UDC: 004.7.056:[728:696-027.15
Professional paper

NETWORK SECURITY IN A SMART HOME

Enkelejdë BYTYÇI[1*], Florinda IMERI[1]

[1]*Department of Informatics, Faculty of Natural Sciences and Mathematics*
[*]*Corresponding author e-mail: e.bytyci211574@unite.edu.mk*

Abstract

Today when everything revolves around technology, we are constantly looking for the easiest possible ways to live well and comfortably. One of these ways is home automation or smart home. Technology offers new opportunities to increase the internal connection of the house to automate the house.
Today we can connect any electronic device and can control the house without moving any muscle. But we have to be very careful about how we make these devices that enable home automation safe for us because unfortunately, we have a lot of people trying to find the vulnerabilities of these devices and systems and misuse them and cause a lot of problems and damages. In this paper, I will discuss how this is enabled, what is a smart home, the devices, and how to make it safe for us.

Keywords: Smart home, smartphone, devices, technology, ZigBee, Z-Waves, etc.

1. Introduction

Whether you are buying a new home or looking for some upgrades to your current living space, chances are some smart home ideas have crossed your mind as part of the process. It is easier than ever to set up the smart home of your dreams, monitoring and controlling it are also easier to do as well, but to be effective and safe, some steps must be taken that guarantee accurate conFig uration by not allowing unauthorized access. The Internet today represents the largest system ever created by mankind. There are billions of devices connected, and there are billions of users connected to laptops, smartphones, and other devices. The desire for everyone and everything to be connected is continuing to grow regularly. By using the computer, someone can commit illegal activities such as committing fraud, identity theft, invasion of privacy, and others. [1]

In this research, in addition to mentioning how the network should be secured in a smart home, we will also list the problems and solutions that an engineer or a homeowner may encounter with the network within the smart home. Some drawbacks still challenge companies and homeowners when thinking about automating the house, some are the perceived complexity, protocols, security, or data privacy that makes many homeowners vulnerable to keep data untouchable because there are hackers who could disable all the lights and alarms, unlock the doors, get in the house and steal whatever they wish inside. Hackers are surrounding and anytime they get access to encryption or passwords they will steal data stored in public buildings, homes, hospitals, or wherever devices are. Wireless Sensor Networks are trendy in smart homes technologies due to their great advantages, but there are still many challenges to overcome and make this feasible from devices to the cloud. Therefore, smart homes use algorithms to gradually build systems with high performance and credibility [2].

The purpose of this study is to inform people what a smart home is, what devices make a smart home, how can we use them, and how can we make it safe for us.

2. Smart Home systems

A smart home uses devices connected via the Internet to allow for remote monitoring and management of appliances and systems. Smart home technology, also known as home automation, provides homeowners with added security, convenience, and energy efficiency. It allows them to control smart devices simply with an app on their smartphones, or other networked devices [3]. A smart home makes our everyday life much easier. A smart home is a place that has highly advanced automatic systems for controlling and monitoring lighting and temperature, home appliances, multi-media equipment, security systems, and many other functions [4]. Door locks, televisions, thermostats, home monitors, cameras, lights, and even appliances such as the refrigerator can be controlled through one home automation system. The system is installed on a mobile or other networked device, and the user can create time schedules for certain changes to take effect [5]. Communication between the individual smart home components is increasingly wireless. The data is usually transmitted either by radio, WLAN, or Bluetooth. Wired solutions are sometimes also used in new buildings. The reason: If more and more devices are working in a network, it quickly becomes overloaded. Wired systems are also considered to be less susceptible. However, their installation is much more complex. [6]

