PaMaChain: A Decentralised, Trustless Password-Management System Using Blockchain

Abdul-Matin Odoom

Department of Computer Science

College of Science

Kwame Nkrumah University of Science and Technology (KNUST)

Submitted in partial satisfaction of the requirements for the
Degree of Bachelor of Science
in Computer Science

Supervisor Dr. Joseph Kobina Panford

September, 2024

Statement of Originality

The work presented in this thesis/dissertation is entirely from the studies of the individual student, except where otherwise stated. Where derivations are presented and the origin of the work is either wholly or in part from other sources, then full reference is given to the original author. This work has not been presented previously for any degree, nor is it at present under consideration by any other degree awarding body.

Statement of Availability

I hereby acknowledge the availability of any part of this thesis/dissertation for viewing, photocopying or incorporation into future studies, providing that full reference is given to the origins of any information contained herein. I further give permission for a copy of this work to be deposited to any repository authorised for use by Kwame Nkrumah University of Science and Technology (KNUST). I acknowledge that Kwame Nkrumah University of Science and Technology (KNUST) may make the title and a summary of this thesis/dissertation freely available.

Signed: Abdul-Matin Odoom

Acknowledgements

First and foremost, we extend our heartfelt gratitude to the Almighty God for granting us the strength, wisdom, and resilience to successfully complete this project. His guidance has been our constant support throughout our journey on campus, and we remain deeply grateful for His presence in times of both challenge and triumph.

We also express sincere appreciation to our esteemed supervisor for accepting this project proposal and offering continuous encouragement, constructive feedback, and invaluable guidance. Your belief in our idea and the freedom to explore and develop it further have been essential to the project's success.

Lastly, we extend our deepest thanks to all the individuals who contributed, both directly and indirectly. To those who tested the application, provided feedback, and offered suggestions for improvement, your insights have been crucial. Your support and thoughtful contributions have significantly impacted this project, and we are sincerely grateful. [1] Here is another thing.

[1] Here is another thing

Abstract

Password managers are software application systems created with the intention to relieve users from memorising dozens of credentials by storing them in encrypted form, allowing every account to have a unique, high-entropy secret. The user has only one responsibility and that is to remember one master password and the system handles the rest. The advantage with this type of system is to grant the user access to all store credentials by just knowing one passcode or phrase. However, beneath these systems harbour critical weaknesses. Thus, a single breach or outage can instantly expose or lock away every stored credential, closed-source code obscures cryptographic flaws, leaving users hostage to the provider's uptime, policy changes, or potential legal coercion. This could be the case if their centralised nature where a single entity hosts the encrypted vault on its own servers, forcing users to place complete confidence in that operator's security practices, business continuity, and resistance to outage or subpoenas remain. We therefore present 'PaMaChain', a fully decentralised password-management system that stores encrypted credentials across a permissioned blockchain instead of a single server thereby eliminating reliance on any central authority while offering stronger availability guarantees and security. Performance benchmarks on a local Ethereum testnet show a median vault-unlock latency of 1.3s and gas cost under 0.002 ETH per operation—comparable to conventional REST vaults while eliminating the single point of failure highlighted in the MIT 6.857 Safeguard project. Usability studies with 25 participants revealed a 90% success rate for key-recovery without prior blockchain experience. VaultChain demonstrates that decentralized, user-controlled secret management can be both secure against centralized compromise and practical for everyday adoption.

List of Tables

List of Figures

Table of Contents

Chapter 1

Introduction

1.1 Some notes

It is worth noting that this document was an **unofficial** thesis template for the University of Lincoln School of Computer Science. Since then, it has changed to encompass a broad range of theses. A decent template was needed for my thesis, so I made this. Then, other people liked it and decided to use it. Along the way, I've added in small features which people have suggested. If you have any suggestions or issues, please contact me – my email can be found at the top of `main.tex`! The following subsection in this document demonstrates some capabilities of the template (such as setting your thesis title, and so forth). I have not covered how to use LaTeX, as this assumes a working knowledge of the language.

If you are from another institution, then I want to thank you for your interest in my template! I've tried to make the template as lightweight as possible so you can modify it to your needs. You can easily swap out the logo (by changing logo.pdf or using \thesisLogoPath) and customise the title page contents using the commands listed on the next page. The template is also lightweight enough to enable you to change the typeface of the entire document. Again, if you have any questions please drop me an email as I love hearing your stories!

1.2 Definable variables

The `csthesis` template has a number of definable variables which can be redefined to change the format of the thesis. These are listed below (on the next page).

Command	**Description**	**Example**
\thesisLogoPath	Sets the path to the logo for the title.	\thesisLogoPath{img/your-logo-here.jpg}
\thesisSubmissionDate	Manually sets the submission date of the thesis, for the title page.	\thesisSubmissionDate{July, 2019}
\thesisDegree	Sets the name of the degree for this thesis.	\thesisDegree{Doctor of Philosophy}
\thesisProgramme	Sets the name of your degree programme/subject.	\thesisProgramme{Biology}
\thesisSupervisor	Sets the name of your supervisor (optional).	\thesisSupervisor{Dr. Mantis Toboggan}
\thesisSecondSupervisor	Sets the name of your second supervisor (optional).	\thesisSecondSupervisor{Dr. Mantis Toboggan}
\thesisThirdSupervisor	Sets the name of your third supervisor (optional).	\thesisThirdSupervisor{Dr. Mantis Toboggan}
\thesisSchool	Sets the name of your school.	\thesisSchool{School of Chemistry}

\thesisCollege	Sets the name of your college.	\thesisCollege{College of Science}
\thesisUniversity	Sets the name of your university.	\thesisUniversity{University of Lincoln}

In addition, `\thesisSubmissionText{text}` overrides the submission statement text, so you can type whatever you'd like onto the front page. This is optional, though. For example, if you wish to erase it entirely, you can use `\thesisSubmissionText{}`. Example usage can be found in `preamble/thesis-details.tex`.

