there is no use of IoT data distribution without understanding the data. Data analytics (Big Data), artificial intelligence (AI) and cognitive computing, and so on play major roles here.

Depending on the context, business process automation, industrial automation, or automatic software update all these can be remotely handled and monitored using IoT.

New technologies, innovations, and new applications need to grow proportionally. The estimated growth potential of IoT depends on market demands and customer needs. New devices with compatibility protocols to interact with different devices should be developed to suit customer requirements in terms of availability anywhere and anytime.

## IV. IoT Architecture [6]

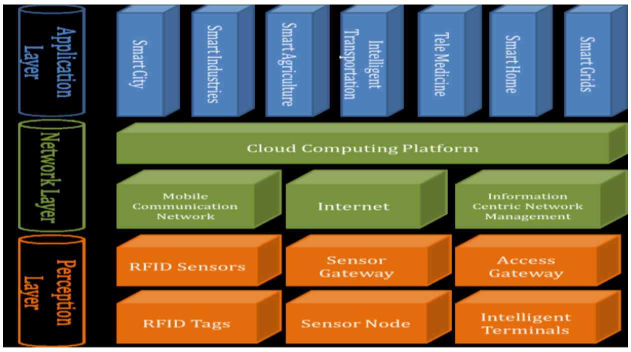

Fig. 4. IoT Architecture

IoT architecture as shown in Fig. 4 above [6], has three layers, but some researchers support the four-layer and five-layer architecture. IoT applications and enhancements require a broad architecture to fulfill the challenge in IoT in terms of security and privacy. A well-designed three-layer architecture can fulfill IoT security and privacy requirements. This network of devices also generates, collects data, and communicates through sensors, electronics, and software.

Perception, Network and Application layers are simplified and basic versions of IoT layers as shown in Fig. 4 [6].

The perception layer is the identification layer, it collects data and integrates with the physical world of hardware like RFID, sensors, etc. In this layer, different smart devices use sensors depending on the application requirement and can automatically sense and exchange information such as location, motion, vibration, and changes in the air among various other devices and systems.

The network layer also called the transmission layer provides basic networking support and data transfer over different networks, acts as a bridge between the other two layers. This layer manages the data by aggregating, processing, transmitting, a grouping of data as required. It handles the existing IT infrastructures such as fixed, wireless, mobile, etc. for transmission and energy efficiency, QoS requirements.

The deployment of various applications in IoT is defined in the application layer. Applications are depending on the customer service request. Few examples of the application layer are smart buildings, smart homes, smart transportation systems with intelligent traffic control, smart and efficient automation in manufacturing industries, and smart healthcare.

The four-layer architecture includes a support layer to take care of security by way of an authentication method.

The five-layer architecture approach includes the processing layer to overcome security and storage and business layer to manage and control applications, user’s privacy, business, and profits models of IoT

## V. Major Components of IoT

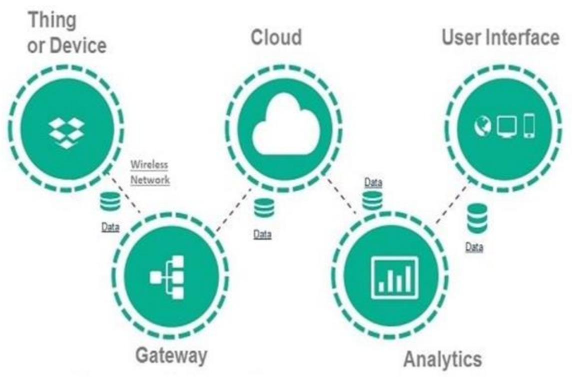

Fig. 4. IoT Major Components

Major Components of IoT are shown in Fig. 4 [7]

### *Device*

They are connected to collect and share data over the internet to perform a specific application.