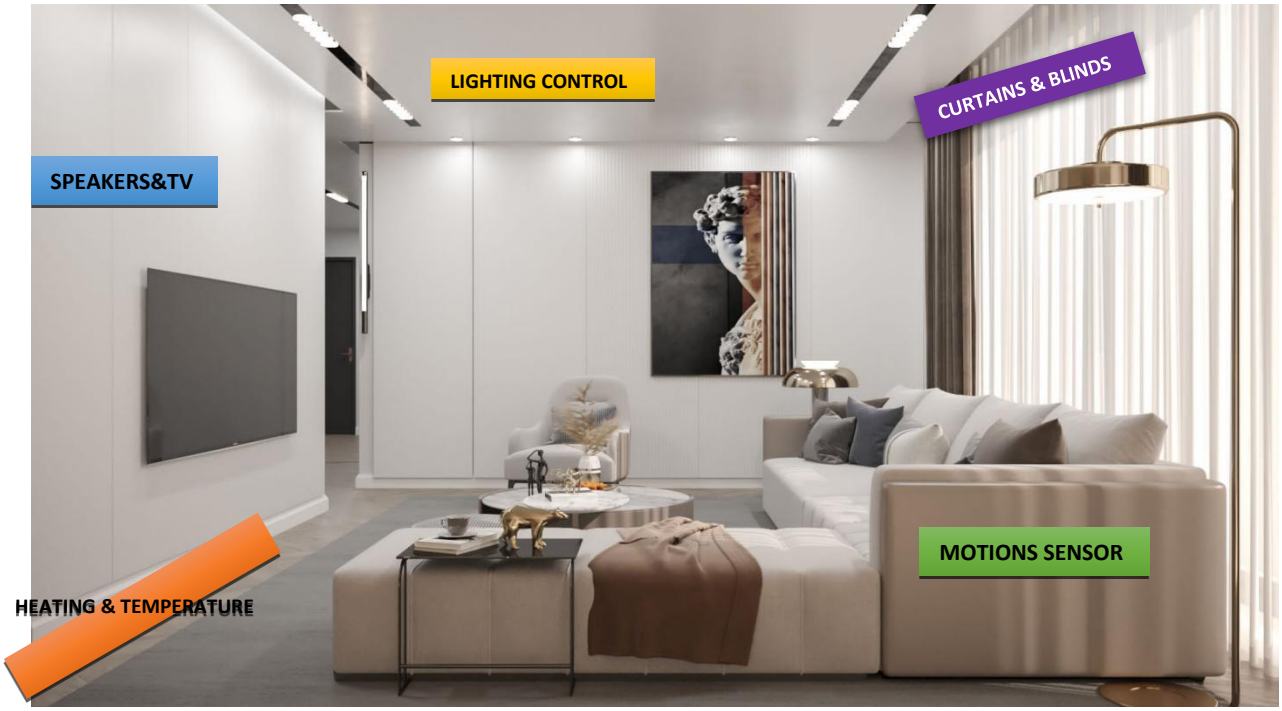

Fig 1. Smart Home Technology Automation

2.1. Smart Home Technology: In 1975 with the development of the X10, by a Scottish company, the development of smart home technology was noticed. [3] X10 is a versatile home automation technology that uses your home's existing electrical wiring to remotely control lights, appliances, security systems, pools, and much more. [7] The X10 industry standard is the oldest industry standard, which can control all of these things at home. A Basic X10 system includes a Transmitter & Receiver:

- Transmitters are control devices that send X10 signals through your home's electrical wiring to X10 Receivers. X10 controllers, switches, modules, and transmitters can be plug-in devices or can be installed directly into your home's electrical wiring.

- When a Receiver receives a command, it responds by turning a light, appliance or other electrical devices On or Off, and sometimes Dim or Bright. They also come in plug-in or wire-in options.

Wireless X10 Transmitters broadcast RF control signals to Transceivers, which plug into standard wall outlets. The Transceiver then converts the RF signal into an X10 system signal and transmits the command to your X10 Receivers [7]. If you want to turn off a light in another room, the transmitter will issue a message in numerical code that includes the following:

- An alert to the system that it's issuing a command,
- An identifying unit number for the device that should receive the command and
- A code that contains the actual command, such as "turn off."

