The Integration of Internet of Things (IoT)

Data Security and Privacy

Lekhaz.Adapa

Lead3201@student.su.se

Abstract

The Internet of Things (IoT) and smartphones have ushered in a new era of ease and connectivity. However, they have also raised concerns about data security and privacy. As connected devices proliferate, a growing quantity of data is created and transmitted, raising questions about who has access to this data and how it is utilized. Similarly, smartphones may capture massive quantities of personal data, including locations and browsing history. While this data may be utilized to improve user experience, it also poses privacy concerns.

This study used a web-based questionnaire interview with thirteen students with prior knowledge of Data Security and Privacy. This questionnaire aims to capture the experience faced by the participants and how they have overcome it, what measures they have taken for the future, and what features they would like to see in future IoT devices and smartphones. The questionnaires were then analyzed using thematic analysis.

Throughout, the investigation, four main topics emerged: Knowledge, Data, Authentication, and Security. These four categories were highlighted as areas of participants' experience, actions implemented, and future development of IoT devices and smartphones. This research found that security, privacy, and authentication could all be enhanced.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

IoT – Internet Of Things

DSV – Department of Computer and System Sciences

ICT – Information Communication Technologies

1 Introduction

In 1999, British technology pioneer Kevin Ashton co-founder of the Auto-ID Laboratory at MIT, invented the term Internet of Things to describe a system where the Internet is connected to the physical world via ubiquitous (Jeremy, 2023). In recent years, the Integration of the Internet of Things (IoT) with data security and privacy has become a major topic of concern. The IoT is a network of physical devices that can gather, store, and share data and are connected to the internet. IoT and smartphone devices are vulnerable to a variety of security concerns, including unauthorized access, data breaches, and malware assaults. These dangers have the potential to jeopardize the integrity, confidentiality, and availability of data being gathered and sent. To mitigate these threats, different security and privacy mechanisms, including encryption, authentication, and access control, can be applied. The problem, however, is establishing a balance between security and usability, since security measures may influence device performance and user experience. Policy and legal frameworks, in addition to technological solutions, play an important role in guaranteeing data security and privacy. Governments and industry organizations are working on standards and laws to control the usage and handling of IoT devices and data.

Overall, the integration of IoT, data security, and privacy is a complex and dynamic environment that necessitates collaboration among many stakeholders in order to leverage the benefits of IoT devices and smartphones without jeopardizing data security and privacy.

1.1 Background

As mentioned in the introduction, integrating Internet of Things (IoT) devices into the infrastructure of smart cities is a rapidly growing trend in urban development. IoT devices are sensors, actuators, and other connected devices that collect and exchange data. In smart cities, these devices are used to monitor and control various aspects of urban life, such as low traffic flow, energy consumption, waste management, and public safety.

Humans have become more dependent on networked Information and Communication Technologies (ICT) than ever (Kaushal, 2016). In our day-to-day life, we are connected to things worldwide through many types of technologies; one of the main types is the Internet. This is due to several factors, including technology's rapid growth and evolution, the increasing availability of devices and networks, and the growing demand for information and communication. The main reason for this increased dependence is the widespread use of smartphones and other IoT devices, which have become essential tools for many people in daily life. These devices allow people to stay connected to their friends and colleagues and access information and entertainment whenever and wherever they need it.

IoT devices and smartphones have become indispensable elements of modern life. The Internet of Things refers to an interconnected network of objects that can speak with one another, whereas smartphones are portable, versatile devices that can connect to the internet and gather massive quantities of personal data. While these technologies have many advantages, such as increased convenience and efficiency, they pose major data security and privacy vulnerabilities. As the number of connected devices grows, so does the possibility of data breaches and cyber-attacks. Similarly, a large amount of personal data is being utilized. Because of the rise of IoT and smartphones, regulators, technology manufacturers, and consumers have prioritized data security and privacy. End-to-end encryption, data reduction, and user consent for data collection and usage are all being used to reduce risks and safeguard user privacy.

One of the leading concepts and ideas regarding the smart city is the increase in the technology of IoT devices. IoT devices can be used to monitor the traffic flow, monitor and control the energy consumption in buildings and other infrastructure, track and optimize waste collection, reduce the amount of waste generated, and increase recycling rates. IoT has a wide range of impacts on urban life, which can be both positive and detrimental. On the plus side, IoT devices have the potential to make cities more efficient, sustainable, and habitable. Sensors, for example, can be used to monitor traffic flow and improve vehicle routes, minimizing congestion and pollution. Smart room heater systems can conserve energy by lowering the temperature level. Smart lighting systems can conserve energy by dimming lights automatically when no walkers or cars are present. IoT devices can contribute to better public safety and deliver real-time information on occurrences and emergencies.

A paper by, Tawalbeh et al. (2020) states the security and privacy challenges faced by IoT devices. IoT devices collect and process vast volumes of personally identifiable and sensitive data, subjecting them to cyber-attacks and illegal access. This can result in data breaches and the theft of personal information, both of which can cause substantial harm to persons and organizations. To address these issues, it is critical that the design and development of IoT devices emphasize security and privacy features such as data encryption, secure storage of sensitive data, and access control methods. Furthermore, it is critical for enterprises and governments to have legislation and standards in place to enable the safe use of IoT devices while protecting individuals' privacy.

The next problem will be reconciling IoT devices' advantages with maintaining security and privacy. Innovative safety and privacy solutions and ongoing education and awareness will be required to ensure IoT devices' safe and secure integrations in smart cities.

1.2 Research problem

The importance of security and privacy in the Internet of Things (IoT) devices became widely recognized with these devices' growing use and population. As IoT devices collect and transmit a large amount of personal and sensitive information, the risks of unauthorized access, data breach, and other security threats increase. In response, researchers and experts in the field started to address the need for enhanced security measures to protect the privacy of users and the integrity of the data collected by these devices. In their study, Atzori et al. (2010) indeed, it is emphasized that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date." Through this study, I have understood the security level of IoT devices and how it deals with data.

In their study, Belli et al. (2020) examined the connections of IoT devices in various areas of our world. In their article "Guide on IoT Data Collection" (Kamal, 2023) knew how the data is being captured and then how the data is transmitted, and how the data is consumed. In this article, I have addressed what kind of data is collected, how it works, and whether it is processed.

