

f

by Daniels Zelinskis

Submission date: 20-Oct-2023 03:00PM (UTC+0100)

Submission ID: 213780268

File name: 32700_Daniels_Zelinskis_f_508662_489551047.docx (111.47K)

Word count: 1925

Character count: 11409

Secure File Sharing Platform
Improve privacy and security in the
context of file sharing

Daniels Zelinskis

Nitheesh Murugan Kaliyamurthy

Friday, 20 October 2023

Table of Contents

Figures.....	3
1. Introduction	4
2. Background to the Proposed Research	5
3. Aims & Objectives.....	6
4. Methodology	7
4.1 Research Methodology	7
4.1.1 Philosophy.....	7
4.1.2 Approach.....	8
4.1.3 Strategies	8
4.1.4 Risks & Limitations	8
4.1.5 Validity & Reliability	8
4.1.5.1 Validity	8
4.1.5.2 Reliability.....	8
4.1.6 Data Collection	8
5. Resources and Planning.....	9
5.1 Hardware Resources	9
5.2 Software Resources	9
5.3 Project Plan	9
6. Reference List	10

Figures

Figure 1. Data Collection 9

1. Introduction

In a time characterised by extensive digital information exchange, protecting the security of data transmitted through file sharing platforms is of the highest significance. Effective measures are necessary to protect against unauthorised access, data breaches, and malicious intent because to the extensive spread of personal information on these platforms. Users expect a fast and simple sharing process, while also needing guarantees of data confidentiality and protection.

This research project intends to solve this difficulty by focusing on the creation and assessment of a Secure File Sharing Platform improved by the incorporation of end-to-end encryption and multifactor authentication. The fundamental focus of this research activity is to find a compromise between the ease of use for users and the implementation of strict security measures.

2. Background to the Proposed Research

File-sharing platforms allow to exchange, edit and share files within multiple organisations and persons. File-sharing platforms (including services) allow efficient, effective and trackable sharing of data. However, the security of these systems and platforms might be limited due to the multi-user interface, common targets for hackers and potential loss of data due to the ability to edit data. Although these possible issues have been addressed by multiple companies, the security of the data remains the key priority [1]. Currently, the top file-sharing platforms include files.com, filewhopper and Dropbox. Dropbox implements a 245-bit advanced encryption standard (AES) and Secure Sockets layers (SSL) and Transport Layer Security (TLS) encryption technology to keep the files secure [2]. A recent study analysed the use of file-sharing platforms (such as Zapaya and SHAREit) in the forensic scenario which showed that these platforms benefit law enforcement and provide digital evidence [3]. Furthermore, in addition to law enforcement, the use of file-sharing platforms may benefit the healthcare professions. The study analysed the apps and file-sharing services that allowed healthcare professionals to contact, share and input patient information, improving the health care and clinical practice [4]. In addition, the file-sharing platforms offer support in scientific research. The use of open data and file-sharing platforms to study wild-bird data in China has been utilised. However, the authors noted the limitations of these systems include disruption in the collaboration between institutions and storage of the data [5]. Nevertheless, the use of file-sharing platforms pose some risks and disadvantages. For example, clinical research (clinicaltrials.org.co.uk) has shown to have records linked to the platforms. Furthermore, other platforms have been shown to be linked to external websites and primary publications [6]. Importantly, a study was done on the analysis of the personal data file sharing between peer-to-peer of the clinical information on Limewire and Morpheus [7]. Following the analysis of the data in USA and Canada, the study advised to not install file-sharing platforms to limit the disclosure of personal health information (PHI) and personal financial information (PFI). An open platform Open Spectral Database (<http://osdb.info/>) has been developed to share and research spectral data [8]. Taking together, there is a strong requirement for a secure, time-efficient and user-friendly file-sharing platform that could be used by public, but also not limited to potentially used in a clinical or law enforcement system.

3. Aims & Objectives

The aim of this research effort is to improve the security of file sharing platforms by examining the efficacy of incorporating end-to-end encryption and multifactor authentication. The study aims to establish the extent to which this integration can enhance the security of file sharing while also ensuring a user-friendly experience.

