OsloMet - Storbyuniversitetet

Spring 2022

Final Report, SIFO

Communications to raise public awareness about risks of living with smart devices in the home

DATA3710 - Practical IT-project

By

Arian Saralani - s354589

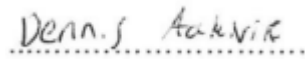Dennis Sviggum Aakvik - s354546

Preface

In the age of digitalization of standard home appliances being somehow connected to the internet, we face a lot of challenges concerning all of the data that they can collect about us and our lives. This is the topic we were faced with when we took on the task of making a visual aid which would inform and warn people about these potential threats. The result of which is presented in this report.

We would like to thank Henry Mainsah, our project leader, and Nuno Marquez, our project supervisor, for their immense support and guidance throughout this project.

This report was written on May 11th, 2022, at OsloMet Campus.

Dennis Sviggum Aakvik

Arian Saralani

Table of Contents

List of Figures

1. Introduction

In our current digital age, many people have grown accustomed to having devices in their home which they can "talk to". We can give commands such as "turn on the lights" or "remind me of my project meeting at 08:00", we can ask them what the weather is like, how tall Mt. Everest is and much more. These devices and many other smart-home devices are constantly "listening" and, if connected to your phone, collects a lot of information about you that you may not realize.

The title for SIFO's project is to "create a form of communication to raise the public awareness about risks of living with smart devices in the home". The team members are Dennis Sviggum Aakvik and Arian Saralani. The background for the project is that we get to collaborate with our supervisor, Henry Mainsah, who is a researcher and leading an ongoing Norwegian Research Council-sponsored project called RELINK. They are a research project which develop frameworks, tools, and scenarios that address current and future risks related to Internet of Things in connected homes and households.

The team members are Dennis and Arian, with our supervisor Henry. Since our first meeting we had a lot of creative freedom as to how to approach this topic. As such, we wanted to focus on a specific target group which are adults, particularly those with children. The aim of the project is to inform parents and kids about potential dangers that smart technologies in the home can bring and make them well-informed about what they can do about these dangers.

The theme of our project is digital vulnerabilities that come with smart devices in the home and the challenge we address by undertaking this problem is to raise awareness and for people to be able to make risk evaluations of these devices that are connected to the internet and collect personal data.

2. Aims

The aim of the project is, as the title of our project suggests, to create a communication to raise public awareness about risks of living with smart devices in the home. This can be security risks or other vulnerabilities related to smart technology that we use every day and have become such an integral part of our society. The project also aims to get people to be able to inform people, so they can make risk evaluations by themselves about the devices.

3. Specification

At the start of the project, we spent some time reading different research papers about this topic. Some we found on our own, and others were provided to us by RELINK. Our original target demographic were elderly people above the age of 60. We thought they would be the most uninformed group concerning this topic, but we felt it would be difficult to explain what all this information and technical terms would mean. This is why we changed our target group to parents with children instead. This was with the thought of educating the kids as well as the parents. If the parents were more informed about this, they could be more aware of what privacy policies they and their kids actually accept and agree to.

We wished to make a whole informative website with one interactive element, however we had to change this to just the interactive element due to a group member leaving. This meant we had to change the scope of our original vision and make it doable for two people with the limited time we had. The interactive element we thought would work best was a quiz. This was so it would be engaging for the users and at the same time convey the information we wished to spread.