In their paper, Nadikattu et al. (2018) state, " Identifying is IoT will offer proper security to the devices is a primary concern as securing such devices means that the actual devices themselves are secured more." which made me think a bit about the way of security and privacy how the public perception would be more taken into consideration as consumers are already a bit aware that their data isn't so secure. They always keep questioning the security levels of IoT devices as they will not buy them because they know the risks involved and how the hackers are trying to breach the data for other miscellaneous activities.

Based on the research done by Tawalbeh et al. (2020), further research is required in the security field by either implementing and analyzing the currently existing schemes or developing new ones. They added, "Based on the findings, we provide recommendations to avoid such risks and remedy the possible security vulnerabilities." Nadikattu et al. (2018) state that IoT security and privacy issues start with public perception.

1.3 Aim and research question

This research aims at different users' experiences in terms of Data Security and Privacy issues with their smartphones or any IoT device. And if they have experienced them, what kind of issue is it, and have they overcome them? This specific information can provide insights into what people find most challenging when dealing with security or privacy issues in their smartphones or any IoT devices.

The respondents will be students from DSV. Found in the foregoing data, the following research question will be addressed in this paper:

Data Security and Privacy in smartphones or IoT devices?

1.4 Delimitations of the study

This research involves some constraints, like the samples collected from only students around age 18 to 24, to ensure that this research will be in a limited time. And furthermore, research can be done on how the security and privacy models can be developed in smartphones or IoT devices. Another limitation of this research is that only the users have prior knowledge about how the data is insecure in today's life, focusing on only the research question. As we have limited time and resources for this research, the scope was limited to interviewing only thirteen participants, focusing on more in-depth thoughts rather than large-scale data collection.

2 Method

2.1 Research strategy

Many research methods are involved. According to Denscombe (2017), A strategy is a plan of action designed to achieve a specific goal. As a researcher, everyone has their own approach to research methods and strategies. A research strategy is different from a research method (Denscombe 2017).

Coming up with the research strategies and conducting a survey is the best fit for my kind of. The Internet of Things industry is a mix of both qualitative and quantitative aspects. Quantitative aspects of IoT include collecting, analyzing, and interpreting large amounts of data generated by IoT devices. Qualitative aspects of IoT include the user experience and understanding of how IoT devices impact daily life.

Strategies like action research and ethnography are not suitable for the study. The phenomenology strategy was considered when choosing the best strategy (Denscombe, 2014). Phenomenology is appropriate because it deals with human experiences, and its fundamental goal is to characterize these personal experiences and sentiments (Denscombe, 2014). As this research goes through the opinions of how the experience they felt on the security and privacy while using a smartphone or an IoT device, its goal is to find some self-measures to be safe while using a smartphone or an IoT device in the case of data. Hence, phenomenology is not determined to be an excellent strategy. Coming to another strategy, a case study is a standard qualitative research method that involves an in-depth investigation of a single or a small number of instances, events, individuals, or organizations. It is particularly well-studied for small-scale studies where the researcher can focus on a limited number of cases and gain a deep understanding of the participants' experiences, perspectives, and behaviors. Cases are specific instances of a large category of objects, and a case has particular characteristics with other things of its sort (Descombe, 2017, p.57). A case study research method will be followed in this paper.

2.2 Data Collection Method

As mentioned in the above part, performing a survey is a good research strategy for this study. From this book, Denscombe (2010, p.13) portrays many types of surveying methods, which include postal surveys, internet surveys, telephone surveys, group administrative surveys, face-to-face surveys, observational surveys, and surveys of documents. There are four main methods that social researchers can use: questionnaires, interviews, observation, and documents (Denscombe, 2010). Questionnaires are which gather information by asking people directly about the points concerned with the research (Denscombe, 2010). Questionnaires are used when what is required tends to be pretty straightforward information and even when the respondent can read and understand (Denscombe, 2010, p.156); these are the most productive (Denscombe, 2010, p.156). While face-to-face surveys involve direct contact between the researcher and individual respondents, they usually use various forms of questionnaires and interviews as their data collection method (Denscomb, 2010, p.16).

This study primarily focuses on administering a questionnaire survey to users and investigating how t be more secure when using a smartphone or an IoT device in terms of data. And a questionnaire is ideally suited to this type of small-scale, which tries to answer a research topic; this data gathering approach was determined to be the best for this research.

There are broad types of questionnaires like structured, semi-structured, unstructured, interview schedules, self-completion questionnaires, web-based, postal, telephone, and face-to-face questionnaires. For this study, we will use web-based questionnaires as this survey mainly reaches out to students from various parts, and these questionnaires are available online. The respondents can complete them using a computer or a mobile device. They can either be structured, semi-structured, or unstructured. A web-based questionnaire is a web page on an internet site waiting for people who visit the site to complete it (Desncombe, 2010, p.14). This study is for a limited time, and this questionnaire

will be sent to various students in the form of Google Forms to answer the questionnaire. To do that, the respondent should log in with the e-mail ID, fill out the form, and submit it.

A questionnaire will be listed in the form of google forms; it will consist of structured questions so that each participant is consistent and standardized. The questions are carefully designed to cover specific topics and are asked in the same order as each other to compare and analyze data. Structured interviews involve tight control over the format of the questions and answers. The researcher has a predetermined list of questions to which the respondent is invited to offer limited options for responses (Desncombe, 2010). Here, we are replacing the interviews armed with clipboards and paper questionnaires with those using laptop computers to input information directly into a suitable software program (Descombe, 2010).

As this is small-scale research, Grounded theory's affinity with qualitative research, its desire to generate explanations from the study of particular instances, its need for detailed data about activities and practice, and its value for exploratory research combine to make it an approach that is well suited to small-scale research conducted by individual researchers operating within the constraints of a tight budget (Denscombe, 2010).

The data collection method in this study follows as in Ha, M.T et al. (2022); the data is collected through Google Forms from thirteen participants who were interviewed as a part of this study. The interview is sent to the respondent through a link that takes them to the questionnaire in Google Forms. This questionnaire consists of demographic data such as name, age, gender, and e-mail. And also open-ended and closed-ended questions.

2.3 Data Sampling

As this study is small-scale qualitative research, Google Forms can be used to gather qualitative data from participants. Still, the data collection strategy would depend on the specific research design and methodology. As we will use phenomenology, which aims to understand the essence or structure of lived experience, data is often collected through in-depth, open-ended interviews, observations, and/or written reflections.