IoT devices include wireless sensors, actuators, software, and other computer devices. Industrial components, environmental sensors, medical devices, mobile devices, will have this type of device fixed in it. The embedded technology in these objects transfers data by interacting with the external environment through the internet to accept and take decisions. For example, a pacemaker which is an IoT device communicates with other systems to save a life through rhythmic breathing patterns.

### *Gateway*

Internet of Things (IoT) gateway enables the communication between the devices and the cloud. It is a device or program that connects the sensors, controllers, intelligent devices to the cloud. It manages the data flow between different networks and protocols. As an intelligent gateway, it provides security for the IoT network. The security is offered with higher-order encryption techniques to protect the system from malicious attacks and unauthorized access. IoT Gateway features include Data caching, buffering, and streaming, Data pre-processing, filtering and optimization, data visualization, and basic data analytics via IoT Gateway applications and System diagnostics.

### *Cloud*

An IoT cloud platform provides the capabilities of IoT and cloud computing together to add value for consumer and business applications. It provides appropriate, convenient, safe, and complete IoT enablement service.

IoT cloud solution includes an IoT platform where it enables provisioning, management, and automation of smart objects within a given IoT infrastructure and cloud computing where the consumer and business applications are moved to the web, thus enabling IT performance and costs optimization. On-site IT infrastructure to store data and to run applications can be saved. The advantages of the IoT system in the cloud are scalability, data mobility, security, less time to implement, and cost-effectiveness.

### *Analytics*

IoT technology requires intelligent analytics to manage and improve the overall performance of the system and its operations. Analytics involves the process of converting analog data which is collected from smart devices and sensors through a detailed analysis for further interpretation. Real-Time smart analytics solutions reduce irregularities in the collected data and act fast to prevent any undesired scenarios. This data utilization provides and helps organizations in their future business opportunities and to plan for market demands.

The data collected through the IoT ecosystem helps to derive important business initiatives, visions, and decisions.

### *User interface*

User interfaces are the perceptible part of an IoT system as this is the one seen and accessed by the user. A well-designed user interface like new multicolor touch panels with interactive design, modern technology, common wireless standards is required to make it user friendly. To encourage users to buy smart devices or gadgets for more interactions, a well-designed user-friendly interface is required. Attractive interface with minimum effort and compatible device standards.

## VI. IoT Communication Technologies [8]

In IoT, multiple devices and diverse communication technologies are used to create seamless connectivity and operation. Design requirements include low power consumption, seamless communication, controlled resources, scalable, modular, and interoperable among various things which are to be connected.

IoT, a fast-developing concept, comprises smart devices networked worldwide as the Internet. Wireless communication technologies like Bluetooth, ZigBee, Lora WAN, 6LoWPAN-IPv6, Z-Wave, Wi-Fi, and RF Link are used depending on the requirement of speed, security, power utilization, data transfer rate, and overall efficiency in range, latency rate, and throughput.

IoT ecosystems depend on many different connectivity technologies, each of them for specific needs and requirements with advantages and limitations. Further developments in each protocol can create potential applications for its usage. In IoT applications, requirements such as range, QoS, security, power consumption, and network management are to be considered when selecting the best wireless technology. Fig. 5 below shows various Wireless technologies used in IoT [9].