With this quiz as our main project, we looked for inspiration on other educational quizzes. Predominantly Kahoot, as we were both very familiar with it. We sketched up a design for how the website would look and, with the computer development software "IntelliJ", we would program and build up the JavaScript code which would upload each of the questions we had made and set up different answer alternatives and which would be the correct one. This would also tally up the number of correct answers the user got, which would be presented to them at the end of the quiz.
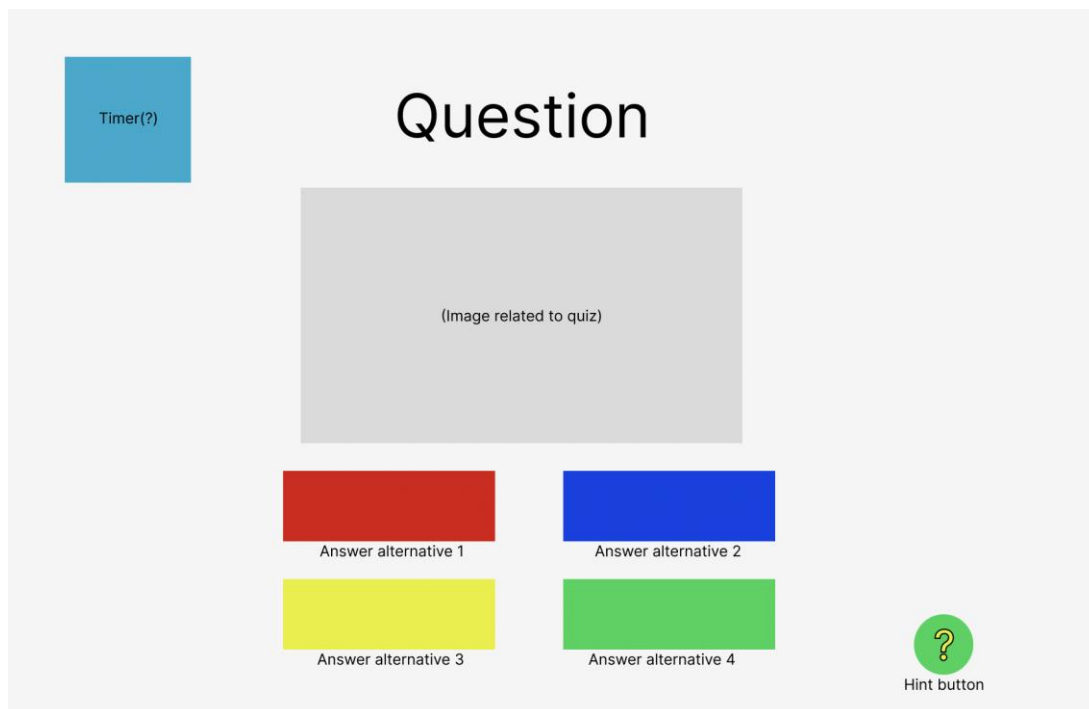
(Figure 3.1: One of our first sketches and initial designs for the quiz)

We wished to have more color in our prototype because we wanted to make it look interesting and engage kids more, with a user interface more like Kahoot, as per our design. There were however time limitations which made us not able to implement this to our current prototype. As we had a big inspiration from Kahoot for our prototype, we were wondering if we could add a competitive element where users who answered correctly quickly would get more points. We wanted to implement this competitive feature to keep the players more engaged in the quiz and actually care about getting the answers right. This also had to be cut from the current prototype we have today due to time restrictions.

4. Work Processes

First, we had a research phase where we found as much information as possible to get a bigger and better view of what smart devices are. Then we began talking about how we want to create a way to communicate the risks of smart devices. The first and most important choice we made was the demographic to focus on, and how we would make the project relevant for this group.

In these first days of developing an idea for what we could make, we spent time figuring out which demographic we wished to reach. In the beginning we thought of the elderly (people above the age of 60). In general, elderly people are not incredibly familiar with technology or the potential threats they can hold. We thought of our own families and all had examples of a younger generation in the family buying some sort of smart home device for the older generation, so we assumed that this would be the case for a lot of other households. Based on this assumption, this would mean that elderly people with smart home devices in their homes would probably not be aware of the threats that might come with it.

However, we soon switched our target group to children, to hopefully educate them from an early age of what to be considerate of when using these devices. We quickly added their parents to our target group, so we wish to reach out to adults with kids. If the parents are aware of the potential threats and dangers, then they would probably pay more attention to, not only what their children are doing, but also be more careful of what kind of information they allow these devices to collect. This was our hope and goal from an early stage of development.