In the book by Denscombe (2010), the point of small-scaled is, that the researcher feels it is not feasible to include a sufficiently large number of examples in the study. There are multiple non-probability sampling techniques based on Descombe (2010). This study involves a purposive sampling technique (Denscombe, 2010). As per Denscombe (2010), purposive sampling operates on the principle that we can get the best information through focusing on a relatively small number of instances deliberately selected on the basis of their own attributes (Denscombe, 2010). This method involves the selection of respondents based on their knowledge so that it can lead to getting some informative data from the respondents. In this study, the purposive method is preferred so that the respondents have knowledge about the security and privacy in smartphones or in an IoT device in the context of the data.

There are certain drawbacks and biases connected with the sampling method employed. Sampling bias can introduce bias into the sample because it relies on the researcher's judgment to select participants who fit specific criteria. Experimenter bias, where can influence the selection of participants leading to the inclusion of individuals who align with the researchers' views, experiences, or expectations. Purposive sampling can make it challenging to replicate results because the sample selection process is not standardized.

The time given for this study is also one factor that provides only a limited amount of samples of only thirteen participants. Review is taken into consideration, and a large number of participants or the time is quite good enough would offer precise and thorough data information.

2.4 Data Analysis Method

As the data is collected through structured questionnaires, the data we expect to be in the form of text. The questionnaire consists of open-ended questions; besides this data, we will also have the nominal data, which includes the name, age, gender, and how many years of using the smartphone or an IoT device (Denscombe, 2010, p.243).

Our study uses qualitative research, which means it uses words as a unit of analysis (Denscombe, 2010). In this book Denscombe (2010). Thematic analysis was chosen as the data analysis method for this research because it is commonly used in qualitative research where words are utilized as data and are well suited for questionnaires with open-ended questions. Braun & Clarke (2006) suggest that a study can use the proposed six-phase approach to maintain the essential rigor in this thematic analysis process. The six phases are Familiarizing with data, Generating initial codes, Searching for themes, Reviewing themes, Defining and naming themes, and writing a report.

This study will follow the thematic analysis method, and many software tools can convert the data into themes. We will use the MAXQDA(*All-in-one qualitative & mixed methods data analysis tool*) software. These topics were later examined, and they provided insights.

2.5 Research Ethics

According to Descombe (2010), research ethics ensures that research participants are treated with dignity and respect and are not subjected to harm.

In this study, the participants are made known that this interview is completely voluntary, and informed consent (Appendix A) will be acquired from each participant to ensure that the purpose and scope of the research are apparent. Participants will also be informed that their personal information will be kept confidential. And also, letting participants know this research will not harm them or society. And to take and follow all the other principles of research ethics by Desncombe (2010, p.331-342).

According to Denscombe (2010, p331-342), this research will follow every fundamental principle of ethics, such that the participants are not misled in any way and that the scientific integrity is not compromised by guaranteeing that the “highest standards of professionalism” are kept. There were no legal hazards discovered.

3 Results

3.1 Data Collection and Analysis

The initial step as we have to identify the participants for the interview mentioned above. And these selections are made purely among people with some basic knowledge about data security in their smartphones. So the choice was made initially by asking my friends in DSV if they had ever experienced any data security situations in their smartphones or any IoT device if they had one. Furthermore, they were asked if any friends or relatives have faced the above situations. This interview consists of ten participants at the given time. The data taken from the participants consist of their full name, age, e-mail, and gender.

The next step is to forward the questionnaire in the form of Google Forms to some of the students in DSV via emails or text messages through the iLearn platform. There will be some describing answers which deal with the experience in data security, and some of them will be in the form of multiple choice questions regarding their opinion on data security in smartphones or IoT devices. And the data is collected in the form of spreadsheets from Google Spreadsheets in the .csv format. Later, they are visualized using the inbuilt MacO application Numbers. Numbers is an application in Apple devices that makes creating beautiful spreadsheets possible. Now check if the original data is present in the .csv and exported files into the application of the numbers. If the application made any mistake while converting the files. And download the responses from each participant.

After receiving the required amount of responses from participants, the responses are rechecked again if anyone has submitted the form multiple times, so this will reduce the purity of the research. Then these files are imported into MAXQDA(*All-in-one qualitative & mixed methods data analysis tool*) software, which is used for qualitative and quantitative data analysis. This research follows the Thematic analysis as Braun & Clarke (2006) suggest that a study can use the proposed six-phase approach to maintain the essential rigor in this thematic analysis process, after importing and defining the data into codes and variables depending upon the open-ended questions and closed-ended questions. The code includes demographic and issues faced by the participants. After this step, we will create themes related to our data on which part the participants have faced an issue, how they resolved it, and what measures they have taken.

The below passage from Participant 13 was coded as “hacking” and “social media”:

“The issue with the social media accounts and personal details being hacked.”

The below passage from Participant 6 was coded as “security”:

“Unknown persons might have access to homes and operate with hacking methodologies like code decryption etc.”

Then my data is grouped together as this study is a case study reporting on the experience of the thirteen participants. Figure 1 gives you an idea of how the reports from all the participants are grouped together.