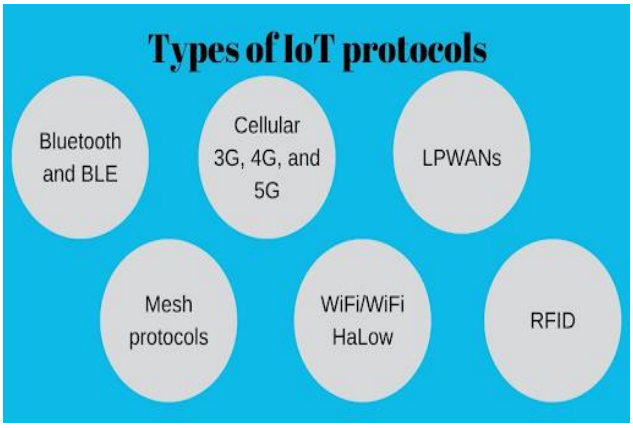

Fig. 5. IoT Wireless Technologies

*Wi-Fi*

Wireless fidelity is called Wi-Fi, the IEEE 802.11x standards are used to connect devices to the Internet. Wi-Fi interfaces are available in smartphones, laptops, tablet PC, and wireless router to communicate effectively and access the Internet. The features are star topology, 54mbps bandwidth, low power consumption, up to 20m range, 2.4GHz spectrum. The key advantage of Wi-Fi networks is easy to establish for instant connectivity.

*Bluetooth*

Bluetooth is an IEEE 802.15.1 standard**,** short-range, low-cost wireless technology designed to operate with very low power consumption. The features are star topology-based, 1Mbps bandwidth, up to 30m range, operates in 2.4GHz spectrum. Another name is Wireless Personal Area Network because it can create a personal area network during communication with other devices without essential to be in the line of sight. Bluetooth Low Energy LE uses less power to transmit data than standard Bluetooth, its usage can be seen in smartwatches and fitness trackers.

*Zigbee*

ZigBee is designed specifically to be employed in M2M networks. The technology is cheap to run and doesn't need loads of power, creating it a perfect resolution for several industrial applications. The technology features low latency and allowing products to maximize battery life.

Zigbee is based on IEEE 802.15.4 standard is suitable for application which needs lower date rate transfer and short-range. The features are Mesh, star and tree-based topology, 1Mbps bandwidth, very low power consumption, up to 300 m range, 2.4GHz spectrum. Home Automation, Lighting, Smart energy devices, HVAC are few applications.

*LPWANs*

Low Power Wide Area Network is used for long-range applications like industrial, smart city, and vast commercial buildings. It employs a centralized server unit to connect different devices with low-power consumption, higher security encryption methods, and supports large networks with devices, from 0.3 kbps to 50 kbps data rate ranges.

LPWANs have both the licensed and unlicensed spectrum. Parameters such as power consumption, Quality-of-Service, standardization, performance, reliability, scalability security, and interoperability plays a vital role while selection.

*Z-wave*

Z-wave operates on the 800-900MHz radio frequency range**,** a mesh network wireless communication technology, with a simple network protocol, low power consumption, AES-128 symmetric encryption**,** lower data rates, operates using low-energy radio waves, and completely interoperable.

Few Z-Wave devices are Flood Sensor, Smart Lock, Ring Door/Window Sensor, Dual In-Wall Switch, Logitech Hub Extender, Smart Lock, Bulb, Gateway, D-Link sensors, Security Hub, Lighting Control. It is used largely in design for home automation products such as lamp controllers and sensors.

*Cellular (3G/4G/5G)*

Cellular networks provide reliable broadband communication applications. Next-generation 5G enables real-time voice, data, and video applications due to its high-speed mobility support and ultra-low latency. Its high bandwidth cellular connectivity usage is in industrial automation applications like connected cars and fleet management. This requires high-power requirements and very high operational costs in the future.

Cellular IoT presents the following benefits: Large coverage area, open roaming capability, Connectivity choices to suit the needs, Remote management, and analytics, Private networks & security options. Type Selection depends on factors like response times, cost, and the amount of data being transferred.

*RFID Radio Frequency Identification*

RFID uses radio waves to transmit small amounts of information from an RFID tag to a reader within a short distance. By attaching an RFID tag to varied products and equipment, businesses can track inventory and assets in real-time – enabling better stock and production planning with supply chain management optimization and its usage can be seen in smart shelves, self-checkout, and smart mirrors in retail and logistics applications.

IoT Network protocols are depicted in Fig. 6 below [10].