This is designed to happen in less than a second, but some misunderstandings can occur when using this type of technology. Communicating over electrical lines is not always dependable because the lines get "noisy" from powering other devices. An X10 device could interpret electronic interference as a command and react, or it might not receive the command at all. Instead of going through the power lines, some systems use radio waves to communicate, which is also how Wi-Fi and cell phone signals operate. Zigbee and Z-Wave are two of the most common home automation communication protocols used today. Both technologies use short-range radio signals with low power to connect smart home systems. Z-Wave uses a Source Routing Algorithm to determine the fastest route for messages. Each Z-Wave device is embedded with a code, and when the device is plugged into the system, the network controller recognizes the code, determines its location, and adds it to the network. Z-Wave has developed a hierarchy between devices: Some controllers initiate messages, and some are "slaves," which means they can only carry and respond to messages. ZigBee's name illustrates the mesh networking concept because messages from the transmitter zigzag like bees, looking for the best path to the receiver. Like Z-Wave, ZigBee has fully functional devices (or those that route the message) and reduced function devices (or those that don't). [8]

2.2. Examples of smart home products and their functions in 2021: There are 4 ways to control our smart homes devices: (1) *Manual Control*: turning the lights on and off with a light switch. (2) *Controlling by voice*: you can ask Google or Amazon or whatever voice assistant you want to use. (3) *Automation*: With automation, you can have certain triggers so when you walk into a room you have a motion sensor that automatically turns on the lights. (4) *Smartphones*, using apps for controlling these devices. [9]

- *Alarm Systems*: Motion sensors, window sensors, and a siren are in constant contact to secure the building while you are on the move. If one of the sensors reports an alarm, the alarm system goes off and you also receive a warning message on your smartphone. As soon as you stand in front of the front door, the alarm system switches off automatically. Smart lighting illuminates the escape route to the outside as soon as your security system detects danger. This automatic function is particularly useful in connection with smoke alarm devices.
- *Blind smart shades*: automatically turn off or close every day at sunset, and in the morning, they turn on or open up at a set time. You can have them set on automation or schedule for opening up.
- *Controlling the lights* by voice, with help of a voice assistant. Also using a smartphone, you can control the lights by touch for a single room or the whole house. In holiday mode, the smart lamps switch on and off randomly throughout the day. This simulates your presence and increases security against burglars. The installation of motion-controlled light is particularly suitable in hallways and basements. To do this, you connect the smart lamp to a motion sensor. After the motion is detected, the lighting lights up for the length of time you set and then it switches off automatically. Smart lighting simulates sunrise in the bedroom in the morning by gradually increasing the brightness.

This ensures a more restful wake-up. You can also pair certain lamps with other smart home devices. A distinctive red of the lamp then signals to you that, for example, the washing machine is ready.

- *Smart faucet*: You can set up your water bottle in the app to tell it exactly how much water you need to fill a bottle, and then it will go until it fills it up just by using your voice, you can also set presets on temperature and certain things, and then you wave your hand over the sensor on top or under for it to dispense the water.
- *Smart cameras*: For example, if you want to check the front door, you can simply tap on the app and you can see what's happening out the front door, you can also talk to the doorbell, and you can hear them and their response. Indoor and outdoor cameras are used to protect against burglary. They record either 24/7 or only based on motion detection. The recordings can then be accessed via your user account.
- *Smart locks*, come in different options, fingerprint identification technology, or with a keypad.
- *Heating*: each room gets its heating schedule. This means that the heating behavior automatically adapts to your daily rhythm. This function can contribute enormously to heating cost savings. In connection with window contacts, smart thermostats detect whether you are currently airing. The heating then shuts down automatically for the duration of the ventilation. Some smart radiator thermostats also have this function without additional window sensors. Some smart heating systems have a geofencing function. The system only heats when someone is actually at home. The heating system does not receive your exact location. Instead, it calculates the distance to your smartphone. When leaving a certain radius, set schedules begin to pause and only turn the heating up again when the first person is on their way home. Some heating systems take additional data into account for efficient heating regulation. For example, the weather forecast is integrated. On warmer days, the system then does not heat up to the maximum level.
- *Vacuum cleaners:* vacuum cleaner robots vacuum your apartment according to a schedule. This will help you keep your home clean during the week.
- *Speakers and TVs.*
- *Smart Fire Alarms*, will notify you on your phone if there's smoke or anything near, etc. [10]

These products are available at home improvement stores, electronics stores, technicians, or online.