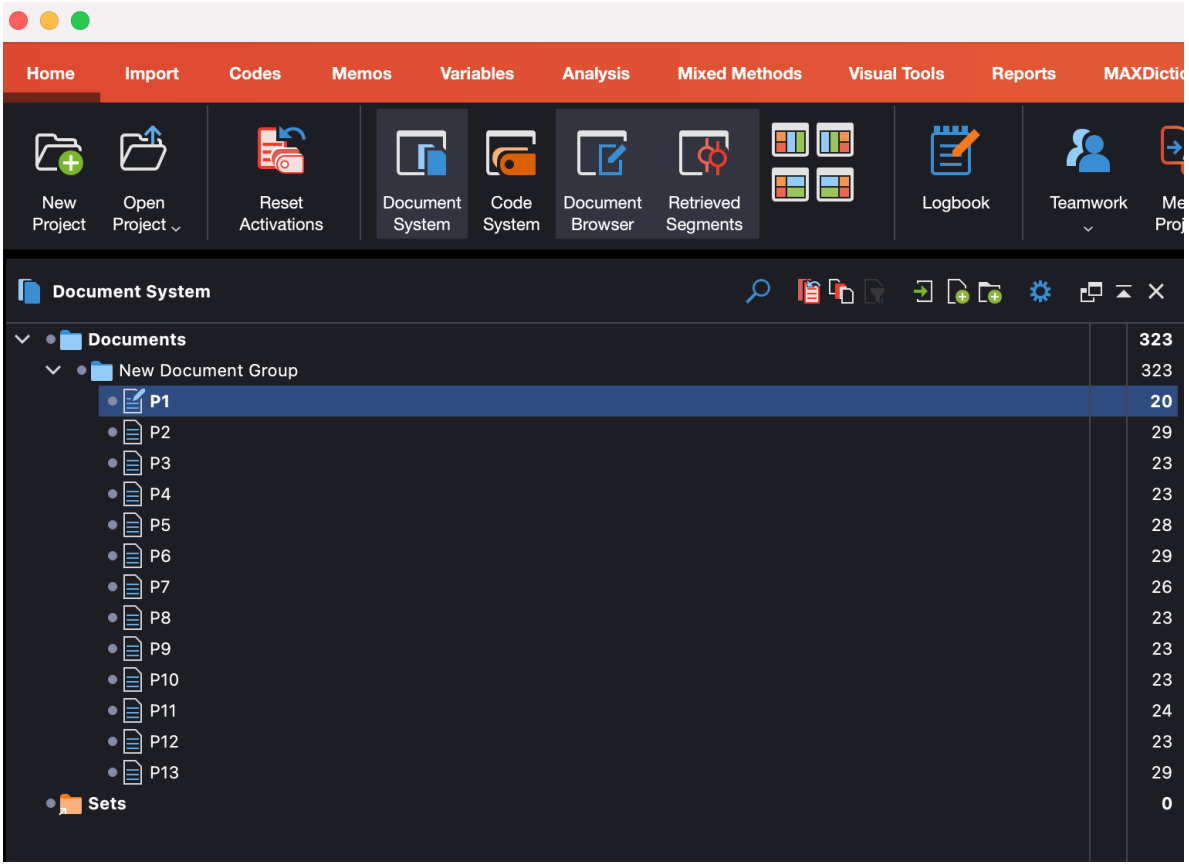

Figure 1. Grouped Data

After looking over the data and becoming acquainted with it, preliminary codes such as keywords were developed, and related to each code were classified. In several paragraphs, we classified under numerous codes (Appendix C gives you the full list and frequencies of themes, categories, and codes). Then after finding the codes that are in common and overlapping. Finally, after coding all the data into the appropriate four themes, they will provide the final analysis results. Figure 2 below shows how the total coding was fitted into the four main themes.

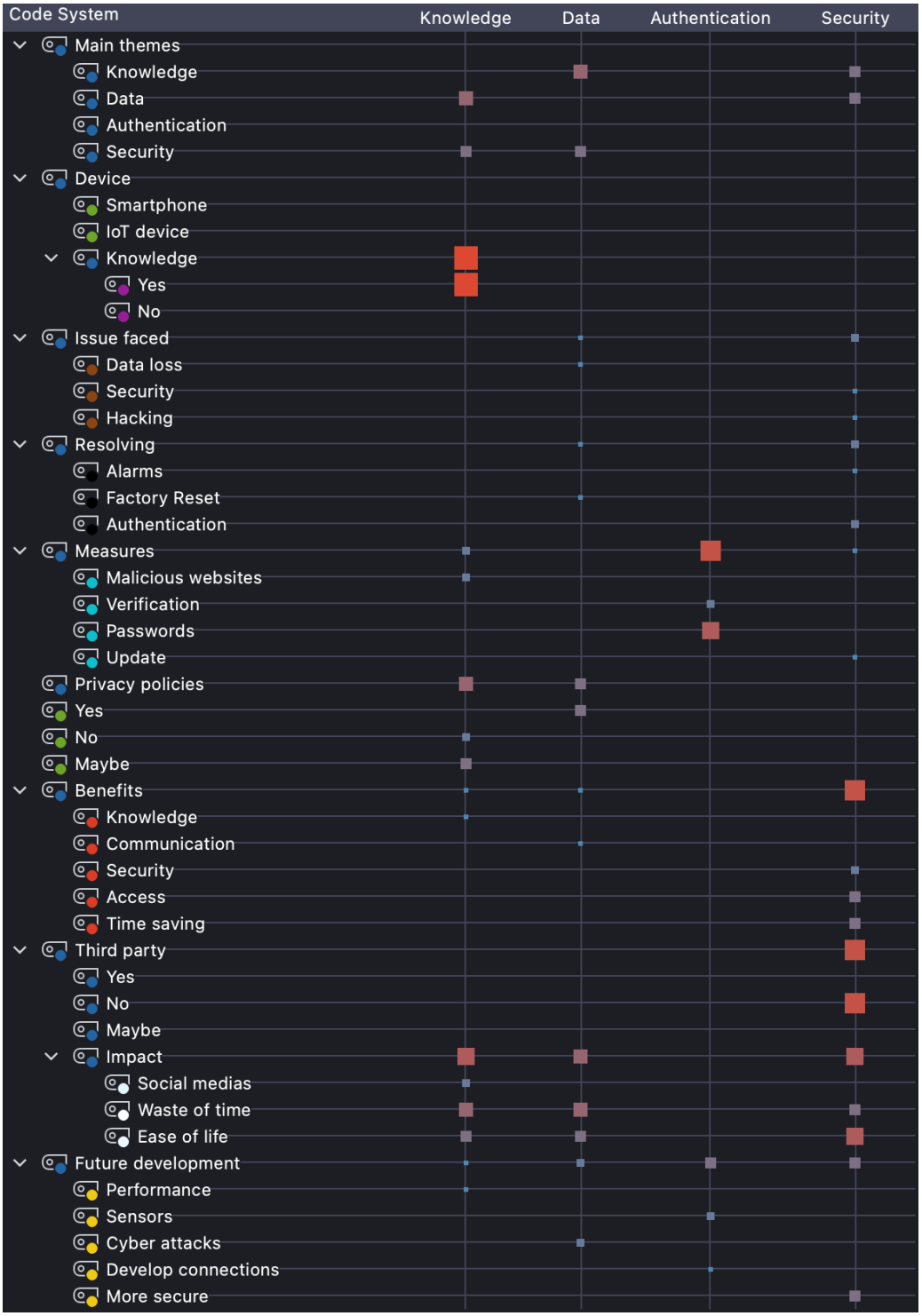

Figure 2. Code Relations

The document comparison chart, like the Code Relations Browser and Matrix, assisted me in reviewing my first codes by employing Braun & Clarke's (2006) guiding questions. The blue and green nodes describe the type of device the participant uses in this particular survey. Likewise, purple and yellow indicate that the participants have prior knowledge and don't know about data security and privacy, respectively.

