**IoT Security and Privacy**



**A Seminar Paper**

**By**

**JOSHUA YULLU**

**S13/09381/17**

**CONTENTS**

[**Abstract**](#_heading=h.1fob9te)

[**1.0. Introduction**](#_heading=h.3znysh7)

[**Figure 1.0**](#_heading=h.2et92p0)

[2.0. IoT Overview](#_heading=h.tyjcwt)

[2.1. IoT and its Architecture](#_heading=h.3dy6vkm)

[2.2.1. Sensor’s layer](#_heading=h.1t3h5sf)

[2.2.2. Network Layer](#_heading=h.4d34og8)

[2.2.3. Application Layer](#_heading=h.2s8eyo1)

[2.3.0. IoT Security Issues](#_heading=h.17dp8vu)

[2.3.1. Part A: Security Concerns at Each Layer](#_heading=h.3rdcrjn)

[Sensors’ Layer](#_heading=h.unf9rg38a4xl)

[Network Layer](#_heading=h.mmpk7vrx55k4)

[Application Layer](#_heading=h.azvl5ia025zr)

[Part B. General Security Requirements and Challenges in IoT](#_heading=h.26in1rg)

[• Data Volume](#_heading=h.qqdy5w8iiqb0)

[• Resource limitations](#_heading=h.8f535evwcr9a)

[• Protection](#_heading=h.yohtqrp6uawj)

[• Scalability:](#_heading=h.t7gei5icmgoo)

[• Autonomic control](#_heading=h.7oa55eu9o0vm)

[PART C: Proposed solutions to IoT security](#_heading=h.lnxbz9)

[4.0. IOT PRIVACY CONCERNS IV](#_heading=h.35nkun2)

[4.1. Device Privacy](#_heading=h.1ksv4uv)

[4.2. During Communication](#_heading=h.44sinio)

[4.3. Privacy in Storage](#_heading=h.2jxsxqh)

[4.4. Privacy During Processing](#_heading=h.z337ya)

[5.0. DISCUSSION](#_heading=h.3j2qqm3)

[6.0.](#_heading=h.1y810tw)

[Conclusion](#_heading=h.1y810tw)

# **Abstract,**

The Internet of Things (IoT) is a rapidly growing technology that has the potential to revolutionize many aspects of our daily lives. IoT devices and sensors are used in many applications, from smart homes and connected cars to industrial automation and healthcare. However, the widespread adoption of IoT technology raises significant concerns about security and privacy. Many IoT devices are not designed with security in mind, making them easy targets for hackers. In addition, the large amount of data generated and collected by these devices can be vulnerable to cyberattacks if it is not adequately protected. It is vital to develop effective security measures for IoT systems and to ensure that personal data privacy is protected. This can be done through a combination of technical solutions, such as encryption and authentication, as well as legal and regulatory frameworks that establish standards and requirements for IoT security and privacy. The security and privacy of IoT systems is a critical issue that must be addressed to realize this technology's full potential.

# **1.0. Introduction,**

The Internet of Things (IoT) is, in simple terms, a collection of many nodes(devices) with the ability to connect and pass information to perform tasks. These nodes are not limited to portable computing devices like laptops, tablets, or smartphones. Nodes also include people, animals, and special-use devices like doorbells. These devices can sense their environment. They can also analyze and communicate. IoT connects business, industrial, and personal devices to a cloud where data can be stored and analyzed to produce information. IoT has applications in healthcare, safety, transport, education, and agriculture, just to name a few.

The number of IoT devices already in existence and those that innovators may create in the future varies considerably. By 2015, IBM predicted there would be more than one trillion connected devices, but this prediction still needs to be realized. By 2020, 50 billion devices were predicted by a widely cited Cisco estimate from 2011. According to frequently referenced research by Gartner Research, there were 8.4 billion devices in use in 2017, and 20 billion are anticipated by 2020. Statista recently forecasted that there will be 75 billion devices worldwide in 2025. Take these figures, along with the feverish market value estimates that follow them, with a grain of salt. It's simple to misjudge this, as the IBM prediction shows. The predictions vary in what they include. Thus it sometimes needs to be clarified as to what they allude.

Computers, mobile phones, industrial equipment, IP- and non-IP-based devices, and gadgets. The precise number of devices and those to come is not easy to determine.

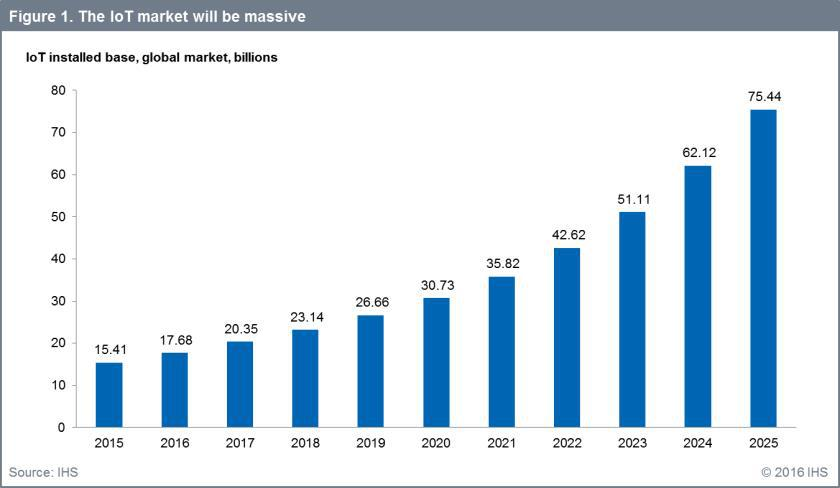
### *Figure 1.0*

| *The Internet of Things encompasses a vast array of merchandise.*  *This is a partial list that is sure to grow because Things is a broad term that will eventually include most digital products.*  *If something has a sensor and networking capabilities, it is considered to be part of the Internet of Things*.  **Consumer**  • smart doorbells  • autonomous cars  • fitness and health wearables  • smart thermostats  • smart TVs  • autonomous vacuums  • internet-connected toys  • smart bathroom devices  • smart door locks  •indoor security systems  •smart speakers  **Enterprise and Industrial**  •employee wellness trackers  •worker tracking devices  •disease management systems  •temperature-sensitive supply chain  •augmented reality maintenance equipment  •automated retail checkout  •autonomous trucking  • drones  •building management sensors  •automated retail checkout  •inventory optimization sensors  •smart office lighting  •face recognition cameras for security | | |
| --- | --- | --- |

Despite IoT shortcomings, IoT has shown considerable benefits to individuals and society. Many books and articles speak of how IoT will benefit humanity. IoT holds the potential to help parents keep their children safe. IoT has improved safety on roads. Some devices automate repetitive daily tasks. Others keep track of health and fitness.