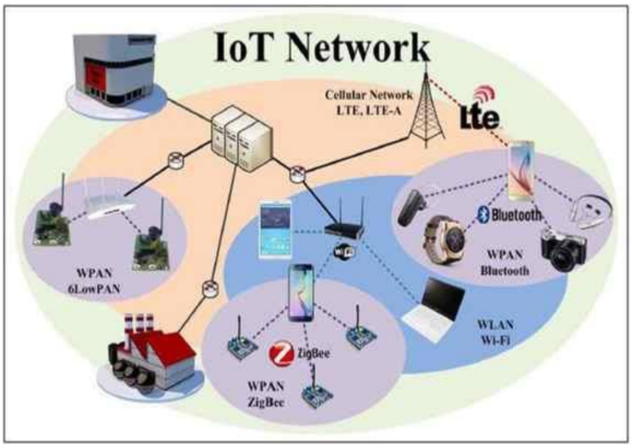

Fig. 6. IoT Network Protocols

## VII. IoT Application Development

Designing, executing, securely functioning, managing, and maintaining IoT projects are complex within an IoT architecture. While developing an end-to-end IoT system, collaboration is required between the open source community, High-Tech government institutions, and IoT provider companies [11].

Many applications, hardware's and ecosystems are being developed to support IoT technology to make life easier, safer, and more productive. The functionality of an IoT Architecture includes connecting devices, ensuring adaptable communication protocols, ensuring security features, data analysis, and management. This also creates new business opportunities by utilizing the collected data.

Various stages of IoT application development are explained in Fig 6 below [11].

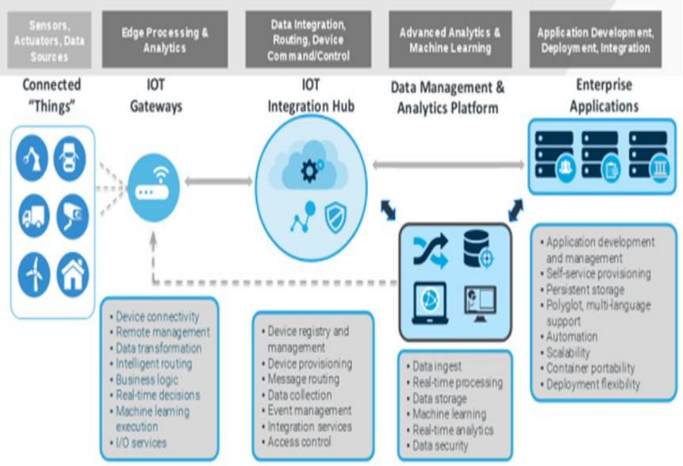

Fig. 6. IoT Application Development Stages

## VIII. IoT Applications

IoT application areas are manufacturing/industrial, Transportation/mobility, Smart Home, energy, Cities, buildings, retail and Trade, Agriculture, Supply chain, Health care, and much more. IoT Platform-enabled projects include other areas such as hospitality, enterprise, finance, and sports.

In this paper, the smart home application in IoT technology will be focused on.

## IX. IoT in Smart Home

Internet, electronic devices, and machines are taking over jobs from humans. By saving time from regular housekeeping tasks like washing dishes, laundry activities, gardening, preparing meals, allows humans time and energy to create new things, rearrange their time with new schedules, and to live differently.

### *Advantages of Home Automation Using IoT*

- A Smart home automation system through automatic control of electronic appliances smartly makes an individual's life easy, convenient, secure and saves time for better things.
- An automatic sensor-controlled time switch enables us to save energy and money.
- Kitchen devices are pre-programmed to work with time management and for remote usage. smart kitchen robot starts preparing food when required with pre-programmed time.
- Open garage automatically when the person reaches home using sensors.
- Smart home devices are used to prepare coffee, ACs and heaters control, doors, and window control.
- Automatic activation of services to make payments for power, gas, water, telecommunications utilities through service providers by collecting information.
- Enabling of emergency medical facilities for elders by sending a request or alarm to hospitals and clinics.
- Enabling home theatre entertainment equipment is automatically and remotely controlled to switch on as soon as a person enters the hall.
- Monitoring and activating control home security systems like CCTV using smartphone applications.
- Enabling a voice assistant device to control all other connected devices handsfree or a tablet with one single interface application.
- Building smart home automation using IoT devices can provide the convenience people want. Internet of Things technology with safe use will continue to make people's lives easier and better.
- Enable the development of various applications that make utilization of the tremendous amount of data produced by such a system to provide new services to various organizations, individuals, and other service-oriented sectors.