Figure 3. Document Comparison Chart

3.2 Findings

The initial portion of the interview consisted of questions concerning the participants' demographics. As previously stated, the participants were chosen to represent a range of ages. The participants consist of five males and five females, and their age is between 21 to 25. As mentioned earlier, this survey takes place with the students only, so the age between the range. The number of participants having an IoT device and smartphone is one and nine, respectively. While reviewing the participants' responses, noticed that everyone has a piece of prior knowledge about IoT and how they have been explicitly explained about it. Everyone has given their opinion about the IoT and how they have learned much.

Moving on to the main topic of this survey, many participants have expressed that they have not faced any issues regarding the security and privacy of the data. Three participants out of ten have only faced issues, for example,

Participant 6 (P6): "*Yes, when I got an immediate call from my home, I just drove my bike a bit harshly and after I reached home after some time noticed that my smartphone is missing*"

(P7): "*The issue with the social media accounts and personal details being hacked.*"

(P10): "*Actually I forgot the passcode to unlock my smartphone, and even I tried it many times, and the smartphone even got timed out of chances to unlock it*"

Later on, focusing on how did these participants have resolved their issues and what measures even they have taken to avoid future problems from their previous experience. Even more broadly, ask them about some future extension from their view regarding any topic they want to express in an IoT device or a smartphone.

As this paper follow Thematic Analysis, the data identified four main themes: **Knowledge, Data, Authentication, and Security**.

Knowledge

As mentioned earlier, many people have expressed their views on IoT explicitly and how they have attained it:

(P1): *"Yes, IoT means Internet of Things, and lately I have studied this as a subject in my bachelors level of education."*

(P2): *"It stands for Internet of Things it was an interesting course, that I have taken it as a online*

course in Udemy."

(P3): *"Internet of Things, I dont have much knowledge on it but, I knew it was one of the course that I have completed in my bachelors degree."*

(P4): *"Yes, I have a good amount of knowledge about Internet of Things and how they connect many devices and exchange of data."*

(P6): *"Internet of Things, I have read it on an article and sometimes in some websites too."*

(P7): *"Yeah, its Internet of Things, and I have done a project on this topic too."*

(P8): *"Internet of Things."*

(P9): *"Internet of Things, I have done a course recently in my Master's degree."*

(P10): *"Internet of Things, yes I know about this course that I have done in my Bachelors."*

Even asking the participants a bit broadly about that do they have prior knowledge in terms of Data Privacy and Security, many of the participants mentioned that they had a piece of prior knowledge about it:

(P1): *"Yes, I do have some prior knowledge about it."*

(P2): *"Yeah, I do."*

(P3): *"Yes, I do."*

(P4): *"Yes, but kind of."*

(P5): *"Yes, I do have."*

(P6): *"No, but I have heard of it."*

(P7): *"Yes, I do have."*

(P8): *"Yes, but kind of."*

(P9): *"Yes, but kind of."*

(P10): *"Yes, I do have."*

Asking participants about they have even read the privacy policies of an IoT device or a smartphone before using it for the first time and have they faced any issues or have they understood them:

(P1): *"Yes, I have read it, but no, they are not easy to understand."*

(P2): *"Yes, I have read it, but maybe sometimes not so clear in someparts."*

(P3): *"Yes, I have read it, and they are easy to understand."*

(P4): *"Yes, I have read it, and they are easy to understand."*

(P5): "*Yes, I have read it, but no, they are not easy to understand."*

(P6): "*Yes, I have read it, and they are easy to understand."*

(P7): *"Yes, I have read it, but maybe sometimes not so clear in someparts."*

(P8): *"No, I have not read about them."*

(P9): *"Yes, I have read it, but maybe sometimes not so clear in someparts."*

(P10): *"Yes, I have read it, and they are easy to understand."*

Furthermore, I have noticed that some of the participants have prior knowledge of how measures to be taken to protect your IoT device or smartphone from security breaches or hacks:

(P6): *"Regularly changing passwords."*

(P7): *"Not clicking on unsecured websites or applications."*

(P8): *"Must use some strong passwords or pins."*

The above part shows that many people know what IoT is and what it means. We have seen how some participants know how to take measurements to protect their IoT device or smartphone from security breaches or hacks. From this, we can conclude that people are aware of IoT and how it works with the basic principles as maximum Participants have done their Bachelor's and Master's degrees in this field. Moreover, when asked whether they had prior knowledge of Data Privacy and Security, every participant mentioned that they had prior knowledge of it and concluded that each participant knew about Data Privacy and Security.

Data

The next theme identified is data and how people are aware of things inside the data; many questions fell under this theme:

The below response is from a participant to one of the questions in the questionnaire, how did you resolve the issue and the participant mentioned how he had resolved the issue and how had overcome the problem.

(P7): *"By maintaining proper standards like protecting or saving or capturing every moment data so that if anything happens, we will get to know immediately and by placing some detection alarms."*

Another participant responded to one of the questionnaire questions: What features would you like to see in future IoT or smartphones, and what would motivate you to adopt these devices? Then, the participants explained how the future could be from their perspective of thoughts.

(P4): *"To maintain the security of our devices and maintain data privacy."*

(P6): *"Enhanced security features related to the data in the devices."*

(P10): *"Any Iot device makes us lazy and provides us more flexibility while doing anything without letting us know any of the pain to gain that.*

Nevertheless, they have helped in a way big in hard times."

Another question adds to this theme: how often do you use data daily to communicate, exchange, or work on the data? Then the response from the participants is listed below.

(P1): *"I use data occasionally, for example, I might check weather data to plan a weekend trip or look up nutrition data when deciding what to eat. However, I don't rely heavily on data for daily communication or personal projects."*

(P2): *"Quite frequently in my personal life for communication and exchange information. I might use data to share photos with family and friends to collaborate on a project with a team. However, I don't*

typically use data."

