htw saar

Hochschule für Technik und Wirtschaft des Saarlandes
University of Applied Sciences

INTERNET OF THINGS

Fatemeh Zarsaz
Tim Blittersdorf

CONTENTS

1.1 About Internet of Things [1][2]

Kevin Ashton(MIT´s Excutive Director of Auto-ID Lab in 1999)

Kevin Ashton, the Executive Director of Auto-ID Labs at the Massachusetts Institute of Technology, is often credited with coining the term "Internet of Things" (IoT) in 1999. While there were earlier mentions of similar concepts, Ashton's presentation for Procter & Gamble on the potential of connecting Radio Frequency Identification (RFID) tags to the internet to enhance supply chain management helped popularize the term.
Ashton's choice of "Internet of Things" was influenced by the growing prominence of the internet in the late 1990s and the idea of extending its reach to physical objects. While the initial focus of IoT was on using RFID tags for supply chain management, But this the term started to develop and change in the next decades and has since evolved to encompass a broader range of connected devices and systems that can collect, analyse, and share data in real-time.

1.2 Definition

Technically IoT means “Implementing functionality in everyday objects through interconnection so that they can send and receive data”.
In simple terms, “IoT enables things in our daily life to interact and communicate with each other so that they can perform useful tasks”.
Like a smart car driving itself, smart home making mundane tasks easier for a household or a smart city controlling the traffic flow and reducing or even eliminating any chances of car accidents.

1.3 History [1][2][4]

Although the term "Internet of Things" (IoT) was coined only around two decades ago, the underlying technologies and concepts have been in development for much longer. To trace the history of IoT, we must also consider other related technologies such as the internet, which originated as ARPANET in 1969 to interconnect computers in academic and military contexts. Another crucial technology for IoT is RFID (Radio-Frequency Identification), whose first patent for a tag with a rewritable memory was issued in the US in 1973, although its origins can be traced back to World War II.

The first examples of IoT applications can be found in the early 1980s, when vending machines were equipped with sensors to monitor their inventory and performance. In 1991, computer scientist Mark Weiser proposed the concept of ubiquitous computing, which envisioned a world where computing is embedded in everyday objects and environments.

It was not until the 2010s, however, that IoT started gaining more attention in the industry, particularly after the Chinese government made it (IoT-development) a strategic priority in their Five-

Year Plan. In 2011, research firm “Gartner” included IoT in their "hype cycle for emerging technologies," predicting that it would reach the Plateau of Productivity in 5 to 10 years. By the end of 2018, IoT had indeed become a well-established and beneficial technology, with over 17 billion connected devices worldwide.
Despite the impact of the Covid-19 pandemic and the ongoing chip shortage, the number of connected IoT devices is expected to continue growing rapidly in the coming years. In 2022, there were an estimated 13.14 billion connected IoT devices globally, spanning various domains such as smart homes, wearables, and industrial automation. However, the precise number may vary depending on the definition and methodology used by different sources. It is also worth noting that the chip shortage has affected the availability and cost of certain components, leading to temporary disruptions in some IoT markets.

1.4 IoT key Features [1][2][5][6][8]

Although there are numerous features of IoT devices, some of the key ones include **Connectivity, Sensing, Remote-Control and Automation, Interoperability, Endpoint Management, producing Big Data** (which involves processing and storing large volumes of data across different servers and databases),**Cloud Computing** and **Security**. In the next section, we will explore the concept of security in more detail. However, it is important to note that, among the most crucial features, aside from Security, connectivity, data processing and sensing are particularly noteworthy.

- Connectivity

The fundamental aspect of IoT is its ability to establish connections between devices (also known as nodes), allowing them to communicate autonomously. In IoT, devices, sensors, computers, and databases need to interact and exchange data with each other. A fast, stable, secure, and safe connection is essential for IoT devices to be useful. Additionally, IoT facilitates cross-platform connections with technologies like cloud computing, artificial intelligence, and blockchain. These connections can be established through various means such as Wi-Fi, Radio Waves, Bluetooth, or wired connections.

- Sensing

IoT devices are equipped with sensors that detect and gather information from their surroundings, including temperature, light, sound, acceleration, and pressure. This information is then analysed to make decisions, automating tasks that would otherwise be performed by humans. Raw and analysed data serve as the foundation for the operation of IoT devices. Examples of sensors used in IoT include humidity sensors, temperature sensors, motion sensors, image sensors, level sensors, and proximity sensors.

- Big Data

In the context of the Internet of Things, big data is generated through the collection and analysis of vast amounts of heterogeneous data streams from various IoT devices and sensors.

This process involves the use of advanced technologies such as machine learning, artificial intelligence, and distributed computing to extract insights and knowledge from the data. The resulting insights can be used to improve decision-making, optimize processes, and enhance the user experience in a variety of domains, from smart cities to industrial automation.

- Cloud Computing

IoT devices can send their data to the cloud for analysis, enabling real-time insights and decision-making. Additionally, cloud-based IoT platforms can provide services such as device management, security, and application development, making it easier for developers and organizations to build and deploy IoT solutions. Cloud-based services can also enable cross-device communication, allowing IoT devices to share data and work together seamlessly.