As a result of all the research and brainstorming, we thought we could develop a website aimed towards our target group. The website would have articles we would write about the information we wish to spread for the adults, and then a simplified version for the kids. We faced a challenge at this stage, because we wished to make the webpage for the kids more entertaining somehow, because if we barrage all this technical information on children, they would probably be bored very quickly.

Sadly, we had to scratch the idea of the website, or at least a part of it. As the two of us suddenly got a message from the third member of our group informing us that they would no longer be in our group and work alone from then on. We were very confused by this as they never gave us a reason or chance to discuss it. This was our biggest challenge as we had to change our whole approach with only the two of us. Undiscouraged, the two of us would

continue to develop our vision, but the workload would be too much for two people in such a short time. That's when we decided to take a part of our initial idea and fledge it out. The new plan we created was to only make an interactive element, and not a whole website. This was because we thought we could properly see how an interactive element would work, and how this was as a way to create communication with a user group.

We also focused on finding the best ways to engage a user when wanting to communicate information. This was done by creating the prototype and began coming up with questions. Our focus when we began creating our product was to just get a prototype of it and then be able to test it, because we meant that the content would give the user an interest to research more independently.

5. Methods

At first, we began researching about what the technology is and how it is being used in everyday life. This was for example how people used google home, or different security technologies like locks or cameras were being used. We also looked at what some surveys had as results when asking people what they thought about smart home devices. Here we found an article that said, "some 67% agreed with a statement that 'Connected devices are "creepy" in the way they collect data about people and their behaviors.' But the surprising part is that among those who actually own such devices, the percentage was almost identical: 66%." (Lovejoy, 2019).

This showed us that there is a fear around what smart home devices do, and how much they can collect and who is getting this information. It was also interesting here how the percentages of people saying it is creepy and those that own devices were similar. This shows a need to provide information because it seems a lot of people are getting devices without getting enough information first.

We were provided documents by SIFO and we used this as well in our research. We used this research to find out who we wanted to focus the communication on, and we also used it to find what we thought would be one of the best ways to engage a user when talking about smart devices. Some of the things we learned were that "instead of breaching a single individual's smart device to nab their data, a hacker will infiltrate the database of a smart-device company to pilfer the data of all its users." (Reddigari, 2022). If a homeowner has smart door locks, then unidentified security loopholes could grant hackers permission to unlock these doors. Which would leave the doors quite literally open to anyone.

With this we also had to learn more about what counter measures users can make to prevent- or at the very least- limit the chances of these data breaches to occur.

