

Title Page

sobota, 28 lutego 2026 12:04

Project Proposal

Innovation & Research

Module: ACCA5033 - Changemakers: Creativity and value creation

Student Name: Patryk Repetowski

Student ID: 2421737

Lecturer: Dr. Osman Elgawi

Submission Date: 5 March 2026

E-portfolio: <https://sites.google.com/view/patrykrepetowski/home>

Introduction

sobota, 28 lutego 2026 15:08

This project proposal explores innovation in the context of home security with a particular focus on Internet of Things (IoT) devices. The rapid growth of smart home technologies has significantly changed how individuals interact with technology in their daily lives. While these innovations improve convenience and connectivity, they also introduce new cybersecurity challenges.

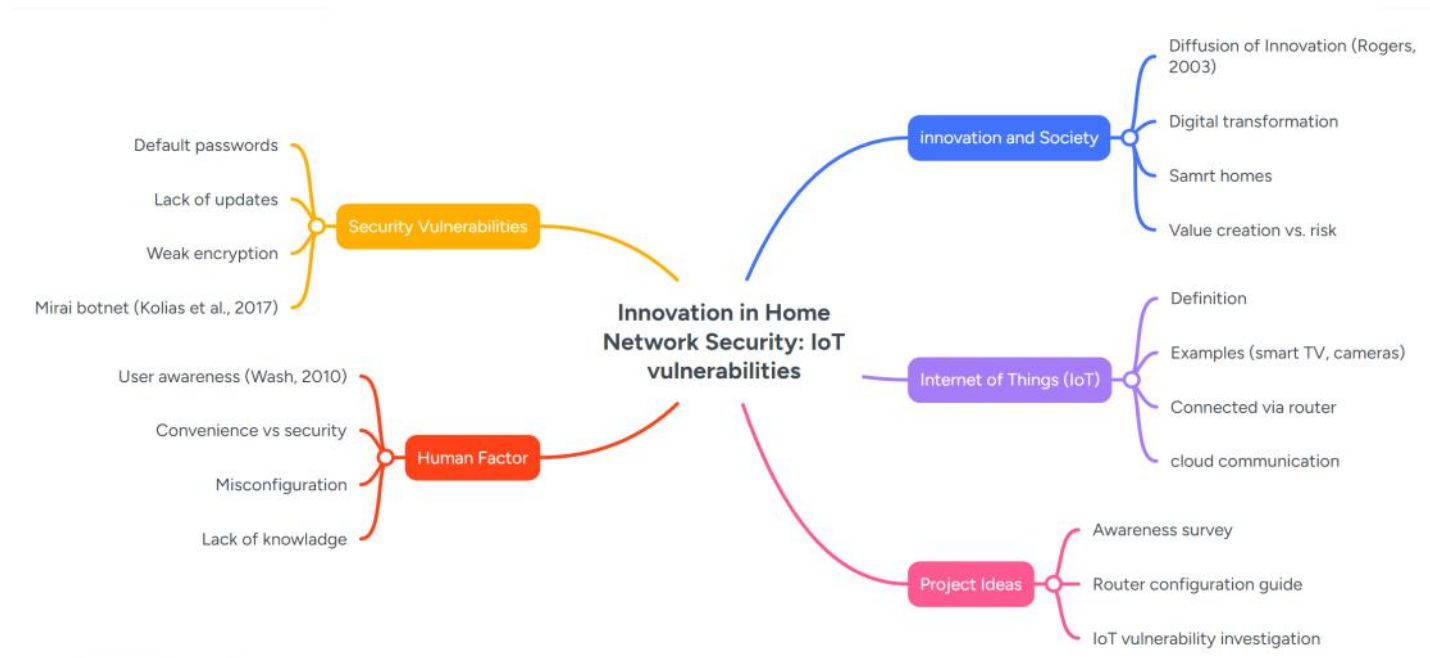
The purpose of this proposal is to investigate security vulnerabilities within home IoT networks and examine user awareness of associated risks. The project combines elements of networking, cybersecurity and human behaviour in order to understand how innovation can create both value and potential risk.