Along with these features, IoT is moving toward automation, which result in a series of shifts in employment and new opportunities in the industry as these technologies are evolving even further, such as endpoint management for automated IoT devices.

1.5 IoT deployment categories [2][10][9]

The widespread integration of IoT devices in our daily lives is becoming the new normal, often going unnoticed. There are a tremendous number of different use cases for IoT devices. From environmental applications to Artificial Things, Smart Things, and many others. But some of these deployment categories are more prominent, , which we will discuss below.

In the **healthcare** sector, IoT is utilized for remote patient monitoring, glucose/heart-rate monitoring, and robotic surgeries. For example, remote patient monitoring can provide real-time data to healthcare providers, helping to detect potential health problems before they become serious. In **transportation and logistics**, IoT can aid in better traffic management and the use of flash warning alarms. In the **public sector**, IoT is applied to various areas, including disaster management, pollution tracking, and natural resource preservation and tracking. It can also be used to send nationwide notifications of water or electricity outages or interruptions. **Manufacturers** can benefit from IoT solutions to optimize production processes and improve workplace safety and use energy more efficiently. For example, IoT sensors can detect equipment issues before they become major problems, reducing downtime, and improving efficiency. In newer generations of **automobiles**, IoT sensors gather real-time data on engine temperature, fuel consumption, fluid levels, and run time to predict potential issues, reducing human errors and preventing traffic accidents. **Smart watches**, **smart homes**, and **smart cities** are other key categories of IoT deployment. Smart homes, for instance, can include various IoT devices such as thermostats, lighting systems, and security cameras, which can be controlled remotely through a mobile device. In a smart city, IoT can be used to optimize traffic flow, reduce energy consumption, and improve public safety. Ultimately, the integration of IoT devices in various sectors can result in increased efficiency, improved safety, and a better quality of life. Another key usage of IoT devices is in the **energy sector**. IoT sensors can be used to monitor energy consumption in buildings, factories, and other facilities, identifying opportunities for energy efficiency improvements. For example, sensors can be used to track lighting, HVAC systems, and other energy-consuming devices, providing real-time data on usage patterns and energy consumption. This data can be used to optimize energy usage, reduce costs, and minimize environmental impact. Additionally, IoT devices can be used to monitor renewable energy sources such as solar panels and wind turbines, providing real-time data on energy generation and performance. This can help operators optimize renewable energy systems and increase their reliability.

2.1 Overview

Securing IoT devices can pose significant challenges due to the lack of strong security measures in place during their design and development. Often, manufacturers prioritize features and usability over security, leading to vulnerabilities that can be exploited by attackers. Additionally, the proliferation of smart technologies has resulted in the generation of vast amounts of data, commonly referred to as big data (as explained in the las part) from various sources, such as healthcare, government, finance, marketing, and media. IoT devices collect a wealth of data that can reveal sensitive information, including users' daily habits, interests, locations, health status, and investment preferences. Therefore, unauthorized access to this data can be highly lucrative for cybercriminals and pose significant threats to society if it falls into the wrong hands. IoT security involves implementing measures to secure these devices and prevent threats to users or the network. Designing a safe and secure IoT system requires significant investment and resources, but it is essential to maintain trust among users and businesses and ensure the system's long-term demand.

2.2 Most Possible Attacks on IoT [11][13][17]

IoT devices are prone to network attacks, including but not limited to data theft, phishing attacks, spoofing, and denial-of-service (DDoS) attacks, which can lead to cybersecurity threats such as ransomware attacks and data breaches that can result in significant financial and resource expenditures to remedy. As technology continues to advance, the range of potential cyberattacks also expands. Nevertheless, some of these attacks are more popular among attackers than others. In the last twenty years, the following attacks have been more frequently used against IoT devices or carried out via malicious use of such devices.

- **Firmware vulnerability exploit**

Firmware, which is the software that operates hardware, is present in all computer-based devices. While computers and smartphones have operating systems running on firmware, in IoT devices, the firmware acts as the operating system. Unlike sophisticated operating systems that run on computers, IoT firmware typically lacks sufficient security safeguards, and often contains known vulnerabilities that are difficult or impossible to patch. These vulnerabilities make IoT devices highly susceptible to attacks aimed at exploiting them. Hackers exploit vulnerabilities in the firmware to gain access to sensitive data or take control of the device. Once an attacker gains access to an IoT device, they can use it to launch further attacks or steal valuable data. Proper security measures must be taken to prevent firmware vulnerability attacks in IoT devices.

- **Credential based attack**

IoT devices are often shipped with default administrator usernames and passwords that are not secure, and sometimes, all devices of a given model share the same credentials, which are not even reset. Attackers are aware of these default credentials, and a large number of successful attacks on IoT devices are attributed to attackers simply guessing the correct credentials. In the

subsequent section, we will elaborate on some major real-world attacks that have been executed exploiting this vulnerability.