3. Security technology

With the development of technology and the growing need for the Internet, the need for network security arises, which has become a major concern for companies around the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has increased that concern. [11]

3.1. Protecting Confidential Information: Confidential information can lie in two states on a network. It can reside on physical storage media such as a hard drive or memory, or it can reside in transit across the physical network wire in the form of packets. These present numerous attack possibilities from users on your internal network and other Internet users. Our concern is the network security issues, the five common methods of attack that present opportunities to compromise the information on your network are:

- Network packet sniffers
- Password attacks
- IP spoofing
- Man-in-the-middle attacks
- Distribution of sensitive internal information to external sources,

The protection of this information prevents the theft, destruction, corruption, and entry of information that may cause irreparable damage to sensitive and confidential data. [11]

Network packet sniffers

A packet sniffer, protocol analyzer, or network analyzer, is computer program or computer hardware such as a packet capture appliance that can intercept and log traffic that passes over a computer network or part of a network. Packet sniffing is a technique by which packet data flowing across the network is detected and observed. Network administrators use packet sniffing tools to monitor and validate network traffic, while hackers may use similar tools for nefarious purposes. [12]

Password attacks

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password. Another type of approach is password spraying, which is often automated and occurs slowly over time in order to remain undetected, using a list of common passwords. [13]

IP spoofing

IP spoofing is the creation of Internet Protocol (IP) packets that have a modified source address to either hide the identity of the sender, impersonate another computer system, or both. It is a technique often used by bad actors to invoke distributed denial-of-service (DDoS) attacks against a target device or the surrounding infrastructure. [14]

Man-in-the-middle attacks

In cryptography and computer security, a man-in-the-middle attack is a cyber-attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. [15]

Distribution of sensitive internal information to external sources

Sensitive information is data that must be guarded against unauthorized access and unwarranted disclosure to maintain the information security of an individual or organization. Sensitive information is not collected from unrestricted directories and does not include any information made lawfully available to the general public from government records. This means that exposure of sensitive data can potentially cause financial or personal harm. For the organization, the consequences of a data breach of sensitive information can range from minor to disastrous. In particularly devastating cases, companies may be required to pay tens of millions of dollars in damage compensation to customers and financial institutions. [16]

4. Smart Home Security

Connecting devices to the network internally is one of the most common issues faced by smart device owners. From smart cameras that need power to smart living room lights that you can't turn off, network connectivity and interaction issues can be annoying and even seriously confusing. Smart home goes through comfort and safety risks. Hackers can often take control of smart devices, thermostats, doorbells, and other related devices. A smart home is the most wonderful thing that has been developed and is expected to continue to be developed, but when cameras can be hacked to spy on us, microphones on smart speakers can be manipulated with lasers, and smart plugs can compromise all security systems, it is understandable to have reservations about connecting your home with internet.

Consider what you need

Before you buy a smart speaker, thermostat, or doorbell video, think carefully about comfort when it comes to balancing convenience with security and privacy. A security camera can provide some form of protection, but are you comfortable uploading footage online? A voice assistant like Alexa never sleeps, always listening to your command. Is it upsetting or a benefit? Understand what you need from a smart home and where, for you, privacy transcends comfort. [17]

Secure Your Wi-Fi Network

Most routers are either not secured or use a generic password like "123456," making it easy for hackers to poke around and access devices that are connected to your router. So, the first thing you should do is secure your Wi-Fi network with a strong password. [17]

