# **INTRODUCTION**

In the contemporary digital landscape, the pervasive adoption of public cloud storage services has fundamentally reshaped how individuals and organizations manage and access their data. Services such as Google Drive and Dropbox offer unprecedented convenience, scalability, and accessibility, yet their widespread use introduces significant concerns regarding data privacy and security. A critical issue arises from the inherent model where users relinquish direct control over their data's confidentiality, leaving it susceptible to unauthorized access by cloud service providers themselves, or through internal breaches and external cyberattacks. While existing security measures implemented by these providers are robust for their infrastructure, they do not inherently prevent access to unencrypted user data, creating a fundamental "trust issue" that undermines user confidence and restricts the storage of highly sensitive information in these environments.

This dissertation directly addresses this critical gap by proposing and developing a client-side cryptographic overlay designed to enhance data confidentiality and integrity in public cloud storage. The core of this initiative lies in ensuring that user files are encrypted *before* they are transmitted to cloud storage, thereby rendering them unreadable to any unauthorized entity, including the cloud provider, even if the underlying infrastructure is compromised. A central and innovative component of this work involves the development of a novel, secure, and user-friendly key management system. This system is meticulously designed to ensure that encryption keys remain supremely secure, are easily manageable by the user, and are never exposed to the cloud service provider.

This report will detail the design, implementation, and evaluation of this proof-of-concept client-side cryptographic overlay. It will explore the technical challenges associated with achieving a delicate balance between robust security, user-centric usability, and resilient key recovery mechanisms in a decentralized environment. By providing a practical framework and a functional prototype, this dissertation aims to demonstrate the feasibility and tangible benefits of empowering users with absolute control over their data's privacy in the cloud. Ultimately, this work seeks to contribute to the understanding of secure and usable key management strategies for client-side encryption, paving the way for a more trust less cloud storage solution where the cloud provider serves purely as a storage utility, devoid of access to unencrypted content.

# **LITERATURE REVIEW**