- **MitM (Man in the Middle) aka. On-Path attack**[18]

A man-in-the-middle (MitM) attack in IoT involves an attacker intercepting communication between two IoT devices or between an IoT device and a server. The attacker then manipulates the communication by inserting, altering, or deleting messages, potentially leading to data loss or unauthorized access to sensitive information. The attack is usually performed by exploiting vulnerabilities in the communication protocols or by impersonating a trusted entity. The consequences of a successful MitM attack on IoT devices can be severe, ranging from financial loss to privacy breaches and even physical harm (an attacker could intercept and manipulate data from a medical device, such as a pacemaker, causing harm to the patient's health. Similarly, an attacker could manipulate data from a smart home device, such as a thermostat or smoke detector, leading to physical damage or harm).

- **Physical hardware-based attack**

IoT devices such as surveillance cameras, traffic lights, and fire alarms are often located in public areas and have fixed physical positions. An attacker who gains physical access to an IoT device can steal data or take control of the device. This type of physical attack can compromise only one device at a time, but the attacker could gain information to exploit other devices on the same network. As a result, physical attacks can have a significant impact on the security and integrity of the entire IoT system.

- **DDoS (Disturbed Denial of Service)attacks** [20]

A denial-of-service (DoS) attack is a type of cyber-attack that involves overwhelming a network or website with traffic, rendering it inaccessible to users. In the case of IoT devices, attackers can use them to create a botnet. Once a botnet has been created, the attacker can launch a coordinated DoS attack on a target, using the combined processing power of all the devices in the botnet to flood the target with traffic. In the next section, we will explore this attack further, but first, we need to understand what a botnet is.

2.3 Botnet of Things [6]

A botnet is a collection of internet-connected devices that have fallen under the control of cyber criminals to be used for their own malicious purposes. By using malware to infect large numbers of vulnerable PCs, servers, mobile devices, and Internet of Things (IoT) devices, "bot herders"(the main attacker controlling the botnet) can use massive amounts of concentrated computing power and functionality to unleash automated distributed denial-of-service (DDoS) attacks, extract data, commit click fraud, demand ransom, and send spam emails. In recent years, botnets have also played a rising role in crypto mining, as cybercriminals utilize their resources for the massive computing power required to mine cryptocurrencies.
While botnets typically remain invisible to users of the infected devices and use only a fraction of the available resources, the impact of their activities can be devastating if, for example, a volumetric DDoS attack or a protocol DDoS attack disrupts network services or takes an entire

network offline. Botnets, often offered for rent by criminal organizations for even a price of merely 100-150$, have become a popular tool for hackers of all kinds, as one relevant example we can mention university students looking to stall an exam.

To create a botnet, a hacker uses malware like Mirai (more about Mirai in the next section) to find devices with vulnerabilities. Any type of device that is connected to the Internet and has weak security protection is enough to get the job done: a router, a security camera, or a smart TV with a security breach.

When devices are added to this expanding zombie army, they can be controlled by the bot herder using command-and-control (C&C) software via standards-based communication channels such as IRC (Internet Relay Chat, a text-based chatting system for instant messaging), HTTP, or peer-to-peer (P2P) connections. [1]

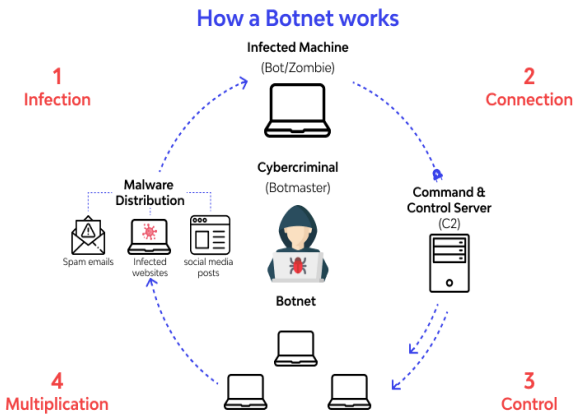


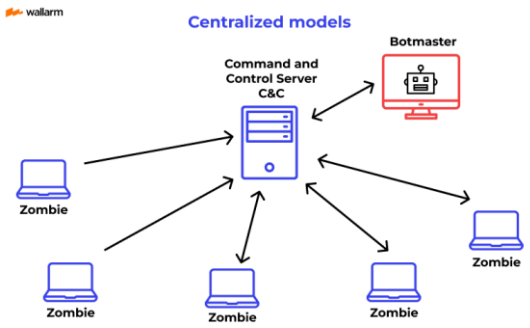
Figure 1 -Botnet of Things

2.4 Botnet Control Models[6][8][19]

To achieve the intended goals of a botnet, attackers must maintain continuous control over it. Two primary models are typically used for this purpose:

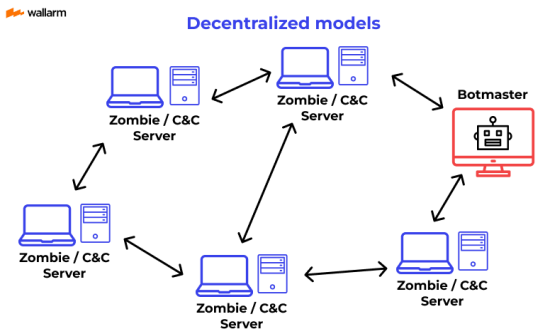
- **Model 1- Centralized or The client-server model**[2]

Centralized botnets rely on a basic network infrastructure to establish a communication network with the targeted devices. This model is highly functional as command and control (C&C) servers can facilitate robust communication. However, the C&C servers are easily detectable and can be shut down effortlessly, rendering the bot herder unable to communicate with the bots.