We have installed many sensors in our homes and places of work. These have many benefits, but the risks are also evident.

This paper explores IoT architecture and the dangers of their increase in number. We will also discuss some solutions for these issues. By understanding this technology, one may take action to improve their security and privacy. As a community, we can start regulating the collection of consumer data. Governments can put laws in place on the proper handling of consumer data.The following chapter looks into the architecture of IoT devices.



## **1.1. Justification**

IoT security is essential because it protects the devices and networks that make up the IoT from being hacked or otherwise compromised. A breach of an IoT device or network can have serious consequences, such as the loss of sensitive data, the disruption of critical services, or even physical harm to individuals. For example, a hacked IoT device could spy on someone's home or launch a cyberattack on a power grid.

IoT privacy is also a key concern. Because IoT devices collect and transmit data, IoT can be used to track an individual's movements and activities. Hackers or malicious actors could use this to steal personal information or target individuals with unwanted advertising or harassment. In addition, the sheer volume of data generated by the IoT makes it challenging to ensure that this data is handled responsibly and ethically.

In short, the IoT can bring many benefits, but we must prioritize security and privacy to protect ourselves and our devices from harm. Let's take a look at the consequences of a breach in iot security and privacy.

## 1.2 Consequences of a breach in IoT security and privacy

IoT security and privacy breaches can severely affect individuals and organizations. Some potential consequences of a breach include

1. **Loss or theft of sensitive data, such as personal information, financial data, or other confidential information. This can lead to identity theft, financial fraud, or other types of damage to an individual's reputation or finances:**

Sensitive data can include personal information, such as a person's name, address, social security number, or other identifying information. It can also include financial data, such as credit card numbers, bank account information, or sensitive financial information. This data can be valuable to hackers, who can use it to commit identity theft, fraud or damage an individual's reputation or finances. For example, a hacker who gains access to a person's credit card information could use that information to make unauthorized charges, potentially causing financial losses for the person whose information was stolen. This type of data loss can have severe consequences for individuals. It is important for companies and individuals who use IoT devices to take steps to protect their sensitive data from potential breaches.

1. **Damage to an organization's reputation, financial losses, or legal liabilities if sensitive data is stolen or exposed as a result of a breach:**

If an organization's sensitive data is stolen or exposed as a result of a breach, this can have severe consequences for the organization. For example, suppose an organization's customer data is stolen. This can damage the organization's reputation, as customers may lose trust and be less likely to do business with it. In addition, the organization may incur financial losses if it is required to pay for credit monitoring services for its customers or if it is sued for failing to protect its customers' data adequately. Finally, the organization may face legal liabilities if it is found to have violated any laws or regulations related to data protection or privacy. These potential consequences highlight the need for organizations to protect their sensitive data from potential breaches of IoT security and privacy.

1. **Disruption of critical services or infrastructure if IoT devices are used to launch attacks on other systems, such as websites, servers, or power grids:**

Because IoT devices are often connected to other systems, such as websites, servers, or power grids, a breach in one device can potentially be used to launch attacks on these other systems. For example, suppose a hacker gains access to an IoT device connected to a power grid. In that case, they could potentially use that access to disrupt the power supply, causing widespread damage. Similarly, suppose a hacker gains access to an IoT device connected to a server. In that case, they could potentially use that access to launch attacks on the server, disrupting the services it provides. These types of attacks can have serious consequences, highlighting the need for companies and individuals who use IoT devices to take steps to protect them from potential breaches.

1. **Loss of trust in IoT technology and a decrease in its adoption:**

Suppose consumers or businesses are concerned about the security and privacy of IoT devices. They may be less likely to use these devices or to adopt new IoT technologies as they become available. This could hurt the growth and development of the IoT industry and the companies and individuals who rely on these technologies. To prevent this from happening, it is important for companies and individuals who use IoT devices to take steps to protect themselves from potential breaches and to educate others about the importance of IoT security and privacy. By doing so, they can help to maintain trust in IoT technology and ensure that it continues to be widely adopted and used.

1. **A breach of IoT security and privacy can cause physical harm to individuals:**

For example, if an attacker gains access to an IoT device or sensor that is used to control a critical infrastructure or service, such as a power grid or transportation system, they may be able to manipulate the operation of this system in a way that could cause physical harm to individuals.

In addition, if an attacker gains access to an IoT device or sensor that is used to monitor or control a medical device, such as a pacemaker or insulin pump, they may cause physical harm to the patient. Furthermore, suppose an attacker gains access to an IoT device or sensor to monitor or control a home security system. In that case, they may be able to manipulate the operation of this system in a way that could put the safety of the individuals living in the home at risk.

1. **Legal liabilities for the organizations or individuals responsible for the security of these systems:**

For example, if a company fails to implement appropriate security measures for their IoT devices and sensors, a breach occurs. As a result, they may be held legally responsible for any damages or losses that result from the breach. In addition, if an individual fails to protect the privacy of the personal data collected by their IoT devices and sensors, a breach occurs. As a result, they may be held legally responsible for any damages or losses that result from the breach.Furthermore, if a company or individual fails to report a breach of IoT security and privacy to the appropriate authorities, they may be subject to legal penalties or fines.

1. **Loss of intellectual property:**

Intellectual property refers to the creations of the mind, such as inventions, literary and artistic works, symbols, names, and images used in commerce. If an attacker gains access to an IoT device or sensor used to collect, transmit, or process intellectual property, they may be able to steal or misuse this property. For example, suppose an attacker gains access to an IoT device to collect data from a manufacturing process. In that case, they may be able to steal trade secrets or other sensitive information related to the manufacturing process. In addition, if an attacker gains access to an IoT device that is used to transmit or process intellectual property, they may be able to manipulate or misuse it. For example, suppose an attacker gains access to an IoT device used to transmit copyrighted works. In that case, they may be able to alter or distribute these works without permission, which could violate the copyright owner's rights.

1. **National security threats:**

Many IoT devices and sensors are used in critical infrastructure and services, such as power grids, transportation systems, and healthcare facilities. If an attacker gains access to these systems, they may be able to manipulate or disrupt the operation of these systems, which could pose a threat to national security. In addition, many IoT devices and sensors are used in defense and military systems, such as surveillance systems, communication networks, and weapons systems. If an attacker gains access to these systems, they may be able to manipulate or disrupt the operation of these systems, which could pose a threat to national security. Furthermore, many IoT devices and sensors are used in sensitive environments, such as government buildings, military bases, or other critical facilities. If an attacker gains access to these environments, they may be able to gather sensitive information, disrupt the operation of critical systems, or even launch physical attacks.