Home Automation includes different types of sensors for different applications, devices with different protocols, and technologies put together to make it an efficient design of a reliable system.

The concept of smart home applications and connected homes are being developed to create a smart city.

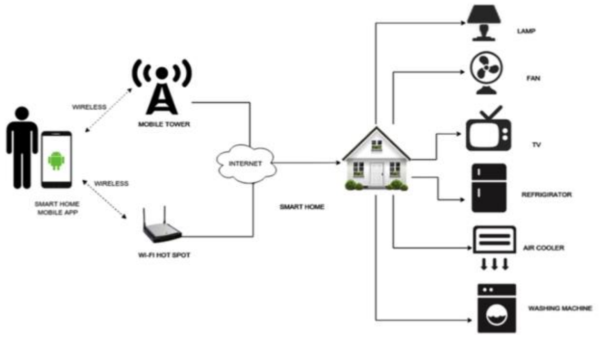

Fig. 7. Smart home

A typical IoT application in a smart home is shown in Fig. 7 above [12]

## X. IoT Security Risks and Challenges

When IoT technology usage is becoming important and growing in everyone's life, security issues associated with this technology are also increasing proportionately.

Shutting down the whole city, causing vehicle accidents, putting the patient's life in danger can be thought of as risks when IoT enabled devices compromised. IoT increases social efficiency and ease, but it also creates an array of latest problems concerning breach of privacy and information security at the same time. The privacy of users and the protection of their data is always at risk.

*IoT Security Challenges [13]*

Technology advancement in IoT with the invention of more and more IoT devices with new features leads to more unique security challenges.

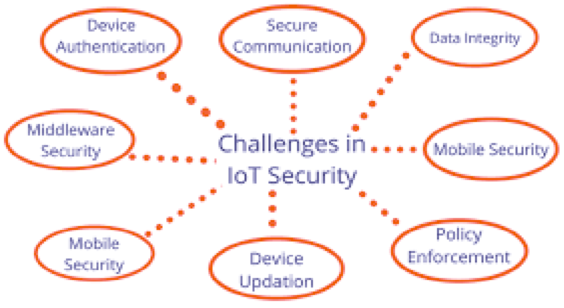

Fig. 8. IoT Security Challenges

Major challenges faced by IoT systems is shown in Fig. 8 above [14].

IoT-enabled devices and programs such as sensors, actuators, OS-based firmware, application software, and Wi-Fi communication, router are the components that are vulnerable to attacks on the system. These attack surfaces can become the entry point for malware introduction and system compromise.

- Weak authentication and authorization in IoT applications such as poor password protection and poor encryption.
- Distributed denial of service and spam attacks bringing the systems down.
- Data manipulation through system compromise by malware attacks such as spyware and ransomware.
- Artificial intelligence tools and automation can help hackers to detect patterns and use them to their advantage.
- Leakage of sensitive information by unauthorized manipulation by hacking into devices.