- Perform a Security Assessment:

The main purpose of doing a security assessment is to develop the fundamental basis for the study endeavour. A security evaluation is a comprehensive examination of current file sharing platforms to identify weaknesses and strengths in their security framework. This aim is crucial as it establishes the foundation for specific security improvements. Without a thorough comprehension of the present security environment, it would be difficult to concentrate on the weak areas that need to be enhancement.

- Enforce Advanced Security measures:

The primary aim of this research is to enhance the security framework of the Secure File Sharing Platform. This initiative includes the practical execution of strengthened security measures, such as the incorporation of end-to-end encryption and multifactor authentication. This target prioritises the practical elements of security to actively enhance the platform's resilience against possible attacks and unauthorised access.

- Assess User Impact:

This purpose acknowledges the utmost significance of user experience. The process includes assessing the effects of implementing security measures on users' engagement with the Secure File Sharing Platform. Evaluating the influence on users involves considering factors such as the simplicity of use, user contentment, and overall efficiency.

- Assess Effectiveness of Security:

Assessing the effectiveness of security measures is a crucial process to establish if they successfully fulfil their intended objectives. This objective is to gather actual evidence using rigorous testing and analysis to demonstrate the effectiveness of security measures in avoiding unauthorised access and data breaches. Establishing the practical usefulness of the security measures is crucial.

- Ensure Regulatory Compliance:

This aim involves doing thorough compliance audits to verify that the Secure File Sharing Platform complies with pertinent data protection requirements. It is crucial to guarantee that the platform complies with regulatory regulations on data management, access control, and privacy rules.

4. Methodology

4.1 Research Methodology

The first step of the research is doing a thorough security evaluation of current file sharing services. This evaluation is crucial since it forms the foundation for the entire project. This step involves a comprehensive examination of weaknesses and strengths within these platforms. This comprehensive research provides a foundation for identifying specific areas where security may be effectively enhanced, therefore presenting a focused approach to improvement.

After the security assessment, the research moves into a practical phase focused on implementing complex security measures. The project's main focus is the implementation of end-to-end encryption and multifactor authentication in the Secure File Sharing Platform. Implementing these security measures necessitates technical proficiency and diligent implementation.

In order to assess the efficiency of these security improvements and their influence on user satisfaction, the research approach includes a comprehensive user evaluation phase. This phase aims to gather input from users of the platform, focusing on usability, user satisfaction, and productivity within the framework of the improved security measures. Data gathering during this phase is diverse, encompassing user surveys, questionnaires and the research of platform usage records.

Usability testing is performed to assess the user-friendliness of the platform, particularly the recently incorporated security elements.

Data analysis is a crucial component of the research approach, since it includes the meticulous scrutiny of data gathered from many sources. This research provides valuable insights into the impact of security improvements on both user experience and the overall security status of the platform. The research results serve as the foundation for the next phase, which entails creating data security rules and guidelines and also verifying the platform's compliance with legal standards and assessment of data processing practices, access controls and privacy policies.

4.1.1 Philosophy

The philosophy of research is positivist gathering quantitative information from the users. In addition, the data gathered from the research would also include qualitative data, therefore, the research would also cover the phenomenological philosophy. The advantages of this approach include covering a range of data with a detailed analysis of the outcomes. The disadvantages of this approach would require a thorough analysis of the results, which might be time-consuming.

4.1.2 Approach

An inductive approach will be applied in this research which would allow us to observe the outcomes of the testing and then conclude the observed.

4.1.3 Strategies

Strategies would include the use of literature review, software development and survey. The combination of these approaches would allow (i) to analyse the current data, (ii) to develop a new system, and (iii) to investigate and analyse the system using the survey.

4.1.4 Risks & Limitations

The possible external factors that might affect the research would include the reduced number of participants. However, not limiting the participants (such as students [any course] in the university) would overcome this potential limitation.

4.1.5 Validity & Reliability

4.1.5.1 Validity

The combination of literature review, development of the system and then analysis of this system by participation, and then recording the effectiveness, usability and applicability would validate the research.

4.1.5.2 Reliability

The research plan is valid as other researchers would be able to conduct the same research and get reproducible results.