1. **Damage to personal relationships and reputation:**

For example, if an attacker gains access to an IoT device or sensor that is used to collect personal data, such as a home security system or a fitness tracker, they may be able to steal this data and use it to harm the individual's reputation or relationships. In addition, if an attacker gains access to an IoT device or sensor that is used to control a personal Device, such as a smart home system or a medical device, they may be able to manipulate the operation of this device in a way that could damage the individual's reputation or relationships. Furthermore, if an individual's personal data is stolen or exposed as a result of a breach of IoT security and privacy, this could damage their reputation and relationships, as other people may lose trust in them or may be concerned about their privacy.

The consequences of a breach of IoT security and privacy can be significant, and it is important for companies and individuals who use these devices to take steps to protect themselves from these risks.

## **1.**3**. Objectives**

The main objectives of looking into IoT security and privacy are to:

1. **Protect the personal data collected by IoT devices:**

By implementing effective security and privacy measures, companies and individuals can help to protect the personal data collected by IoT devices from being accessed or used without the user's consent. This can include measures such as implementing robust authentication and access controls, using encryption to protect data transmitted by devices, and implementing privacy controls to prevent the unauthorized collection or sharing of personal data. By implementing these measures, companies and individuals can help to ensure the privacy of the users of their IoT systems and can help to prevent data breaches or other privacy violations.

1. **Prevent unauthorized access to IoT devices and sensors:**

By implementing security measures such as robust authentication and access controls, companies and individuals can help to prevent unauthorized users from gaining access to their IoT devices and sensors. This can help to prevent attackers from gaining access to sensitive data, tampering with the operation of the devices, or using the devices to launch attacks on other systems. By implementing these measures, companies and individuals can help to ensure the security of their IoT systems and can help to prevent seizures or other security incidents.

1. **Protect critical infrastructure and services:**

Many IoT devices and sensors are used in critical infrastructure and services, such as power grids, transportation systems, and healthcare facilities. By implementing security measures such as encryption, access controls, and network segmentation, companies and individuals can help to protect these critical systems from being compromised by attackers. This can help to prevent disruptions to critical services and can help to ensure the reliability and resilience of these systems.

1. **Maintain trust in IoT technology:**

One of the main objectives of looking into IoT security and privacy is to maintain trust in IoT technology. As the number of IoT devices and sensors continues to grow, companies and individuals need to demonstrate that these systems are secure and trustworthy. By implementing adequate security and privacy measures, companies and individuals can help to ensure the security of their IoT systems and can help to build trust and confidence in this technology.

The main objectives of looking into IoT security and privacy are to protect the personal data collected by IoT devices, prevent unauthorized access to these devices, protect critical infrastructure and services, and maintain trust in IoT technology. By implementing adequate security and privacy measures, companies and individuals can help to ensure the security and privacy of their IoT systems. They can help to ensure the continued growth and adoption of this technology.

# **2.0. IoT Overview**

## **2.1. IoT and its Architecture**

Include three layers:

1. Sensors Layer
2. Network Layer
3. Application layer

Each layer has its security concerns.

### 2.1.1. Sensor’s layer

Is also known as the perception layer. This layer collects and processes data and then sends it to the network layer. It employs Radio Frequency Identification, sensors, and GPS.

### 2.1.2. Network Layer

Routing and forwarding of data are done at this layer. Some devices used at this layer include routers, gateways, hubs, and switches. Network technologies include Bluetooth, WIFI, Cellular (2G/3G, LTE), and others. This layer is used for collecting data and distributing filtered data between devices and hubs.

### 2.1.3. Application Layer

This layer offers an interface where the user can interact with the IoT device. The user can configure the device to work as they want. These are made simple and easy to use to reduce the evaluation curve.

The figure below represents a summarized view of what each layer in IoT architecture entails.

*Figure 1.0*

# The diagram presents a brief description of what each layer in IoT architecture entails.3.0. IoT Security Issues

Confidentiality, integrity, and availability are the core security objectives. We are going to take a look at how IoT devices perform at these objectives. IoT has many constraints that make securing these devices a difficult task. These constraints include the diverse nature of IoT devices and the small number of embedded security devices. This chapter takes a general look at security issues and then an objective look at each layer.

### 3.1**. A general look,**

The vulnerabilities of IoT devices can lead to a wide range of security and privacy issues, such as data breaches, identity theft, and unauthorized access to sensitive information. For example, suppose a hacker gains access to an IoT device. In that case, they may be able to steal the data that is collected by the device, potentially exposing sensitive information such as personal information, financial data, or other types of confidential information. In addition, if a hacker is able to gain access to multiple IoT devices on the same network, they may be able to use that access to launch attacks on other systems, such as websites or servers, potentially causing widespread damage. These security and privacy issues can have serious consequences for individuals and organizations, and it is important for companies and individuals who use IoT devices to take steps to protect themselves from these risks.

The issues of IoT security and privacy are as follows.

**The networks that connect IoT devices are also vulnerable**:

For example, an attacker could use a technique called a "man-in-the-middle" attack to intercept communications between an IoT device and the internet, allowing them to steal data or gain control of the device. We will look deeper at the network vulnerabilities in the next chapter.

**Malware and hacking are both major threats to IoT devices:**

Malware is a type of software that is designed to harm or exploit a computer or network. In the context of the IoT, malware can be used to gain unauthorized access to an IoT device or to steal sensitive data. For example, malware could be used to turn an IoT device into a "zombie" that is part of a larger botnet, or it could be used to extract sensitive information, such as login credentials or personal data. Hacking, on the other hand, refers to the unauthorized access of a computer or network. In the context of the IoT, hacking can be used to gain control of an IoT device or to steal data. For example, an attacker could use a "man-in-the-middle" attack to intercept communications between an IoT device and the internet, allowing them to steal data or gain control of the device.

**Many IoT devices are used in settings with little oversight or control, such as in a home or small business.**

This can make it easier for attackers to compromise these devices without being detected, as there may be no one monitoring the devices or the network they are connected to. For example, a hacker who gains access to an IoT device in a home may be able to use that access to move laterally to other devices on the same network, potentially compromising the security of all of the devices on that network. This lack of oversight and control can make it difficult to detect and prevent attacks on IoT devices, and it highlights the need for better security measures to be put in place in order to protect these devices from potential attacks.

**The lack of standardization in IoT devices is a security risk because it makes it difficult to ensure that these devices are secure and properly protected:**

In general, standardization refers to the process of establishing agreed-upon norms, rules, or criteria for a product or system. Regarding IoT devices, standardization could include agreed-upon communication protocols, security measures, or other technical specifications. Without standardization, different IoT devices may use different protocols or standards, making it difficult to ensure that they are interoperable and secure. For example, one IoT device may use a different security protocol than another, making it difficult to connect the two devices securely. In addition, the lack of standardization can make it harder for manufacturers to develop and implement security measures, as they may have to support multiple protocols or standards.

