SANTA CLARA UNIVERSITY
DEPARTMENT OF MOLECULAR ENGINEERING
DEPARTMENT OF RELIGIOUS STUDIES

Date: November 24, 2015

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Noah Tall
Mae Bea Wright

ENTITLED

On the Construction of Matter, or Is There a God Particle?

BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREES OF

BACHELOR OF SCIENCE IN MOLECULAR ENGINEERING
BACHELOR OF ARTS IN TRANSCENDENTAL MEDITATION

Thesis Advisor

Thesis Advisor

Department Chair

Department Chair

On the Construction of Matter, or Is There a God Particle?

by

Noah Tall
Mae Bea Wright

Submitted in partial fulfillment of the requirements
for the degrees of
Bachelor of Science in Molecular Engineering
Bachelor of Arts in Transcendental Meditation
School of Engineering
Santa Clara University

Santa Clara, California
November 24, 2015

On the Construction of Matter, or Is There a God Particle?

Noah Tall
Mae Bea Wright

Department of Molecular Engineering
Department of Religious Studies
Santa Clara University
November 24, 2015

ABSTRACT

A good abstract is a concise summary (1–2 paragraphs) of the entire project: introduction, problem statement, work accomplished, results, conclusions, and recommendations. When you write the abstract, imagine that the reader will not read anything else, but that you must get your major point across immediately. This requires efficiency of words and phrases. An abstract is written to stand alone, without jargon or reference to figures and tables in the report body.

Table of Contents

List of Figures

Chapter 1

Introduction

Data loss is a fundamental, widespread problem in computing. In a single year, 25% of PC users will lose their data. Furthermore, 100% of all data storage technologies, ranging from magnetic tapes to hard drives to solid state storage, will inevitably fail. [1] Data loss is not only unavoidable, it is potentially devastating. 70% of small businesses that experience major data loss go out of business in a year. [1] Moreover, the U.S. loses an estimated $18.2 Billion every year due to data loss. [2] Almost every industry relies on accurately storing and accessing information, whether this be in the form of financial archives, software developmental codes, customer data, order records, etc. Backups, which are systems for duplicating ones data and storing it in another place, counteract data loss.

1.1 Motivation

Many current solutions implement data backup. We observe, however, that all systems suffer problems with privacy, accessibility, resilience, or a combination of all three. Three general categories describe current solutions: enterprise backup, cloud backup and personal backup. Unfortunately, current enterprise solutions cannot be examined as they are often highly customized and proprietary. Cloud backup is a service in which users upload files to be stored in a data center. These systems, while they are highly redundant, are not immune to corporate problems. If the company providing your backups goes out of business, your backups will no longer be accessible. In addition, these services may go down from time to time. Amazon S3, a common back end for such systems, has been known to have long outages. [3] [4] Finally, there is the problem of privacy: when one uses a cloud backup service, one gives ownership of one's data to the corporation running the service. Even though anyone who uses a cloud backup service should encrypt their data to preserve privacy, data encryption really just boils down to password protection, which is not reliable. [5] Even if one trusts the individual corporation who runs the backup, it gives a single point of attack for hackers, criminals, or governments to steal one's data. The 2014 celebrity photo hack is an example of this, in which vulnerabilities of Apple iCloud were exploited. [6] Personal backup, on the other hand, is the solution used by diligent individuals who regularly save their files to an external storage device or media. While personal backup addresses the privacy and accessibility issues, the system is not resilient, since the external storage device will lose all the backup data if it ever fails. [7] In addition, accessibility to the data relies on constant access to a single device.

1.2 Solution

Our backup system will address the issues of privacy, accessibility, and resilience. It will use redundancy and wide geographic distribution to create greater resiliency. We imagine at least one storage system per network. These storage systems will be interconnected, allowing them to share data. The data will be distributed as widely as the networks using these devices, encouraging hardware redundancy and making sure the data is constantly accessible. The protocol, once designed will be frozen, ensuring that these systems will continue to provide their services, even if support is no longer possible. Regarding privacy, we will not have access to the users' data, and each user's data will be only be accessible by the user who owns the data through encryption as mentioned above.

Bibliography

[1] http://www.imagineiti.com/backup/biggest-backup-mistake

[2] https://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/

[3] https://gigaom.com/2008/07/20/amazon-s3-outage-july-2008/

[4] http://www.rightscale.com/blog/cloud-industry-insights/amazon-ec2-outage-summary-and-lessons-learned/

[5] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6859779&isnumber=6859515

[6] http://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence

[7] https://www.backblaze.com/blog/hard-drive-reliability-stats-for-q2-2015/