The following sections present the ideation process, research aims and objectives, and proposed research strategies.

Task 1

sobota, 28 lutego 2026 15:17

Q1. Create a mind map that includes some of the areas/ concept from Topic 1 and include some project ideas related to your programme of study.



The mind map of this project focused on innovation in home network security with particular attention given to Internet of Things (IoT) devices. Innovation plays a significant role in shaping modern society, especially through digital transformation and the increasing use of connected technologies. Innovation spreads gradually as individuals adopt new technologies at different stages (Rogers, 2003). The rapid growth of smart home devices represents a clear example of this process.

IoT devices such as smart televisions, security cameras, voice assistants and thermostats are now commonly connected to home networks. These devices provide convenience and efficiency, creating value for users in their daily lives. Porter and Heppelmann (2014) argue that smart and connected products are transforming how organisations and customers create and experience value. However, while connectivity increases convenience, it also introduces new cybersecurity challenges.

One key area identified in the mind map is security vulnerabilities. Many IoT devices are released with weak default passwords, limited encryption or poor update mechanisms. Reports from the European Union Agency for Cybersecurity (ENISA, 2020) also identify weak authentication mechanisms and poor device configuration as common security concerns in domestic IoT environments. Koliass et al. (2017) describe how insecure IoT devices were exploited during the Mirai botnet attack, leading to large-scale distributed denial-of-service (DDoS) attacks. This demonstrates how vulnerabilities in individual home networks can contribute to wider global cybersecurity issues.

Another important branch of the mind map focuses on the human factor. Research suggests that many users have limited understanding of cybersecurity risks and may not fully understand how to secure their devices (Wash, 2010). In many cases, convenience is prioritised over security, such as keeping default passwords or ignoring firmware updates. This highlights that IoT security is not only a technical issue but also a behavioural one.

During the ideation stage, several potential project ideas were considered. These included developing a practical home router configuration guide, creating a cybersecurity awareness framework for students and investigating common vulnerabilities in domestic IoT environments. Each idea reflects the connection between innovation, networking and value creation, while also addressing the risks associated with technological development.

Q2. Select a project idea that you would like to take forward and add this to the map.

From the ideas identified during the ideation process, the selected project focuses on investigating security vulnerabilities

in home IoT networks and examining user awareness of associated cybersecurity risks. This topic was chosen because it relates directly to networking and cybersecurity within the Computing discipline, while also addressing a growing challenge in modern digital environments.

The adoption of IoT technologies has increased significantly in recent years. According to Rogers (2003), innovation spreads gradually through society and smart home devices are now becoming more common in everyday households. While these technologies create value by improving convenience and connectivity, they also introduce new risks that many users may not fully understand. Porter and Heppelmann (2014) explain that smart products generate value through connectivity but this connectivity can also increase security exposure within networks.

Research suggests that user behavior plays an important role in cybersecurity outcomes, as many individuals lack awareness of threats or fail to follow basic security practices (Wash, 2010). For this reason the project will examine both technical vulnerabilities and user awareness, recognising that improving security requires attention to both technological and behavioural factors.

The selected idea has been clearly highlighted in the mind map as the main direction for further research.

Task 2

poniedziałek, 2 marca 2026 11:36

Aim, Objectives and Research Area

Q1. Create and document a single Aim and several Objectives for your project.

Aim:

The aim of this project is to investigate common security vulnerabilities in home Internet of Things (IoT) networks and examine user awareness of associated cybersecurity risks.

Objectives:

To achieve this aim, the following objectives have been identified:

1. To review academic and industry literature related to IoT security and home network vulnerabilities.
2. To identify common technical weaknesses found in IoT devices and domestic router configurations.
3. To explore user awareness and behaviour in relation to IoT security practices.
4. To collect primary data through a small-scale online survey.
5. To provide practical recommendations for improving home network security.

These objectives combine both technical and behavioural aspects of networking. Research suggests that IoT vulnerabilities are often linked to weak authentication mechanisms, outdated firmware and poor device configuration (Kolias et al., 2017). At the same time, user behaviour significantly influences cybersecurity outcomes, as individuals may not fully understand the risks associated with connected devices (Wash, 2010). Therefore, this project aims to examine both dimensions in order to develop a balanced understanding of the issue.