**Many IoT devices are not designed with security in mind, making them easy targets for hackers:**

Sensors, smart devices, and other connected objects, that are embedded with electronics, software, and other technologies that enable them to collect and exchange data. Many of these devices are not designed with security in mind, meaning that they do not have adequate security measures in place to prevent hackers from accessing or compromising them. This makes them easy targets for hackers, who can potentially gain access to these devices and use them to steal data, launch attacks on other systems, or cause other forms of damage. This lack of security is a major vulnerability of IoT, and it highlights the need for better security measures to be put in place in order to protect these devices from potential attacks.

**IoT devices often have weak or default passwords that are easy to guess, making it easy for attackers to gain access:**

Another of the vulnerabilities of IoT devices is that they often have weak or default passwords that are easy to guess. This means that hackers can potentially gain access to these devices by simply guessing the password or by using password-cracking tools to try different password combinations until they find the right one. This makes it easy for attackers to gain access to these devices, and once they have access, they can potentially use them to steal data, launch attacks on other systems, or cause other forms of damage. To prevent this from happening, it is important for users to set strong, unique passwords for their IoT devices and to avoid using the default passwords that come with the devices. This will make it much more difficult for hackers to gain access to these devices and help to protect them from potential attacks.

**IoT devices generate and collect a large amount of data, which can be vulnerable to cyberattacks if it is not properly protected:**

Another vulnerability of IoT devices is that they generate and collect a large amount of data, which can be vulnerable to cyberattacks if it is not properly protected. IoT devices are often used to collect data about the environment, people, or other objects, and this data can be valuable to hackers who want to steal it or use it for other nefarious purposes. If this data is not properly protected, it can be accessed by hackers and used to compromise the security of the devices or the systems they are connected to. To prevent this from happening, it is important for companies and individuals who use IoT devices to implement strong security measures to protect the data they collect, such as encrypting the data, using secure communication protocols, and regularly updating their security software. This will help to prevent attackers from accessing the data and protect it from potential cyberattacks.

**The interconnected nature of IoT devices** It is a feature and also a vulnerability of these systems. Because IoT devices are typically connected to each other and to other systems, a breach in one device can potentially compromise the security of many others. For example, if a hacker gains access to a single IoT device, they may be able to use that access to move laterally to other devices on the same network, potentially compromising the security of all of the devices on that network. This interconnectedness makes it difficult to secure IoT devices individually, and highlights the need for a more holistic approach to security that takes into account the entire IoT ecosystem. To address this issue, it is important for companies and individuals who use IoT devices to implement robust security measures that protect all of the devices on their network, and to regularly monitor and update their security systems to protect against potential breaches.

**Insufficient authentication and authorization.**

Authentication is the process of verifying the identity of a user or device, while authorization is the process of determining what actions a user or device is allowed to perform. If an IoT device does not have sufficient authentication and authorization measures in place, it may be possible for an attacker to gain unauthorized access to the device. For example, an attacker could use a brute-force attack to guess the password for the device, or they could use a spoofed device to impersonate a legitimate user or device. In either case, the attacker would be able to gain access to the device and potentially steal sensitive data or disrupt its operation. To address this security threat, it is important for IoT devices to have strong authentication and authorization measures in place. This can include using strong passwords, implementing multi-factor authentication, and carefully controlling access to the device. In addition, it is essential to regularly monitor and update these measures to ensure that they remain effective against evolving threats.

### **2.3.1. Part A: Security Concerns at Each Layer**

**The Sensors’ Layer and Network Layer:** The sensors layer and the network layer are critical parts of IoT systems, as it is responsible for collecting data from the environment and transmitting it to other devices and systems. There are several security issues that can affect the sensors layer in IoT, which can make these systems vulnerable to attacks. Some of the most common security issues at the sensors layer and the network layer include

1. **Physical tampering with sensors.**

For example, an attacker who gains access to a sensor that is collecting temperature data may be able to manipulate the sensor's readings in order to cause false data to be transmitted. This can have serious consequences, as it can lead to the collection of inaccurate data or to the disruption of the sensor's operation. To prevent this from happening, it is important for companies and individuals who use IoT sensors to implement physical security measures to protect these sensors from physical tampering. This can include measures such as installing sensors in secure locations, using tamper-resistant hardware and implementing access controls to prevent unauthorized users from gaining physical access to the sensors.

1. **Use of weak or default passwords on IoT devices,**.

Many IoT devices are shipped with default passwords that are easy to guess or with passwords that are very weak and can be easily cracked by attackers. This can make it easy for attackers to gain access to these devices and to use them to steal data or launch attacks on other systems. To prevent from happening, it is important for companies and individuals who use IoT devices to change the default passwords on these devices, and to use strong, unique passwords that are difficult for attackers to guess or crack. This will help to protect the security and privacy of the devices and the systems they are connected to, and will make it much more difficult for attackers to gain access to these devices.

1. **Lack of encryption for data transmitted from sensors to other devices,**

This can make it easy for attackers to intercept and read this data, potentially exposing sensitive information or allowing attackers to gain access to the devices and systems that the sensors are connected to. For example, if a sensor is transmitting unencrypted data about the temperature in a building, an attacker who intercepts this data may be able to use it to gain access to the building's heating and cooling system. To prevent this from happening, it is important for companies and individuals who use IoT sensors to implement encryption for the data transmitted by these sensors. This will make it much more difficult for attackers to intercept and read the data and will help to protect the security and privacy of the devices and systems that the sensors are connected to.

1. **Lack of authentication and access controls,**

This can allow unauthorized users to gain access to the sensors and the data they collect, potentially compromising the security and privacy of these devices and the systems they are connected to. For example, if a sensor does not have authentication or access controls in place, an attacker who gains access to the sensor may be able to collect data from it or interfere with its operation. To prevent this from happening, it is important for companies and individuals who use IoT sensors to implement authentication and access controls for these sensors. This can include measures such as requiring users to provide a password or other form of credentials in order to access the sensors or using encryption to secure the data transmitted by the sensors. By implementing these measures, companies and individuals can help to prevent unauthorized access to the sensors and protect the security and privacy of the data they collect.

1. **Use of outdated or insecure protocols, such as older versions of the TCP/IP protocol,**

The latest disclosures are based around a fundamental aspect of TCP communication in embedded devices: Initial Sequence Number (ISN) generation. These ISNs are designed to ensure that every TCP between two computers or other internet-connected devices is unique and that third parties can't interfere with or manipulate connections.

In order to ensure this, ISNs need to be randomly generated so an attacker can't guess it, hijack it or spoof it. It's a fundamental of computer security that was already known in the 90s – but when it comes to security of IoT devices, researchers found that this old vulnerability was present as numbers weren't completely random, so the pattern of ISN numbers in these TCP communications could be predicted.