4.1.6 Data Collection

1. Structured surveys and questionnaires - will be created to collect quantifiable data on user perspectives on security, user-friendliness, and their actions inside the platform.
2. Behavioural observation - the research will use observational techniques to record and analyse how users interact with the platform in real-life situations, with a special attention on activities related to security.
3. Usability testing - representative users will be involved in conducting usability testing to assess the user-friendliness of the platform, especially in relation to the integrated security aspects.
4. Log analysis - will collect and analyse platform usage logs to detect regularities in user conduct, specifically concentrating on security-related actions like login attempts and access controls.
5. Security assessment tools - specialised tools will be employed to examine the efficacy of security measures, detect risks, and perform penetration testing to evaluate security issues.

5. Resources and Planning

5.1 Hardware Resources

In addition to standard networked PCs, I may need servers, storage devices, security and monitoring applications and also virtual machine.

5.2 Software Resources

I will use various software tools, such as Wireshark, Nmap, Cisco, Phyton, VMware the last versions. Most of them I can download from their official websites.

5.3 Project Plan

	2023			2024				
Objective	Oct	Nov	Dec	Jan	Feb	March	Apr	May
Research Proposal								
Project objectives and planning								
Development of the proposed file-sharing platform								
Testing of the platform by developer								
Interim Viva								
Participants for the survey								
Survey								
Data analysis and presentation of the results								
Discussion and conclusion of the results and usability of the platform								
Report								
Report submission								
Final viva								
Exhibition: Poster								

Figure 1. Project Gantt Chart

6. Reference List

- [1] Indeed (2023). Top 10 file-sharing platforms (with pros and cons). Available at <https://uk.indeed.com/career-advice/career-development/secure-file-sharing-platforms>. Accessed on 17th October 2023.
- [2] DropBox (2023). How DropBox keeps files and data secure. Available at https://www.dropbox.com/en_GB/features/security. Accessed on 19 th October 2023.
- [3] Teng, S. Y., & Wen, C. Y. (2021). A forensic examination of four popular cross-platform file-sharing apps with Wi-Fi P2P. *Journal of forensic sciences*, 66(1), 315–322.
- [4] Ventola C. L. (2014). Mobile devices and apps for health care professionals: uses and benefits. *P & T : a peer-reviewed journal for formulary management*, 39(5), 356–364.
- [5] Yang, H., Li, Y., Zhou, H., Zhao, Y., & Song, L. (2022). A Research on the Sharing Platform of Wild Bird Data in Yunnan Province Based on Blockchain and Interstellar File System. *Sensors (Basel, Switzerland)*, 22(18), 6961.
- [6] Wilson, P., & Huser, V. (2021). Discoverability of information on clinical trial data-sharing platforms. *Journal of the Medical Library Association: JMLA*, 109(2), 240–247.
- [7] El Emam, K., Neri, E., Jonker, E., Sokolova, M., Peyton, L., Neisa, A., & Scassa, T. (2010). The inadvertent disclosure of personal health information through peer-to-peer file sharing programs. *Journal of the American Medical Informatics Association: JAMIA*, 17(2), 148–158.
- [8] Chalk S. J. (2016). The Open Spectral Database: an open platform for sharing and searching spectral data. *Journal of cheminformatics*, 8, 55.

FINAL GRADE

GENERAL COMMENTS

76

/100

[PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT](#)Student Daniels ZelinskisMark: 76

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	16
- The SMART (Specific, Measurable, Achievable, Relevant, Time-bound) objectives are not explicitly defined in this section, nonetheless good attempt. The introduction clearly highlights the problem of data security on file-sharing platforms and the aim to improve		

it. It sets the stage for the research project. - Could be more comprehensive		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts - While the background information is detailed, it could benefit from a more critical analysis of existing security measures and their limitations.	20	16
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed	30	24

- The project design outlines the steps involved in the research process, including security assessment, security measure implementation, user impact assessment, and regulatory compliance. It provides a clear structure for the research. - More details about the methods that will be used for user impact assessment and regulatory compliance verification could enhance this section.		
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices - The section mentions hardware and software resources required for the research, providing a basic understanding of what's needed.	15	11
Document Presentation		
Correct spelling, grammar and	15	13

punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit		
- The narrative flows reasonably well, but some sentences are lengthy and could be divided for better readability.		
TOTAL	100	76

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7
PAGE 8
PAGE 9
PAGE 10