Q2. Identify an appropriate research philosophy for your project.

For this project, a pragmatic research philosophy is considered the most suitable approach.

Pragmatism focuses on practical solutions to real-world problems and allows researchers to combine different research methods where appropriate. Since this project investigates both technical vulnerabilities (which can be observed and measured) and user awareness (which is based on personal perceptions and experiences), a flexible approach is required.

Unlike positivism, which mainly focuses on objective and measurable data or interpretivism, which concentrates on subjective understanding, pragmatism allows the integration of both perspectives. This supports the mixed-method design of the project, combining literature review with primary survey data.

A pragmatic approach is appropriate because the overall aim of this project is not only to understand IoT security risks but also to propose practical recommendations that could improve home network security in real-life environments.

Q3. Select and document appropriate search tools including some specific research databases.

In order to support this research, several academic search tools and databases will be used.

Google Scholar will be used as a primary search engine due to its accessibility and wide coverage of peer-reviewed journal articles, conference papers and academic books. It is particularly useful for identifying foundational research related to innovation and cybersecurity, such as Rogers (2003) and Wash (2010).

IEEE Xplore will also be used because it provides access to technical research in networking and cybersecurity. For example, Kolias et al. (2017) discuss IoT botnet vulnerabilities in detail, which directly supports the technical focus of this project.

In addition, industry and governmental reports, such as those published by ENISA (2020), will be consulted to provide up-to-date information about IoT security risks and recommended practices. These sources help to balance academic theory with practical industry perspectives.

Search strategies will include the use of keywords such as:

- "IoT security vulnerabilities"
- "home network security risks"
- "default passwords IoT"
- "user awareness cybersecurity"
- "smart home device security"

Boolean operators such as AND and OR will be used to refine search results. For example:

- "IoT security" AND "home network"
- "IoT vulnerabilities" OR "smart device security"

Using multiple databases and structured search strategies helps ensure that the literature review is comprehensive and relevant to the research aim.

Task 3

wtorek, 3 marca 2026 09:37

Research strategies

Q1. Consider and document strategies to enhance validity, reliability, generalisability and ethical considerations.

To ensure the quality of this research, several strategies will be implemented to enhance validity and reliability. In this project, validity will be strengthened by aligning survey questions closely with the research aim and objectives. Questions will focus specifically on IoT device usage, password practices, update behaviour and network configuration awareness. The design of survey questions will also be informed by existing literature on IoT vulnerabilities and user behaviour (Kolias et al., 2017; Wash, 2010), ensuring that relevant security issues are addressed.

Reliability relates to the consistency of research results. To enhance reliability the survey will primarily use structured questions, including multiple-choice and Likert-scale questions. Clear and simple wording will be used to reduce ambiguity. In addition, conducting a pilot survey before full distribution will help identify unclear or misleading questions, further improving consistency.

Generalisability may be limited due to the relatively small sample size and the focus on students as participants. However, the purpose of this study is exploratory rather than predictive. While findings may not represent the entire population, they can provide useful insight into common behaviours within a defined group.

Ethical considerations are particularly important when collecting primary data. The survey will be anonymous and no personal identifying information will be collected. Participants will receive a short information statement explaining the purpose of the research and confirming that participation is voluntary. Data will be stored securely and used solely for academic purposes.

Q2. Select research strategies/ data collection methods and design a pilot method.

This project will adopt a mixed-method research strategy, combining a literature review with primary data collection.

The literature review will provide a theoretical understanding of IoT security risks and user behaviour. Primary data will be collected through an online survey distributed to students. The survey method is appropriate because it allows data to be gathered efficiently and supports both quantitative and qualitative responses.

A purposive sampling approach will be used, targeting students who are likely to use multiple connected devices in shared or private accommodation. While this sampling strategy may limit generalisability, it ensures relevance to the research topic.