- **Model 2- Decentralized or The peer-to-peer model**[1]

An advanced model, the decentralized approach involves establishing communication among all nodes or peers connected in the network. In this type of botnet control model, all infected nodes are commanded to communicate within the network without requiring a dedicated C&C server or authentication. Botnets following the P2P model are more resilient compared to those that rely on the client-to-server model and are harder to disrupt. This advantage has made the P2P model increasingly popular in recent times.



[1] Picture Source
[2] Picture Credit to: wallarm.com

- **Model 3- Hybrid Botnet**

This model combines elements of both centralized and decentralized models. A hybrid botnet may have a central C&C server for initial communication, but then switch to P2P communi-cation to avoid detection.

2.5 Some Examples of IoT-Botnet Attacks [17,..,25]

While numerous Botnet attacks leverage IoT devices as nodes in their networks, this discussion will focus on only the most significant and widely-recognized attacks. Specifically, we will delve deeper into one particularly destructive attack to better illustrate the significant security vulnerabilities present in IoT devices.

- **Mirai**: One of the largest and most well-known IoT botnets, Mirai infected hundreds of thousands of IoT devices in 2016, causing widespread disruption to internet services.
- **Reaper**: Also known as **IoTroop**, Reaper is a botnet that primarily targets routers and IP cameras. It was first detected in 2017 and is known for its ability to rapidly infect devices.
- **IoT Worm**: This botnet targeted security cameras made by a specific manufacturer and was first discovered in 2017. The worm was able to spread itself to other vulnerable devices on the network and was difficult to detect and remove.
- **Chaos:** The Chaos malware exhibits a high level of sophistication in its architecture and evasion capabilities, which allows it to evade detection by conventional security solutions. Its propagation primarily relies on exploiting unpatched security vulnerabilities in target devices, in addition to leveraging brute-force techniques against SSH protocols. Furthermore, the malware can hijack Internet of Things (IoT) devices using stolen SSH keys. Although Chaos has a primary focus on European targets, its bots are distributed globally, with concentrated activity in the Americas and the Asia Pacific regions.

  "*Using Lumen global network visibility, Black Lotus Labs enumerated the C2s and targets of several distinct Chaos clusters, including a successful compromise of a GitLab server and a spate of recent DDoS attacks targeting the gaming, financial services and technology, and media and entertainment industries – as well as DDoS-as-a-service providers and a cryptocurrency exchange*" the researchers said.

Currently, the Mirai and Chaos botnet attacks are causing significant threats to network security by exploiting vulnerabilities in IoT devices. However, Chaos is evolving and rapidly changing, making it difficult to understand its precise functionality. Due to this uncertainty, we will focus our attention on the Mirai attack and its operational framework.

2.6 A real danger called Mirai [18][19][23][24]

There are various malware programs that use IoT devices to form a vast botnet and execute DDoS attacks. However, Mirai had a more extensive and pervasive impact in 2016 and serves as a quintessential example of the pressing need for robust security in IoT devices.

The Mirai botnet was first discovered in August 2016 by a white-hat malware research group called "**MalwareMustDie**." It has been deployed in some of the most significant and disruptive distributed denial of service (DDoS) attacks, such as the attack on **Krebs on Security** website in

September 2016, a 1Tbit/s attack on French web host **OVH**, and several large DDoS attacks on DNS services provided by **DNS service provider Dyn** on October 21, 2016. In these attacks, the Mirai malware was installed on hundreds of thousands of IoT devices, including home security cameras, routers, and smart refrigerators, using default usernames and passwords. These attacks rendered several high-profile websites, including **GitHub**, **Twitter**, **Reddit**, **Netflix**, and **Airbnb**, inaccessible.
In the Krebs on Security DDoS attack, which reached 620 Gbps, Mirai was used in combination with **BASHLITE**, a malware that infects Linux systems to launch DDoS attacks. The developers initially created the software to DDoS Minecraft servers. Later, the source code of Mirai was made available on hack forums, and its techniques were adapted into other malware projects. It was discovered that Mirai was also used in DDoS attacks against **Rutgers University** from 2014 to 2016, leaving faculty and students on campus without access to the internet for several days. Moreover, a failure of the university's central authentication service caused course registration and other services to be unavailable during critical times in the academic semester. It was later revealed that the attacker was a Rutgers University student.
Mirai was also employed in an **attack on Liberia's internet infrastructure** in November 2016. These DDoS attacks were also noteworthy in **Brazil, Taiwan, Costa Rica, and India**.
Mirai-like ancestors, such as **Bashlite, Gafgytm, QBot, Remaiten, and Torlus**, have existed since 2014, according to independent security journalist Brian Krebs[3]. Mirai's bot code was built from improved codes of its predecessors, compiled by several developers.
Developers Josiah White, Paras Jha, and Dalton Norman, who were between 18 and 20 years old, created Mirai, which hijacked approximately 150,000 IoT devices and united them as a digital army. Initially, it was intended to attack rival Minecraft videogame hosts, but it evolved into an online tsunami of nefarious traffic that knocked entire web-hosting companies offline.