One of the research papers that SIFO provided was about the privacy concerns in IoT. It mentions how many IoT devices have vulnerabilities that are similar to each other. They for example say "Usually, the deployment of IoT comprises a set of alike or nearly identical appliances that bear similar characteristics. This similarity amplifies the magnitude of any vulnerability in the security that may significantly affect many of them." (Tawalbeh et al,.
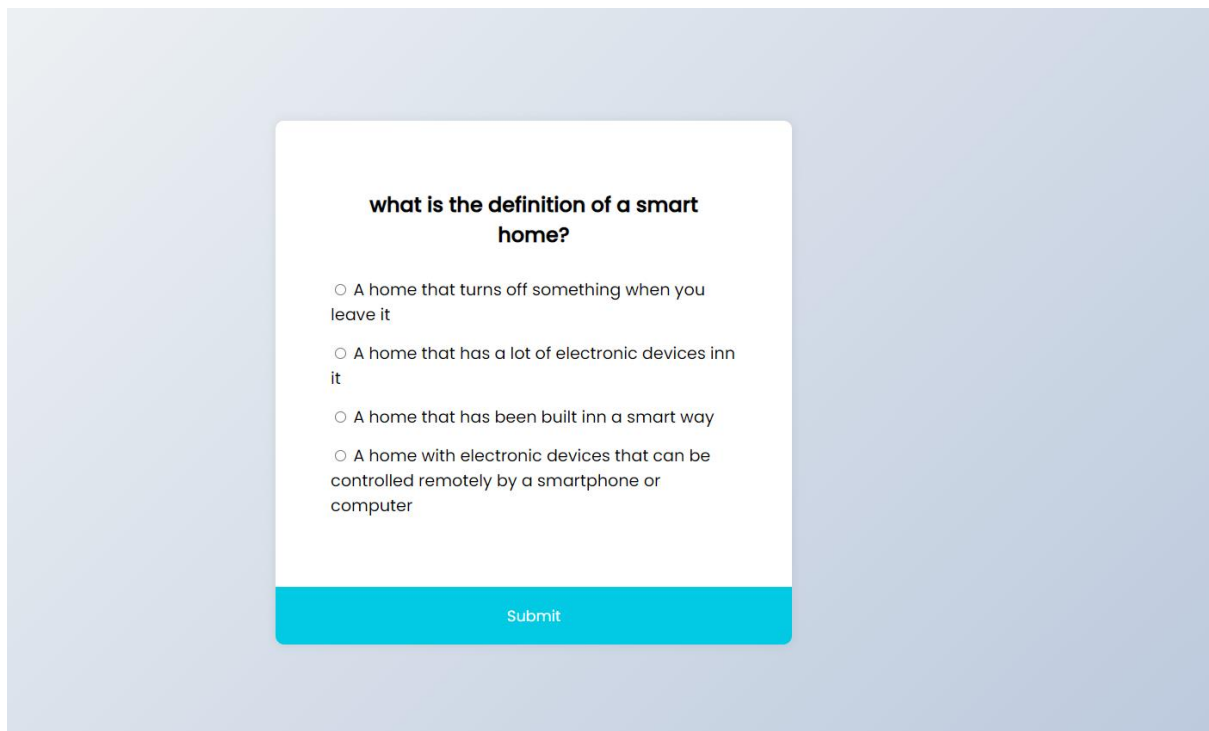
2020). This is information that we did not know before and gave us new insight into how the different companies produce their technology.

6. The Result

The product makes an introduction into smart devices that are in the home and is meant to create an interest in learning more about the risks that come with smart devices. It is a quiz like for example Kahoot where it is easier to engage a child and an adult because of a colorful and vibrant design. It is a great way to create communication through the way it engages the user through a fun and competitive game. This comes from the way you can implement a score board or other ways to show off results.

As the final product is just a draft with focus on the content it does not have too much going in the design department, but it does stack up to our want of having questions that are relevant and not too difficult. We wanted to also create a colorful and vibrant design but unfortunately did not get enough time for this. But it is not what we wanted to make in the start, as we wanted to create a website with an interactive element. In the end we only made the interactive element because of complications that arose during the development process.

We feel that we have achieved a better understanding of how to create communication about a topic with someone else, and how to create engagement from a user. We also achieved our aim of creating a simple prototype for the quiz, and then having questions that are relevant to follow with the quiz.