"This stuff has been mostly fixed in Windows and Linux and the typical IT world. But when you look into the IoT world, this stuff is happening again," Daniel dos Santos, research manager at Forescout told ZDNet.

"It's not difficult for us or an attacker to find this type of vulnerability because you can clearly see the way the numbers are generated by the stack is predictable," he added.

By predicting an existing TCP connection, attackers could close it, essentially causing a denial-of-service attack by preventing the data from being transferred between devices. Alternatively, they could hijack it and inject their own data into the session, through which it's possible to intercept unencrypted traffic, add file downloads to serve malware or use HTTP responses to direct the victim to a malicious website. It's also possible for attackers to abuse TCP connections of the embedded devices to bypass authentication protocols, which potentially provide attackers with additional access to networks.

All of the vulnerabilities were discovered and disclosed to the relevant vendors and maintainers of affected TCP/IP stacks by October 2020.

1. **Lack of network segmentation**

This refers to the practice of dividing a network into smaller, isolated segments in order to prevent compromised devices from spreading malware or other malicious content to other devices on the network. If a sensor is not properly segmented on a network, an attacker who gains access to the sensor may be able to use it to spread malware or other malicious content to other devices on the network. This can compromise the security and privacy of the entire network. To prevent this from happening, it is important for companies and individuals who use IoT sensors to implement network segmentation and to regularly monitor and maintain the segmentation of their networks. This will help to prevent compromised sensors from spreading malware or other malicious content and will help to protect the security and privacy of the devices and systems connected to the network.

These security issues can make the sensors layer and the network layer in IoT systems vulnerable to attacks, and it is important for companies and individuals who use these systems to take steps to address these issues and protect their sensors from potential attacks.

**Application Layer.**

The application layer is another critical part of IoT systems, as it is responsible for running the software and applications that allow users to interact with the devices and systems in the IoT. There are a number of security and privacy issues that can affect the application layer in IoT, which can make these systems vulnerable to attacks. Some of the most common security and privacy issues at the application layer include

1. **Unencrypted data transmission between devices applications,**

This can make it easy for attackers to intercept and read this data, potentially exposing sensitive information or allowing attackers to gain access to the devices and systems that the applications are connected to. For example, if an IoT device is transmitting unencrypted data about a person's location, an attacker who intercepts this data may be able to use it to track the person's movements. To prevent this from happening, it is important for companies and individuals who use IoT devices and applications to implement encryption for the data transmitted by these devices and applications. This will make it much more difficult for attackers to intercept and read the data, and will help to protect the security and privacy of the devices and systems that the applications are connected to.

1. **Lack of authentication and access controls,**

This can allow unauthorized users to gain access to the devices and applications in the IoT, potenially compromising the security and privacy of these devices and systems. Since the application layer acts the control center, access to it mean the intruder has freedom to do whatever thy want with the device. To prevent this from happening, it is important for companies and individuals who use IoT devices and applications to implement authentication and access controls for these devices and applications. This can include measures such as requiring users to provide a password or other form of credentials in order to access the devices or applications or using encryption to secure the data transmitted by the devices and applications. By implementing these measures, companies and individuals can help to prevent unauthorized access to the devices and applications and protect the security and privacy of the data they collect.

1. **Use of weak or default passwords on applications,**

Many IoT devices and applications are shipped with default passwords that are easy to guess or with passwords that are very weak and can be easily cracked by attackers. This can make it easy for attackers to gain access to these devices and applications and use them to steal data or launch attacks on other systems. To prevent this from happening, it is important for companies and individuals who use IoT devices and applications to change the default passwords on these devices and applications and to use strong, unique passwords that are difficult for attackers to guess or crack. This will help to protect the security and privacy of the devices and systems that the applications are connected to and will make it much more difficult for attackers to gain access to these devices and applications.

1. **Inadequate security testing of applications and software,**

Many IoT applications and software are developed and released without being thoroughly tested for security vulnerabilities, which can leave them open to exploitation by attackers. To prevent this from happening, it is important for companies and individuals who manufacture IoT applications and software to ensure that these applications and software are properly tested for security vulnerabilities before they are released. This can include measures such as conducting penetration testing and running security audits in order to identify and fix any vulnerabilities that may exist in the applications and software. By doing this, companies and individuals can help to ensure that their IoT applications and software are secure and can protect the security and privacy of the devices and systems that these applications and software are connected to.

1. **Lack of privacy controls,**

Many IoT applications and devices are designed to collect and transmit a large amount of personal data, such as location information, usage data, and other sensitive information. However, many of these applications and devices do not have adequate controls in place to protect this data, which can make it easy for the data to be collected and shared without the user's knowledge or consent. For example, an IoT application may collect data about a person's location without their knowledge and then share this data with third-party companies without the person's consent. To prevent this from happening, it is important for companies and individuals who use IoT applications and devices to implement privacy controls that protect the personal data collected by these applications and devices. This can include measures such as requiring users to opt-in to the collection and sharing of their personal data, providing clear and transparent information about how the data will be used and implementing technical controls to prevent the unauthorized collection or sharing of personal data. By implementing these measures, companies and individuals can help to protect the privacy of the users of their IoT applications and devices and can ensure that personal data is collected and used in a responsible and transparent manner.

These security and privacy issues can make the application layer in IoT systems vulnerable to attacks, and it is important for companies and individuals who use these systems to take steps to address these issues and protect their devices and applications from potential attacks.

## Part B. Security Requirements and Challenges in IoT

Research explores the primary security requirements of the Internet of Things from many perspectives. We can use five critical needs to outline IoT security requirements. Due to the limits of IoT devices' capacity and ability to apply conventional security protocols, meeting these requirements is challenging.

### Data Volume

The large volume of data collected by the perceptive layer can make it difficult to manage and protect this data and to ensure that it is stored and accessed securely.

One of the main challenges of dealing with the large volume of data collected by the perceptive layer is the need to store this data securely. In order to store this data on a central network, such as the cloud, it will be necessary to implement secure storage solutions that can protect the data from unauthorized access and tampering. This can include measures such as encrypting the data, implementing access controls, and regularly backing up the data to prevent loss or corruption.

Another challenge of dealing with the large volume of data collected by the perceptive layer is the need to manage and process this data in a way that is efficient and effective. In order to make use of the data collected by the perceptive layer, it will be necessary to implement algorithms and other techniques to process and analyze this data to extract valuable insights and information. This can be a complex and challenging task and will require the development of sophisticated algorithms and other tools to effectively manage and process the large volume of data collected by the perceptive layer.