2.7 How does Mirai work?[18][24][25]

Mirai is a self-propagating worm which its task is to create a Botnet and cuase DDOS attack.
Its malicious program replicate itself by attacking and infecting vulnerable IoT devices.
It is also considered a botnet because the infected devices are controlled via C&C (Command-and-control) server.
Mirai is made of two key modules: a **replication module** and an **attack module**. It uses various techniques to spread and infect new devices, such as brute-forcing default credentials, exploiting known vulnerabilities, and using a list of commonly used credentials to gain access to devices. It can also identify and target specific devices with known vulnerabilities to maximize its impact.
Mirai's architecture consists of three key components: **the loader, the bot, and the command and control (C&C) server.** The loader scans the internet for vulnerable devices and infects them with the Mirai bot. The bot is responsible for carrying out the instructions received from the C&C server, such as launching DDoS attacks. The C&C server controls the botnet and issues commands to the infected devices.

[3] krebsonsecurity.com

2.8 Mirai's come back [23][24]

Mirai's creators designed it to be highly adaptable and capable of mutating to evade detection and defense mechanisms. It has been modified and customized by other attackers and used in various attacks since its initial discovery in 2016.
In March 2019, security experts discovered new variants of Mirai that primarily targets IoT devices within companies. **OMG, Okiru, Satori, Masuta** and the **PureMasuta** are new strains of Mirai.
The OMG strain of malware is capable of turning IoT devices into anonymous proxies for cybercriminals, which can provide access to greater attack power through corporate networks. The latest version of Mirai includes 11 new exploits, bringing the total number of exploits to 27 and expanding its attack surface.

However, the focus should not only be on Mirai or similar malware, as these threats are common with the advancement of technology. Instead, we need to focus on improving the security of all internet-connected devices to protect against such threats and ensure the safety of the world's technology infrastructure.

2.9 Security of IoT

IoT security refers to the measures taken to protect the confidentiality, integrity, and availability of Internet of Things devices and networks. This includes securing IoT devices, cloud, mobile application, communication channels, and data transmitted over the network. The goal of IoT security is to prevent unauthorized access, data theft, and other malicious activities that could compromise the functionality and safety of IoT devices and systems. It also involves ensuring that devices are resilient to attacks and can continue to operate effectively even in the face of threats. The scale of IoT application services is large, covers different domains and involves multiple ownership entities. There is a need for a trust framework to enable users of the system to have confidence that the information and services are being exchanged in a secure environment.
To do that, we must take appropriate security measures.

2.10 Security Countermeasures[11][12][13][17][21][22]

In order to ensure the safe development and use of Internet of Things (IoT) devices, it is essential to implement security measures that prevent them from being easily exploited by attackers. Various security countermeasures can be employed to safeguard IoT devices against malicious attacks, including:

❖ For Manufacturers:

- **Implementing security-by-design:** security should be an integral part of the design process from the beginning, rather than being added as an afterthought.
- **Secure Boot**: Ensuring the firmware and software are not tampered with during the boot process.
- **Code Signing**: ensuring that only authenticated and authorized code is executed on the device and Incorporate hardware security modules (HSMs) for secure key storage
- **Network Segmentation**: segregating devices into smaller subnetworks to contain potential attacks and reducing the impact of a compromise.

- **Data Integrity**: Implement secure communication protocols (e.g., TLS) and encryption for data in transit and at rest
- **Security Tests**: Conduct regular security testing and assessments to identify vulnerabilities and improve security posture
- **Firmware Updates:** implementing mechanisms to update firmware and software regularly to address known vulnerabilities.
- **Provide Unique Credentials**: Releasing devices with unique Admin- username and passwords or forcing the users to define their own unique credentials before starting to use the device.

❖ For IoT Device Users:

- **Changing Default Passwords**: setting unique and strong passwords to prevent unauthorized access.
- **Regular Firmware Updates**: keeping firmware and software updated to address known vulnerabilities.
- **Network Security**: securing home Wi-Fi networks with strong passwords and encryption, using firewalls and intrusion detection/prevention systems.
- **Restricting Device Access**: limiting the devices that can access the network, and only allowing those with appropriate credentials.
- **Disable Unnecessary Services**: disabling services and features that are not needed to reduce the attack surface.

Overall, it is important for manufacturers and IoT device users to work together to ensure IoT devices are secure, and not vulnerable to attack.

2.11 Conclusion

In this section, we have covered the definition and origin of the term "Internet of Things" (IoT), as well as the impact of IoT devices on our world. As IoT technologies become increasingly ubiquitous, they are transforming the way we live and interact with our environment. As we have explained, IoT is characterized by interconnectivity, and this feature is driving the development of a more connected society where virtually everything is networked.

However, with the benefits of IoT come significant security and safety challenges. As we have seen in real-world examples, the growing prevalence of IoT devices has exposed us to a range of new threats and vulnerabilities, and malicious actors are increasingly leveraging IoT technologies for their own purposes. Therefore, it is critical that we take measured actions to ensure the security and integrity of IoT systems and the data they generate.