(P3): *"It is like a fifty-fifty ratio that the usage of data in my daily life. However, when I do, it's usually for researching a topic of interest or fact-checking information I come across. I might also use data to make informed decisions about purchases or investments."*

(P4): *"I do not use much data daily. I prefer to rely on intuition and personal experience for decision-making. I might use data occasionally for my assignment works."*

(P5): *"I rely on data heavily in my personal life for a wide range of tasks, from tracking my fitness progress and monitoring my health. I also use it to manage my personal photography portfolio and analyze social engagement."*

(P6): *"I use data to track expenses, monitor the stock market, or to examine running times and distances."*

(P7): *"I mostly use data as in the form to store all the project work that I usually do in Google Drive in large spaces in order even to have a backup for my projects that I shoot on my camera for any kind of events."*

(P8): *"I use data in my personal life for a range of tasks, from managing my photographs and even to tracking my health data on my smartphone every day. I will check on it for sure."*

(P9): *"Data usage for me in my personal life for different kinds of tasks, including my fitness and to track it down how my progress is going on daily and also sleep patterns, and also looking on to tock market daily. And also, I used to do some food blogs in recent times, and I used much data to store them."*

(P10): *"I use data to track my running time and distances, and also analyzing wine tasting notes, or study trends in the music industry."*

As I noticed, many participants use vast amounts of data to satisfy their hobbies, and some track their health as they are concerned about it. Some participants are much into stock markets and some projects to deal with.

Authentication

The third theme was identified as Authentication. Per the participants' responses, there is much to code and deal with in the context. We will look at how the participants responded: One of the participants mentioned a response to one of the questions on how they resolved the issue.

P(10): *"Really, yes. I use an online banking service, and one day I received an email informing me that someone had attempted to enter into my account using a device I did not recognize. I was concerned that my account had been hacked or otherwise compromised, so I quickly went into my account settings to see if there was anything I could do to boost security. Thus, I enabled it because the online banking provider provided two-factor authentication. After registering my phone number and downloading the authentication app, I attempted to log in again. It was honestly rather easy. As I attempted to log in again, I was asked to input a verification number delivered to my phone via the authentication app. After entering the code, I was successfully connected to my account and could see no fraudulent transactions. Knowing that my online banking account was now safeguarded by two-factor authentication made me feel better and more secure. Because I always have my phone, utilizing the authentication app to obtain the verification codes was also quite straightforward. I am delighted I could swiftly and simply handle the issue with two-factor authentication."*

Moreover, the participants have avoided harming their data or sensitive smartphone information.

(P1): *"Well, one of the most important things is to ensure that all software and systems are updated with latest security patches. That means regularly checking for updates and ensuring they are installed*

immediately. Security patches are often released in response to new vulnerabilities that have been discovered in software or system. If these vulnerabilities are not addressed, attackers can exploit them to access sensitive information or to carry out other malicious activities."

(P2): *"I think there are a few important measures that individuals can take. Firstly, they should always use strong passwords for their online accounts. This means avoiding commonly used passwords and combining letters, numbers, and special characters. Using strong passwords in important because weak passwords can be easily guessed or cracked by hackers, giving them access to personal information or sensitive data. By using strong passwords, individuals can significantly reduce their risk of being hacked. Another important measure is regularly updating their devices with their latest security patches and software updates."*

(P6): *"One measure is to ensure that all online transactions are verified using a strong verification process. This means using methods like two-factor authentication, biometric authentication, or other strong verification methods to confirm the user's identity. It helps to prevent unauthorized access to sensitive information or financial transactions. By requiring users to verify their identity, it becomes much more difficult for attackers to impersonate and gain access to their accounts."*

Regarding the features, you would like to see in future IoT or smartphones, what would motivate you to adopt these devices?

(P2): *"One feature that I would like to see is better security measures built directly into the devices themselves. This could include things like secure boot processes, secure enclaves for sensitive data, and stronger encryption for data at rest and in transit. This would give me more confidence that my devices are secure, making it more difficult for attackers to compromise them."*

(P9): *"The stronger authentication must be implemented into the future, as in the form of biometrics and one-time-code sent to a separate device for logging in. This would make it much more difficult for attackers to gain access to devices, even if they manage to obtain the password."*

(P10): *"The feature that I would like to see in the future IoT or smartphones is more robust encryption for the data stores on the device. This would make it much more difficult for attackers to access my data if my device were lost or stolen. Another feature would be more granular control over the data shared with third-party apps and services. I would like to able to choose exactly what data is shared and with whom, rather than having to give blanket permissions to all apps."*

As per the participants, the above information can be used to improve the present situation and future development of this theme, mainly in increasing authentication.

Security

The fourth theme was identified to be Security.

Security, many of the participants mentioned that they had a piece of prior knowledge about it:

(P1): *"Yes, I do have some prior knowledge about it."*

(P2): *"Yeah, I do."*

(P3): *"Yes, I do."*

(P4): *"Yes, but kind of."*

(P5): *"Yes, I do have."*

(P6): *"No, but I have heard of it."*

(P7): *"Yes, I do have."*

(P8): *"Yes, but kind of."*

(P9): *"Yes, but kind of."*

(P10): *"Yes, I do have."*

As mentioned earlier, one participant has faced an issue regarding theme security:

(P10): *"The issue with the social media accounts and personal details being hacked."*

Furthermore, another person mentioned that they faced an issue:

(P6): *"Unkown persons might have access to home and operate with hacking"*

In another question, what benefits do you see from using any IoT device or smartphone, and participants have mentioned their benefits regarding the theme security.

(P4): *"I have some benefits regarding the security, as it protects my data."*

(P5): *"Security is the main benefit of my smartphone. It can prevent malware attacks, resulting in the theft of sensitive information on my device. A strong security system can detect and prevent malware from infecting my device."*

Another question that falls under the theme security is, have you ever used any third-party security apps on your IoT device or smartphone:

(P1): *"Maybe"*

(P2): *"Yes, I have installed."*

(P3): *"No, I have not installed it."*

(P4): *"No, I have not installed it."*

(P5): *"No, I have not installed it."*

(P6): *"No, I have not installed it."*

(P7): *"Yes, I have installed it."*

(P8): *"No, I have not installed it."*

(P9): *"No, I have not installed it."*

(P10): *"No, I have not installed it."*

Some participants have mentioned security as one of the measures for the future.