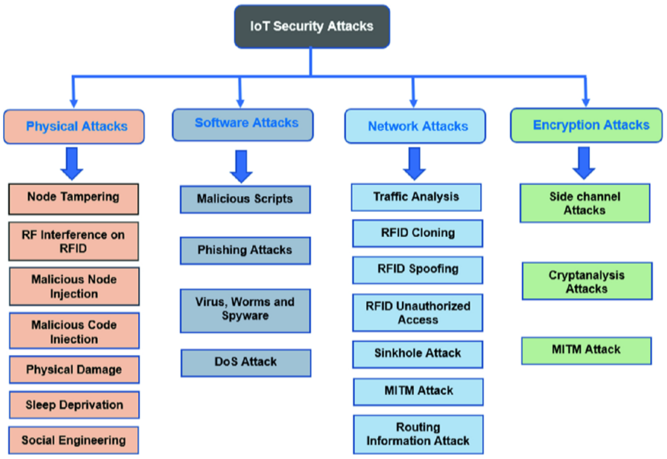

Fig. 9. IoT Attack Types

Various IoT attack types are explained in Fig.9 above [15].

## IoT Security Requirements.

IoT security is becoming a concern because the connected devices collect personal information and store in different platforms, which can be stolen by criminals. IoT Security protects these devices and networks from cybercrime.

Security mechanisms should be implemented throughout the life cycle of the IoT ecosystem which includes Security risk assessment and risk mitigation. Digital security must be designed by ensuring the integrity and confidentiality of IoT solutions and data by preventing vulnerabilities while mitigating cybersecurity risks.

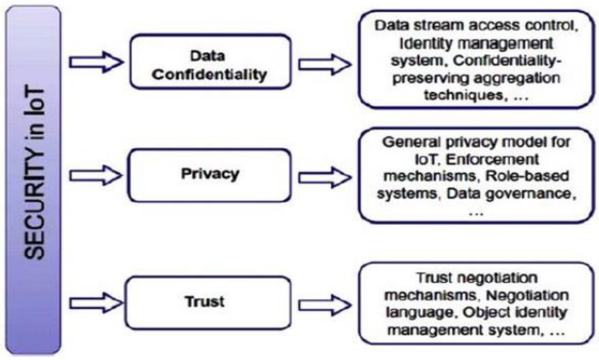
SECURITY in IoT
Data Confidentiality
Data stream access control, Identity management system, Confidentiality-preserving aggregation techniques, ...
Privacy
General privacy model for IoT, Enforcement mechanisms, Role-based systems, Data governance, ...
Trust
Trust negotiation mechanisms, Negotiation language, Object identity management system, ...

Fig. 10. IoT Security

Important IoT security features are shown in Fig. 10 above [16].

*IoT security features [16]:*

- Trust Establishment in Integration, Transactions, Platforms
- Embedded Security Measures, obtain digital certificates
- Brute Force Protection: Enable strong credentials for all devices in networks
- Network Security: secured Firmware, antivirus security software, and regular updates.
- Data Confidentiality and Privacy: Minimize Sensitive Data entry, check the privacy policy of the apps, disable unwanted features
- Secured Application programming interfaces (API)
- Use a secure end to end communication with encryption
- Security of managed IoT Cloud Solutions for integration with cloud computing.
- Secured VPN for data transmission through Wi-Fi
- Regular scanning and auditing to check attack logs.

## XI. CONCLUSION

IoT devices provide the ease that everyone wants in life. The government has taken many initiatives such as the adoption of IoT in smart cities development, traffic management, and healthcare services. Many industries and businesses are developing advanced solutions utilizing this fast-growing IoT technology for process automation and efficiency. During the implementation process of this technology, privacy and security risks should be carefully measured and assessed.

In this paper, we have presented the architecture and design of the Internet of Things, the components and protocols used. We have also discussed IoT applications of real smart home applications and how it helps in changing the lifestyle of humans. Besides, we have identified several security risks and challenges. Lastly discussed various security measures to overcome these challenges in IoT technology applications.

## REFERENCES

[1] A Al-Fuqaha, M Guizani, M Mohammadi, A, Mohammed & M Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications.” IEEE Communications Surveys &amp Tutorials. 17. Fourth-quarter 2015. 10.1109/COMST.2015.2444095.