Manage Your Account Passwords

Once you have secured the Wi-Fi network, you must also protect the individual devices and services that are connected to it. Many smart devices are controlled through a connected mobile app and you will need to set up an account with each one. Using the same password for everything is convenient, and it may seem easy to remember but it is a security nightmare. If one of these accounts is compromised and the password is discovered, hackers now potentially have the keys to all the other accounts in which you used that password. For more security, use a random password generator to generate hard-to-guess codes and a password manager to remember them for you. [17]

Enable Two-Factor Authentication

By activating two-factor authentication in the services that support it, the security of your smart home becomes stronger. Those accounts will ask for your password, plus a second form of authentication - usually, a six-digit code sent by text message or created through a verification application like Google Authenticator. So even if a hacker gets your password, he will not be able to access your account without that six-digit code. [17]

5. Conclusions

The Internet of Things (IoT) is changing the way we live by connecting the devices we use. Now, any device, from your hi-fi and TV to your heating, door locks, and lighting, can be connected to a single controller through the internet, giving you total control of your home. A smart home can make your life easier and more enjoyable. However, it also comes with a downside. By connecting your home systems to the internet, you're opening it up to too many security risks. So, we must be very careful and take measures to prevent any danger.
Security is an important issue in smart home applications. In this paper, we discussed smart homes and security.

References

[1]. L. Rainie and J. Anderson, "The Internet of Things Connectivity Binge: What Are the Implications? " 6 June 2017. [Online].Available:https://www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/.

[2]. A. E. Coboi, T. A. Tran, S. Q. Tran, and M. T. Nguyen, "Security Problems in Smart Homes," ICSES Transactions on Computer Networks and Communications, 2021.

[3]. V. Rediksson, "TechTarget," 2005. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building#.

[4]. T. Malche and P. Maheshwary, "Internet of Things (IoT) for building Smart Home," International conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud), 2017.

[5]. A. Hayes, "Smart Home," 10 January 2022. [Online]. Available: https://www.investopedia.com/terms/s/smart-home.asp.

[6]. Phillip, "Was ist ein Smart Home? Alles, was Du über Geräte und Systeme wissen musst!," 12 july 2019. [Online]. Available: https://www.tink.de/blog/was-ist-smart-home/.

[7]. "Home Controls Autonomation Products & Support since 1989," [Online]. Available: https://www.homecontrols.com/Manufacturers/x10.

[8]. R. J. Robles and T.-h. Kim, "A Review on Security in Smart Home Development," International Journal of Advanced Science and Technology, vol. 15, p. 10, 2010.

[9]. "SONOFF," 21 June 2021. [Online]. Available: https://sonoff.tech/news-and-events/home-automation-10-ways-to-control-your-smart-home/.

[10]. "Smart Home Beispiele und Möglichkeiten," [Online]. Available: https://komwoh.de/smart-home-beispiele/.

[11]. C. Press, "Internetworking Technologies Handbook, Chapter 51".

[12]. P. Sniffing, "NETSCOUT," [Online]. Available: https://www.netscout.com/what-is/sniffer.

[13]. D. Poza, "What Is Password Spraying? How to Stop Password Spraying Attacks," Autho, 8 July 2021. [Online]. Available: https://auth0.com/blog/what-is-password-spraying-how-to-stop-password-spraying-attacks/.

[14]. "What is IP spoofing?," CLOUDFLARE, [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/.

[15]. M. A. Elaktrat and J. C. Jung, "Development of field-programmable gate array-based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," Nuclear Engineering and Technology, vol. 50, no. 5, pp. 780-787, 2018.

[16]. R. Carr, "What is sensitive information?," Zettaset, [Online]. Available: https://www.zettaset.com/blog/what-is-sensitive-information/.

[17]. J. Cohen, "How to Protect Your Smart Home From Hackers," 18 February 2021. [Online]. Available: https://www.pcmag.com/how-to/how-to-protect-your-smart-home-from-hackers.