(P7): *"Security mechanisms need to be improved, and keeping the apps and devices always up to date. Nt encouraging third-party apps are always being priority"*

(P9): *"Security must be increased in all the fields like social media and banking accounts like to improve the security."*

As identified, many participants are also concerned about the security and privacy of their smartphones and IoT devices. As they exchange a large amount of data every day and also store the data, which is both related to work and personal life, a maximum number of participants are aware of data security and privacy and the issues caused, like data breaches and misusing the data. As many of the participants are aware of the issues, they haven't faced any issues regarding data security and privacy. On the other hand, some have experienced it, and they have overcome it by improving their

account security, like enabling two-factor authentication for login purposes. One of the participants mentioned that improving or creating strong passwords and regularly changing them can avoid data security and privacy issues. Another participant mentioned two-factor authentication, like biometrics and strong verification methods.

After analyzing each participant, the maximum number of participants are aware of data security and privacy, issues caused by them, what the initial steps have to be taken, and what measures to be taken in the future to avoid such issues.

4 Discussion

4.1 Analysis of the results

The purpose of this study was to investigate Data security and privacy in a smartphone or an IoT device. However, the analysis produced just one kind of positive result. This states that the participants are aware of the data security and privacy issues that are going on in smartphones and IoT devices. Moreover, they have some kind of solutions or backup plans regarding their sensitive data in their respective devices. This is quite a positive sign that people are aware of security breaches and issues caused by them.

This study aimed to investigate data security and privacy in a smartphone or an IoT device; thirteen participants were interviewed, and collected the required data in the form of surveys. Then, the data were analyzed using thematic analysis. Thematic analysis was carried out using MAXQDA(*All-in-one qualitative & mixed methods data analysis tool*) software. It allowed for a complete data assessment, classifying and combining the areas of interest, and creating common themes from the data. The study discovered regions where the participants had faced security and privacy issues, how they have overcome the problems, and what measures they have taken for the future.

The first theme, Knowledge, focused on whether the participants have some basic knowledge of security and privacy in smartphones or IoT devices. This also includes when the participants are asked the question, *"Have you ever read the privacy policies of your IoT device or smartphone?"* this also points out whether the participant is aware of the privacy policies of a particular device. After reviewing this question, I noticed that a maximum number of participants read the policies; on the other hand, some didn't. When the participants were asked, *"Have you ever changed the privacy settings of any apps on your IoT device or smartphone?"* some of the participants answered yes, and some of them answered no; while coming to the privacy setting of any application, must not be changed as of basic knowledge, I knew some of them are getting mislead for their needs. A few other questions are straightforward: *"Have you heard of IoT, and what does it stand for?"* and *"Do you have prior knowledge in the terms of Data privacy and security?"*, the responses from them are yes, they have heard about IoT and what does it stand for and what is Data privacy and security in terms.

The second theme, Data, focused on whether participants rely on data exchange in their day-to-day life with the question, *"How often do you use data daily to communicate, exchange, or work on the data?"* making analysis on this question, many of the people are dependent on the exchange of the data. Some participants exchange the data as part of their work purpose, some do it as their passion, and some store their files as a backup to access whenever they need to.

The third theme, Authentication, focused on where participants have faced an issue and resolved it. In the question, *"Have you ever faced any issues regarding the security in your IoT device or smartphone?"* after analyzing, there are very few participants who have faced issues regarding authentication. And when the participants asked, *"What features would you like to see in future IoT devices or smartphones, and what would motivate you to adopt these devices?"* they replied that terms of authentication must be increased and improved.

The fourth theme, Security, focused on how the participants have faced issues regarding security, and they want to see that security must be improved and, more new techniques must be brought up. After analyzing, participants are much more concerned about the level of security in their smartphone or IoT device, and they are aware of the issues caused by being so lenient with security.

All the above four themes identified are connected and address the study question: *Data security and privacy in a smartphone or IoT device?* The answer is that the measures regarding data security and data privacy must be improved in many of the fields, the means of increasing and implementing different types of authentication methods and securing sensitive data. Even more, creating awareness in people in terms of what is data security and privacy, their roles, and what measures they have to take before and even after the effect on their smartphone or an IoT device.

4.2 Future research

Further research is advised due to the limitations of this study. Due to time constraints, a small number of participants was chosen; nevertheless, a more extended study might give further insights into peoples' experiences and how they have solved the issue and eliminate participant selection bias.

Moreover, the participants were students and highly educated. Further analysis of the different age groups of people can also lead to future research of this study. As we go back to the '90s and '80s, people might not be much aware of data security and privacy, what its uses are, the advantages and disadvantages of having the data on a smartphone or an IoT device, and even what is an IoT device. The questionnaire, with some changes in the frame of security and privacy, can be implemented, which may lead to another dimension. As many cities are not much improved in terms of technology, furthermore research can also be considered another factor.

4.3 Conclusion

This study investigates the experience of people in Data security and privacy in a smartphone or IoT device. Four main themes were identified Knowledge, Data, Authentication, and Security. Some participants are aware of how to protect their data and what security measures to be taken in advance to secure their personal data, while others are not much aware of the security attacks and the measures to be adopted in advance. While the research focused on how they have handled a situation regarding data security and privacy, how they have resolved the issue, and what measures they have taken for the future in order to avoid security breaches and authentication. In addition, the features they would like to see in future IoT devices or smartphones.

References

All-in-one qualitative & mixed methods data analysis tool. *MAXQDA*. Available at: https://www.maxqda.com/ (Accessed: February 20, 2023).

Atzori, L., Iera, A. and Morabito, G., 2010. The internet of things: A survey. *Computer networks*, *54*(15), pp.2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010.

Belli, L., Cilfone, A., Davoli, L., Ferrari, G., Adorni, P., Di Nocera, F., Dall'Olio, A., Pellegrini, C., Mordacci, M. and Bertolotti, E., 2020. IoT-enabled smart sustainable cities: Challenges and approaches. *Smart Cities*, *3*(3), pp.1039-1071. https://doi.org/10.3390/smartcities3030052.

Braun, V. and Clarke, V. (2006) "Using thematic analysis in psychology," *Qualitative Research in Psychology*, 3(2), pp. 77–101. https://doi.org/10.1191/1478088706qp063oa.

Denscombe, M., 2010. *The good research guide: For small-scale social research projects 4th Edition* McGraw-Hill Education (UK).

Denscombe, M., 2014. *The Good Research Guide: For Small Scale Social Research Projects, 5th Edition*. [online] Open University Press.

Denscombe, M., 2017. *The good research guide: For small-scale social research projects, 6th Edition*. [online] McGraw-Hill Education (UK).

Ha, M.T. (2022) "Data collection using online questionnaires in marketing." Available at: https://doi.org/10.4135/9781529603569.