(Figure 6.1: One of the questions on the prototype quiz)
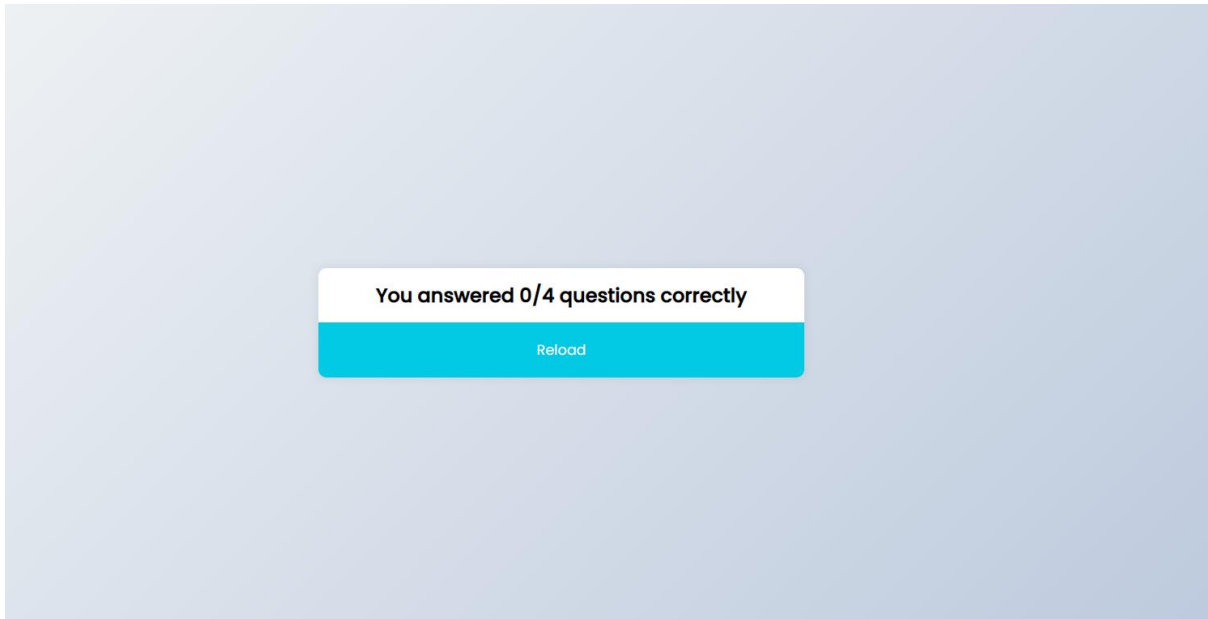
(Figure 6.2: What the user will see as they finish the quiz)

We managed to get a way of loading quiz questions to work, but we unfortunately did not get it to be a randomized quiz like we wanted. This script looks like this

```javascript
const quizData = [
    {
        question: "what is the definition of a smart home?",
        a: "A home that turns off something when you leave it",
        b: "A home that has a lot of electronic devices inn it",
        c: "A home that has been built inn a smart way",
        d: "A home with electronic devices that can be controlled remotely by a smartphone or computer",
        correct: "d",
    },
    {
        question: "Is a smart home completely secure?",
        a: "No because it can be hacked/breached",
        b: "Yes because the user can see everything that is happening",
        c: "Depends on the user",
        d: "Yes because it is created to create security in the home",
        correct: "a",
    },
    {
        question: "What is one way someone can get into your smart home security?",
        a: "They can get trough just by hacking from home",
        b: "They get access to the internet that the smart home techonology is connected too",
        c: "Someone can get access trough knowing where the device is located",
        d: "There is no way someone can get access",
        correct: "b",
    },
    {
        question: "Is there a way to make sure your home security is more secure",
        a: "No its already completely secure",
        b: "Yes the user can stay updated about potential bugs or leaks with the devices",
        c: "No the user cannot do anything about security",
        d: "Yes by making sure to not let anyone get access to your internet",
        correct: "b",
    },

];
```

(Figure 6.3: Here we have the questions that will be loaded)

14

```
const quiz= document.getElementById( elementId: 'quiz')
const answerEls = document.querySelectorAll( selectors: '.answer')
const questionEl = document.getElementById( elementId: 'question')
const a_text = document.getElementById( elementId: 'a_text')
const b_text = document.getElementById( elementId: 'b_text')
const c_text = document.getElementById( elementId: 'c_text')
const d_text = document.getElementById( elementId: 'd_text')
const submitBtn = document.getElementById( elementId: 'submit')


let currentQuiz = 0
let score = 0

loadQuiz()

function loadQuiz() {

    deselectAnswers()

    const currentQuizData = quizData[currentQuiz]

    questionEl.innerText = currentQuizData.question
    a_text.innerText = currentQuizData.a
    b_text.innerText = currentQuizData.b
    c_text.innerText = currentQuizData.c
    d_text.innerText = currentQuizData.d
}

function deselectAnswers() {
    answerEls.forEach( callbackfn: answerEl => answerEl.checked = false)
}

function getSelected() {
    let answer
    answerEls.forEach( callbackfn: answerEl => {
        if(answerEl.checked) {
            answer = answerEl.id
        }
```

(Figure 6.4: Here we see the script for loading the questions)

Our initial aim was to create a website, and this was not achieved because of complications during the work process, and that made it so that our first aim of a way to communicate was not achieved.