Overall, the large volume of data collected by the perceptive layer in IoT systems presents several challenges for security and privacy, and it is important for companies and individuals who use these systems to address.

### Resource limitations.

Another challenge of securing IoT systems is the limited storage capacity and computing power of many IoT nodes, which are the devices and sensors that make up the perceptive layer in IoT systems. Many of these devices have limited storage capacity and compute power and often feature low bandwidth communication channels, which can make it difficult to implement certain security solutions. For example, many security solutions, such as asymmetric encryption, require a significant amount of storage and computing resources in order to be implemented effectively. However, the limited storage capacity and computing power of many IoT nodes may make it difficult or impossible to implement these solutions, which can create security vulnerabilities and make it easier for attackers to compromise these devices.

To address this challenge, companies, and individuals who use IoT systems may need to implement solutions that are designed specifically for low-power, low-bandwidth devices. For example, they may need to use lightweight encryption algorithms that are designed to be efficient and require minimal storage and computing resources. They may also need to use other security measures, such as implementing access controls and authentication, in order to protect the security of these devices and prevent unauthorized access. By implementing these solutions, companies and individuals can help to ensure the security of their IoT systems, even when the devices and sensors in these systems have limited storage capacity and computing power.

### Protection

Most Radio-frequency identification (RFID) systems use a cagy authentication method. This weakness makes it easy for network analysis to identify the identity of things. The intruder can access, modify, and even delete data [H]. RFID systems are commonly used in IoT systems to identify and track objects, such as inventory items or supply chain assets. However, many RFID systems use a weak authentication method, which can make it easy for attackers to identify the identity of these objects and gain access to the data associated with them. For example, an attacker who is able to conduct network analysis on an RFID system may be able to identify the unique identifier of an object, and then use this identifier to access, modify, or delete the data associated with that object.

This weakness in RFID systems can create significant security and privacy risks, as it can allow attackers to gain unauthorized access to data, interfere with the operation of the system, or even compromise the security of other devices and systems that are connected to the RFID system. To address this challenge, companies and individuals who use RFID systems in their IoT systems may need to implement stronger authentication methods, such as using encryption or other security measures, in order to protect the security and privacy of these systems. By doing this, they can help to prevent attackers from gaining access to the data associated with RFID-tagged objects, and can help to ensure the security and privacy of their IoT systems.

### Scalability

The number of IoT devices is gowing fast each day. One of the challenges of securing IoT systems is the need to ensure that security solutions are scalable in order to keep up with the fast-growing number of IoT devices and sensors. As the number of IoT devices and sensors continues to grow, the security solutions that are implemented to protect these devices must also be able to scale and adapt to the increasing number of devices. This can be a complex and challenging task, as it requires the development of security solutions that are able to handle large volumes of data and that can be easily deployed and managed across a large number of devices and sensors.

To address this challenge, companies, and individuals who use IoT systems may need to implement security solutions that are designed to be scalable and flexible. This can include solutions such as cloud-based security platforms, which can be easily scaled up or down to meet the changing needs of the IoT system. It can also include the use of automation and other tools to manage the security of large numbers of devices and sensors and to ensure that the security of the entire system is not compromised by a single vulnerable device. By implementing scalable and flexible security solutions, companies and individuals can help to ensure the security of their IoT systems, even as the number of devices and sensors in these systems continues to grow.

### Autonomic Control

Devices in the Internet of Things should be able to connect and set themselves up to change according to the platform. Therefore, it must include certain procedures and approaches like self-configuration, self-management, and self-healing because IoT requires additional security and control due to automation [I].

One of the challenges of securing IoT systems is the need to ensure that the devices and sensors in these systems are able to connect and configure themselves in order to adapt to the platform on which they are deployed. Many IoT systems are designed to be flexible and adaptable, and the devices and sensors in these systems must be able to connect and configure themselves in order to work effectively in a wide range of environments. To address this challenge, companies, and individuals who use IoT systems may need to implement procedures and approaches such as self-configuration, self-management, and self-healing in order to ensure that the devices and sensors in these systems are able to connect and configure themselves effectively. Lets look at aspects of autonomic control.

* **Self-configuration**

Refers to the ability of IoT devices and sensors to configure themselves automatically based on the platform on which they are deployed. For example, an IoT device may be able to automatically configure itself to connect to the network, communicate with other devices, and perform its intended functions without the need for manual configuration. This can be a useful feature in IoT systems, as it can help to ensure that the devices and sensors in these systems are able to connect and configure themselves quickly and efficiently without the need for manual intervention.

* **Self-management**

Refers to the ability of IoT devices and sensors to monitor their own health and performance and to take corrective action if necessary. For example, an IoT device may be able to monitor its own power consumption, memory usage, or other performance metrics and to take action to optimize its performance or to prevent problems from occurring. This can be a useful feature in IoT systems, as it can help to ensure that the devices and sensors in these systems are able to operate reliably and efficiently without the need for constant human oversight.

* **Self-healing**

Refers to the ability of IoT devices and sensors to detect and repair any problems that may occur automatically. For example, an IoT device may be able to detect disconnection from the network and take action to diagnose and fix the problem without the need for human intervention. This can be a useful feature in IoT systems, as it can help to ensure that the devices and sensors in these systems are able to recover from problems quickly and efficiently without the need for manual intervention.

## PART C: Proposed solutions to IoT security

Some studies have been conducted to enhance IoT security and suggest remedies for security problems. Several potential solutions can help improve the security of IoT systems, including:

### Implementing robust authentication and access controls:

One of the key solutions for improving the security of IoT systems is to implement robust authentication and access controls for devices and sensors. This can include measures such as requiring users to enter a unique password or PIN in order to access a device, implementing multi-factor authentication, and using encryption to protect the data transmitted by these devices. By implementing these measures, companies and individuals can help to prevent unauthorized access to their IoT devices and sensors and can help to protect the data collected by these devices from being intercepted or stolen.

Et and Tahir ICMetric framework for adding security Internet of Things. It’s based on cryptography keys. The metric technology provides a different level of using cryptographic techniques to address key theft issues. It may be applied to block illegal access. An example of this in the application is in healthcare facilities. IoT-based healthcare apps also need to meet the metric requirements. Metric Technology also protects data storage devices, computers, and the storage devices between them.

Scalable Security with Symmetric Keys, developed by ***Raza [J]***, introduces a highly scalable and adaptable key management strategy for the DTLS security standard for IoT devices with limited resources.

### Using secure protocols and encryption:

Another solution for improving the security of IoT systems is to use secure protocols and encryption to protect the data transmitted by devices and sensors. This can include measures such as using secure versions of the TCP/IP protocol, implementing end-to-end encryption for data transmitted over the network, and using secure channels for communication between devices and sensors.