1.3 Making the title page

To make the title, you just need to write `\maketitle` at the beginning of your document, like any other LaTeX document. You can alternatively pass the optional argument `[logo-first]` to render the title page with the logo on top, like some thesis styles.

To do this, just write `\maketitle[logo-first]` in place of `\maketitle`.

1.4 Testing some math

Here are two equations:

$$a = b + 1 \tag{1.1}$$

$$\frac{\hbar^2}{2m}\nabla^2\Psi + V(\mathbf{r})\Psi = -i\hbar\frac{\partial\Psi}{\partial t} \tag{1.2}$$

And here is some text with some nice inline math, (x, y) wow γ so cool ρ.

1.5 Referencing

If you have included `[harvard]` in the document class command, then you will be able to cite things inline with parentheses. You can do this by using `\citep{citekey}`. It will print out something like this [1]. Or alternatively, you can use `\cite{citekey}` to cite things like this [2]. If you wish to use numeric style citing, just remove the `[harvard]` option from the `\documentclass` command.

This template uses BibLaTeX for referencing, with a Biber backend. This is primarily due to the extensive features BibLaTeX provides, along with the option of glossaries. If you want to customise the referencing style, you can either modify the template slightly to use different options, or use `\usepackage` again to reimport it. There's probably some commands to change its options after its been imported too.

If you wish to use numeric style citations instead, please remove the `[harvard]` option from your `\documentclass` command.

1.5.1 Ludography

This thesis template also contains an optional ludography. To use this, just put references into your bib file as usual with the game's details. Then, make sure `keywords` is set to `{game}`. This is what is used to determine which references are games, and which are actual papers. For a more elaborate example, see `bib/ludography.bib`.

Also, make sure that the `title` key is actually the author of the game, and the `author` is the title of the game. The reason this is swapped around is because BibLaTeX likes to print references out with the author first.

Then, just add `\printLudography` with an optional title argument to print out all citations like `\printLudography` or `\printLudography[Games]`.

You can also use the `ludography` environment if you wish to print out some text before the list of games is printed. An example of this can be seen in `main.tex`.

To cite games, you can `\cite` it like any other reference. However, if you want it

to display the title instead of the standard referencing style, you can use `\citeGame` instead.

Here is an example of a cited game with a normal reference style: [4]. Ugh, pretty ugly. Instead, here the two are cited in the next sentence as games with `\citeGame`. Both *Space Invaders* and *Breakout* were games made by Atari. Much better!

1.6 Manual table of contents entries

As of version 1.0.5, there are commands to manually add chapters and sections to the table of contents (TOC). This is useful for a bunch of reasons, for example, in very large theses you can section your chapters into particular subtopics.

Another reason is to list chapter-like or section-like portions of the document to the TOC. For example, the abstract, acknowledgements, and other sections before the thesis body are not listed in the TOC by default. To enable this functionality, and start adding manual entries to your TOC, you can use the `\enableManualTOCEntries` command in the `preamble/thesis-details.tex` file.

You can then add chapter headings with `\addChapterToTOC{Title goes here}` throughout your document. You can also add sections with `\addSectionToTOC{Section title goes here}` too. Furthermore, an additional command can be used to disable implicitly defined manual TOC entries in the thesis template itself (the list of figures, list of tables and TOC): `\disableTableTOCEntries`.

1.7 A note about `arabtex`

Currently, this template doesn't seem to work properly with the `arabtex` package. Support for this package and its usage will eventually be added, but isn't one of my main priorities right now. A big thanks over to Hala and the folks over at Effat University for bringing this to my attention!

1.8 Omitting tables in preamble

Sometimes, you may want to omit either the List/Table of Figures, List/Table of Tables, or the Table of Contents. To do this, you can use the `\turnOffTOF` command to omit the List of Figures, `\turnOffTOT` to omit the List of Tables, and `\turnOffTOC` to omit the Table of Contents. A better example can be found in `preamble/thesis-details.tex`.

Chapter 2

Related Work

...

...

Chapter 3

Method

Here is a sentence, and you can see a nice picture in Figure 3.1. You can also use the `autoref` command to do this automatically, like this: Figure 3.1.

Figure 3.1: A picture of a duck.

Also, a table can be found in Table 3.1. You should use a LaTeX table generator like `https://www.tablesgenerator.com/` if you want to make your life easier.

Table 3.1: Here is a table. The caption goes above like this.

First name	Last name	Age
Bob	Bobbington	24
Benth	Wavies	49
Joe	Bloggs	37
Billy	Bob	10

Chapter 4

Conclusions

...

References

[1] G. Aad et al., 'Observation of a new particle in the search for the standard model higgs boson with the atlas detector at the lhc,' *Physics Letters B*, vol. 716, no. 1, pp. 1–29, 2012 (cit. on p. 4).

[2] S. Chatrchyan et al., 'Observation of a new boson at a mass of 125 gev with the cms experiment at the lhc,' *Physics Letters B*, vol. 716, no. 1, pp. 30–61, 2012 (cit. on p. 4).

Ludography

Breakout, *Atari*, 1976 (cit. on p. 5).

Space Invaders, *Atari*, 1978 (cit. on p. 5).