The significance of this project is to provide parents and their kids a better understanding of the risks that smart home devices can have. For the parents it is to make them feel like they are keeping up with technology that is changing fast and provide them more control over it. For the kids it is more about understanding how to be safe when using technology and give them an understanding that something can have risks. It also is to make sure that they know what type of technology that they have in their own home, because this makes it easier for them to understand potential risks that the technology might have. There is actual research on this topic of what users need to want a product. The paper says, "The research validates that trust, awareness, enjoyment, and perceived risks, perceived usefulness, and perceived ease of use significantly influence customers' attitude and intention to use smart homes" (Liu et al., 2021). This gives them a feeling of safety and a trust for the technology that they have at home. It might also make it so that more people get this type of technology because they understand it better and feel like they know what to do to make it trustworthy.

The value of our product and the results we got comes from the way it creates communication around the topic of risks with smart home technology. This can be used later as a feature in a website or a standalone product that can be used to introduce a user to the risks. It also shows how a quiz can be used to engage both children and adults by using a game setting to let them get an interest and understanding of a topic.

7. Conclusion

In conclusion, it was relatively easy for us to gather our thoughts and ideas for this project early on, as there are only two of us in the group. So, when we came together to discuss what we wanted to implement and what we wished to have as a goal, we rarely reached an impasse.

Moreover, even though we are IT students and used a lot of our previous knowledge in the development of the prototype. We think that every time you develop new code or new software, you will gain new knowledge, because it is never exactly the same. We had also never collaborated before this, so it was very interesting to see what we both could bring to the table and see how our individual limitations could be solved by the other person. Neither of us had developed anything similar to a quiz before, and we both learned some new skills regarding programming with JavaScript and web development from that.

Furthermore, we also learned a lot about what we researched in the beginning of the project. Not only did we learn of new potential ways your data can be used against you, such as identity theft, targeted attacks and even property damage. We also learned how to deal with these potential threats, or at the very least how to limit the probability of them occurring. Reading previous research and articles about the subject certainly gave us new insight to the topic, as well as being directly challenged with questions from Henry.

In the end, we are certainly satisfied with the result of our prototype. However, we are still a bit sentimental about the original scope of what we wanted to build, and still wish we could've made that had we not lost a group member. We also wish that we could've managed our time to work with the current prototype more efficiently, as we sadly did not get to give it the final polish that we wanted to make it look as good and function a bit more as we had originally envisioned. Despite that we are satisfied with our work and effort and think that should we ever be given the chance to continue this project, that we would have made RELINK and Henry a very good visual aid for parents and their kids to learn about cyber security in the home.

References

Liu, Y. Gan, Y. Song, & Y. Liu, J. (2021) *What Influences the Perceived Trust of a Voice-Enabled Smart Home System: An Empirical Study. Sensors* 2021, *21*, 2037. https://doi.org/10.3390/s21062037

Lovejoy, B. (2019) *Smart home devices 'creepy' say two-thirds of people … who own smart home devices.* https://9to5mac.com/2019/05/02/smart-home-devices-creepy/

Reddigari, M. (2022) *The 10 Biggest Security Risks in Today's Smart Home.* https://www.bobvila.com/slideshow/the-10-biggest-security-risks-in-today-s-smart-home-53081

Tawalbeh, L. Muheidat, F. Tawalbeh, M. & Quwaider, M. (2020) *IoT Privacy and Security: Challenges and Solutions.* Appl. Sci. 2020, 10, 4102. https://doi.org/10.3390/app10124102

Appendices

1. Link to GitHub page for the quiz: https://github.com/Dsaakv/quiz