[2] G. Press, “Internet of Things By The Numbers: What New Surveys Found,” 02-Sep-2016. [Online]. Available: https://www.forbes.com/sites/gilpress/2016/09/02/internet-of-things-by-the-numbers-what-new-surveys-found/.

[3] “Internet of Things Meets the Military and Battlefield,” IEEE Computer Society Internet of Things Meets the Military and Battlefield Connecting Gear and Biometric Wearables for an IoMT and IoBT Comments. [Online]. Available: https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt.

[4] “Internet of Everything: The IoT Market Is Projected to Expand 12x from 2017–2023,” Experfy Insights, 05-May-2020. [Online]. Available: https://www.experfy.com/blog/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023/.

[5] “What is the IoT?” NORDIGI. [Online]. Available: https://nordigi.no/index.php/en/blog/55-what-is-the-iot.

[6] “(PDF) Introduction to IoT Security,” ResearchGate. [Online]. Available: https://www.researchgate.net/publication/336406296_Introduction_to_IoT_Security.

[7] Rajiv, “What are the major components of Internet of Things,” RF Page, 10-Jan-2018. [Online]. Available: https://www.rfpage.com/what-are-the-major-components-of-internet-of-things/

[8] Rajiv, “Top 5 wireless technologies for IoT and 5G networks,” RF Page, 10-Jan-2018. [Online]. Available: https://www.rfpage.com/top-wireless-technologies-iot-5g-networks/

[9] N. Joshi, “Six types of IoT network protocols: IoT protocols: Artificial Intelligence,” Allerin, 07-Dec-2019. [Online]. Available: https://www.allerin.com/blog/six-types-of-iot-network-protocols.

[10] S. Mandal, “Internet of Things (IoT) - Part 4 (Network Protocols and Architecture),” C# Corner. [Online]. Available: https://www.c-sharpcorner.com/UploadFile/f88748/internet-of-thingsiot-part-4-network-protocols-and-arc/

[11] D. B. Lacima, “Building an Open End-to-End Internet of Things Architecture,” now + Next, 19-Dec-2017. [Online]. Available: https://next.redhat.com/2017/12/19/building-an-open-end-to-end-internet-of-things-architecture/

[12] V. Govindraj, B. Abubakar, and M. Sathiyanarayanan, “Customary homes to smart homes using Internet of Things (IoT) and mobile application,” ResearchGate, 2017. [Online]. Available: https://www.researchgate.net/publication/325516236_Customary_homes_to_smart_homes_using_Internet_of_Things_IoT_and_mobile_application

[13] “IoT Security 2020 Trends: Solutions, Technologies, Challenges, Platform,” brsoftech, 10-Jun-2020. [Online]. Available: https://www.brsoftech.com/blog/iot-security-solutions-technologies-challenges-platform

[14] D. F. Team, “IoT Security - Major Problems Faced by IoT System,” DataFlair, 15-Sep-2018. [Online]. Available: https://data-flair.training/blogs/iot-security/

[15] H. Atlam, G Wills, “IoT Security, Privacy, Safety, and Ethics.” In book: Digital Twin Technologies, and Smart Cities (pp.1-27) Publisher: Springer Nature Switzerland AG 2020, Mar-2019, 10.1007/978-3-030-18732-3_8.

[16] M. Gloukhovtsev, “IoT security: challenges, solutions & future prospects,” 2018. [Online]. Available: https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS_Gloukhovtsev-IoT_Security_Challenges_Solutions_and_Future_Prospects.pdf

[17] “IoT Solutions for Smart Home Automation: Future of Technology,” Ecosmob. [Online]. Available: https://www.ecosmob.com/iot-solutions-smart-home-automation-future-technology/

[18] “The Internet of Things (IoT) - essential IoT business guide”, 18-Aug-2020. [Online]. Available: https://www.i-scoop.eu/internet-of-things-guide/