***Liu et al. [B]*** suggested a method based on the biological immune system. Whereas static security solutions may not be appropriate, the suggested solution uses a dynamic defense framework for IoT. The proposed circular defense has five links:

1. security threat identification,
2. risk calculation,
3. security reactions,
4. security defense,
5. and lastly, formulation of the defensive plan.

Researchers used immunity-like antigens and a real IoT detector to replicate the real IoT platform. They are simulating the techniques that biological systems employ to identify infections.

***Zhou and Chao*** [E] created and assessed the traffic management strategy while creating a security architecture for media-aware traffic. Physically unclonable functions (PUFs) were cited by ***Liu et al***. [D] as an illustration of how security protocols and primitives are implemented for IoT devices. He explained how the PUF could offer security upgrades through strong authentication or secret key creation in the IoT context.

***Zegzhda and Stepanova [C]*** suggest a method for enhancing IoT security that uses topological sustainability to address security attacks that try to interrupt, degrade, or destroy any IoT components or services. By preserving adaptive d-regular graph topology and considering various IoT constraints, such as limiting computation resources at IoT devices, the goal is to ensure IoT security through topological sustainability. There are many different encryption techniques that can be used in the context of the Internet of Things (IoT). Some common encryption techniques for the IoT include

1. Symmetric encryption:

This is a type of encryption where the same key is used to both encrypt and decrypt the data. This technique is relatively fast and efficient, but it requires that the sender and receiver have a shared secret key, which can be difficult to manage in large or distributed networks.

1. Asymmetric encryption:

This is a type of encryption where different keys are used to encrypt and decrypt the data. This technique is more secure than symmetric encryption, but it can be slower and more computationally intensive.

1. Public key cryptography:

This type of encryption uses a pair of keys, a public key and a private key, to encrypt and decrypt data. The public key is made available to anyone, While the private key is kept secret, this technique allows for secure communication without the need for a shared secret key.

1. Elliptic curve cryptography:

This is a type of public key cryptography that is based on the algebraic structure of elliptic curves. It is considered to be more secure than other public key cryptography techniques, but it can be more complex to implement.

### Conducting regular security testing and audits:

Regular security testing and audits can help to identify potential vulnerabilities in IoT systems and can provide valuable information about the security posture of these systems. By conducting regular security testing and audits, companies and individuals can help to identify and address potential vulnerabilities in their IoT systems and can help to prevent attackers from exploiting these vulnerabilities to gain unauthorized access to devices and sensors.

### **Implementing privacy controls:**

Another essential solution for improving the security of IoT systems is to implement privacy controls that protect the personal data collected by devices and sensors. This can include measures such as requiring users to opt-in to the collection and sharing of their personal data, providing clear and transparent information about how this data will be used and implementing technical controls to prevent the unauthorized collection or sharing of personal data. By implementing these measures, companies and individuals can help to protect the privacy of the users of their IoT systems and can help to ensure that personal data is collected and used responsibly and transparently.

### **Implementing network segmentation:**

Network segmentation can be a valuable tool for improving the security of IoT systems, as it can help to isolate compromised devices and prevent them from spreading malware to other devices on the network. By implementing network segmentation, companies and individuals can help to prevent the spread of malware and other malicious content in their IoT systems and can help to ensure that the security of the entire system is not compromised by a single vulnerable device.

***Lessa dos Santos [F]*** created a design that enables IoT-restricted devices to share data with other devices on the Internet using "Datagram Transport Layer Security (DTLS)" with authentication. A third-party device, Security Support Provider (IoTSSP), and two 6LoWPAN Border Router (6LBR) mechanisms are the foundation of this security architecture. They are used to direct DTLS handshaking to the IoTSSP.

# 4. IOT PRIVACY CONCERNS

Privacy in IoT the Internet security glossary is defined as "the right of an entity (typically a person), acting in its own behalf, to determine the extent to which it will interact with its environment, including the extent to which the entity is willing to share information about itself with others."

In the IoT, a network of devices seeks to collect data from the surrounding area before broadcasting it along with some events to a server that houses apps. Privacy must be managed throughout each stage, including in the device, storage, communication, and processing. One of the crucial concerns that need to be resolved in IoT is the privacy and protection of sensitive data ***[G]***.

## 4.1. Device Privacy

When illegal access occurs in hardware or software, the hacker could target sensitive information in the IoT device. For instance, a camera that has been reprogrammed by an intruder to broadcast information to invaders as well as the authorized server. Many issues need to be resolved to provide device privacy, such as protecting the identity of the nature of the device by adding noise. When a device is stolen, sensitive information can be secured using Quick Response Code Technique. Device location should also be secured.

Other measures include requiring users to opt-in to the collection and sharing of their personal data, providing clear and transparent information about how this data will be used, and implementing technical controls to prevent the unauthorized collection or sharing of personal data. By implementing these measures, companies and individuals can help to protect the privacy of the users of their IoT devices and can help to ensure that personal data is collected and used in a responsible and transparent manner.

## 4.2. During Communication,

Data secrecy is frequently ensured via encryption techniques when data is sent over network channels. Sometimes, data is added to packets during encryption to give them tracing properties. Some solutions can be found in communication protocols. Pseudonyms can be used for encryption in communication, which might lessen susceptibility. Devices should only communicate when necessary to reduce privacy exposure. Devices must have the ability to detach from the network when inactive to reduce location tracking. Only approved devices are permitted to communicate, and even after being enabled, they must authenticate again with the network before they handle any data ***[G]***.

More measures include encrypting the data, implementing access controls, and regularly backing up the data to prevent loss or corruption. By implementing these measures, companies and individuals can help to protect the personal data collected by their IoT devices from being accessed or tampered with by unauthorized users.

## 4.3. Privacy in Storage

The least quantity of information that can be saved while maintaining privacy protections is what should be done. Transport of information only occurs in "need-to-know" situations. The stored information's identity could be hidden through anonymization. Access to a database must be restricted to only statistical data. Differential privacy or the adding noise technique can be utilized to guarantee the output's independence from other database records ***[23]***.

Additional measures include using secure versions of the TCP/IP protocol, implementing end-to-end encryption for data transmitted over the network, and using secure channels for communication between devices and sensors. By implementing these measures, companies and individuals can help to prevent attackers from intercepting or tampering with the personal data transmitted by their IoT devices and can help to ensure that this data is protected from unauthorized access.

## 4.4. Privacy During Processing

Sensitive and Personal data must be appropriately processed solely for the intended purpose. Before disclosing personal information to third parties, acceptance and data owner confirmation must be obtained. Digital Rights Administration is a valuable way to manage transferred data rights and protect against improper processing. Before processing personal data, consent from the data owner and knowledge of the situation must be sought. User notification aids in preventing the unauthorized use of sensitive data and private information ***[G]***.