Ultimately, IoT and security are two sides of the same coin. As the adoption of IoT technologies continues to accelerate, it is essential that we prioritize the development and deployment of secure and trustworthy systems. By doing so, we can ensure that the benefits of IoT are realized while minimizing the risks and negative impacts associated with insecure or compromised systems.

3.1 State of Art [26]

The Internet of Things (IoT) market has continued to grow in importance for both consumers and companies since its inception. In 2022, despite challenges such as the Covid-19 pandemic and widespread chip shortages, the IoT market still saw significant growth. Furthermore, there was an increase in the number of people joining the DIY and open-source communities, who are discovering IoT and Smart home solutions for themselves. This increase can be attributed to the lockdowns from the Covid-19 pandemic, where more households had the time to think about IoT solutions for their own homes.
However, the most significant change and "game changer" is still in its early stages, as almost every big IoT company has changed their viewpoint. This change can be seen in the "Matter" standard, where every IoT device should share an open standard, making it easier to use IoT devices from different brands seamlessly. This approach promises to enable interoperability between devices and enhance the end-user experience.
As of the end of 2022, an estimated 13.1 billion IoT devices were connected globally. According to the Global IoT Markets forecast, this number is expected to rise to approximately 21 billion by 2024. This growth in the number of IoT devices underscores the need for open standards and interoperability between devices to ensure that they can communicate with one another, thereby enhancing the value of IoT solutions for consumers and businesses alike.

3.2 Protocol

3.2.0 Definition [27]

Protocols are defined formats of communication. Which allows for different host and clients to communicate between each other. Putting it in a simple way, Protocols can be seen as languages. Understanding one such language allows one to communicate with other who know the same language. To quote Cloudflare.com:
“In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless. “
In the following, an overlook of the most common IoT protocols will be provided

3.2.1 Protocol - Wi-Fi [28][29]

Wi-Fi is a ubiquitous wireless communication protocol that is widely used in households and companies worldwide. It functions like a cable LAN connection but without the need for physical cables. Its popularity stems from its simplicity and relatively low cost, making it an ideal protocol for expansion.

Wi-Fi is utilized by a wide range of smart devices and applications that require high data transfer rates. For example, security cameras require constant data streaming, making Wi-Fi a suitable choice due to its high data transfer rate. However, Wi-Fi also has its drawbacks, such as signal overlapping caused by having too many access points in one region. This can disrupt or impede data transfer, especially since Wi-Fi uses the 2.4GHz spectrum. Additionally, every IoT device that connects to the router takes up space on the IP list, which can be problematic in large networks.
Therefore, it is crucial to determine which devices require full Wi-Fi access and consider using alternative communication protocols for other devices to avoid signal overlapping and IP address issues.

3.2.2 Protocol - Zigbee [30][31]

Zigbee is a well-known IoT protocol that provides a simple and efficient way to connect multiple IoT devices. This protocol consumes a low amount of power as data is only transmitted when needed, which allows devices to be powered by low-voltage batteries. Zigbee networks require only one Zigbee gateway to start, and devices can function as access points automatically, as long as they are not battery-powered, which can increase the signal range by adding new devices to the network.
However, Zigbee shares the same 2.4GHz frequency range as Wi-Fi, which may result in potential signal overlap. Zigbee is best suited for devices such as sensors and relays, which require low data transfer rates to be used efficiently.
One disadvantage of Zigbee is that it has a single point of failure, which is the Zigbee gateway. Additionally, Zigbee has limited compatibility with other protocols, which can result in interoperability issues. However, Zigbee 3.0 has made significant improvements in this area, allowing for better integration with other protocols.
Zigbee also offers security features such as encryption and authentication, which can help prevent unauthorized access to the network. The Zigbee Alliance is continuously working on improving and updating the protocol to address emerging security threats and enhance its capabilities.

3.2.3 Protocol - Thread [32]

The Thread protocol is a wireless communication protocol that can be viewed as an improvement on the Zigbee protocol. It builds upon the features of Zigbee while removing its single failure point, which was the Zigbee gateway. Instead, Thread employs multiple Thread routers that can self-manage and heal the network. Additionally, Thread is a low-power protocol, but it offers the option to access Thread devices over IPv6.

Despite its benefits, Thread has a potential drawback. Like Wi-Fi and Zigbee, Thread uses the same 2.4GHz frequency band, contributing to the frequency's overuse. However, this frequency band offers the advantage of being globally available, making it easier for manufacturers to adopt.

As of the writing of this paper, there are still relatively few Thread devices and Thread routers available on the market. This may be due to the protocol's novelty when compared to more established protocols such as Wi-Fi and Zigbee. Nevertheless, Thread is gaining momentum in the industry, and it is expected that more devices and routers supporting Thread will become available in the future.

3.2.4 Protocol - The Matte Standard [33]

Matter is an IoT standard that was created as a collaborative effort by prominent tech companies such as Apple, Google, Samsung, and Amazon, among others. It aims to reduce fragmentation across different vendors and promote interoperability among IoT devices, as mentioned in the State of the Art.

