**SINDH MADRESSATUL ISLAM UNIVERSITY**

Department of Computer Science

**SPRING 2022**

**Term Paper**

**Artificial Intelligence**

**BSCS-6B**

**Topic : Internet of Things (IOT)**

**Student’s Names: M.Huzaifa (csc-19f-093)**

**Noman M.Maqsood (csc-19f-125)**

**Qazi Mubin (csc-19f-130)**

**Course Coordinator: Sir Zubair uddin Shaikh**

**Dated: 04/ June/ 2022**

**Internet of Things (IOT)**

**Introduction:**

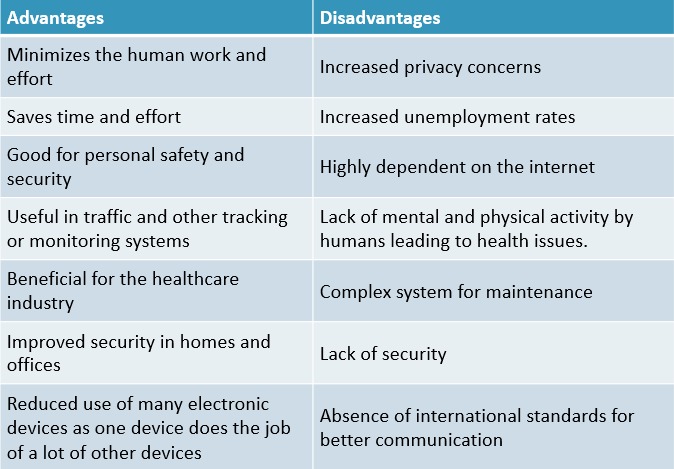
The Internet of Things (IOT) is the network of physical items with electronics built in their architecture that can communicate and perceive interactions with one another and with the outside world. IOT - based technology will provide advanced levels of services in the next years, and it will fundamentally alter how people live their lives. Medicine, energy, gene therapy, agriculture, smart cities, and smart homes are just a few of the categories where IOT is well-established.

At this time, the Internet is connected to almost 9 billion 'Things' (physical objects). This figure is anticipated to reach 20 billion in the not-too-distant future.

The diagram above depicts the connectivity of numerous devices from diverse fields to the Internet and the data exchange between them. As a result, the accompanying diagram depicts the world's connectivity via several existing technologies.



**IOT Pros and Cons:**



**IOT Breif**

A quick look back indicates the path that IOT devices are taking. Consider: In 2016, more than 4.7 billion things were connected to the internet, according to IOT Analytics. What if we jump to the year 2021? By 2025, the worth for IOT devices will be worth more than 10 Billion Dollars

**IOT Future Scope:**

Here are some assumptions about the future of IoT.

1. IoT is going very trendy topic, in 21st century, according to stats more 4 billion connected to web. If we move forward to the next 10 years this market will be reach to another level by 2030.

2. Cybercriminals will continue to use high-end IoT devices to carry out multiple attacks. The software turned infected machines into bootstrap networks for intitiating a distributed Daniel of Service (DDoS) attack, which seeks to flood websites with traffic. The attack flooded one of the largest internet hosting companies in the world and shut down many popular websites and services for hours. This type of malware is called "open source", which means that anyone can modify the code.

This is when your home router comes in helpful. The router is the main point of entry for the internet into your home. While many of your linked devices are unpredictable, the router can provide security at the entrance point. Manufacturers of routers will probably certainly keep looking for new ways to increase security.

5. Routers will continue to improve in terms of security and intelligence.

The router serves as the Internet's main entry point into your home. While many of your connected devices are unpredictable, the router can give protection at the point of entry. Password protection, firewalls, and the ability to configure a router to only allow particular devices on your network are all features of a traditional router. Router manufacturers will almost certainly continue to seek for innovative ways to make your security better.

6. Automobiles will become much more intelligent.

The introduction of 5G technology will force the car industry to evolve. Faster travel data will allow for the development of cars and pre-connected vehicles on the road, resulting in fewer drivers. It's possible that you don't think of your car as an Internet of Things device. New cars, on the other hand, will evaluate your data over time and communicate with other IoT devices, such as other high-tech four-wheeled vehicles.

7 Internet of Things (DDoS)-based The attacks will get more dangerous.

Affected IoT devices were used in botnet-based Distributed Service (DDoS) Daniel attacks to disrupt websites. IoT devices can also be used to launch other types of attacks.. For example, IoT devices may be weaponized in the future. The state that shuts down a home's thermostat in a hostile state during harsh winters is an understandable example.

8 Concerns about security and privacy will lead to legislation and regulatory action.

The rise of Internet of Things devices is one element that has raised security and privacy issues. The European Union implemented the General Data Protection Regulation (GDPR) in mid-2018. The General Data Protection Regulation (GDPR) has triggered comparable security and privacy regulations in other countries throughout the world. The state of California in the US recently implemented a stricter privacy law.