Jeremy, N. (2023) *Kevin Ashton invents the term "The internet of things," Kevin Ashton Invents the Term "The Internet of Things": History of Information*. Available at: https://www.historyofinformation.com/detail.php?entryid=3866 (Accessed: January 30, 2023).

Kamal, R., 2022. *Guide on IoT Data Collection*, *www.intuz.com*. Available at: https://www.intuz.com/blog/guide-on-iot-data-collection (Accessed: February 7, 2023).

Kaushal, A., 2016. *Role of information & communication technology (ict) in smart city.* Available at: http://www.newgensoft.com/blog/role-information-communication-technology-ict-smart-city/ (Accessed: February 2, 2023).

Nadikattu, A.K.R. (2018) *IOT and the issue of data privacy - media.neliti.com*, *IJIERT*. Available at: https://media.neliti.com/media/publications/429163-iot-and-the-issue-of-data-privacy-454f1eb8.pdf (Accessed: February 11, 2023).

Tawalbeh, L.A.A., Rafiq, A., Muthanna, A., Elgendy, I.A. and Abd El-Latif, A.A., 2021. Convergence of blockchain and IoT for secure transportation systems in smart cities. *Security and Communication Networks*, *2021*, pp.1-13. https://doi.org/10.1155/2021/5597679.

Appendix A Informed Consent Form

Data Security & Privacy in your Smartphone or IoT Device

You are cordially invited to participate in a research study on "The Integration of Internet Of Things (IoT) smart cities and their impact on urban life." This research is being carried out as part of the Department of Computer and Systems Science's Scientific Communication and Research Methods (FMVEK) course at Stockholm University. The study aims to acquire primary data from participants through a small-scale research initiative.

This web-based questionnaire is intended for educational reasons and should take between 12 -15 minutes to complete. The questionnaire includes questions about demographic information such as name, age, gender, and email address, as well as 23 questions with multiple choice, short answer, and long answer options. The respondent's responses will be kept anonymous and used for no other purpose than this research project.

By answering the questionnaire, you agree to participate in the study and to the following terms:

- You are over 18 years old and aware of the purpose of the study.
- You are an undergraduate or graduate student participating in this study.
- You understand that your answers to the questionnaire are reliable and can be used for research purposes.
- You are aware of the privacy of the personal information given for the study.
- You understand that you can only fill in this survey once.
- Your participation in this research study is voluntary, and you have the right to withdraw from the study at any time without any consequences. If you have any questions or concerns about the study, please do not hesitate to contact the researcher.

Thank you for your participation,
/ Lekhaz.Adapa(lead3201@student.su.se)

Appendix B Data Collection Protocols Used

Questionnaire

1. Name
2. E-mail
3. Age
4. Gender
5. What type of device are you referring to in your response?
6. Have you heard of IoT, and what does it stand for?
7. Do you have prior knowledge in the terms of Data Privacy and Security?
8. Have you ever faced any issues regarding the security in your IoT device or smartphone?
9. If you have answered “Yes” to your previous question, please describe your experience.
10. How did you resolve the issue on your IoT device or smartphone?
11. On a scale of 1 to 5, how concerned are you about the Security and Privacy of your IoT device or smartphone?
12. What measures do you take to protect your IoT device or smartphone from security breaches or hacks?
13. How often do you use data to communicate, exchange, or work on the data?
14. Have you ever read the privacy policies of your IoT device or smartphone?
15. If you answered “Yes” to the previous question, did you feel the privacy policy was clear and easy to understand?
16. How important to you that IoT devices and smartphones are designed with security and privacy in mind?
17. What benefits do you see from using an IoT device or smartphone?
18. Do you regularly update the software updates to address security vulnerabilities?
19. Have you ever used any third-party security apps on your IoT device or smartphone?
20. Have you ever changed the privacy settings of any apps on your IoT device or smartphone?
21. What features would you like to see in future IoT devices or smartphones, and what would motivate you to adopt these devices?
22. How has any IoT device or smartphone impacted your daily life, both positively and negatively?
23. Do you have any other concerns related to security and privacy on IoT devices or smartphones?

Appendix C Code System

Table 1. Code System

Code System	Frequency	Percentage	Percentage (valid)
Knowledge	13	100,00	100,00
Data	12	92,31	92,31
Authentication	10	76,92	76,92
Security	13	100,00	100,00
Device	13	100,00	100,00
Device\Smartphone	12	92,31	92,31
Device\IoT device	1	7,69	7,69
Knowledge	13	100,00	100,00
Knowledge\Yes	12	92,31	92,31
Knowledge\No	1	7,69	7,69
Issue faced	3	23,08	23,08
Issue faced\Data loss	1	7,69	7,69
Issue faced\Security	1	7,69	7,69
Issue faced\Hacking	1	7,69	7,69
Resolving	4	30,77	30,77
Resolving\Alarms	1	7,69	7,69
Resolving\Factory Reset	1	7,69	7,69
Resolving\Authentication	2	15,38	15,38
Measures	13	100,00	100,00
Measures\Malicious websites	2	15,38	15,38
Measures\Verification	2	15,38	15,38
Measures\Passwords	8	61,54	61,54
Measures\Update	1	7,69	7,69

Privacy policies	11	84,62	84,62
Privacy policies\Yes	5	38,46	38,46
Privacy policies\No	2	15,38	15,38
Privacy policies\Maybe	4	30,77	30,77
Benefits	13	100,00	100,00
Benefits\Knowledge	1	7,69	7,69
Benefits\Communication	1	7,69	7,69
Benefits\Security	2	15,38	15,38
Benefits\Access	5	38,46	38,46
Benefits\Time saving	4	30,77	30,77
Third party	13	100,00	100,00
Third party\Yes	2	15,38	15,38
Third party\No	10	76,92	76,92
Third party\Maybe	1	7,69	7,69
Impact	13	100,00	100,00
Impact\Social medias	3	23,08	23,08
Impact\Waste of time	6	46,15	46,15
Impact\Ease of life	8	61,54	61,54
Future development	13	100,00	100,00
Future development\Performance	1	7,69	7,69
Future development\Sensors	3	23,08	23,08
Future development\Cyber attacks	3	23,08	23,08
Future development\Develop connections	1	7,69	7,69
Future development\More secure	4	30,77	30,77
DOCUMENTS with code(s)	13	100,00	100,00
DOCUMENTS without code(s)	0	0,00	-
ANALYZED DOCUMENTS	13	100,00	-