在現有公開的網路儲存系統中提升檔案的隱私性與穩固性

學生：彭日伸　　指導教授：曾文貴 博士

國立交通大學網路工程研究所碩士班

摘　　要

為了提升使用者儲存在現有的網路儲存服務系統(network storage service system)的檔案隱私性(privacy)與穩固性(robustness)，我們實做了一套系統，讓使用者透過這套系統，可以利用簡單的操作方式，將處理過後的檔案上傳到所有的網路儲存服務系統，並且同時保護上傳檔案的隱私性與堅固性。我們系統與現有的網路儲存系統傳輸的機制是透過各個網路儲存空間系統所提供的共享資料夾，來達到本機端與網路儲存空間同步檔案的效果。在保護檔案的隱私性方面，採用加密的方式，可以達到所有網路儲存服務系統被攻擊成功時，不會洩漏任何的檔案訊息。檔案的穩固性上，採用 Erasure Correcting Code(ECC)來達到保護檔案的穩固性。而使用者在我們系統的操作上，透過簡單的方式，可以保護任何格式的檔案，與重新編輯上傳至雲端的檔案以及刪除雲端檔案的功能。

Improve file privacy and robustness in current public network storage system

Student : Jih-Shen Peng Advisors：Dr .Wen-Guey Tzeng

Institute of Network Engineering
National Chiao Tung University

ABSTRACT

We implement a system to improve the privacy and the robustness of a file in the current public network storage service system. By using our system, users can easily upload files to public network storage service system with trivial UI and also improve the privacy and robustness of this file. Because of the lack of appropriate API, our system uses synchronizing folders to synchronize file with each public network storage service systems. Our system program improves the file privacy through encryption and file robustness via erasure correcting code.

Acknowledgments

Special thanks to my parents, advisor and my friends.

Contents

List of Tables

List of Figures

Notations

M_i : message

C_i : ciphertext

k : the dimension of word

n : the dimension of codeword

u : the number of ciphertext which send to distributed networked storage

v : the number of codeword symbols which are fetched by key servers

σ_i : codeword symbols

KS_i : key servers

$\tilde{e}$: symmetric pairing function

$\alpha_{i,j}$: entry of matrix

$\gamma_{i,j}$: entry of inverse matrix