Extra measures include implementing access controls, requiring users to provide consent for the processing of their personal data, and implementing technical controls to prevent the unauthorized use or sharing of personal data. By implementing these measures, companies and individuals can help to ensure that the personal data collected by their IoT devices is processed and used in a responsible and transparent manner, and can help to protect the privacy of the users of their IoT systems.

# 5.0. DISCUSSION

IoT adoption is significantly impacted by security and privacy concerns. The security and privacy requirements we have seen at each layer should be considered and addressed in the expanding research in this area. Given that the majority of connected heterogeneous nodes are proliferating, the complexity of implementing security solutions is increasing as a result of the increase in the collection of sensitive and personal data. The ease with which IoT may be breached at each layer makes security a crucial subject for investigation.

Confidentiality, availability, authentication, integrity, and authorization are among the primary needs for IoT security. IoT security issues include quality of service, dependability, and confidentiality, securing massive data, software, and hardware vulnerability, and developing appropriate standards that need to be addressed [9].

Authentication and identity are essential to protect IoT data privacy. Although it must be maintained in every IoT component, it frequently goes unnoticed. Adequate security frameworks must cover IoT layer-security issues for protection. More study is required to create and implement appropriate IoT solutions that consider its equipment's limitations. Additionally, there is a need to create comprehensive security and privacy frameworks that address the problems at each tier and take contributing factors into account.

# 6.0. Conclusion

This paper has taken us through the architecture of IoT nodes. We have gone through each layer and examined the security challenges and constraints. We examined privacy issues in IoT and proposed solutions to privacy and security issues. These security and privacy issues slow the adoption of IoT, which is okay. Better safe than sorry.

# 7.0. References

[A]. Assiri and H. Almagwashi, "IoT Security and Privacy Issues," *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 2018, pp. 1-5, DOI: 10.1109/CAIS.2018.8442002

[B] M.R, S., & G, S. (2022). A novel approach in cloud-based IoT devices using a rough set method for ensuring security. https://doi.org/10.21203/rs.3.rs-1361093/v1

[C] Zegzhda, D., & Stepanova, T. (2015). Achieving internet of things security via providing topological sustainability. *2015 Science and Information Conference (SAI)*. https://doi.org/10.1109/sai.2015.7237154

*[D] (PDF) Liu et al. 2016 - researchgate*. (n.d.). Retrieved November 15, 2022, from https://www.researchgate.net/publication/303408121\_Liu\_et\_al\_2016

[E] Zhou, L., & Chao, H.-C. (2011). Multimedia Traffic Security Architecture for the internet of things. *IEEE Network*, *25*(3), 35–40. https://doi.org/10.1109/mnet.2011.5772059

[F] Lessa dos Santos, G., Guimaraes, V. T., da Cunha Rodrigues, G., Granville, L. Z., & Tarouco, L. M. (2015). A DTLS-based security architecture for the internet of things. *2015 IEEE Symposium on Computers and Communication (ISCC)*. https://doi.org/10.1109/iscc.2015.7405613

[G] Sathish Kumar, J., & R. Patel, D. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, *90*(11), 20–26. https://doi.org/10.5120/15764-4454

[H] Arseni, S.-C., Halunga, S., Fratu, O., Vulpe, A., & Suciu, G. (2015). Analysis of the security solutions implemented in current internet of things platforms. *2015 Conference Grid, Cloud & High-Performance Computing in Science (ROLCG)*. https://doi.org/10.1109/rolcg.2015.7367416

[I] Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the internet of things. *Ad Hoc Networks*, *32*, 17–31. https://doi.org/10.1016/j.adhoc.2015.01.006

[J] Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2016). S3K: Scalable security with symmetric keys—DTLS key establishment for the internet of things. *IEEE Transactions on Automation Science and Engineering*, *13*(3), 1270–1280. https://doi.org/10.1109/tase.2015.2511301

💼 Professional

**Intro will be added here.**

**IoT**

* definition of IoT
* what is the IoT?
* what is the Internet of Things (IoT)?
* IoT devices are everywhere
* IoT devices can be hacked
* IoT devices are vulnerable to attacks

Add Generate MoreRegenerate s

Section

**Things connected to internet**

* IoT devices are connected to the internet
* examples of IoT devices
* examples of IoT devices that are not connected to the internet
* IoT devices can be hacked
* IoT devices can be used for surveillance

Add Generate MoreRegenerate s

Section

**Data being shared in the cloud**

* cloud data is shared with other companies
* data can be used to deliver services and sell ads
* data can be stolen
* data can be used to track you
* data can be used to profile you

Add Generate MoreRegenerate s

Section

**Data that is used to deliver services and sell ads**

* data collected from IoT devices is used to deliver services and sell ads
* data is shared with third parties
* data can be used to track users
* data can be used to sell ads
* data can be used to create profiles of individuals

Add Generate MoreRegenerate s

Section

**Potential for abuse**

* data can be used to manipulate or control people
* data can be used to sell products or services
* data can be used to predict behavior
* data can be used to track people

Add Generate MoreRegenerate s

Section

**Surveillance cameras, microphones**

* surveillance cameras, microphones, etc.
* can be used to monitor people
* can be used to track people
* can be used to spy on people
* can be used to record conversations
* can be used to listen in on conversations

Add Generate MoreRegenerate s

Section

**IoT devices are here to stay but preventative measures can be taken.**

* IoT devices are here to stay
* data is being shared in the cloud
* data is being used to deliver services and sell ads
* potential for abuse
* surveillance cameras, microphones

Add Generate MoreRegenerate s

Section

**A Blog Conclusion will be added here**

#### **Company**

[Work With Us](https://jobs.lever.co/CopyAI)[Contact Us](https://www.copy.ai/contact-us)

#### **Help & Support**

[View Tutorials](https://help.copy.ai/04ad06343ad5414ab867236eb458b09d)[Request a New Feature](https://form.typeform.com/to/OKJSvGEy)[Report a Bug](https://form.typeform.com/to/e7V02YP4)[Report an Outage](https://form.typeform.com/to/mv6I2Fmw)[Request Languages](https://form.typeform.com/to/M9gJvGo5)

#### **Community & Tools**

[Join Our Facebook Community](https://www.facebook.com/groups/887950931991543/)[Join Our Affiliate Program](https://form.typeform.com/to/Kww18rv0)[Follow Us On Twitter](https://twitter.com/copy_ai)

#### **Terms & Policies**

[Privacy Notice](https://www.copy.ai/privacy-notice)[Terms of Service](https://www.copy.ai/terms-of-service)[Usage Guidelines](https://www.notion.so/copyai/CopyAI-Usage-Guidelines-38ce4874063d4020b00ef6a206bdeee2)

© 2022

IoT