Matter combines the protocols mentioned in sections 3.2.1 to 3.2.3. It is a royalty-free standard that has gained significant traction in the industry, with many vendors already pledging to update some of their devices to support it. However, some have indicated that they will only include Matter in newer devices.

One of the key features of Matter is that it does not require a connection to the cloud, which means that Matter devices can continue to function even during an internet outage. This is an important consideration for businesses and individuals who rely on IoT devices for critical operations.

At the time of writing this paper, the Matter standard had only been "soft-launched" with the 1.0 version on October 4, 2022. Currently, it supports only a few devices such as smart lightbulbs. However, the development of Matter is ongoing, with new features being planned and tested. Devices that support Matter can be identified by the Matter symbol displayed on their casing.

The Matter standard promises to provide a unified approach to IoT connectivity, making it easier for devices to communicate with one another regardless of their vendor or protocol. This could significantly reduce the complexity of IoT ecosystems and make it easier for businesses and individuals to adopt IoT solutions. However, the success of Matter will depend on its adoption by vendors and the wider industry, as well as its ability to address security and privacy concerns associated with IoT devices.

3.2.5 Protocol Conclusion

In the end, there are many protocols with various capabilities that are continuously developed and improved. Currently, there is no single universal protocol that can be used for all situations, so personal use cases must be evaluated to determine the appropriate protocol for the given requirements. However, it is possible that in the future, there will be a solution that eliminates the need for such evaluations. Matter is a potential solution for this purpose.

3.3 Devices [34][35]

These are the object used as the physical components of IoT and are as Important as the Digital protocols themselves. IoT Devices can generally be set in to two subcategories: “DIY” and “Pre-Build”.

- **DIY**

So called “Do it yourself” devices are IoT solutions created by private or contracted personal. These solutions are often hyper-personalised. Created by an individual for one or multiple specific purpose, that only applies to their situation, only. DIY solutions are utilizing the ever-increasing options in microprocessor and open-source software. With many people sharing and helping each other in the creation of more “Homemade” solution. Be it creating one from scratch or modifying already existing options.
Most popular microprocessor option are, but not limited to, the ESP32, ESP8266 and RP2040. With the Custom „ESPHome“ firmware and „Arduino programming language "and the „Python language " being the most common software choices.

- **Pre-Build**

The devices that are considered „Pre-Build "are the devices that can be bought from many different vendors. These devices can come in many ways. From being a simple Zigbee temperature and humidity sensor to a Smart-TV capable of voice commands.
However, these devices often offer little to no customisation possibilities, forcing the user to use the devices with the software made and setup by the vendor. With this vendor lock in, a concern for privacy can arises.

Conclusion

Both DIY and Pre-Build devices are correct options. It's up the user to decide which option they wish to utilise. With Pre-Build Devices offering an easy start into the world of IoT. Giving and option to just “plug and play”. However, this comes with the possible cost of privacy and device freedom.
Whilst DIY offers and almost infinite possibility of options, ensuring that the solution is truly in owned by the user. Only if the user is willing to learn how to build IoT devices for themself. Which can be time consuming and difficult task for some.

3.4 Control Applications

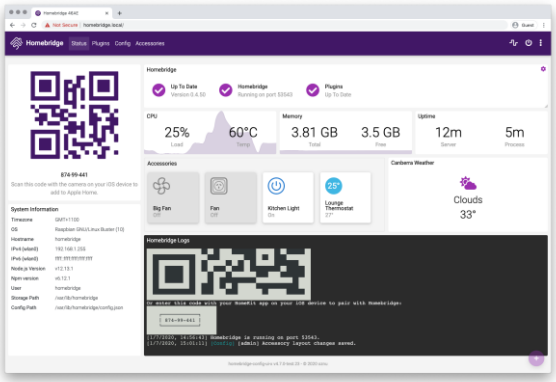
Control applications, also known as control apps, are necessary to manage IoT devices using a web browser or a smartphone app. These applications can be divided into three main categories: hubs, bridges, and companions.

- **Hubs** [36]

IoT hubs serve as the central point of the IoT network, providing control and access to every device. They allow for the creation and modification of key automations. One such hub is Home Assistant, which can be easily installed and run on a Raspberry Pi, an old PC, or a virtual machine, providing local management of every local IoT device.

- **Bridges** [37]

Bridge applications are used to add hub support to IoT devices that don't typically support hub applications. Homebridge is one example of a bridge application that enables the integration of IoT devices into Apple's HomeKit, even if they don't support HomeKit natively. Homebridge can be hosted on a variety of platforms, including but not limited to Raspberry Pi and Docker container.



- **Companions**

Companion apps are vendor-provided apps that are designed to control specific types of devices or vendor groups. Some companion apps require users to create a web account with the vendor in order to use or set up their IoT device.

4.1 Future perspective, Challenges & Technologies[38]

In the future, IoT is expected to become an increasingly seamless and integrated part of our daily lives. With advancements in IoT technology, room climate control, automatic door and window functions, and self-writing shopping lists are just a few examples of what we can expect. Additionally, there may be potential for human beings to interface with IoT technology directly through brain implants, allowing for even more efficient and streamlined interactions with IoT devices.

As AI continues to advance, it is also expected to play a greater role in our daily lives. With the ability to assist with decision making and workflow management, AI will help us become more productive and efficient.

