Research Project 2021

Merel Steenbergen[1] , **Martijn de Vos**[1] , **Johan Pouwelse**[1]
[1]TU Delft
M.A.Steenbergen@student.tudelft.nl, {SUPERVISOR1, SUPERVISOR2}@tudelft.nl

Abstract

The abstract should be short and give the overall idea: what is the background, the research questions, what is contribution, and what are the main conclusions. It should be readable as a stand-alone text (preferably no references to the paper or outside literature).

1 Introduction

When the World Wide Web was introduced in 1990, users identified themselves with usernames and passwords, creating a new account for every service. Even though Single Sign-On has reduced the amount of passwords per user, passwords are still a major security risk. In 2017, the password manager LastPass analysed the data of employees of over 30.000 companies using the service and found that the average amount of accounts per employee is 191 [1]. This is because identity storage is still centralized. If one wants to login at a service, the username and password are stored in a database owned by the service.

This approach has many disadvantages. The first being that the service has control over the users data. As an example, the terms of service of Instagram state the following[1]: "We reserve the right to modify or terminate the Service or your access to the Service for any reason, without notice, at any time, and without liability to you". [2] clearly explains the impact that this might have on end users. "Because the only online identities most people have are centralised, the removal or deletion of an account effectively erases a person's online identity which they may have spent years cultivating and may be of significant value to them, and impossible to replace."

In addition, these data duplicates ensure that the estimated total cost of identity assurance in the UK exceeds 3.3 billion pounds. CTRL-Shift has estimated that using 'make once, use many times' strategies could reduce this to 150 million pounds [3].

Self-sovereign identity aims to solve the problem by providing users with complete control over their data. This is achieved with decentralized data management, such as blockchain. The TrustChain SuperApp is a mobile application under development by the BlockChain Lab of the TU Delft. It aims to create a digital foundational identity. However, it currently lacks the ability to transfer data to other applications. This is an essential aspect of SSI to ensure third parties, like the government, can request data from a user.

This research will focus on creating a workflow for transferring data to confirm the identity of a user. A possible use case for this is buying alcohol online. The SuperApp could be used to confirm that the buyer is actually of legal drinking age. *This section isn't done, but I have some questions that I want to ask first.*

Here will be a paragraph stating which sections will discuss which topics, but I don't want to change that too often, so I'll leave that for a later day.

2 The Sixth Principle (Problem Description)

To define Self-Sovereign Identity, often the ten principles that were devised by Christopher Allen are used. The sixth of which is Data Portability: "Information and services about identity must be transportable" [4, p. 14].

This is where my writing ends and the template begins

3 Your contribution

In computer science typically the third section contains an exposition of the main ideas, for example the development of a theory, the analysis of the problem (some proofs), a new algorithm, and potentially some theoretical analysis of the properties of the algorithm.

Do not forget to give this section another name, for example after the method or idea you are presenting.

Some more detailed suggestions for typical types of contributions in computer science are described in the following subsections.

Experimental work

In this case, this section will mostly contain a description of the methods/algorithms you will be comparing. Although not all methods need to be described in detail (providing appropriate references are available), make sure that you reveal sufficient details to a reader not familiar with these methods to: a) obtain a high-level understanding of the method and differences between them, and b) understand your explanation of the results.

[1]Instagram's terms of service 2021

Improvement of an idea

In this case, you would need to explain in detail how the improvement works. If it is based on some observation that can be proven, this is a good place to provide that proof (e.g., of the correctness of your approach).

4 Experimental Setup and Results

As discussed earlier, in many sciences the methodology is explained in section 2 and this section only discusses the results. However, in computer science, most often the details of the evaluation setup are described here first (simulation environment, etc.). Very important here is that any skilled reader would be able to reproduce this setup and then obtain the same results.

Do we include the tools used here? E.g. Android Studio

Then, results are reported in an accessible manner through figures (preferably with captions that allow them to be understood without going through the whole text), observations are made that clearly follow from the presented results. Conclusions are drawn that follow logically from the previous material. Sometimes the conclusions are in fact hypotheses, which in turn may give rise to new experiments to be validated.

You may want to give this section another name.

5 Responsible Research

Reflect on the ethical aspects of your research and discuss the reproducibility of your methods.

6 Discussion

Results can be compared to known results and placed in a broader context. Provide a reflection on what has been concluded and how this was done. Then give a further possible explanation of results.

You may give this section another name, or merge it with the one before or the one hereafter.

7 Conclusions and Future Work

Summarize the research question(s) and the answers to the research question(s). Make statements. Highlight interesting elements.

Discuss open issues, possible improvements, and new questions that arise from this work; formulate recommendations for further research.

ideally, this section can stand on its own: it should be readable without having read the earlier sections.

References

[1] LastPass Enterprise, "The password exposé. 8 truths about the threats - and opportunities – of employee passwords," tech. rep., LastPass, 2017.

[2] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," March 2017.

[3] A. Mitchell and J. Smith, "Economics of identity. the size and potential of the uk market for identity assurance," tech. rep., October 2015.

[4] K. Wagner, B. Némethi, E. Renieris, P. Lang, E. Brunet, and E. Holst, "Self-sovereign identity: A position paper on blockchain enabled identity and the road ahead.," pp. 13–14, October 2018.

A The obvious

A.1 Reference use

- all ideas, fragments, figures and data that have been quoted from other work have correct references
- literal quotations have quotation marks and page numbers
- paraphrases are not too close to the original
- the references and bibliography meet the requirements
- every reference in the text corresponds to an item in the bibliography and vice versa

A.2 Structure

Paragraphs

- are well-constructed
- are not too long: each paragraph discusses one topic
- start with clear topic sentences
- are divided into a clear paragraph structure
- there is a clear line of argumentation from research question to conclusions
- scientific literature is reviewed critically

A.3 Style

- correct use of English: understandable, no spelling errors, acceptable grammar, no lexical mistakes
- the style used is objective
- clarity: sentences are not too complicated (not too long), there is no ambiguity
- attractiveness: sentence length is varied, active voice and passive voice are mixed

A.4 Tables and figures

- all have a number and a caption
- all are referred to at least once in the text
- if copied, they contain a reference
- can be interpreted on their own (e.g. by means of a legend)