The survey will include:

- Multiple-choice questions (e.g. "Do you change default passwords on smart devices?")
- Likert scale questions (e.g. "I feel confident in securing my home network".)
- One or two open-ended questions (e.g. "What security measures do you use at home?")

A pilot survey will be conducted with 3-5 participants prior to full distribution. The purpose of the pilot is to test clarity, structure and timing. Feedback from pilot participants may lead to rewording technical terms or adjusting response options. Evidence of the pilot process will be included in the Appendix.

Q3. Outline some different types of quantitative and qualitative analysis.

Quantitative analysis will be used to examine structured survey responses. This may include calculating percentages, identifying patterns and comparing levels of awareness among participants. For example, the percentage of participants who change default passwords or update device firmware regularly can be calculated and presented using simple charts.

Qualitative analysis will be applied to open-ended responses. A basic thematic analysis approach will be used to identify recurring themes, such as low awareness, prioritisation of convenience or misunderstanding of technical terms. Responses will be reviewed and grouped into categories to highlight common behavioural trends.

By combining quantitative and qualitative analysis the research can provide both measurable trends and deeper insight into the reasons behind user behaviour. This mixed analytical approach supports a more balanced understanding of IoT security challenges in domestic environments.

Conclusion

wtorek, 3 marca 2026 10:48

This project proposal has explored innovation in the context of home network security with particular focus on Internet of Things (IoT) devices. The rapid growth of smart home technologies demonstrates how innovation can significantly improve convenience, automation and connectivity in everyday life. However, as discussed throughout this proposal increased connectivity also introduces new cybersecurity risks that many users may not fully understand.

The project aims to investigate both the technical vulnerabilities present in home IoT networks and the level of user awareness regarding these risks. By combining literature review with primary data collection the research intends to provide a balanced understanding of how innovation can create both value and potential security challenges. The integration of technical and behavioural perspectives reflects the complexity of modern networking environments.

The proposed mixed-method approach allows for practical insights that may contribute to improving home network security practices. Although the research may be limited by sample size, it is expected to provide meaningful findings within the chosen participant group.

Overall, this proposal demonstrates the importance of addressing cybersecurity concerns alongside technological development. Understanding IoT security not only supports academic research in networking but also contributes to practical awareness that is increasingly relevant in today's digital society.

Appendix A - Pilot Survey Instrument

Survey title:

Home IoT Security Awareness Survey

Section 1 - Device usage

1. Do you use any smart home devices (e.g. smart TV, camera, voice assistant)?
 - Yes
 - No
2. How many IoT devices are connected to your home network?
 - 1-2
 - 3-5
 - More than 5
 - Not sure

Section 2 - Security practices

1. Do you change default passwords on your smart devices?
 - Yes
 - No
 - Not sure
2. How often do you update your smart devices?
 - Regularly
 - Occasionally
 - Rarely
 - Never
 - Not sure
3. I feel confident in securing my home network.
 - Strongly agree
 - Agree
 - Neutral
 - Disagree
 - Strongly disagree

Section 3 - Open response

1. What steps do you take to improve the security of your home network?

Appendix B - Pilot survey summary

A pilot version of the survey was conducted with three participants. The purpose of the pilot was to test clarity, structure and timing.

Feedback received included:

- One participant suggested simplifying technical terms such as "firmware updates".
- One participant recommended adding a "Not sure" option to certain questions.
- All participants confirmed that the survey took less than five minutes to complete.

Based on this feedback, minor wording adjustments were made and additional response options were included to improve clarity.

Reference List

poniedziałek, 2 marca 2026 11:35

Rogers, E.M. (2003) *Diffusion of Innovations*. 5th edn. New York: Free Press.

Porter, M.E. and Heppelmann, J.E. (2014) 'How Smart, Connected Products Are Transforming Competition', *Harvard Business Review*, 92(11), pp. 64–88.

Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J. (2017) 'DDoS in the IoT: Mirai and Other Botnets', *Computer*, 50(7), pp. 80–84.

Wash, R. (2010) 'Folk Models of Home Computer Security', *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*.

ENISA (2020) *Guidelines for Securing the Internet of Things*. European Union Agency for Cybersecurity.