However, security remains a significant challenge for IoT development, as malicious attacks such as Mira and Chaos continue to threaten IoT systems. It is imperative that IoT systems are designed with security in mind, ensuring that developer access cannot fall into unauthorized hands.

Another major challenge for the future of IoT is the expansion of new infrastructure and the replacement of outdated systems. Despite the advancements in IoT technology, many companies, institutions, and governments still rely on outdated systems. The replacement and retraining of personnel to use new systems will be a significant undertaking, both in terms of time and cost.

4.2 Conclusion

In conclusion, in Part 2 of this paper, the definition of protocols was provided and the most important IoT protocols were highlighted, including the emerging Matter standard. Additionally, the Devices used for IoT were discussed and categorized into Pre-Built and DIY options. The various types of Applications used to control and automate these devices were also presented. Finally, a perspective on the future of IoT and its challenges was provided.

REFERENCES

[1] Valentina E.Balas , Vijender Kumar Solanki , Raghvendra Kumar , Manju Khari; Internet of Things and Big Data Analystics for Smart Generation

[2] Knud Lasse Lueth; IoT analystic

[3] Trevor Harwood ; Internet of Things (IoT) History: A closer look at who coined the term and the background evolution into today's trending topic

[4] The Gartner Hype Cycle for emerging technologies ; https://www.gartner.com/

[5] IoT 2022; https://tinyurl.com/yckrk3xj

[6] R. Sri Skandha Moorthy, N. Nathiya. Botnet Detection Using Artificial Intelligence. Procedia Computer Science,Volume 218, 2023, Pages 1405-1413. https://doi.org/10.1016/j.procs.2023.01.119

[7] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini,Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, Volume 76,2015,Pages 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[8] Wallarm. What is Botnet Attack? . https://www.wallarm.com/what/what-is-a-botnet

[9] How the Internet of Things Will Transform the Public Sector. https://tinyurl.com/2h2k3382

[10] 10 Internet Of Things (Iot) Healthcare Examples, And Why Their Security Matters. https://ordr.net/article/iot-healthcare-examples/

[11] 7 IoT Security Issues And How To Protect Your Solution. https://www.designrush.com/agency/software-development/trends/iot-security-issues

[12] How to Secure IoT Devices in the Enterprise. https://tinyurl.com/453mpkpj

[13] Polat, Gokhan. senior manager at EY Risk Advisory Services, Turkey. Sodah, Fadi. Security Issues in IoT: Challenges and Countermeasures.

[14] Gatlan, Sergiu. New Chaos malware infects Windows, Linux devices for DDoS attacks. https://tinyurl.com/y6zhb4ph

[15] Black Lotus Labs. Chaos Is A Go-Based Swiss Army Knife Of Malware. https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/

[16] Montalbano, Elizabeth. Chaos Malware Resurfaces With All-New DDoS & Cryptomining Modules. https://tinyurl.com/yspzynyh

[17] What is IoT security? | IoT device security. https://www.cloudflare.com/learning/security/glossary/iot-security/

[18] What is an on-path attacker?. https://www.cloudflare.com/learning/security/threats/on-path-attack/

[19] What is the Mirai Botnet?. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[20] What is a denial-of-service (DoS) attack?. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[21] Protection! The Importance Of Security In IoT Systems. https://www.iotsolutions.com.mt/post/security-in-iot-technologies

[22] What is IoT Security?. https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

[23] Mirai Botnet Continues to Plague IoT Space. https://www.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space
[24] Inside Mirai the infamous IoT Botnet: A Retrospective Analysis. https://tinyurl.com/2p8s7d4r
[25] Sempf, Julia. .Mirai – Das Botnet of Things. https://www.hornetsecurity.com/de/security-informationen/mirai-das-botnet-of-things/
[26] IoT Analytics. IoT 2022: Connected Devices Growing 18% to 14.4 Billion Globally. https://www.iotforall.com/state-of-iot-2022
[27] Cloudflare, Inc. https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/
[28]] SoumikMondal. What is Wi-Fi? - https://www.geeksforgeeks.org/what-is-wifiwireless-fidelity/
[29] Wi-Fi Alliance®. https://www.wi-fi.org/discover-wi-fi/papers
[30] Connectivity Standards Alliance. Zigbee. https://csa-iot.org/all-solutions/zigbee/
[31] Silicon Labs. IoT-Developer-Boot-Camp. Introduction of Zigbee Basic. https://github.com/SiliconLabs/IoT-Developer-Boot-Camp/wiki/Introduction-of-Zigbee-Basic
[32] Thread Group. https://www.threadgroup.org/
[33] Connectivity Standards Alliance. Matter. https://csa-iot.org/all-solutions/matter/
[34] ESPHome. https://esphome.io/
[35] Arduino. Language Reference. https://www.arduino.cc/reference/en/
[36] Nabu Casa. Home Assistant. https://www.home-assistant.io/
[37] Tait Brown. Homebridge webpage. https://homebridge.io/
[38] Justin Lam. The Future of IoT: What Should We Expect?

https://www.iotforall.com/what-can-we-expect-for-the-future-of-iot